2001

Survival in the e-conomy: 2nd Australian information warfare & security conference 2001

William Hutchinson (Ed.)

ECU
EDITH COWAN
UNIVERSITY

2ND AUSTRALIAN INFORMATION WARFARE & SECURITY CONFERENCE 2001

PERTH, WESTERN AUSTRALIA 29 & 30 NOVEMBER, 2001

survival in the e-conomy

PROCEEDINGS

www.We-Bcentre.com
working with e-business

2ND AUSTRALIAN INFORMATION WARFARE & SECURITY CONFERENCE 2001

PERTH, WESTERN AUSTRALIA 29 & 30 NOVEMBER, 2001

"survival in the e-conomy"

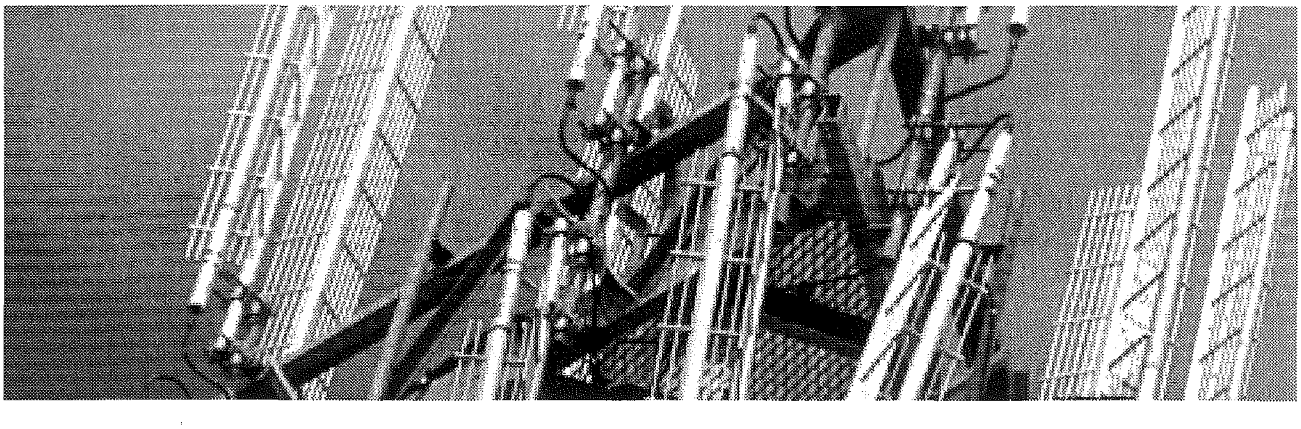
PROCEEDINGS

EDITORS:

Dr William Hutchinson

Dr Matthew Warren

Prof Janice Burn



2ND AUSTRALIAN INFORMATION WARFARE & SECURITY CONFERENCE 2001

PERTH, WESTERN AUSTRALIA 29 & 30 NOVEMBER, 2001

"survival in the e-conomy"

PROCEEDINGS AND CD-ROM PUBLISHED BY:
We-B Centre | School of Management Information Systems
Edith Cowan University
CHURCHLANDS WESTERN AUSTRALIA

CONTACT FOR ADDITIONAL COPIES OF PUBLISHED AND
CD-ROM OF PROCEEDINGS:
We-B Centre | School of Management Information Systems
Edith Cowan University
Tel: +61 8 9 273 8607
Fax: +61 8 9 273 8332
Email: l.davies_moore@ecu.edu.au

ISBN 0-7298-0499-2

All papers that appear in these Proceedings have been subjected to a blind review by two and three anonymous reviewers.

FOREWARD

Welcome to Perth, Western Australia, and to the 2nd Australian Information Warfare & Security Conference 2001 "survival in the e-Conomy" hosted by the We-B Centre, School of Management Information Systems at Edith Cowan University.

This is an international conference for academics and industry specialists in information warfare, security, and other related fields. The conference has drawn participants from national and international organisations.

All submitted papers were subjected to an anonymous peer review process managed by the Conference Committee. Stringent review criteria resulted in an unprecedented number of papers declined this year. Based on these reviews, the final programme was determined. A total of 45 papers were submitted for consideration and 37 were accepted for presentation.

The Conference Committee would like to recognise the efforts of many people who have contributed to the success and support in the organising of this conference and without their efforts the conference could not have occurred. The authors are thanked for their continued support to the 2nd Australian Information Warfare & Security Conference 2001 and we hope that the conference will receive similar support into the future.

The reviewers deserve a special vote of thanks for their commitment and dedication in having their reviews conducted professionally.

Thank you and enjoy the conference.

DR WILLIAM HUTCHINSON
Chairman

ORGANISING COMMITTEE

Dr William Hutchinson	Conference Chair
Dr Mathew Warren	Conference Co-Chair
Ms Lindsay Davies-Moore	Conference Coordinator
Mr Javen Ang	Multi Media Developer | Conference Co-Coordinator
Ms Shirley Anne Knight	We-B Master

TABLE OF CONTENTS

e-Government, Information Warfare and Risk Management: An Australian Case Study

Greg Robins

Edith Cowan University
Perth, W.A. Australia
E-mail: greg.robins@srwa.wa.gov.au

ABSTRACT

This paper looks at a security management framework in e-government. Firstly the paper reviews the issues of e-government and the threat of information warfare. It reviews the issues of information warfare, threat analysis and risk management. Finally, it examines how Sport and Recreation, a W.A. Government agency is implementing the security management framework.

Keywords: e-Government, Information Warfare, Security Management Framework, Risk Management

INTRODUCTION

Following on from e-commerce and e-business the latest "e"volution is e-Government. Within the next five years the Internet will transform not only the way in which most public services are delivered but also the fundamental relationship between government and citizen (Von Hoffman 1999). The Internet has become an important medium for organisations desiring to interact with a wide range of stakeholders. With the emergence of the World Wide Web, a totally new business environment is emerging, companies must work together to create online networks of customers, suppliers and value-added process (Ticoll, Lowry and Kalakota 1998). The Internet has the potential to market products and services, to communicate information to a global community to provide an electronic forum for communications and to process business transactions (Fink and Laupase 2000). With few exceptions, however, governments have arrived late on the scene. Transactions with government are rarely a matter of choice and government employees are unlikely to be rewarded for devising innovative web based strategies to replace them in their jobs. Nevertheless the drive is now on for radical government change (Sprecher 2000). A major driver has been the desire to reduce costs and make revenues go further. Savings of 20% are not unusual in the e-business community as they network their supply chains (Burn and Hackney 2000). U.S. federal, state and local procurement spending on materials and services in 2000 was estimated at around $550 billion, and in the European Union member states' combined procurement spending was around $778 billion (Symonds 2000). With a 20% cut in costs we are looking at savings of around $250 billion.

With Government's increasing dependence on electronic information there are increasing threats from sources such as hackers, viruses and denial of service attacks. As Scott states in relation to long-term or truest causes for an information war against Australia, the principle one would be the growing reliance on information systems and the position that the national information infrastructure holds (Scott 1999). It is vitally important that stakeholders are confident that information is secure and associated risks are minimised through sound management. Security management is based on threat analysis and risk management, with appropriate protective measures to deter, prevent, detect respond and recover from attacks.

This paper looks at e-government in relation to defensive information warfare and security management in the context of the West Australian Government. Firstly it reviews the issues of information warfare, threat analysis and risk management. It then focuses on Western Australia Government and their security management framework. Finally, it examines how Sport and Recreation, a W.A. Government agency is implementing the security management framework.

INFORMATION WARFARE

Panda (1999) describes information warfare as any malicious attack against an organisation's information base through electronic means. Jacobsen (1999) defines it as actions taken to preserve the integrity of one's information infrastructure from exploitation, corruption or destruction while at the same time exploiting, corrupting or destroying an adversary's information systems thereby achieving a military advantage. This is a far more complete definition that goes beyond the defensive definition. Hutchinson and Warren take it one step further by including the aggressive use of information to gain an advantage.

Hutchinson and Warren identify three objectives of Information Warfare:

1. To use information and associated systems to gain advantage over protagonists or competitors;
2. To protect your own information and associated systems from those who would do harm by intent or accident; and
3. To formulate strategies and action that produce detrimental effects on your competitors or protagonists.(Hutchinson and Warren 2000)

'e-Government' is predominately concerned with objective two and to some extent objective one when defined in the terms of utilising information aggressively to provide a more effective and efficient service to its clients and business partners.

Information Warfare is about information as a weapon or a target. The basic strategies used in information warfare are:

- Deny access to data;
- Disrupt or destroy data;
- Steal data;
- Manipulation of data.(Hutchinson and Warren 2000)

To guard against attacks that utilise these strategies the Western Australian Government have identified a set of security management objectives that link to a security and risk management strategy for 'e-Government'.

SECURITY IN E-GOVERNMENT

Information technology is increasingly becoming core to the operations of Government departments. The Internet is playing an even more important role in service delivery and electronic commerce. Security is an ongoing risk and the degree of risk is escalating as the use of public networks increases.

The Western Australian Government have identified five objectives of security management in e-Government:

Authentication – of both sender and receiver;

Availability – ensuring that denial of service does not occur;

Confidentiality – protection from intrusion and ensuring only the intended recipient has access to the information;

Integrity – ensuring data being transmitted is not lost, altered or defaced either deliberately or accidentally;

Non-Repudiation – ensuring the sender cannot deny sending the information and the recipient cannot deny receiving it. (Western Australian Government 2000)

As Jones states Information security policies and ongoing security education form the cornerstone of security programs. Monitoring and audit trails should be built into systems and controls established so that each event is non-repudiated (Jones 1998).

RISK MANAGEMENT

Security demands that ready access to information is restricted as far as possible to only those who 'need to know' and made as difficult as possible for all other people. E-Government on the other hand seeks to provide an environment as open as possible, to allow maximum access to key stakeholders, clients and the public.

It is therefore essential to identify all risks and effectively manage these risks. Key IT risk areas are:

- Security
    - Physical and electronic
    - Passwords
    - Firewalls (and back doors)
    - Backup and disaster recovery

- Application Development/Purchase
    - Functionality
    - Time
    - Costs

E-Government has increased the risks of external attack, unauthorised external access to systems and information and increased reliance on electronic records that must be protected from unauthorised access and modification.

A fundamental approach to risk management is to begin by identifying assets likely to be at risk:

- Data – information about clients, suppliers, sensitive documents in particular relating to Government policy;
- Software – applications, browsers, operating systems;
- Hardware – servers, workstations;
- Infrastructure – networks, intranets, extranet;
- People – internal, external to the organisation;
- Other – physical access to the buildings or computers, power supplies, fire protection systems.

The Western Australian Government have identified three levels of controls for e-Government security management (Western Australian Government 2000):

Level 1: Basic in house information security practices
These include:

- Effective password controls, including mandatory periodic change of passwords;
- Periodic review of users (access, removal of access when a users leaves, etc.)
- Monitoring of any changes to critical data and having appropriate backup and recovery procedures;
- Effective control over, and recording of, system changes; and
- Maintaining physical security.

Level 2: Protecting the Information System – building a shield
Utilising the Internet for e-business/e-commerce exposes an organisation to the world and the risk of attack is multiplied. Additional measures are required including:

- Extension on level 1 controls beyond the organisation's boundaries;
- Development of policies and procedures on internet usage;
- Ability to maintain continuity of service in the event of failure; and
- Protection against breaches: use of firewalls.

Level 3: Transmission protection
This level addresses the protection of data being transmitted over public networks with the key elements including:

- Authentication;
- Encryption;
- Integrity checking; and
- Non-repudiation.

The WA Government have developed a Security Controls Matrix to address each of the three levels of controls for security management. The matrix summarises the objectives, controls and tool sets related to security controls.

Control Objective	Control Description	Control Mechanisms
Access Control	A technique used to define or restrict rights of individuals or application programs to access, read, modify, insert or delete data	• Application level access rights • File and directory permissions • Firewall access lists • Public Key Infrastructure • X.509 certificates
Audit trail	A chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event.	• Application and server logs • Biometrics • Network intrusion detection system • Token based systems (eg secure ID)
Authentication	Security measures designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information.	• Biometrics • Digital signatures • Application and server logs • Public Key Infrastructure • X.509 certificates • Token based systems (eg secure ID)
Authorisation	Determining whether a user, program, system or network is approved to connect to an information system.	• Biometrics • Domain validation • Firewall controls • IP address validation • Passwords • Token based systems (eg secure ID)
Availability	The characteristics of data, information and information systems being accessible and usable on a timely basis in a required manner	• Anti-virus tools • Backups • Business Continuity Plans • Incidence response plans • Network intrusion detection system
Confidentiality	The characteristics of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner.	• Encryption • Secure Shell • Secure Socket Layer 3
Integrity	Security measures designed to ensure that data transmitted or stored electronically is neither accidentally nor deliberately altered, defaced or lost.	• Anti-virus tools • Encryption • Content security tools • Network intrusion detection system
Non-Repudiation	A service used to counter repudiation of a communication by any party involved in the communication.	• Biometrics • Digitally signed personal certificates • Public Key Infrastructure • Token based systems (eg secure ID)

Figure 1: Security Controls Matrix
(Western Australian Government 2000)

The following case study utilises the matrix to evaluate Sport and Recreations security management and preparedness to combat and counteract information warfare.

CASE STUDY – SPORT AND RECREATION WA

Research Method

The research methodology was based on action research. The author is the newly appointed Manager of the Information branch and responsible for implementing security measures within the Department.

The research began in June 2000 and is based on direct observation and interviews with key internal stakeholders, information system custodians, the Corporate Executive team, IS system administrators and software developers.

Background

Recently the Auditor General for WA completed an Internet and Network Security Audit on a cross section of WA Government Departments. This audit provided the following results.

Vulnerabilities increasing the risk of external access to the Department network:

- 22% did not have a firewall;
- 55% had weaknesses in remote dial up facilities;
- 66% did not regularly monitor security events.

Of the Departments with firewalls:

- 18% had backdoors to other networks;
- 72% had substantial weaknesses in firewall settings, configuration or access rules;
- 36% had unnecessary services on firewalls increasing the risk of vulnerability.

Vulnerabilities increasing the risk of unauthorised access to services and data:

- 100% had software installed with known security weaknesses;
- 100% had weak and default passwords available to access both networks and/or databases;
- 33% had unnecessary services on servers increasing the risk of vulnerability.

Corporate Context

The Ministry of Sport & Recreation had a history of decentralized development. All regional offices were isolated from the central office and as such had developed their own policies and procedures. Many had developed their own web presence, lacked internal information systems and had no access to corporate information. Within the central office the various divisions worked independently of each other, there were no corporate information systems nor effective management of electronic or paper based documents. Staff were provided with computers for email and developing documents but stored these in personal areas making the information inaccessible to the organisation.

The organisation did not have an information management section, paper based corporate information was managed by individuals and relied on each staff member establishing an individual filing cabinet. The IT section consisted of two staff members with responsibility for providing technical advice and setting up computers on desks. There was limited strategic information planning. The limit of IT planning revolved around a hardware replacement strategy.

In 1999 a new Chief Executive Officer was appointed and there was a complete change of the corporate executive team. This lead to a refocus on Information Management and an Information Branch was initiated with the responsibility to develop a statewide network and information infrastructure to support the development of corporate information systems and the implementation of Knowledge Management principles. The project to implement a statewide network and information infrastructure began in January 2000.

As the Chief Executive Officer put it a new management framework was required that:

- Guaranteed all staff focused on approved outputs and outcomes;
- Guaranteed corporate communications on achievements and work plans;
- Ensured that all staff have the opportunity to be informed;
- Ensured that resource issues and program management issues are discussed and that major issues 'bubble up' for executive consideration.

Very little attention was given to aspects of Information Warfare, risk assessment or security management.

Security Controls

Between January 2000 and April 2001 Sport and Recreation have implemented local area networks into all their offices across WA, established high speed data links between their major sites and implemented Virtual Private Network links between the central office and their minor sites. The Department's web site is hosted by an external ISP with no links to the Department's information systems or network infrastructure.

Access Control

All information systems within Sport and Recreation are accessed through the Department's intranet site and authenticated by the network as they enter each application. Each application stores a list of users requiring administration and superuser rights.

Users have read access only to directories with the exception of three directories where they store their files. One directory is their personal area that is restricted to the individual owner, one is an open directory for storage of non sensitive corporate documents which allows full control to all users and a secure directory for sensitive corporate files in which individual files are restricted to the owner. Whilst all applications have inbuilt rights to restrict access, modification, insertion and deletion of data by users these rules are stored within the database and could be access by anyone able to directly access the backend database. The only protection method is read only restrictions on the data directories and staff are not provided with the client component of the corporate database.

Audit Trail

Whilst all servers have logging turned on these logs are not reviewed on a regular basis nor are there any review procedures in place to detect attempted intrusions.

Sport and Recreation do not have a network intrusion detection system.

Authentication

The Department has not put in place digital signatures, a public key infrastructure nor do any of its applications have log files.

Authorisation

On entry to all applications users are authenticated against their network login.

The Department's firewall is set up to only allow known IP addresses through. These are associated with the VPN sites. The VPN sites do not have a firewall and as such could provide a back door entry to the Department's systems.

The Department's ISP firewall is set up to only allow email through, traffic from VPN sites and outgoing network traffic.

Availability

The Department has implemented virus software on all servers and each workstation. All files are automatically checked prior to access and external emails are scanned on delivery. The Department's ISP utilised for Internet access and email has set its firewall to automatically delete email attachments with certain extensions such as exe.

Whilst all servers are backed up on a nightly basis there is no business continuance plan nor does the IT section do regular testing of their backup and recovery strategy or have a disaster recovery plan.

Confidentiality

The Department does not have a particular confidentiality strategy. Its only method of confidentiality is through making information only available to internal staff. Whilst all information systems have internal security to identify users and apply access privileges the Department is vulnerable to attack internally or to internal staff providing confidential information externally.

Integrity

The Department does not have any procedures in place to safe guard data integrity.

Non-Repudiation

The Department only has email as external communication and does not have any strategies in place to counter repudiation of emails.

LESSONS LEARNED

Whilst the Department has been mindful of security issues and its web site is completely separate from its internal network it is vulnerable in a number of areas. It is particularly vulnerable from attacks by internal staff and its web site vulnerability is completely unknown.

Whilst its Web site is separate and mainly brochureware it is predominately vulnerable from hacker attack intent on modifying or deleting information. As a Government Department this could prove extremely embarrassing for the Government particularly if the site had links added linking to inappropriate sites or the information was altered that contradicted Government policy. The Department needs to looks at this threat seriously and put in place procedures to guard against this type of hacking.

A significant management adjustment is required to achieve the desired security level including:

- **Documented Policies:** Information security policies form the cornerstone of any sound information security programme (Jones 1998). The Department's security policy must start with identifying who should be protected from what. That is its customers, employees and business partners. Each has specific requirements related to security, including privacy assurance, theft avoidance, intellectual property protection and assurance that operational capability cannot be maliciously denied. The senior executive must decide what level of attention and investment each of the identified risks will receive. The decisions must be documented and must guide all implementation plans for e-business applications and their related security measures. Currently this is left to the IT section, which deals with procedures and technology selections as opposed to risk allocation. Policies must address control issues, cost distribution, implementation responsibilities, and the like. Because of the enterprise-wide impact of these the senior executive must set policy.

- **Implementation Management:** Security decisions should be based on the documented policies. This requires an analysis of the system's vulnerabilities and risks that highlights any unique exposures caused specifically by integration. It should also highlight all uses of sensitive information and reflect on the degree of knowledge about business partner configurations. The analysis should be the basis for decisions on budget levels versus risk levels. Sport and Recreation lacks documented policies to perform such an analysis.

- **Dedicated Budget:** Most companies do not have a separate budget for security. Instead, security budgets are usually embedded in individual projects. Since money spent on security is for risk avoidance as opposed to revenue creation, security investments frequently receive a low priority. This is the case with Sport and Recreation and, since separate projects don't deal with ancillary effects on other business units or the organisation as a whole, risk management does not cut across lines of business.

- **Accountability:** In the end, organizations should hold specific individuals accountable for risk. This can be done through formal procedures, including documented, independent third-party evaluations. After an incident, a manager should perform an analysis and present the results to a governing body, such as an audit committee or the corporate executive. Currently Sport and Recreation do not review the documented basis for security decisions.

Sport and Recreation have tackled security management in an ad hoc fashion with limited input from the senior executive team and lack the development of appropriate policies and procedures that identify risks or assist in implementation of the three levels of control required for security management.

CONCLUSION

With the introduction of 'e-Government' it is critical that Government Departments understand the nature of information warfare, identify all risks and effectively manage these risks. As Hutchinson and Warren state very little can occur in an organisation until the critical nature of I-War is accepted and its concepts comprehended (Hutchinson and Warren 2000). The Western Australian Government have considered the need for defensive information warfare and are introducing a security management framework to assist Government Departments to implement appropriate defences. For 'e-Government' to be successful departments must also consider the aspect of aggressively exploiting their information in much the same manner as private organisations utilise their information to gain a competitive advantage, to provide better services

There is much research left to be done on information warfare, security and risk management particularly in relation to 'e-Government'. Within the context of the WA Government research must continue into its security management framework, how to best implement the framework, measure its effectiveness and develop appropriate policies and procedures to support the framework.

As indicated by Standards Australia suitable management fora with management leadership should be established to approve the information security policy, assign security roles and coordinate the implementation of security across an organisation (Standards Australia 1999). A multidisciplinary approach needs to be implemented involving cooperation and collaboration of managers, users, application developers, auditors and senior executive.

When considering these matters, several questions arise for future research:

- How will agencies deal with information and communication that must be passed both up and down, across functional boundaries, and to business associates and customers whilst defending the information and associated systems?
- How can security risk be managed in the absence of an accepted industry-wide measurement system that would enable managers to judge the risks embedded in their current e-business systems?
- How can it be determined if the investments related to reducing risks are warranted?

REFERENCES

Burn, J. M. and R. Hackney (2000). *Strategies for I-Business Change in Virtual Markets: a co-evolutionary approach.* International Journal of e-Business Strategy Management Vol 2(2): 123-133.

Fink, D. and R. Laupase (2000). *Perceptions of Web Site Design Characteristics: A Malaysian/Australian Comparison.* Internet Research: Electronic Networking Applications and Policy Vol 10(1): 44-55.

Hutchinson, W. and M. Warren (2000). *Information Warfare: illusion and reality in the information age.*

Jacobson, M. R. (1999). *War in the Information Age; International Law, Self Defence, and the problem of Non-Armed attacks.* [On-line]
www.infowar.com

Jones, R. (1998). *The Internet and Healthcare Information Systems: How Safe Will Patient Data Be?* IS Audit and Control Journal 1: 25-30.

Panda, B. (1999). *Defensive Information Warfare.* Communications of the ACM 42(7): 30-32.

Scott, T. (1999). *The Causes of an Information War Against Australia.* Journal of the AIPIO 8(1): 36-51.

Sprecher, M. H. (2000). *Racing to e-government: Using the Internet for citizen service delivery.* Government Finance Review Vol. 16(5): 21-22.

Standards Australia (1999). *Information Security Management - Part 1*; AS/NZS 4444, Standards Australia.

Symonds, M. (2000). *Government and the Internet: The Next Revolution.* The Economist (June 24).

Ticoll, D., A. Lowry and R. Kalakota (1998). *Joined at the Bit. Blueprint to the Digital Economy: Creating Wealth in the Era of e-Business.* D. Tapscott, A. Lowy and D. Ticoll, McGraw-Hill.

Von Hoffman, C. (1999). *The Making of E-Government.* COI Enterprise Magazine (November, 15).

Western Australian Government (2000). *A Security Management Framework for Online Services,* Western Australian Government.

Small Business In The New Battlefield: Government Attempts At Providing A Secure Environment

Ian Martinus

Edith Cowan University
Office of Economic and eBusiness Development
City of Wanneroo
E-mail: ian.martinus@wanneroo.wa.gov.au

ABSTRACT

The Australian small business segment has received much attention in the press and within government during recent times. As Government departments constantly scramble to realise their own key performance indicators, there is a new need to incorporate achieving results for small business. Researchers have acknowledged the need to understand the systems and processes of small businesses, while suppliers and customers attempt to show how margins can improve by using new methods of transacting. This paper investigates small business response in a localised area to the Australian federal government's attempt to implement a Government Online policy. The National Office of Information Economy (NOIE) has embarked upon a campaign of getting government agencies online through its Gatekeeper program. Increasingly, these government agencies whether it is the Department of Minerals and Energy or the Department of Main Roads will be dealing with small businesses through an online relationship. For the first time, a relationship involves transacting through the Internet brought about by an exchange of goods and services for payment. The Gatekeeper program is explored specifically relating to small business getting online and doing business with government. This study reports the results of an online survey conducted within the Wanneroo/Joondalup small business region in Western Australia. This area services a population of 250,000 and around 8,000 businesses. The survey questioned small business about a range of issues including Internet security, knowledge of Public Key Infrastructure (PKI) encryption technology, the Gatekeeper program and concerns with privacy. The online survey results show the uncertainty small business has regarding their involvement in the new economy.

Keywords: Security, public key infrastructure, Government Online, Gatekeeper, competitive intelligence, battlefield

INTRODUCTION

Much of the work produced in the area of information warfare is concerned with descriptive narrative. Rich imagery of battlefields, warriors, ninja, and the art of war are used as descriptors that tend to romanticise danger and threats. The events of recent days and the turbulent global environment ignited by the World trade Centre bombing in New York City have increased the threat of physical security to new heights. The reality for small business is that they are caught between attempting to come to terms with a new business environment and the programs launched by government bureaucracies to assist them in the new economy. This paper has chosen to address a less enticing, but nonetheless strategic question of the business landscape that small businesses and government agencies find themselves operating within.

It has been stated that small business owners are the heads of their kingdom constantly fighting fires and waging war with daily adversary. Chararcterised by a tight operational budget with low margins, the small firm is in a constant state of battle with contracts, purchase orders, customer order fulfilment, Pay-As-You-Go taxation, and Business Activity Statements. The pre-destined conservatism is inherent in a firm that cannot afford to make mistakes with people, systems or processes. Mistakes are punishable with rapid customer loss, mistrust by suppliers, employee abandonment, or worse, litigation. One of these mistakes is the lack of security deployed to protect their exposed accounting, billing and customer detail systems.

Without a secure and trusted infrastructure, companies and individuals will become increasingly reluctant to move their private business or personal information online. For small business to have reason to trust the de facto Internet standards for security such as Digital Certificates, simple reasons have to be projected effectively to the target market. (Caron, 1999)

The need for information security is all pervasive, and affects both user and non-user of information technology. The electronic form of communication is not immune to containing increasing amounts of sensitive information. Small business means of business communications include:

- Facsimile
- telephone conversations
- electronic mail
- electronic funds transfers (EFT) and other financial transactions (http://www.cdt.org/crypto/risks98)

Managing customer relationships is crucial to small business, which traditionally treads water in its narrowly focussed niche area. However, when the small business seems to outgrow its birthstate, and is developing in size and opportunity, there becomes an increasing need for the introduction of formal structures, systems, procedures and controls (O'Gorman & Doran, 1999).

As online business becomes more of a standard for doing business, the small enterprise has to continually revise the way in which business practices allowed things to be done in the past. Included in the list of things for small business to consider is the ability to:

1. continue a dialogue between itself and potential clients and suppliers
2. conduct transactions in a safe and secure environment
3. assure itself and partners that competitors and unwanted others cannot access, record, intercept and alter what is being relayed.

O'Gorman and Doran note that many small businesses fail to grow because the manager or owner lacks the ability to learn new skills. It is believed that due to agility and the ability to react quickly because of size, small businesses can understand and apply technology, its applications and enhancements (Martinus, 2000). This paradox is compounded as these candidates of early adoption fail in their uptake of new procedures and precautions.

Alberts (1999) explains that within commerce, dominant competitors have developed information superiority and translated it into a competitive advantage by making the shift to network-centric operations. Customers are provided with more value through the businesses' skill at utilising information technology to reshape internal processes. Alberts 1999; Kahaner, 1997 also argue that by tracking changes in the marketplace, it will be rare for business to be surprised by events. The process of competitive intelligence, once instituted, can lessen vulnerabilities and exposure. Research cited in the Kahaner paper indicates that only 5% of small businesses in the United States have a full-scale formalised competitive intelligence system. This system incorporates the necessity for small business to learn about new technologies and develop processes that reduce vulnerability.

In almost a state of self-realisation, the business (small business) has a greater environmental awareness allowing it to create opportunities, align well, and watch its back when threats appear. If it is accepted that information superiority can afford a business greater market force and power, then systems such as Gatekeeper deploying information security tools should be of some interest.

The impact on small business through the Australian federal government's launch of the Gatekeeper program is explored in an attempt to rationalise the benefits small business will realise by understanding Internet security. The Telstra Small Business index uses a panel of approximately 1,200 randomly selected small business proprietors who are interviewed by telephone every three months. Small business owners express concern about a lack of informed control over the process of migrating to e-commerce. The fear of being unable to make informed management decisions about the technology they used or are asked to buy causes discomfort among proprietors.

Still a top-of-mind concern among many businesses is security of payment systems and processes. The rejection of eCommerce due to the security variable is still between 21-29%. Procurement fulfilment may be one concern about paying online, but security using credit cards for online payment through small purchases is considered risky. Larger transactions are likely to be settled by electronic interbank transfers, and therefore not as high on the list in terms of risk and concern. (www.noie.gov.au/publications/NOIE/SME/yellowpages_index.htm)

This research underpins the interrelationship between a small business' degree of comfort with the use of technology as part of doing business. The level of willingness or inertia also influences the decision to use of the Internet to conduct business.

When the benefits and risks of online commerce are understood equally, it can be argued that acceptance of programs to add secure means of transacting and engaging in dialogue between the business and the external world is greater. Gatekeeper is one such program that has a greater chance of acceptance and success due to the underlying education that small business has had time to absorb. Of little or no concern to small business is the research that many global security and academic professionals are pursuing to protect their business as it does business.

The IP Security Protocol Working Group (IPSEC) that has gathered the world's greatest minds in Information Security and networks may spend a lifetime researching the field. The development of a security protocol in the network layer has almost no relevance to the operational requirements of the landscape gardener who has to decide which type of deciduous tree to plant in the winter season. That particular business, if connected to customers in a payment gateway cares nil for the type of cryptographic security services employed. There is more chance of interest in the knowledge that billing a customer for the African Tangelo tree is supported by a system that protects both buyer and seller.

OPENING THE GATE

This section briefly outlines the broad objectives of the Gatekeeper program. The Australian Federal Government is beginning to involve itself in the highly problematic space of small business. The thread tying the Information Warfare theme together is multi-pronged. The justification of government and business involvement is outlined in the argument below.

- Firstly, the new economy environment itself is a threat to the survival of small business if it chooses to upskill and reskill using the new economy tools, namely technology. Once the business decides that involvement is necessary, the business has agreed to all of the potential risks, hazards and minefields, regardless of their state of awareness as to what these may be.

- Second, once in this game strewn with endless permutations for disaster, the small business is also given access to the opportunities that arise from being part of the new economy. For the purpose of this exercise, the academic debate of the existence of such an economic state is ignored.

- Third, given that government objectives generally include the creation of a positive economic environment, small business has now tacitly agreed that government has a right to facilitate the safe passage of business citizens as they navigate within this monitored environment.

- Government attempts to map involvement of all by producing policy that demands programs be developed, tested and established to provide this safe and secure environment for the economic producers of the nation. Given that the majority of all developed nations' Gross Domestic Product (GDP) is harvested from SMEs, it is no wonder that strategies begin to recruit small business as champions.

The nature of the threat to a national economy increases when the enlisted (in this case small business) is threatened. What is being evaluated in this paper is whether the intentions of government to prevent cases of attack to its recruits are at all known or understood by its legion. The worst possible case can be imagined where small business networks are exposed, sensitive information is easily extracted and business is suspended due to attacks that have crippled that business. Government sees this type of scenario as reason enough to be legitimately involved in what it is doing through programs such as Gatekeeper.

GATEKEEPER PROGRAM

Ensuring integrity, security and authenticity in the transmission of information and transaction of business was the main objective for the Australian federal government developing a strategy in 1997 that led to the formation of the Gatekeeper program. Government developed a national framework for the authentication of users of electronic online services. The Public Key Authentication Framework is a framework for the generation, distribution and management of public key certificates. These certificates bind the identity of users to their public key material in a trusted and legally based manner.

The link being investigated is to small business. The question is raised as to whether Gatekeeper enhances the procurement of services for the government from entities such as small business.

The Gatekeeper Implementation project area is responsible for:

- Development of the Australian Business Number – Digital Signature Certificate (ABN-DSC)
- Monitoring and development of PKI standards
- Formulation of policy for PKI implementation
- Assisting Government agencies in PKI implementation
- Liaison with industry bodies and PKI vendors
- Development of the Gatekeeper Accreditation Certificate (GAC) (www.govonline.gov.au/projects/publickey/GatekeeperImplementation.htm)

The Australian landscape is increasingly becoming flooded with regional portals, which are typically in the form of business and community webs. Some of these have identified the potential revenue streams as flowing out of 'buy local' frameworks. Due to policies involving restrictive practices and anti-competition legislation, buy local tends to be implied and tacit in nature.

The implication for Government and its agenda setting comes in the form of greater access for small business to government contracts, tenders and invitations to submit to expressions of interest. As it makes more sense (both politically and economically) to source locally or show to be doing so, government and regional small business interaction needs to be nurtured through the implementation of secure means of doing this.

LOCAL BUSINESS E-COMMERCE SECURITY SURVEY

What is missing in the rationalisation of the platform to help small business is awareness. The security survey distributed to small business proprietors sought to gain some feedback from small business within a defined geographic area. The territory is one currently in the development phase of producing a business and community portal.

Membership to the portal by business will automatically guarantee that local government purchasing officers have access to the type of business they are, their location, their ability to fulfil and possible pricing structure in their specialist field of trade or service. For the first time, the link is intended to be established where buyer and local seller come together through an online aggregator. The budgets for the two local government authorities within this defined region exceed $AUD 120M and the region relies heavily on the industries of construction and retail.

The questions attempted to cover areas of Internet security and concerns as well as explore the depth of knowledge about the Federal Governments' attempt to facilitate safe passage for commerce through the provision of specific strategies and initiatives.

METHOD AND SURVEY RESULTS

The online business survey was sent to the members of two local business associations between the end of February 2001 and the beginning of March 2001. Respondents e-mailed their completed surveys to a designated person and address. From the 140 surveys sent to member's e-mail addresses, 43 responses were received.

To provide a more detailed understanding of the attitudes and perceptions of small and medium sized businesses towards eCommerce and security issues, and to complement the online survey, detailed discussions were held with managers in a range of small and medium businesses. The structure of the discussions was generally in an unstructured and open environment, with a mix of prompted and unprompted questioning. There was a mixture of group discussions and one-on-one interviews.

These groups and interviews sought to explore the online survey findings in greater depth. The online survey covered three main areas to do with Internet security. These included privacy concerns and the risk associated with Internet transactions, customer concerns and dealing with customers on the Internet, and the Australian federal government's push in the area of Internet security through its Gatekeeper program.

While a majority of respondents agreed that Internet security is an important issue for their business, an even greater number saw the issue being of more concern in the future. Many businesses also feel that the level of maturity of systems that are supposedly in place to protect them is still low, and are skeptical of trying secure systems on a regular basis. An automotive business commented that his company's view of security was broader than the transaction implication, and includes the oversupply of valuable competitive information available over the Internet. This manager considers that putting too much product detail, pricing or methods on their website as asking for the possibility of theft by competitors.

One of the surprising results involved a question concerning the relative risk of using the Internet as a means of transacting. 65% of businesses thought that the Internet is more risky than handing over credit card details through conventional means. Paying for a restaurant bill through credit card in a situation where a waitperson physically takes the credit card with the bill from the diner's possession was considered safer.

Through the follow-up telephone interview, respondents had a perception that, when faxing their credit card details to complete the purchase, this still constituted a less risky option of transacting. Another point reinforced strongly was that giving of personal and credit card details to a live person was a safer option than the Internet one.

" I think that once I give my credit card details over the Internet when I buy something, I will never know if the details have not been blasted all over the world for people in China to use"
(Owner/Operator Automotive)

Despite small business being one of the main target markets in the government's push for the security of Internet transactions, the gatekeeper program was recognised by only a third of respondents.

"I don't understand why the government is trying to help us...there must be a buck in it somewhere or votes at the next election..." (Owner/Manager Printing)

Promotion of the government online campaign fared a little better with almost half of the respondents having heard of the campaign. The interview process confirmed the skepticism of small business proprietors however.

The thrust of the government online campaign as it relates to small business is protecting the integrity of data and information. While a large amount of businesses agree that private details should be protected strongly when dealing over the Internet, few had heard of the gatekeeper program.

An encouraging result was recorded to the question of whether the respondent would be interested in joining a secure online business community that trades with other businesses and government. Nearly 80% responded positively, and a few even sought more information. This result may have been influenced by the extensive eCommerce workshops and seminars run in conjunction with the business associations and through the local government Economic Development units in the region.

RISKS AND COSTS OF INFORMATION PROTECTION POLICIES

Another area of the security prism that will likely afford mountains of polarised research and argument has to do with the topic of the risks associated with the design system of secure systems. The focus of this area, despite being beyond the scope of this paper, is cryptography policy. Government policy as it impacts small business is important enough to be addressed briefly.

Myriad problems associated with cryptography need to be considered whether they are political, social or economic. As government departments deploy systems that provide them access to encryption keys, the risks and costs are still poorly understood.

In another survey conducted within the first quarter, 2001 within Wanneroo/Joondalup small businesses has returned figures that show small business email use to be over 60%. On first glance, the figure gives great hope for the acceptance of communicating electronically. After a double take however, it also raises the alarm to possibilities of attack for the small business. As most Internet electronic mail is still sent "in the clear" it is extremely vulnerable to interception and manipulation. With network protocol analyser software readily available over the Internet, small businesses with little or no network protection in the form of firewalls or basic NT password systems remain highly exposed.

With the lack of basic *critical infrastructure* government efforts to offer a minimum standard of security to its own departments and to business is still part of the network coverage nemesis. Expense and establishment costs will discourage and dampen widespread implementation efforts, with the likelihood that government opts for 'trial' and pilot projects as the small business sector is tested.

Government, by becoming more aware of the need to address security and protection begins to assign more internal and external people to the task of finding a solution. As more people work in this sensitive area, the risk of attack also increases. Increasing the number of people with authorized access to the critical infrastructure and to business data will increase the likelihood of attack, whether through technical means, by exploitation of mistakes or through corruption.
(http://www.cdt.org/crypto/risks98)

Schneier (2000) contributes another point of view to the issue of risk and protection. The argument centres around the tenet that businesses generally do not need long term privacy. He argues that where detailed financial information might need to be secure for a few years, information to do with marketing and product plans may only have a useful half-life of months. The argument is driven by the assumption that information in the new economy is diffused rapidly. This type of thinking may fuel the antithesis of the need for prolonged protection. It is also put that government and their policies need only short-term protection, thereby downgrading the risk inherent within systems. Where security is approached on a best efforts basis, slogans of "We are doing the best we can" come to mind.

FURTHER RESEARCH POSSIBILITIES

If bureaucracies operating within local areas can be considered *medium sized regional businesses*, the need for them to form stronger relationships with small business within their sphere of influence is plausible. For this to occur, the premise has been put that a secure and trusted environment is needed.

Initial research has indicated that a lack of knowledge on the part of small business on the efforts of this *medium business (*government*)* is known. The legacy relationship between the two can be described as both parties being tolerant of one another, but with a great deal of ignorance to the others' intentions. The strength of this new online relationship is enhanced if clear benefits for small business are established by the *medium business.*

An in-depth investigation of small business skepticism toward the government online campaign could be attempted. This research could further the argument that small business segregated into discrete verticals will yield different attitudes and opinions. When a federal government categorises all businesses with less than 20 employees as small, it is bound to generalise. Policies attempting to develop and implement one-size-fits-all strategies will find themselves strewn across the new battlefield.

CONCLUSION

The deliberate government decision to involve itself in the realm of Internet security raises many issues. As the self appointed protector of information integrity and security, government maintains and enhances its position of power within the new economy. The Orwellian images of Big Brother need not be elaborated on. With regional areas beginning to work toward the possibility of government buying from local business, new models and problems are emerging. The implementation of a secure and trusted infrastructure will itself become credible if certain criteria are clearly met and standards applied.

Small businesses by their ad hoc nature of informal processes rarely have a competitive intelligence system. They are vulnerable to things in the environment which they know little or nothing about. An understanding of new technologies is an example of this weakness.
The role of government to facilitate safe passage is helped by a greater reliance on the two entities to actually do business. The Australian public key infrastructure framework through the Gatekeeper program is one effort that seeks to enhance the procurement of services for the government from small business.

REFERENCES

Abelson, H. et. al., (1998) *The Risks of Key Recovery, Key Escrow, & Trusted Third Party Encryption: A Report by an Ad Hoc Group of Cryptographers and Computer Scientists* [On-line] http://www.cdt.org/crypto/risks98/ Accessed: 23/03/2001, 26/04/2001, 03-04/05/2001.

Alberts, D.S., Garstka, J.J., Stein, F.P. (1999) *Network Centric Warfare*, CCRP Publications, p.1-51

Caron, J., (1999) *Banking on Trust*, Tele.Com, Manhasset

Kahaner, L., (1997) *What Competitive Intelligence can do for your Company*, Competitive Intelligence, Touchstone, New York, Chapter 2, p20-35

Martinus, I., (2000) *Baby S to Little M: Small Business IT Readiness and Overcoming Their Fear Factor*, Proceedings of the We-B Conference, Fremantle, 4-6 November, 2000

NOIE (2001) *National Office of Information Economy* [On-line]
http://www.noie.gov.au Accessed: 21-28/02/2001
http//www.noie.gov.au/publications/NOIE/SME/yellowpages_index.htm Accessed: 3-7/03/2001; 2-3/05/2001

O'Gorman, C., Doran, R. (1999) *Mission Statements in Small and Medium Enterprises*, Journal of Small Business Management,

Schneier, B (2000) *Secrets and Lies: Digital Security in a Networked World*, Wiley, New York, Ch.5, p.59-81

APPENDIX 1

Local business e-commerce security survey

	Question	Y/N
1	Do you think that Internet security is an important issue for your business at the moment?	
2	Do you think that this issue will be of more concern in the future?	
3	Do you know of Public Key Infrastructure (PKI) Encryption Technology?	
4	Have you heard of the government's push in the area of Internet Security through its Gatekeeper program?	
5	Have you heard of the Government Online campaign, which promotes businesses being online?	
6	Would credit card security be a concern for you when dealing with customers over the Internet?	
7	Would you join an online business community if the most secure methods were used to protect you, your suppliers and your customers?	
8	Do you think that your customers will use this type of electronic business marketplace if you were a part of it?	
9	Do you think that private details should be protected strongly when dealing over the Internet?	
10	Do you think that using the Internet is more risky than handing over your credit card at a restaurant, faxing your credit card numbers with personal details over fax or giving details over the phone?	

Thank you for your participation in this survey, you responses will greatly enhance our ability to provide an effective service focused on the requirement of the local business community.

Please email completed questionnaire to ian.martinus@wanneroo.wa.gov.au

Impact of Information Warfare on Business Continuity Planning

Nick Lethbridge

School of MIS,
Edith Cowan University
e-mail: n.lethbridge@ecu.edu.au

ABSTRACT

The threat of information warfare (IW) is presented within the framework of a standard model for business continuity planning. IW risks are outlined, together with relevant methods of defence and recovery. The new risks should be incorporated into the business' existing plans for business continuity. Recovery may involve more than recovery of data and systems, the business must also protect and recover its image in the marketplace. With good planning and the ability to provide a flexible response, the business will recover from disaster and the crisis will be managed to a positive conclusion.

Keywords: Information warfare, IW, Business continuity planning, BCP, Disaster recovery, Crisis management

INTRODUCTION

Information warfare (IW) has, as the name suggests, developed from a military background. And just as military strategy has found application in non-military business thinking – "Sun Tzu on the Art of War" (Giles, 1910) is almost compulsory reading for aspiring business managers – so too has information warfare found business applications. And – as with any form of warfare – it is not necessary to be a protagonist in a war, or even to have particular enemies, in order to suffer collateral damage from information warfare.

This paper introduces IW concepts and risks, from a business perspective. In particular, IW may pose a threat to the public image or reputation of a company. In the public image arena, "disaster recovery" becomes "crisis management". Planning for crisis management must be an integral part of business continuity planning.

INFORMATION WARFARE

In a very broad definition, Information Warfare is "activities by a state or non-state actor to exploit the contents or processing of information to its advantage in time of peace, crisis, or war and to deny potential or actual foes the ability to exploit the same means against itself." (Cimbala, 1999) In simpler terms, there are several aspects to IW: the use of information to gain advantage over another, and to defend against information attacks.

IW has been given several sub-categories, with a variety of names given to each of the overlapping categories. This paper will use two simple categories: Network Centric Warfare (NCW) and Info-terrorism.

- NCW is the use of information and information networks to improve the operational efficiency of war. More formally: "an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization." (Alberts, Garstka, & Stein, 1999)

- Info-terrorism involves the use of information itself as both a weapon and a target. Netwar, a similar concept, is defined as "a comprehensive information-based approach to societal conflict." (Arquilla and Ronfeldt, quoted in (Cimbala, 1999)) Info-terrorism is the tool of non-state actors and unconventional wars.

In the business world, NCW uses the information and communication tools that are increasingly available to a business or an individual. Effective NCW depends on effective integration of the tools with the business processes. War – and business – has always relied on some form of communication. Recent technology has improved the available options. A business may choose to use those options, or risk losing the war.

Info-terrorism attacks information stores, processes or exchange. There are a number of info-terrorism tools that may be used: Denial of service; Deliberately faulty microchips; System intrusion; Computer virus attack; Physical attack; Electronic jamming; Information interception. (Cobb, 1998)
Who is likely to use info-terrorism? Against whom are we protecting ourselves?

Info-terrorism (or the similar Netwar) involves measures short of actual war. It may be conflict or crime at a societal – or organisational – rather than national level. The protagonists may rely on network forms of organisation, doctrine strategy and communication. They may be new, old or modified protagonists: Terrorists, criminals, fundamentalists, ethnonationalists, competitive businesses or technology-aware individuals. Info-terrorists may be the next generation of radicals and revolutionaries. They may be anyone, anywhere in the world, with knowledge of technology and access to a networked computer. (Adapted from (Arquilla & Ronfeldt, 1996).)

Why do we accept the threat of information warfare? Why not simply detach our businesses from the info-terrorism highway? We leave ourselves open to the IW risk because information and technology also brings benefits. We can take advantage of the opportunities of "the information age". We can benefit from the changes: Changes in the way that wealth is created; Alterations in the distribution of power; Shrinkage of distances around the world; Compression of time and an increase in the tempo of our lives and our businesses. (Alberts et al., 1999)

There is always risk in business, information warfare is simply one more risk. It is, however, essential that we have a sound process and method to assess and deal with each risk. Key factors are: Understand exactly what are the risks; Know the strategies available for dealing with those risks; Know the cost and effectiveness of each strategy. (Abrahami, 1999)

"It's always easier to minimize risk than to recover from a setback. (Rodetis, 1999)" Yet, "No matter how much redundancy and fault-tolerance is built into (a system) a finite probability always remains for disaster to strike." (Chanchani, 2000)

IW (information warfare) may be seen as the aggressive use of information means in order to destroy, degrade and exploit the information systems of adversaries. Information warfare includes defensive actions taken to protect against IW attacks. In broad terms, IW is the use of information and communications systems in order to either damage an enemy or to protect against damage by an enemy. (DiCenso, 1999)

The BCP model presented below has steps for dealing with and minimizing risk. And it also includes steps for dealing with disaster, because disaster may still occur.

THE MODEL FOR BUSINESS CONTINUITY PLANNING

Formal concerns with "disaster recovery" concepts began in the US in the 1970s. The focus was on recovery after an IT failure. In the 1990s interest was increased in the UK by threats of terrorist bombings. Towards the end of the 1990s, disaster recovery was seen as a necessary part of planning for the year 2000. (The Safety & Health Practitioner, 1999) BCP in the lead-up to the year 2000 was taken as an opportunity for some information technology professionals to extend contingency plans to cover both Y2K and broader threats and issues. (Facer, 1999)

In the year 2000 – with Y2K problems safely in the past – representatives of AICPA technology committees still placed disaster recovery – a central part of BCP – amongst the top ten technological challenges and opportunities facing CPAs. The consensus was, that the disaster recovery issues must be confronted and resolved. (Tie, 2000)

DRP (disaster recovery planning) is a part of, or precursor to, business continuity planning (BCP). The focus of DRP has been on tangible assets, such as copies of data and spare equipment. The focus of BCP includes processes, networks, flows, procedures, affiliations – less tangible assets that are still essential for a business to survive and prosper. (Rodetis, 1999) DRP is technically focussed, it has been replaced by the more strategic BCP. (Elliott, Swartz, & Herbane, 1999) Nevertheless, disaster recovery is still an essential part of BCP.

A simple BCP (business continuity planning) model is used to frame the ideas presented in this paper. The author developed this model and used it to support a practical BCP project. The model is based on standards, project requirements, and the need for a practical framework. See Figure 1.

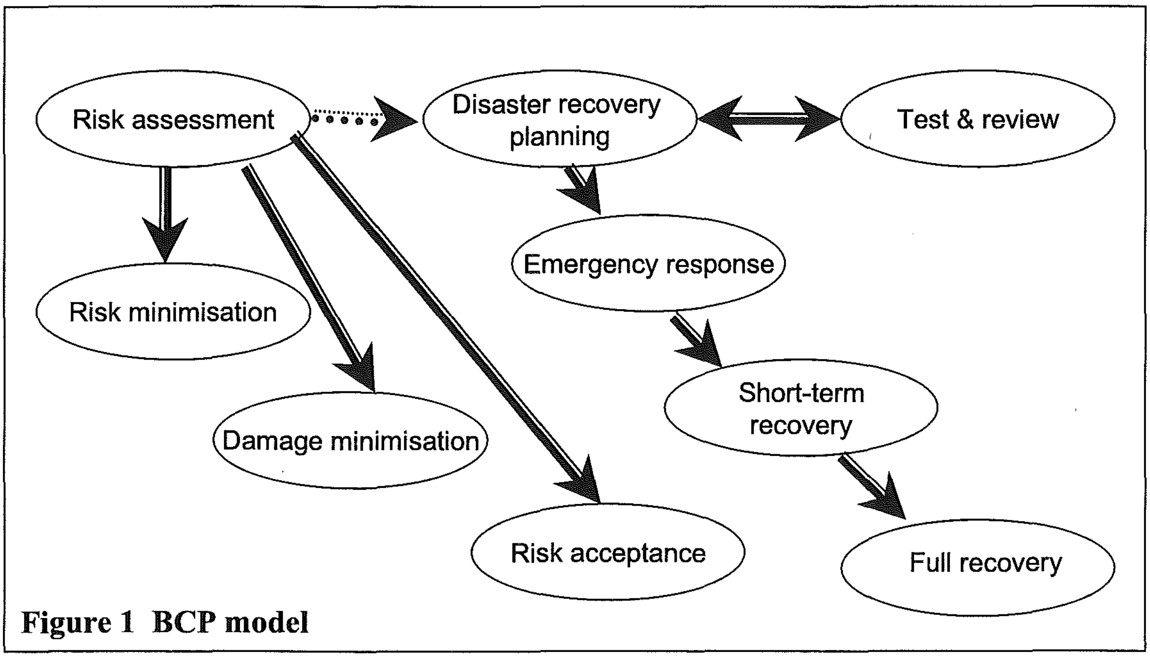


Figure 1 BCP model

The BCP model links the following components:

- **Risk assessment**: What are the chances that damage or disaster could occur? What are the likely effects if it does occur?
- **Risk minimisation**: Reduce the probability of the risk occurring.
- **Damage minimisation**: Reduce the potential damage if the risk does occur.
- **Risk acceptance**: Formally accept that cost of preventive action is not justified by the benefits that would result.

- **Disaster recovery planning**: Planning for the actions to be taken in the event of a disaster.
- **Test and review**: Ensure that the disaster recovery plan works, by testing it before the disaster occurs.
- **Emergency response**: Action to be taken as the disaster is happening.
- **Short-term recovery**: Immediate actions to get the business in operation again as soon as possible.
- **Full recovery**: Restoration of services and operations to get the business back to its normal level of operation.

The first four "risk" components have only a loose link with the remaining "recovery" components. Risk is concerned with assets (and processes, and knowledge) and the threats to those assets. Recovery is concerned with those same assets, but is not directly concerned with the threats. The disaster has happened, the cause is no longer relevant (for recovery purposes). It is enough that the assets must be recovered.

BUSINESS CONTINUITY AND INFORMATION WARFARE

Risk and Recovery

Risk assessment must be expressed in terms which allow a management decision to be made. Most common metrics are time or money. (Abrahami, 1999) "Time" could be mean time between failures. "Money" could be the expected annual cost of damage to the business.
Traditional risks – or threats – to business operations have included fire, flood, theft, breakdowns, computer viruses and human error. These disasters may damage data, hardware, software, personnel or facilities. There could also be: Misuse of authorised or unauthorised access; Physical, electronic or technical failures. There are the less likely but higher profile causes of information systems interruption such as the threats of terrorists and (before 2000) Y2K problems. (Bandyopadhyay & Schkade, 2000; Elliott et al., 1999)

Then there are the risks of information warfare.

Internal integration of systems and technology brings increased risk. Enterprise resource planning and data warehouse systems bring all enterprise data into a single, integrated database. This integration has a significant impact on database recovery procedures. Damage to a small part of the database may affect usability of all of the enterprise's data. (Elstien, 1999)

Even if your own business does not use e-commerce, you are bound up and down the supply chain with intranets, extranets, various other electronic links to suppliers, customers and regulatory agencies. All of these links add to the risks, such as intrusions or leaking of sensitive data. (Rodetis, 1999) The more that you depend on others – depending on suppliers for your own just-in-time inventory, for example – the more you are open to risk.

An attack on information may be directed at one business – or it may be a general attack on a country. An info-terrorist group may wish to support its own cause by causing damage to an entire country. If financial or monetary superiority is seen as a source of power, then damage to a country's economy will reduce that country's power. A successful information warfare attack may destroy commercial information and reduce a country to a state of "information poverty". This would reduce the country's power to act, either internally or externally. (Scott, 1999)

The use of e-commerce is becoming crucial to both business and government, it is essential if public and private sectors wish to remain competitive and efficient. E-commerce is dependent on the national information infrastructure (NII), such as voice and data networks and electricity supplies. Yet in Australia, the NII is both unhealthy and in a state of disrepair. With growing reliance on information technology, e-commerce and the NII, Australia has become a relatively easy target for an aggressive information war. (Scott, 1999)

Information is a "force multiplier": Good information may multiply the effect of an attack. Yet the risk of information warfare may not be destruction, of either physical or information assets. Information is also a "force modifier": It may be used to focus attacks on disruption rather than on destruction. (Arquilla & Ronfeldt, 1996) (p 44) The results may be just as damaging to the business.

A business interruption – due to either "normal" disasters or a disruption due to an information warfare attack – may cause a company to lose market share, image or credibility. It may reduce customer satisfaction or brand value, damage research data, or strain relationships with partners and suppliers. A single, major interruption may also divert management and employees from core business processes, reducing efficiency and perhaps allowing less visible problems to grow larger. (Rodetis, 1999) Information warfare – IW – is a term with military roots. Unfortunately, IW is not restricted to military protagonists. As with any form of warfare it is not necessary to have your own, military enemy in order to be adversely affected by information warfare.

> "After the Oklahoma City bombing, 40 square blocks were barricaded off for weeks," says Mary Carrido, president of Irvine, California-based continuity planning consultant MLC & Associates and national chairwoman of the 1,800 member Association of Contingency Planners... "This devastated 4,000 businesses; 210 are not in existence anymore." (Rodetis, 1999)

An IW attack may be the work of an individual with criminal intent. Non-state adversaries, from warriors to criminals, with the ability to strike across national boundaries, are currently ahead of government actors in using the techniques of info-terrorism. We should expect an increasing amount of info-terrorism and crime by terrorist and criminal "amateurs". (Arquilla & Ronfeldt, 1996) (p 43) An IW attack may be the work of a well organised group with shared goals and distributed physical presence. Power is moving to actors who are skilled at developing networks, at using electronic communications such as the internet, to control and coordinate their activities. The ability to organise concerted activities is, in itself, a source of power. (Arquilla & Ronfeldt, 1996) (p 43)

The same level of public relations crisis may be the result of legitimate concerns about company activities. For instance, when a mathematics professor stumbled upon a flaw in the Pentium chip made by Intel Corp., he posted his finding on message boards, and news of it raced across the Web. Irate consumers, many of whom had never come across the mathematical error, began demanding that Intel replace the chip. The Internet firestorm turned into a full-fledged crisis. (James, 2000)

Crisis Management

The traditional disaster recovery plan involves teams of experts on standby, spare equipment, backup copies of data, hot sites at the ready, all the reassurance that technology and money can provide, but the disaster may affect customers, company image, market share. The recovery plan must also include public relations, crisis communications and coordination with public agencies. (Gluckman, 2000) A company disaster may cause a crisis in public perceptions, this public crisis may have effects well beyond the immediate effects of the disaster itself. A safety problem with a plane, for example, may be quickly fixed. But the public disquiet may affect the entire airline for several years.

Information warfare may attack the public image of a business rather than the information assets. The disaster recovery plan must include a plan for public relations crisis management.

"Crisis management doesn't make the crisis go away, but it helps firms manage the situation, themselves and their response. If they don't manage the flow of information, the media will do it for them, and the vacuum will be filled with a flow of speculation." (Eugene Bacot, director of PR company Oakes Bacot, in (Simms, 2000).
The proliferation of media, including television and internet up-to-the-minute-news sites, means that crises now escalate very quickly. News broadcasters need a story every 15 minutes or less. Consumers, highly attuned to the power of the media, will turn to the internet to voice their concerns. The recent crop of "anti-corporate" web sites exemplify this trend. (Simms, 2000)

> "But not all crises are 'bangs in the night'. A crisis could be a security breach, a product recall, pornographic conversations in the chat rooms of a supposedly family-friendly internet site, or fraud. Many crises begin as 'issues', which creep up on a company because they are neither monitored nor managed." (Simms, 2000)

Crisis management has three major functions: Concern – identifying a response to the issue, including the communications strategy; Containment – ringfencing the issue, ideally designating one senior individual to act as spokesperson; and Control – reclaiming ownership of the issue, through generating rather than responding to press comment. (Simms, 2000)

Companies – and company employees – should monitor internet discussions related to their company or their product. All employees should be encouraged to record and report any Web mention of company-related matters. But only the crisis managers should respond. (James, 2000)

"Crisis managers need to move faster and use communications vehicles that may be unfamiliar, such as Web sites and chat rooms, to reach consumers in real time. And those consumers are more cynical and demanding, thanks to the proliferation of investigative news shows and class-action lawsuits. Finally, experts say pre-crisis planning is the order of the day rather than simply reacting to events that already have happened." (James, 2000)

"Crisis management needs to be seen in the context of reputation management… According to Mike Regester, partner at reputation risk management consultancy Regester Larkin, this is because 'reputation is like a line of credit in a bank, which a company can draw on when it has a problem…'" And the crisis is not over until the public and the media agree that it is over. Regester continues, "The media, not companies, decide when the crisis is over. It's like wrestling a gorilla – you take a break when the gorilla does." (Simms, 2000)

Planning for Business Survival

"When more than inconvenience occurs, the event is determined to be a disaster…" (Glorioso, 1999) The disaster recovery or crisis management plan could be "A current, detailed and flexible plan…" (Gluckman, 2000) or "…very simple – no more than a checklist to be used by people who know what they are doing." (Simms, 2000) The provisions put into place to deal with a crisis or disaster (and the suitability of the depth or detail of those provisions) may be seen as a measure of the resilience of the organisation. (Elliott et al., 1999)

"The old approach to planning for disaster centered on recovery planning only. This is no longer sufficient to ensure that your organization has mitigated existing risk, prepared an organization-wide methodology for meeting disaster, and will ultimately survive. The goal of the BCP process is creating a plan that will assure the organization's disaster survival. Identifying and minimizing existing risk up front supports the process and is essential to creating a BCP that works." (Clifton, 2000)

Business continuity planning – like Sisyphus' work – is never finished. Business continuity, disaster recovery and crisis management plans are living documents. Large companies may have full-time BCP staff with plans under continuous update. Smaller organisations may review each plan annually. The review schedule depends on the rate of change within the organisation. (Rodetis, 1999)

The review schedule should also match the uncertainty and the rate of change of the environment in which the organisation operates. There appear to be at least two vital factors for both high-reliability organisations – those with long-term success at business continuity – and individual excellence: A mindset that expects unpleasant surprises; and the flexibility to adapt and react differently in different circumstances.

> "Only those people or organisations that have invested a considerable amount of preparatory effort in the pre-crisis period will be able to deploy compensatory responses in a sufficiently timely and appropriate manner so as to maintain the necessary resilience." (Reason, 2001)

CONCLUSIONS

Information warfare is not a new concept, but it is gaining importance. As our business increases its dependence on information – and on the rapid and accurate exchange of information – we are more vulnerable to an attack on that information. With increased speed of public communication, we are also more vulnerable to an attack with information being used as the weapon.

Business continuity planning must adapt to the new threats of information warfare. There are a number of new risks that must be assessed, this paper has outlined these risks. Recovery from disaster may involve more than recovery of data and systems, the business must also protect and recover its image in the marketplace. An IW attack may require a crisis management response.

As with any other form of risk, the business must plan – in advance – to recover from the risk. Risk may be reduced or the effects minimised, but there will still be a chance that disaster will happen. With good planning and the ability to provide a flexible response, the business will recover from a disaster and the crisis will be managed to a positive conclusion.

The threat of information warfare has been presented within the framework of a standard model of business continuity planning. This paper provided an outline of the risks associated with information warfare, and the possible methods of defence and recovery. The new risks should be incorporated into the business' existing plans in support of business continuity.

REFERENCES

Abrahami, A. (1999). *IT Investment and Riskless Management.* Management Services (Apr).

Alberts, D. S., Garstka, J. J., & Stein, F. P. (1999). *Network Centric Warfare*: CCRP Publications.

Arquilla, J., & Ronfeldt, D. (1996). *The Advent of Netwar.* Santa Monica: Rand Corporation.

Bandyopadhyay, K., & Schkade, L. L. (2000). *Disaster Recovery Planning by HMOs: Theoretical Insights.* Health Care Management Review (Spring).

Chanchani, D. (2000). *A "Killer-proof" Application for Linux.* Enterprise Systems Journal (Jan).

Cimbala, S. J. (1999). *Nuclear Crisis Management and Information Warfare.* Parameters (Summer).

Clifton, R. W. (2000). *Business Continuity Planning.* Occupational Health & Safety (Oct).

Cobb, A. (1998). *Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks.* Parliament of Australia [On-line] http://www.aph.gov.au/library/pubs/rp/1997-98/98rp18.html [1999, 17 Jan].

DiCenso, D. J. (1999). *IW Cyberlaw.* Airpower Journal (Summer).

Elliott, D., Swartz, E., & Herbane, B. (1999). *Just Waiting for the Next Bang: Business Continuity Planning in the UK Finance Sector.* Journal of Applied Management Studies (Jun).

Elstien, C. (1999). *Reliance on Technology.* Enterprise Systems Journal (Jul).

Facer, D. (1999). *Rethinking: Business Continuity.* Risk Management (Oct).

Giles, L. (trans). (1910). *Sun Tzu on the Art of War.* [On-line] http: //all.net/books/tzu/tzu.html [2001, 22 Jan].

Glorioso, B. (1999). *Recovery or Tolerance?* Enterprise Systems Journal (Jul).

Gluckman, D. (2000). *Continuity...* Recovery. Risk Management (Mar).

James, D. (2000). *When your Company goes Code Blue: How Crisis Management has Changed.* Marketing News(Nov 6).

Reason, J. (2001). *Heroic Compensations: The Benign Face of the Human Factor.* Flight Safety Australia (Jan-Feb), 28-31.

Rodetis, S. (1999). *Can Your Business Survive the Unexpected?* Journal of Accountancy (Feb).

Scott, T. (1999). *The Cause of an Information War against Australia.* Journal of the Australian Institute of Professional Intelligence Officers, 8 (1), 36-51.

Simms, J. (2000). *Controlling a Crisis.* Marketing (Nov 9).

The Safety & Health Practitioner. (1999). *Appetite for Disaster Recovery Fuelled by Millennial Fears.* The Safety & Health Practitioner (Jun).

Tie, R. (2000). *E-business Tops Tech Priorities for CPAs.* Journal of Accountancy (Mar).

The Problem of Categorising Cybercrime and Cybercriminals

S. M. Furnell

Network Research Group
Department of Communication and Electronic Engineering
University of Plymouth
Plymouth, United Kingdom.
Email:sfurnell@plymouth.ac.uk

ABSTRACT

With the continual increase in incidents of hacking and viruses, the issue of cybercrime is now recognised as a major international problem, which has been given increased scope and impact by the pervasion of the Internet. However, defining what is meant by the term can prove to be somewhat difficult and a range of alternative classifications have been devised different sources. This paper considers the problem of categorising cybercrime and identifies the fact that a harmonised nomenclature would be beneficial to both those individuals and organisations concerned with combating the problem, as well as for those concerned with reporting the issue to the general public. The discussion presents a variety of different top-level classifications of cybercrime, each of which has been utilised in practice by authoritative sources in the field. The need for further sub classification (and the difficulty associated with doing so) is then illustrated by examining the specific issue of hacking, which reveals that numerous types and motivations can be identified.

Keywords: Cybercrime, Hackers, Security.

INTRODUCTION

As networked computer systems have grown and matured, so too has the nature of crime and abuse within the environment. In the earlier days of computing, abuse was largely restricted to fraud and theft related activities, which simply represented the extension of traditional crimes into the electronic environment. However, as time has moved on, new and more advanced forms of abuse have emerged (e.g. computer viruses), which often appear not so much a means to an end, but an objective in themselves.

Surveys from recent years have revealed the increasing scale of the cybercrime problem. For example, the 2001 CSI/FBI Computer Crime and Security Survey reports financial losses totalling almost $378 million from 186 respondents, whereas the previous year had witnessed only $265.6 million from 249 respondents (CSI 2001). The 2001 survey also revealed that 85% of the 534 respondents had detected some form of security breach in the preceding twelve months. In view of such findings it is little wonder that many governments and law enforcement bodies around the world are increasing their efforts to address and control the cybercrime issue. In Europe, for example, the recognition of the growing problem and the need for a harmonised approach has prompted the drafting of a European Convention on Cybercrime (CoE 2000). However, whilst the general problem has been recognised, it has also been demonstrated that there are many different ways in which the underlying issues can be interpreted. This paper seeks to expose the significant variety that exists in cybercrime classification schemes, highlighting that this may represent a problem when attempting to make cross-comparisons between different assessments of the issue.

CATEGORISATIONS OF CYBERCRIME

At the most basic level, cybercrime can simply be interpreted as types of crime involving the use of computers. However, this is obviously a very broad description and to examine the issue more precisely it is useful to consider previous interpretations of computer crime and abuse that have been offered by some authoritative sources.

Over the last twenty years, the UK Audit Commission has conducted a series of surveys to determine the extent of the computer crime and abuse problem in both the UK public and private sectors. Looking at the issues encompassed by the surveys, it can be seen that, over the years, the recognised range of crimes has broadened. For example, in the 1981 survey the only categories were fraud and theft. However, by the time of the most recent survey in 1998, the range had more than quadrupled to encompass a variety of other problems. The full range of categories, along with the Audit Commission's own definitions of them, are presented in Table 1 (Audit Commission 1998).

Crime / abuse	Description
Fraud	• for private gain or benefit: – altering input in an unauthorised way; – destroying / suppressing / misappropriating computer output; – altering computerised data; – alteration or misuse of programs (excluding virus infections.
Theft	• of data; • of software.
Use of unlicensed software	• using illicit copies of software.
Private work	• unauthorised use of the organisation's computing facilities for private gain or benefit.
Misuse of personal data	• unofficial 'browsing' through computer records and breaches of data protection legislation.
Hacking	• deliberately gaining unauthorised access to a computer system, usually through the use of communication facilities.
Sabotage	• interfering with the computer process by causing deliberate damage to the processing cycle or to equipment.
Introducing pornographic material	• Introducing pornographic material, for example, by downloading from the Internet.
Virus	• distributing a program with the intention of corrupting a computer process.

Table 1: Computer crime and abuse categories from UK Audit Commission

Looking at the Audit Commission categories more closely, it is possible to draw a distinction between those crimes that are computer-assisted and those that are computer-focused, as defined below.

- **Computer-assisted crimes.** Cases in which the computer is used in an supporting capacity, but the underlying crime or offence either predates the emergence of computers or could be committed without them.

- **Computer-focused crimes.** Cases in which the category of crime has emerged as a direct result of computer technology and there is no direct parallel in other sectors.

Using these classes, it is clear that the Audit Commission headings of fraud, theft, unauthorised private work, misuse of personal data, sabotage and pornography all fall into the computer-assisted category. Meanwhile, hacking and viruses are definite by-products of the IT age and are, therefore, computer-focused. Problems of hacking and viruses clearly fall within this category. Categorising the use of illicit software is a debatable point, as it clearly would not be feasible without a computer. However, the underlying nature of the offence is a breach of copyright – something that frequently occurs in other domains such as music and publishing. As such, for the purposes of this discussion, it will be considered to fall into the computer-assisted class.

A diagrammatic representation of the different categories of cybercrime is presented in Figure 1. The light shaded boxes denote computer-focused crimes, whereas the darker ones represent the computer-assisted variety (the unshaded boxes are used for the higher level categorisations, within which both computer-assisted and computer-focused crimes will exist). The classifications in the table are not exhaustive and represent merely one way of thinking about the issues. For example, they could alternatively be grouped according to their resulting impacts (financial loss, destruction of data etc.) rather than the methods involved.

It can be seen that some further levels of detail have been added over and above the Audit Commission categories. For example, the issue of misuse of personal data has been broadened under the more general heading of invasion of privacy, and placed alongside the issues of harassment and identity theft – both of which can be effected through the online medium. Harassment may occur against organisations or against specific people – in the later case it may sometimes be referred to as 'cyber-stalking'. Equally, identity theft may be applied at both levels and, when targeted against an organisation, may be referred to as 'cyber-squatting'.

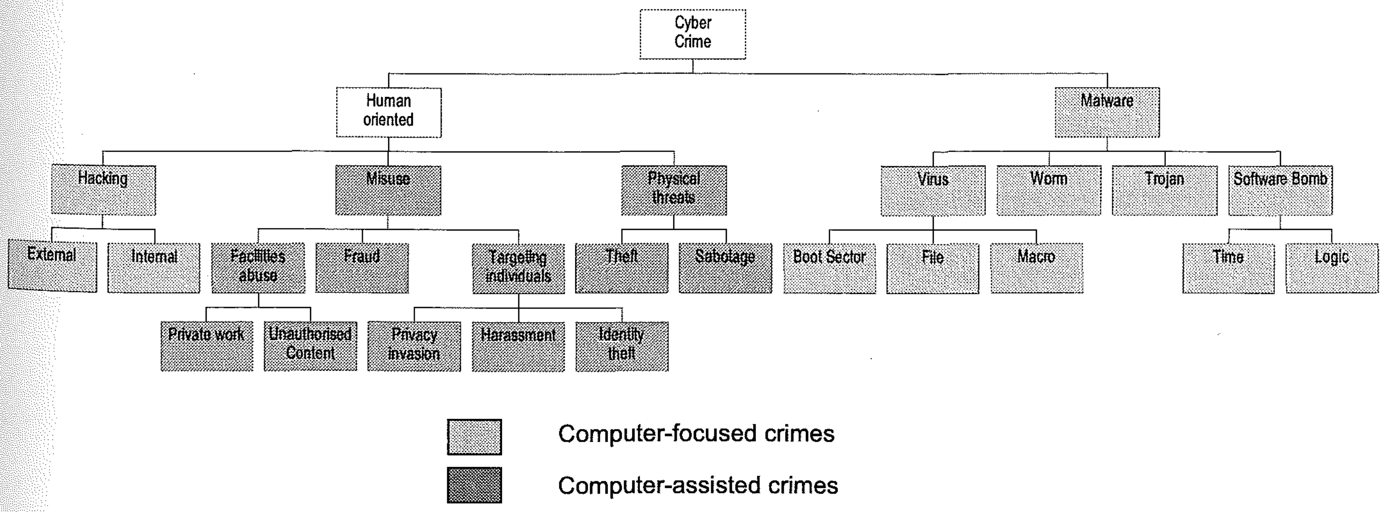


Figure 1: Cybercrime categorisation

An alternative set of computer crime categories is provided by the FBI's National Computer Crime Squad (Fraser 1996), as listed below:

- Intrusions of the Public Switched Network (the telephone company)
- Major computer network intrusions
- Network integrity violations
- Privacy violations
- Industrial espionage
- Pirated computer software
- Other crimes where the computer is a major factor in committing the criminal offence

It can be observed that, in this case, hacking and viruses (the computer crimes with probably the highest level of media and public recognition) are not explicitly named. They are, however, the means by which a number of the categories could be realised.

To offer another, and final, view on the issue, the thirteen classifications used by the Computer Security Institute (CSI), as the basis for their 2001 Computer Crime and Security Survey, conducted in collaboration with the FBI, were as follows (CSI 2001):

- Theft of proprietary information
- Sabotage of data or networks
- Telecom eavesdropping
- System penetration by outsider
- Insider abuse of net access
- Financial fraud
- Denial of service
- Spoofing
- Virus
- Unauthorized insider access
- Telecom fraud
- Active wiretapping
- Laptop theft

It can be seen that in many cases, the descriptions refer to much more specific types of incident (e.g. denial of service, laptop theft), while others categories (such as virus) are very generic by comparison and could easily be subdivided further. At the same time, other classes of crime that were identified by the previous classifications (e.g. use of unlicensed or pirated software), do not appear to be encompassed by the CSI's headings.

The classifications presented here are by no means exhaustive and various other sources can be found that present further alternative versions. However, what should already be apparent from this discussion is that the general issue of cybercrime can be interpreted in many different ways. Although from one perspective this is not a problem, in the sense that each of the different organisations above are attempting to add value by making their own specific interpretations of a general problem, it can potentially become confusing for those wishing to more accurately understand or report cybercrime incidents. If everyone takes a different view of the problem, then it is more difficult to draw direct comparisons between different survey results and other such incident reports. This, in turn, makes it harder to get a full picture of the problem on an international level and make harmonised assessments of the scale.

CATEGORISATIONS OF HACKERS

Having looked at how the general issue of cybercrime can be decomposed into a variety of alternative first level groupings, it is also appropriate to consider how these sub-headings can, in turn, be further subdivided. This section illustrates the point by considering the single issue of hacking. Figure 1 presented a simplified sub-classification of this point, splitting the problem into just 'internal' and 'external' categories. However, it is possible to consider the issue of hacking in considerably more detail than this, which at the same time serves to illustrate that the classification problem continues at lower levels.

The definition of the term 'hacker' has changed considerably over the last 30 years. In the 1960s, hackers were the dedicated software and hardware gurus, and the term largely referred to persons capable of implementing elegant, technically advanced solutions to technologically complex problems. In the new Millennium, the moniker is more commonly used to refer to persons who gain unauthorised access to systems and data. At the extreme are a subset (often distinguished by the term 'crackers') that perform openly malicious actions upon the systems they enter, such as deleting files, modifying data and stealing information. The media is largely credited with misusing the term 'hacker' and an explicit distinction between hackers and crackers is maintained in certain writings. However, to argue that it is just the media that misuses the term is itself misleading – indeed, it is debatable whether this interpretation should be considered misuse at all. The nature of the computing industry has now changed and the commonly accepted meaning of the word 'hacker' (in an IT context) can be illustrated by considering dictionary definitions from recent years:

- 'A person who uses computers to gain unauthorized access to data' - The New Oxford Dictionary of English, 1998.

- 'A skilled and enthusiastic computer operator, *esp* an amateur; an operator who uses his or her skill to break into commercial or government computer or other electronic systems' - The Chambers Dictionary, 1998.

It can be seen that specific emphasis is placed upon the issues of unauthorised access and breaking into systems. As such, for the public at large, the act of hacking is generally synonymous with these factors. In fact, the nature of the wording in some cases serves to imply that if an individual uses a computer for a hobby, but does not engage in unauthorised access, then they do not meet the definition of a true hacker. Clearly, these definitions are not compatible with the viewpoint of first-generation hackers, but they nonetheless seem to represent the generally accepted interpretation in modern society.

Whatever your preference, the use of a term such as hacker or cracker is still sometimes too vague. It is analogous to the use of a simple label such as 'criminal' to refer to a lawbreaker – the label alone is not very informative and there are a number of sub-categories that can be used to enable a more specific classification. Unfortunately, there is no overall set of hacker sub-groups that is regarded as definitive. There are, however, numerous terms that can be used to provide more specific focus and meaning. For example, a fairly high-level distinction can be made using the terms Black Hat and White Hat hackers. The former refers to the majority of hackers – those intruding into systems in an unauthorised, and frequently malicious, manner (to add yet another term, these may also be referred to as 'dark-side' hackers). White Hats, by contrast, are 'ethical' hackers, working for the good of system security. So, in a sense, these groupings can be considered to represent the same basic distinctions as the hacker and cracker labels defined earlier. It should also be noted that another term, Grey Hat, is used to refer to individuals who fall somewhere in between these two camps – those whose motives are unclear or may be prone to change.

In order to further illustrate the lack of a clear-cut black and white, good and bad distinction, the paragraphs below present some other names that are frequently ascribed to members of the hacker community (it should be noted that even this still does not purport to provide an exhaustive list).

- **Cyberterrorists.** Terrorists who employ hacker-type techniques to threaten or attack against systems, networks, and/or data. As with other forms of terrorism, cyberterrorist activities are conducted in the name of a particular political or social agenda. The underlying objective will typically be to intimidate or coerce another party (e.g. a government).

- **Cyber warriors.** Persons employing hacking techniques in order to attack computer systems that support vital infrastructure, such as emergency services, financial transactions, transportation and communications. This essentially relates to the application of hacking in military and warfare contexts.

- **Hacktivists.** Hackers who break into computer systems in order to promote or further an activist agenda. Incidents such as the defacement of web sites are very often linked to these individuals.

- **Malware writers.** Not strictly a classification of hacker – but often considered alongside them – these individuals are responsible for creating malware programs such as viruses, worms and Trojan Horses.

- **Phreakers.** Individuals who specifically focus upon hacking telephone networks and related technologies. Their objectives may range from simple exploration of the infrastructure to actually manipulating elements of it (e.g. to enable free phone calls to be made).

- **Samurai.** Individuals who are hired to conduct legal cracking jobs, penetrating corporate computer systems for legitimate reasons. Such hackers may also be termed **Sneakers**.

- **Script kiddies.** Individuals with fairly limited hacking skills who rely upon scripts and programs written by other, more competent, hackers. Hackers of this type typically cause mischief and malicious damage and are generally viewed with scorn by more accomplished members of the hacking community. Such individuals may also be referred to as **Packet Monkeys**.

- **Warez d00dz.** A sub-class of crackers, who obtain and distribute illegal copies of copyrighted software (after firstly breaking any copy protection mechanisms if appropriate). The spelling used is representative of a common form of hacker slang – in this case the two words, when written properly, are 'Wares Dudes'. More commonly, these individuals are known as **Software Pirates**.

From the above, it quickly becomes clear that the issue of hacking is as riddled with alternative classifications as the top-level issue of cybercrime. At the same time, the definitions have shown that many of the headings are not simply alternative names for the same thing – there is actually some difference between the different types of hacker. As such, saying that an individual is a hacker is really just as generic as saying that someone is a cybercriminal – it does not give enough definition. In the case of hackers, the difference essentially comes down to the motivations behind their actions. To illustrate this, a classification of hacker types against a variety of potential motivations is given in Table 2. Note that the column relating to 'Old School' hackers makes reference to the original hackers of the 50s and 60s, and those who share their values today. The intention is not to cast them as cybercriminals, but to enable a contrast between their motivations and the other groups that are often classed under the generic label of 'hacker'. In each case, the most likely motivator for the class of hacker is also indicated by the emphasized tick mark.

	Cyber- terrorists	Cyber Warriors	lacktivist	Malware writers	Old School	HREAKI RS	Samurai	Script Kiddies	Warez d00dz
Challenge				✓	✓	✓	✓		✓
Ego				✓	✓	✓		✓	✓
Espionage		✓		✓					
Ideology	✓	✓	✓		✓				✓
Mischief				✓		✓		✓	
Money		✓		✓		✓	✓		✓
Revenge	✓		✓	✓				✓	

Table 2: Hackers and their motivations

As the table suggests, a single hacker will not necessarily have a single motivation that drives his or her actions. In this sense, hacking skills can be regarded as generic – able to be applied as appropriate to the needs of a hacker at a particular time.

The above discussion illustrates that, as with the top-level classifications of cybercrime, the issue of hacking can be interpreted in many different ways. In many cases when reading information about hackers, it is essential to be sure that you are attuned to the correct terminology. Many sources, particularly media reports, utilise the different labels quite loosely, happily interchanging them in many cases. By contrast, other writers, demanding a greater degree of specificity, argue passionately for the correct distinctions to be maintained. This section has not sought to resolve the problem – merely to illustrate that the label of 'hacker' can be further decomposed, and that, in the context of discussing and analysing cybercrime, it is useful to do so in order to appreciate that different motivations may be at work. A more comprehensive discussion of the issue is provided in Furnell (2001).

CONCLUSIONS

What should be overwhelmingly clear from the discussion presented here is that cybercrime is not a straightforward concept to define. Whilst all of the classifications are appropriate when considered in isolation, attempting to compare and contrast them immediately reveals inconsistency, overlaps and omissions. As a result, without a clear and standardised nomenclature, the cybercrime issue risks being clouded by misunderstanding.

Of the top-level categorisations presented in this paper, the author considers that the UK Audit Commission's interpretation is the most straightforward – with fewer obvious overlaps between the different categories identified. Having said this, however, the categorisation could still be usefully decomposed into more specific levels of detail – particularly in relation to classifications such as hacking and viruses.

The discussion of hackers has sought to further demonstrate the ease with which different interpretations can be placed upon what some people would prefer to neatly describe as a single issue. Although it removes the simplicity, it is appropriate to make such further distinctions in many circumstances, in order to remove ambiguity and reduce misunderstandings. The desirability of at least distinguishing between hackers and crackers provides an illustration of this, as does the frequent misapplication of the term virus, which is often incorrectly used as a catchall name for other forms of malware such as worms and Trojan Horses.

If a suitably standardised set of names can be devised then it can be used as the basis for improving education and raising awareness in relation to cybercrime at several levels. This could include the security community that seeks to protect systems against cybercrime, as well as the governments and law enforcement bodies that attempt to control the problem, and the media that reports it to the public at large.

REFERENCES

Audit Commission. (1998). *Ghost in the Machine – An Analysis of IT Fraud and Abuse.* The Audit Commission, United Kingdom.

CoE. (2000). *Draft Convention on Cyber-Crime (Draft No 19).* Council of Europe, PC-CY (2000) Draft No 19. Strasbourg 25 April 2000.

CSI. (2001). *2001 CSI/FBI Computer Crime and Security Survey.* Computer Security Issues & Trends, vol. VII, no. 1. Computer Security Institute. Spring 2001.

Fraser, B.T. (1996). *Definition of 'Computer Crime'.* Computer Crime Research Resources [On-line] http://mailer.fsu.edu/~btf1553/ccrr/welcome.htm#definition

Furnell, S.M. (2001). *Cybercrime: Vandalising the Information Society.* Addison-Wesley.

Virus Infection – The "People Problem"

G. Robertson[1] and T.A. Vuori[2]

[1] *School of Commerce*
Murdoch University, Australia,
E-mail: g.robertson@murdoch.edu.au;

[2] *School of Commerce*
Murdoch University, Australia,
E-mail: t.vuori@murdoch.edu.au;

ABSTRACT

In the recent major computer virus outbreaks, including Melissa, 'Love Bug' and others, much of the focus centered on the failure of technical measures to prevent the catastrophes. Whilst software and hardware measures might be implemented to apply mechanistic precision to their watchdog role, recognising that human vulnerabilities played a major part in these devastating outbreaks is important. This will allow appropriate measures to be devised to avoid or minimise the effect of these infections, including raising the level of user awareness more frequently. This paper explores the possibility that much of the responsibility for the diffusion of computer infections could rest with related social dimensions.

Keywords: computer virus, computer security, social dimension

INTRODUCTION

On March 26, 1999, virus developer David Smith released a macro virus labeled as list.doc into the alt.sex Usenet newsgroup that suggested the attachment contained a list of passwords for pornographic websites (Scoblionkov 1999, F-Secure Corporation 2000a, ZDNET UK 2000). This virus was to become known as 'Melissa'. Subsequently generated e-mail had message headers insisting that the e-mail was an important message from a known source, and in the message body, recipients were told that the attachment had been requested and, furthermore, that it was secret (Tocheva et al. 1999). Within a few hours thousands of computers were infected by what could be described as being the most rapidly spreading virus ever to have been released.

A little over a year later, on May 4, 2000, the "I LOVE YOU" worm, soon to become euphemistically known to the world as the "Love Bug", was unleashed (F-Secure Corporation 2000b) and, within 12 hours, had spread around the globe. Where it had taken previous "computer infections" months or, at best, weeks or days to spread as widely, global cover had been achieved with unprecedented and devastating swiftness. Once again, the infection-carrying message appealed to the social nature of the user. This time, as its name would suggest, the "I love you" message heading targeted one of human beings most primitive instincts and strongest social feelings.

Whilst most of the corporate focus in both the Melissa and 'Love Bug' outbreaks centered on the failure of technical measures to prevent the catastrophes, much of the responsibility could rest with related social dimensions. Though software and hardware measures might be implemented to apply mechanistic precision to their watchdog role, recognising that human vulnerabilities played a major role in these devastating outbreaks is important. This will allow appropriate measures to be devised to avoid or minimise the effect of these infections in the future. This paper will explore, at a conceptual rather than technical level, the human or peopleware (Shaw, Ruby & Post n.d.) dimensions of computer infections, including but not limited to the virus creators, the corporate systems that attempt to thwart the attacks and finally, and most important, the end-user whose actions directly impact on the successful spread or otherwise of any particular strain of computer infection.

INFECTION AND TRANSMISSION

The Melissa and 'Love Bug' infections probably hold the dubious distinction of being the most devastating computer infections ever, both in terms of sheer scale of infection and associated cost of damage. For this reason these two infections have been used as the basis for examining the associated social dimensions, so often overlooked when apportioning blame and, more importantly, developing systems that will minimise or eradicate the problem of computer infection altogether. Much has been said about anti-virus software, and there has even been reference to anti-virus hardware (Melcer 2000), but disproportionately little has been said about the associated "people problem", probably the weakest chink in the anti-virus armour (Harrington 2000).

THE MELISSA WORD MACRO VIRUS

Melissa is a simple Word macro that, when activated on opening the Word document which arrived as an e-mail attachment, caused Outlook to e-mail an infected document to the first 50 e-mail addresses in the users address book. Although under certain conditions it did insert some text into Word documents, the virus was essentially not malicious. In order for the virus to spread, infected documents needed to be sent between computers and this was achieved when unsuspecting users opened enticing but infected e-mail attachments and triggered the embedded Word macro. This resulted in automated mail-outs and exponentially propagated infected documents. The estimated US$80 million (Geralds 1999) price tag for damage resulted largely from collateral damage. That is failure of servers due to the sheer volume of e-mail traffic that Melissa generated, the clean-up of each machine that was required as well as the cost of stalled business processes.

THE "LOVE BUG" WORM

Although the world's media screamed "virus", the "Love Bug" was in fact a worm (Symantec, 2000), and a lot more complex than Melissa. Designed to ensure maximum diffusion using the Internet as a means of propagation, the "Love Bug" exploited the emotions of human users to trigger each instance of infection. Thereafter programming code exploited vulnerabilities in popular user software and weaknesses in network protection to continue the infection process with little or no subsequent human intervention. For more detailed description on how "Love Bug" worm exploited the technical weaknesses see (Lovebugvirus.com 2000, Chien and Ewell nd).

REASONS FOR THE OUTBREAKS

Given the high costs associated with these infections, and on a more personal level, the frustration of millions of disgruntled users and thousands of flurried systems administrators, apportionment and avoidance of blame often shifted even more rapidly than the infections themselves. Accountability, it would seem, can be attributed to a variety of factors, depending on the perspective of the attributor.

Focus often centered on the failure of the mostly technical "security systems" in place, with attempts to discern why a particular application or a piece of equipment had failed to prevent widespread computer infection. The social elements of the transmission, if acknowledged, were often begrudgingly peripheral.

AUTHORS OF INFECTIOUS CODE – CHALLENGE, GREED AND POWER

Viruses and worms are not artificially generated but rather, in most cases, the product of an individual or group of people with premeditated intent. The primary motivator would probably include pursuit of the perceived sense of accomplishment that would be experienced when the malicious creation impacted on others. The intensity of these emotions would probably be heightened if one of the motivating forces had been revenge or if the impact and effect of the release was widespread, devastating or both.

Although it is conceded that the "Love Bug" outbreak was probably a rare exception, following on from Melissa, it received exceptional media coverage. This was to be expected as damage estimates were placed at US$10 billion (Geraghty 2000) after the first week and Lloyds of London estimated the total damage bill to be in the region of US$15 billion three weeks later (Clausing 2000). An event of such magnitude certainly warranted the international media frenzy it received. Subsequent investigations tended to indicate that whilst the author, a known hacker (Burke and Walsh, 2000), had sought to obtain unauthorised access to ISP facilities he had previously penetrated, he had not set out to intentionally create such a devastating worm (Chandrasekaran 2000) and certainly not sought the international notoriety that he achieved. The media attention, however, was obviously very appealing to others (Evans 2000) as within two weeks of launch there were already 23 variants of the "Love Bug" in circulation. Copycat behaviour is not uncommon, with many of the worms and viruses ending up having multiple variants as 'wannabe' authors make minor changes to the readily available code, and provides further evidence that a variety of social factors play a central role in outbreaks of computer infections.

THE INFECTOR – EXPLOITING SYSTEM AND USER VULNERABILITIES

The second factor that must be considered is that of the infector, the actual worm or virus code itself (Vaughn-Nichols 2000). Both the Melissa virus and the "Love Bug" worm preyed upon vulnerabilities in Microsoft's Outlook application. The payload caused the malicious code to replicate and distribute using e-mail as the vehicle. Melissa targeted only the first 50 addresses in the users address book whereas the "Love Bug" escalated infection by utilising every last e-mail address available. The widespread use of the Outlook application thus ensured maximum diffusion.

Secondly, by the time the "Love Bug" was launched, Internet Relay Chat (IRC) had become a popular form of communication on the Internet with millions of users congregating in hundreds of thousands of Chat Rooms globally. By manipulating popular IRC software to enable it to act as a diffusion agent (National Infrastructure Protection Center, 2000), the worm's creator was further exploiting the social nature of users, moving beyond the usual tactic of triggering an address book mail-out of malicious code. Many of the viruses and infections that attack humans and animals use various forms of social contact as a means of diffusing.

THE USERS – TRUSTING, NAÏVE AND EMOTIONAL

Even though the actual malicious payloads played a significant role in the "success" of the respective infections, none would have been possible were it not for the users (Wagner 2000) and their actions who are, under normal circumstances, reaping the benefits of unprecedented levels of interconnectivity, speed of information transfer and ease of use of the various communications applications. In many instances computers and the Internet are approached with such a degree of familiarity that users do not even think about their actions, operating almost on 'autopilot' until some event which is extraordinary causes a more considered analysis of actions.

Of all of the social factors associated with the outbreak of computer infections, it is unlikely that any is more powerful than the forces associated with human emotions. Fully aware of this, many of the carriers contain phrases in the message header or main body that play on the emotions of the recipient. These include messages like "I love you", "pictures of my naked wife" and "Very Funny" to mention but a few. In fact, to avoid detection, a number of the variants of the "Love Bug" abandoned the obvious "I love you" header in favour of other socially appealing exhortations, one including reference to a Mother's Day invoice. From the mayhem arising out of multiple user-aided outbreaks, it is clear that many could not resist the 'brilliant social engineering' of the virus writers (McLauchlin 2000).

Despite numerous prior outbreaks the users (victims) continue to be largely responsible for perpetuating the spread of viruses, worms and other malicious Internet and Intranet transmitted infections, mostly due to naïveté. Liebovitch (2000) justly chides users for being more preoccupied with visual stimulation on the Internet than with interacting intelligently with its content and concepts. He accuses users of having attention spans that run on "Internet-time". He does, however, concede that many more businesses than home users appeared to be affected by the "Love Bug" outbreak indicating that companies should also shoulder a fair degree of blame for failing to educate the users and check the spread of the worm.

THE CORPORATES – SYSTEMS WISE, PEOPLE FOOLISH

Although it might be argued that anti-virus technology (both software and hardware) installed by the business world largely failed during the initial stages of both the Melissa and "Love Bug" outbreaks, a stronger argument, pointing to human failings, could be made. In the first instance any subsequent onward transmission required that a user activated the trigger either by opening the suspect e-mail or accompanying attachment. User education is certainly a social issue and, as much of the infection occurred within companies, the efficacy of the corporate education programmes to combat this type of networking threat must certainly be questioned. In fact, the successive Melissa and "Love Bug" outbreaks were probably expensive answers to those questions that were never asked or, at best, not really dwelled upon.

A second corporate issue is the general absence of any formal virus clean-out procedures that could be employed when a company became aware that it's systems had become infected (Wagner 2000). Whilst one might have been able to forgive organisations for their lack of preparedness at the time of the Melissa outbreak, no reasonable excuse for similar vulnerability could be found when the "Love Bug" struck over one year later. It is plausible to suggest that having been exposed to such a major outbreak, and finally having conquered the malicious infector, systems administrators responsible for protecting companies developed a misplaced sense of invincibility. Perhaps, having conquered what must have been considered at that time "the mother of all viruses", they did not believe it possible that they could possibly again be infected in a similar manner. Alternatively, it may have simply been that administrators who had installed anti-virus software were lulled into a false sense of security (Wagner 2000) that grew proportionately with the time since the horrors of Melissa had been put behind them.

MICROSOFT – SUPER-FRIENDLY, SUPER-VULNERABLE

It is no surprise that both of the major computer infections were Windows-based, and preyed on inherent vulnerabilities of Microsoft applications. Windows is the most popular client platform, enjoying around an 87% market share (The Standard 2000) and its accompanying Office Suite also the market leader, 96% market share (McCracken 2000). Firstly, it would be statistically quite likely that a virus-developer would be using a Windows environment (although it is certainly recognised that more than a few Microsoft-haters, who on principle use alternate platforms, might express their emotions by creating Microsoft destroying code, do exist). Secondly, with such market dominance (virtual ubiquity in fact), Windows and Office Suite both offer great potential for the diffusion of malicious code and devastation of individual and networked computers.

Although a Microsoft spokesman attributed the exploitation of Outlook to its widespread usage, the critics argued that there was competitive advantage (speed) to be gained by Microsoft integrating its proprietary applications with its proprietary Operating System (Vaughn-Nichols 2000) and also that Microsoft developed applications that focused more on the ease of use than on security (Kleinbard and Richtmyer 2000). Given that the Windows platform was developed with the intention of making computers more accessible and easy to operate by the average user, and as a result enjoyed unrivalled adoption, it appears reasonable to conclude that the critics' explanation is most accurate.

Although it might initially seem as if the two most damaging computer infections could be attributed largely to poor programming, there is once again a significant social dimension that should be considered. Firstly, Microsoft's philosophy of making its software user-friendly is in direct response to user demands - programmes that are difficult to operate and master are likely to be avoided, particularly by those who are less experienced. This has contributed to the relative ubiquity of Windows and the Microsoft Office Suite and that is what makes it an attractive potential "carrier" to someone intent on wreaking maximum havoc. Unaware, even trusting users, ubiquitous use and an application trading security for user-friendliness certainly proved to be a deadly cocktail of circumstances ripe for exploitation.

REFLECTIONS

In the aftermath of the Melissa outbreak a number of industry observers commented that, owing to the non-malicious payload, the whole experience could probably be heralded a timely wake-up call that did more good than it might have done harm (Bezroukov 2000). Firstly, due to the press frenzy, many companies became more virus aware and scanned their systems, quite a few finding other viruses active within their network (Landry 1999). Secondly, companies that did not have adequate incident handling procedures in place could rectify that deficiency and, in the event of future attacks, minimise future damage. Further, an 'opportunity' was provided for companies to re-configure their servers to prevent or reduce future damage arising from malicious mail floods (Bezroukov 2000). Finally, in addition to heightened corporate awareness, there was obviously unprecedented awareness by the average user of the fact that they needed to be alert to potential threats from viruses and worms.

When the "Love Bug" ravaged computer systems barely 13 months later there were certainly many questions raised, with very few adequate answers forthcoming. In many instances anti-virus hardware and software protection was unable to detect the threat in a timely manner, allowing many more machines than previous to be infected. Even though it would be fair to say that numerous organisations were able to implement pre-determined disaster recovery procedures, many more were not as prepared or capable. It was also apparent that, despite the most unusual patterns of e-mail generation the "Love Bug" precipitated, many servers were not able to detect and act on this incongruity and thus suffered a degree of melt-down not even considered possible at the time of Melissa. Most of all the obviously very low level of awareness demonstrated by the average user who, again, was the major contributor to the disaster. Thus, far from being a costly but worthwhile I.T. blight, for most companies, compared with the "Love Bug", Melissa was simply a less expensive disaster.

Shortly after the Melissa outbreak users were much more likely to follow 'safety' guidelines when dealing with suspicious e-mail. The very fact that users became suspicious of e-mail was an important conceptual leap. However, that level of awareness had dissipated by the time the "Love Bug" was released. Once again, users and their actions played a central role in spreading the mayhem that ensued. Once the damage had been inflicted, users were, no doubt, at peak levels of alertness which, based on historical patterns, would not be sustained. The Kournikova worm struck in February 2001 though it never caused serious, widespread systems damage because its payload was benign (O'Neill and Michelmore 2001). Seduced by offers of pictures of the popular young tennis star, many users worldwide could not resist the temptation to click on the attachment that activated the code which again exploited Outlook and sent infected e-mail to all addresses in the users address book.

By now, the reality should have been very clear to network administrators and engineers – users are the major security threat and require continual reminders if they are to remain vigilant. Perhaps it is in the nature of the guardians of the network – the administrator and engineer – to disregard any assistance from the user, seeking rather to install equipment or applications (Melcer 2000) that would be more amenable to their control. This seems to be supported by representations to the U.S. House of Representatives enquiry into Melissa where a senior virus-fighter suggested that in order to avoid threats in the long term there needed to be fundamental changes to the way in which technology was used, with operators and developers being required to recognise they were operating in a hostile environment (Pethia 1999). In essence, technical solutions were being proposed as the key to longer-term success against infections. However, these unquestioning slaves, without doubt at least part of a total solution, do only as they are instructed (programmed or configured) and are eventually unable to provide protection against attacks specifically designed to exploit their blind spots. At this time the otherwise protected users, lulled into a false sense of security in the absence of any attacks having reached them, would be exposed to the attack and, in all likelihood, be duped by the infector. Having managed to evade detection by the anti-virus systems and been further propagated by unsuspecting users, the infector would be likely to achieve maximum infection because those unsuspecting users would fuel the outbreak. Initially at least, systems would be compromised because the systems-protection measures had been circumvented and their defenses temporarily thwarted. Had users been more responsible for their own protection it is likely that the effects of the infection would be significantly reduced, confined largely to those users who were not practicing 'safe-mail' or 'safe-surfing'.

Whilst network engineers and systems administrators will understandably continue to seek the utopia of system-based, technical protection, a cost-benefit analysis should nevertheless be conducted to assess the potential level of safety that user-centered protection strategies might provide. It would seem reasonable to suggest that, if the users are the major triggers of infection, far more attention be paid to user education within companies. Any awareness program would need to address both new users to the system as well as existing users. It would seem that user awareness is most focused shortly after widespread publicity (internal and external to the company) about the problems associated with computer infections but that these levels wane over time.

If the most recent widespread outbreaks are used as yardsticks then level of awareness appears to last less than nine months (the time between the "Love Bug" and "Kournikova" attacks). The challenge would be for administrators to ensure that they raise the level of user awareness about potential infections far more frequently, and using a variety of methods capable of overcoming familiarity that a dull and repetitive program is sure to evoke. In essence the awareness activities probably need to be novel and at frequent but irregular intervals. Prevention must surely work out to be substantially cheaper than cure.

CONCLUSION

There seems to be significant evidence for the notion that the "people problem" dimension in computer infections really does exist and apparently requires urgent, special attention. It may not be possible to eliminate the risk of individuals generating malicious code, but what would be achievable is the adoption by organisations of a more "people (end-user) focused" set of strategies to reduce the spread of computer infections. Future research might examine the nature of effective end-user "anti-infection" training and also the optimum frequency of refresher warnings to keep awareness of virus-safe practices top-of-mind.

REFERENCES

Bezroukov N. (2000). *Melissa Worm/Virus – a Worm Parasiting on Ms Office 97 Architectural Problems and Ms Word Users' Igonorance* May 16 [On-line]
www.softpanorama.org/Antivirus/AV_Secrets/Vgallery/melissa.shtml.

Burke J. and Walsh N. (2000). *Supervirus threatens IT meltdown.* Daily Mail & Guardian, 8 May [On-line]
www.mg.co.za.

Chandrasekaran R. (2000). *Virus May Have Been Act of 'Youthful Exuberance' Newsbytes.* 12 May [On-line]
www.newsbytes.com Accessed: 20 April 2001.

Chien E. and Ewell B. (undated). *VBS.Loveletter.* Variant, Symantec [On-line]
www.symantec.com Accessed: 11 April 2000.

Clausing J. (2000). *In Hearing on 'Love Bug', Lawmakers Go After Software Industry.* The New York Times on the Web, 11 May [On-line]
www.nytimes.com Accessed: 28 May 2000.

Evans D. (2000). *Counting the cost of the Love Bug.* vnunet.com, 9 May [On-line]
www.vnunet.com Accessed: 16 April 2001.

F-Secure Corporation (2000a). *F-Secure Virus Information Pages: Melissa* [On-line]
www.datafellows.com Accessed: 23 May 2000.

F-Secure Corporation (2000b). *F-Secure Virus Information Pages: LoveLetter* [On-line]
www.datafellows.com Accessed: 23 May 2000.

Geralds J. (1999). *Melissa virus creator pleads guilty.* vnunet.com, 10 December [On-line]
www.vnunet.com Accessed: 16 April 2001.

Geraghty J. (2000). *The Global Fight Against Computer Viruses.* Policy.com, Rev. 11 May [On-line]
www.policy.com Accessed: 21 May 2000.

Harrington T. (2000). *Virus wars' new battlegrounds.* vnunet.com, 20 October [On-line]
www.vnunet.com Accessed: 16 April 2001.

Kleinbard D. and Richtmyer R. (2000). *U.S. catches 'Love' virus.* CNNFN.com, 4 May [On-line]
cnnfn.com Accessed: 26 May 2000.

Landry J. (1999). *It All Depends on Your Definition of Benign.* Computer Press Association, June [On-line]
www.computerpress.org Accessed: 16 April 2001.

Liebovitch E. (2000). *Tough Love? Windows users must like walking around with big "Kick Me" signs on their backs.* ZDNet, 9 May [On-line]
www.zdnet.com Accessed: 1 May 2001.

Lovebugvirus.com (2000). [On-line]
www.lovebugvirus.com Accessed: 24 May 2000.

McCracken H. (2000). *The Suite Hereafter: Sneak Peek at the Next Microsoft Office*. IDG.net, October 5 [On-line]
www.idg.net Accessed: 20 April 2001.

McLauchlin T. (2000). *Love bug bites e-mail users around the world*. Boston Herald.com, 5 May [On-line]
www.bostonherald.com Accessed: 16 April 2001.

Melcer R. (2000). *Viruses spawning opportunity for some*. Business Courier [On-line]
www.cincinnati.bcentral.com Accessed: 26 April 2001.

National Infrastructure Protection Center. *Love-Letter-For-You/AKA Love Bug Virus*. Alert 00-041c, May 6 [On-line]
www.nipc.gov Accessed: 20 September 2001.

O'Neill J. and Michelmore K. (2001). *Kournikova hits 100,000 within hours*. f2.com.au, 13 February [On-line]
www.f2.com.au, Accessed: 16 April 2001.

Pethia R. (1999). *The Melissa Virus: Inoculating Our Information Technology from Emerging Threats*. Testimony before Subcommittee on Technology, Committee on Science, U.S. House of Representatives, April 15 [On-line]
www.house.gov Accessed: 16 April 2001.

Scoblionkov D. (1999). *'Melissa' Police Work Lauded*. Wired.com, 2 April [On-line]
www.wired.com Accessed: 23 May 2001.

Shaw E.D., Ruby K.G. and Post J.M. (updated). *The Insider Threat to Information Systems* [On-line]
www.smdc.army.mil Accessed: 20 September 2000.

Symantec (2000). *Learn More About Viruses and Worms* [On-line]
www.symantec.com Accessed: 24 May 2000.

The Standard (2000). *Microsoft Dominates 87 Percent of PCs Operating Systems*. 3 April [On-line]
www.thestandard.com Accessed: 20 April 2001.

Tocheva K., Hypponen M. and Rautianinen S. (1999). *Virus Descriptions*. F-Secure [On-line]
www.europe.f-secure.com Accessed: 11/04/2001.

Vaughn-Nichols S.J. (2000). *Who Deserves the ILOVE YOU Blame?* Yahoo.com [On-line]
dailynews.yahoo.com Accessed: 28 May 2000.

Wagner M. (2000). *Lesson Of Love: IT Needs Better Defense Plans*. Internetwork.com, 11 May [On-line]
www.internetwk.com.

ZDNET UK (2000). *Melissa: Simple Facts*. 29 March [On-line]
www.zdnet.co.uk.

Weaving The Tangled Web – Deception On the Internet, A Travellers Tale?

Lorraine O'Neill-Cooper

Edith Cowan University, Australia,
E-mail: l.o_neill@ecu.edu.au

ABSTRACT

The abundance of users on the Internet is reflected not only in the enormous numbers of web pages that exist but also in the diversity of industries they represent. The travel industry is one of those industries. With the growth of electronic commerce the Internet gives people the ability to personalise holiday packages to fit particular budgets and tastes.

This preliminary paper discusses travel web page deception using a three level framework: 1. Hiding the real. 2. Showing the false and 3 Suspect a scam. It discusses the concept that fraud occurs within travel web pages and that travel consumers do not recognize the differences between their perceptions of reality and reality itself.

Keywords: Internet, Travel, Fraud, Deception, Perception.

INFORMATION WARFARE ENTERS THE TRAVEL INDUSTRY

Sun Tzu, the 5th Century Chinese military tactician observed that all warfare is based on deception. Throughout his book 'The Art of War Sun' Tzu reiterates the importance of deception and tactical maneuvers for survival, victory and minimising loss (Sawyer 1994). As with Sun Tzu's philosophy on military warfare, information warfare is about competition, there is no win/win affect, it has only a win/lose affect, there is only one victor in war. This paper discusses fraudulent activities such as deception and perception within travel websites; it focuses on the 'e.vendors' or the owners of the websites and how they deceive consumers. The paper also focuses on the travel consumer and how their perceptions of travel websites can lead them to being deceived so frequently and with apparent ease.

Information warfare is about dominating cyberspace or as Hutchinson and Warren (2000(a)) would call it the 'info-sphere'. The Internet is re-shaping all forms of commerce and competition (Frew 2000) including exploitation. The fundamental weapon and target in information warfare is, by definition, information, it is a product that is manipulated to the advantage of those trying to influence events (Hutchinson and Warren 2000(a)). In the case of the travel website, data and the way it is used has a powerful role in the decision-making process of a would-be consumer, it can manipulate an individuals perception of reality.

Lasry (2000) states that any type of dishonest conduct can be classed as fraud. Fraudulent activities that distort reality, such as deception (Hutchinson et.,al 2000(a)) are being widely used on the Internet. With the ease of web design and the low cost of entry (O'Neill 2000), it is not necessarily the high-tech criminal fraternity that are using these deceptive tactics online, it is possible that e.travel vendors are now using tactical deception as a means of self-survival, success and financial gain. Illegal web pages are often the same standard as legitimate ones – not only making it harder to distinguish between them but also making the consumer more likely to choose the better value product (Ramsden

2000). Many tourism vendors see the Internet as one of the most effective weapons for competing in today's business world (CRC 2001; McKee 1999).

METHODOLOGY, LITERATURE REVIEW AND OBJECTIVES

The aims of this preliminary study were to set some parameters that could then be used as the starting point for a more comprehensive quantitative study. An interpretive approach was taken for this paper as the study focuses on human actions and perceptions and social constructs (Hussey and Hussey1997). The paper aims to promote an understanding of Internet deception in tourism from the point of view of two separate types of stakeholders, the e.travel vendor, those using the Internet to sell travel products (the term e.travel vendor will incorporate both legal and illegal vendors), and the e.consumer, those who purchase travel products over the Internet.

Examination of literature shows that tourism and technology research is becoming popular, especially in the web-based marketing and distribution areas (Frew 2000; MacKay and Fesenmaier 2000; Tierney 2000; Weber and Roehl 1999). Although there are many articles written on Internet fraud in general, little academic research could be found on illegal or improper use of the Internet specifically relating to online travel consumers and online travel fraud. Tierney (2000) states that published research into the effectiveness of tourism websites is still limited.

THREE LEVELS OF CLASSIFICATION

People and/or organizations that bring together core competencies and skills to exploit an opportunity to their supposed mutual advantage typically form deceptive Internet sites. (Valli 2000). The Internet is an instrument that gives once unknown perpetrators a perfect site for a camouflage attack. In the travel industry this includes those individuals or businesses wishing to obtain money and/or customers through deceptive means.

Hutchinson and Warren (2000(a)) in their book "Illusion and Reality in the Information Age" describe a two level framework for classifying deception, using this framework the author has incorporated a third level to accommodate the three types of e.tourism fraud occurring online:

□■ Level 1 : Hiding the real – Unknown or Ignorant.
□■ Level 2 : Showing the false – Creating a false impression or hiding facts.
□■ Level 3 : Suspect a scam – Non-existent.

All three levels could be inter-related yet the intentions of individual e.travel vendors and their expected outcomes would be specific to their expected outcomes.

Level 1 : Hiding the real

The majority of Internet travel deception is connected to false information and relates to the buyers perceptions or ideals. Level 1 is based on perception management. According to Cohen (1998) perception management causes people to believe things that forward their goals. Perception management is not necessarily related directly to lies, deceit or fraudulent attempts but a mismanagement of the truth – they may simply leave out the unsavory parts or they do not personally perceive any unsavory parts.

The Level 1 e.travel web page is designed using the e.vendor's personal perception of the product they are selling. This product when viewed by an e.consumer can be perceived differently by both the e.travel vendor and the e.travel consumer, the ideals of one person may not be the ideals of another. Image perception and attractiveness varies not only between individuals but also across religions, cultures or countries. MacKay and Fesenmaier (2000) confirm that there can be commonalities and differences between two cultural groups. To put it simply people see what they want to see (Spinney 2000).

Level 2 : Showing the False

The second level e.travel vendors depict aspects of travel products on websites by falsifying information, this information entices e.travel consumers to purchase travel products from them. Level 2 incorporates two types of e.travel vendors:

a. The careless e.travel vendor and
b. The dishonest e.travel vendor

The careless e.travel vendor may inadvertently put incorrect information onto a website due to poor management, sloppy record keeping or insufficient attention to detail (Lasry 2000). The dishonest e.travel vendors use words and pictures on a website to portray the desired travel destination e.travel consumers look for. Photographs are considered by MacKay and Fesenmaier (2000) important to successfully creating and communicating an image of a destination on the internet, they not only present an idea of what the destination looks like but can contribute to values and ideals of the viewer (McKay and Fesenmaier 2000; Frew 2000).

Level 2 e.travel vendors may want to develop, or have every intention to develop on-going relationships with their consumers, they do not see a win/lose affect but see a win/win affect, they believe they have a value creating strategy (McCormick 2000), even though their perception of consumer needs are wrong.

Level 3 : Suspect a Scam

Level 3 specifically relates to the on-line criminal. An imposter posing as an e.travel vendor, who has no product to sell, has significant effect on the financial stability of their consumer and are there to obtain financial advantages by deception, falsification of travel products, or fraudulently inducing persons to invest money.

Scams are not a spur-of-the-moment crime (Ramsden 2000), it takes time to set-up a web page, organise processes for on-line credit card payments and decide what market niche to focus on. This type of tactical deception, as stated by Infowar.com (1999)

> '... is similar to the sweet blossom that entices the insect to its nectar,
> only to discover it is a Venus Flytrap.'

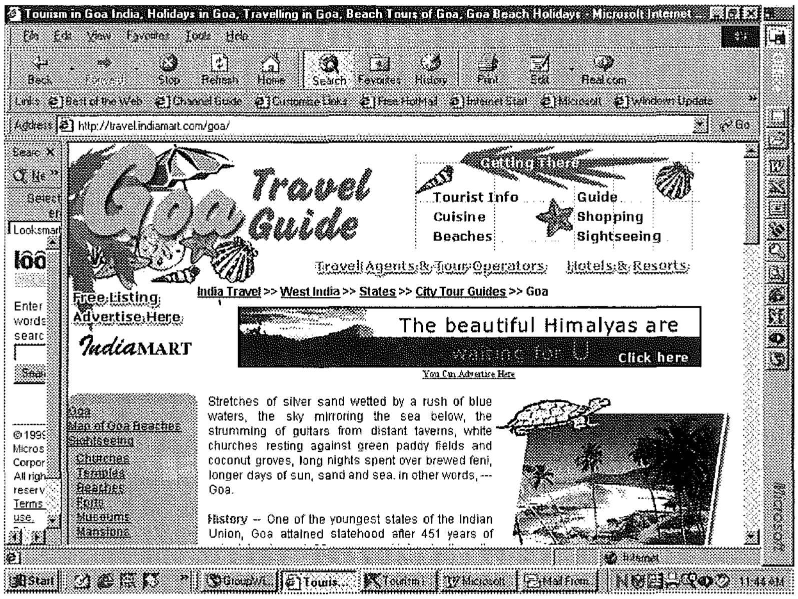
One aggressive tactic stated by Hutchinson and Warren (2000(b)) is that information can be manipulated or 'created' (disinformation) to provide the target or its environment (for example consumers) a perception that develops behaviours beneficial to the attacker (the vendor). Consumers most likely to be scammed online have the money or credit to purchase expensive items (McKee 1999; Weber & Roehl 1999).

IS IT DECEPTION OR PERCEPTION?

The Internet allows individuals to shift from a perceived world to a hyper-real world, a world where representation gives way to stimulation, via sight and sound, almost to a point where consumers can electronically see what they want to see and have the ability to book it online instantaneously.

The following examples (figures 1, 2 and 3) are of travel destinations where mismanagement of the truth, perception or deception occurs:

Goa



Tourism in Goa India, Holidays in Goa, Travelling in Goa, Beach Tours of Goa, Goa Beach Holidays - Microsoft Internet ...

Address http://travel.indiamart.com/goa/

India Travel >> West India >> States >> City Tour Guides >> Goa

Stretches of silver sand wetted by a rush of blue waters, the sky mirroring the sea below, the strumming of guitars from distant taverns, white churches resting against green paddy fields and coconut groves, long nights spent over brewed feni, longer days of sun, sand and sea. In other words, --- Goa.

History -- One of the youngest states of the Indian Union, Goa attained statehood after 451 years of

Figure 1: Goa Travel Guide
Source: http://travel.indiamart.com/goa/

> 'Stretches of silver sand wetted by a rush of blue waters, the sky mirroring the sea below, the strumming of guitars from distant taverns, white churches resting against green paddy fields and coconut groves, long nights spent over brewed feni, longer days of sun, sand and sea.' --Goa (Indiamart.com 2001).

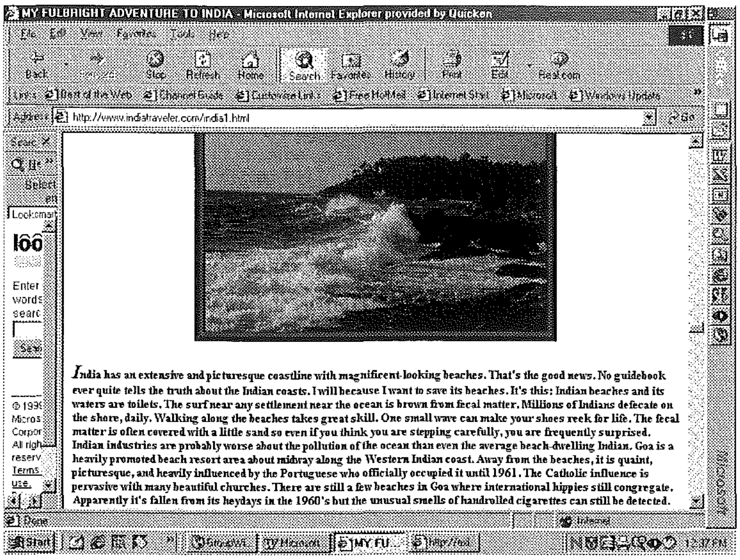
Even brochures and magazines complement particular parts of Goas' attributes:

'White sand fringed with swaying coconut palms and picturesque crags. The thing about Palolem is that it's not exactly undiscovered, so if you're looking for somewhere a tad more secluded try Morjim. A group of sea turtles has chosen this gorgeous spot for nesting and as a result it is protected and peaceful. Ah, here's to an Indian summer...'

(Vive 2001 p16)

These words, attached to a photo of an empty pristine white beach, indicates some quiet idyllic spot to spend a few weeks relaxing. But beware research and surf a few more pages and read on...

"The first sight of this city can be an unnerving and a shocking experience. Expect it to be extremely crowded and polluted...as far as disorganization and filth is concerned Goa is fast catching up with many other Indian cities" (Colaço 2000).


MY FULBRIGHT ADVENTURE TO INDIA - Microsoft Internet Explorer provided by Quicken
File Edit View Favorites Tools Help
Back Stop Refresh Home Search Favorites History Print Edit Real.com
Address http://www.indiatraveler.com/india1.html
Go
Looksmart
Enter words search
Done
Internet
Start
MY FU...
12:37 PM

India has an extensive and picturesque coastline with magnificent-looking beaches. That's the good news. No guidebook ever quite tells the truth about the Indian coasts. I will because I want to save its beaches. It's this: Indian beaches and its waters are toilets. The surf near any settlement near the ocean is brown from fecal matter. Millions of Indians defecate on the shore, daily. Walking along the beaches takes great skill. One small wave can make your shoes reek for life. The fecal matter is often covered with a little sand so even if you think you are stepping carefully, you are frequently surprised. Indian industries are probably worse about the pollution of the ocean than even the average beach-dwelling Indian. Goa is a heavily promoted beach resort area about midway along the Western Indian coast. Away from the beaches, it is quaint, picturesque, and heavily influenced by the Portuguese who officially occupied it until 1961. The Catholic influence is pervasive with many beautiful churches. There are still a few beaches in Goa where international hippies still congregate. Apparently it's fallen from its heydays in the 1960's but the unusual smells of handrolled cigarettes can still be detected.

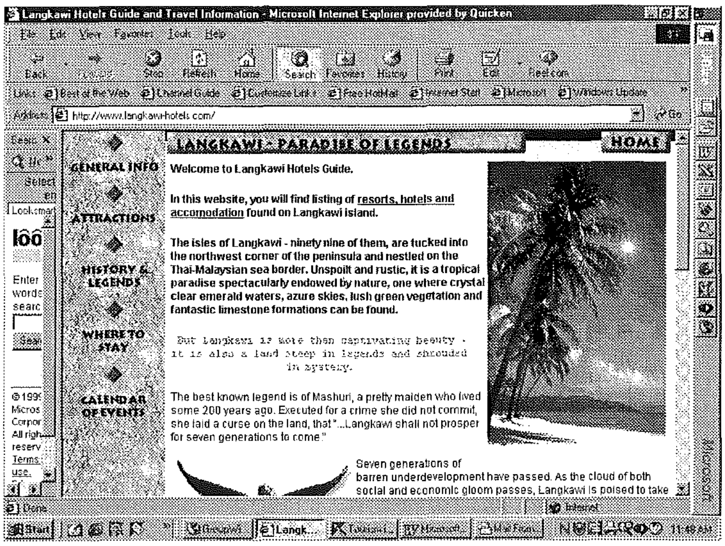
Figure 2: Brown Beaches
Source: http://www.indiatraveller.com/india.html

Figure 2 depicts a web page of a traveller who has experienced Indian beaches, he advises:

"India has an extensive and picturesque coastline with magnificent-looking beaches. That's the good news. No guidebook ever quite tells the truth about the Indian coasts. I will because I want to save its beaches. It's this: Indian beaches and its waters are toilets. Its surf near any settlements is brown from fecal matter. Millions of Indians defecate on the shore daily…"

He goes on to praise the country he is in but also makes travelers aware of some of its unadvertised peculiarities.

Langkawi



Langkawi Hotels Guide and Travel Information - Microsoft Internet Explorer provided by Quicken
Address http://www.langkawi-hotels.com/
GENERAL INFO
ATTRACTIONS
HISTORY & LEGENDS
WHERE TO STAY
CALENDAR OF EVENTS
HOME

LANGKAWI - PARADISE OF LEGENDS

Welcome to Langkawi Hotels Guide.

In this website, you will find listing of resorts, hotels and accomodation found on Langkawi island.

The isles of Langkawi - ninety nine of them, are tucked into the northwest corner of the peninsula and nestled on the Thai-Malaysian sea border. Unspoilt and rustic, it is a tropical paradise spectacularly endowed by nature, one where crystal clear emerald waters, azure skies, lush green vegetation and fantastic limestone formations can be found.

But Langkawi is more than captivating beauty - it is also a land steep in legends and shrouded in mystery.

The best known legend is of Mashuri, a pretty maiden who lived some 200 years ago. Executed for a crime she did not commit, she laid a curse on the land, that "...Langkawi shall not prosper for seven generations to come."

Seven generations of barren underdevelopment have passed. As the cloud of both social and economic gloom passes, Langkawi is poised to take

Figure 3: Langkawi – Paradise of Legends
Source: http://www.langkawi-hotels.com/

'The attractions and things to do while holidaying in Langkawi are numerous and can be categorized conveniently under five broad Ss: Sun and Sand; Sea and Water sports; Shopping; Sightseeing; Sailing/cruising...The pristine beaches, clean and azure-blue waters that border the island shores and provide the beach front to most beach resorts stand out as a prime attraction to visitors. They can simply sit back on the beach front under palmy and shady trees and savour the balmy air at leisure.'(Langkawi Hotel Guide 2001).

Once again these words are surrounding photos of clean wide stretching beaches and underwater photos of colourful reefs and a multitude of fish species. The comments from a recent traveller were:

'I'm sure that not so long ago Langkawi was a beautiful tropical island but due to the increased tourist numbers and building activity on Langkawi the trip from the airport to the hotel is not attractive. The beaches are not clean, rubbish, especially plastic bags, comes in with the tide, but fortunately when the tide goes out so does the cow dung!' (A. Cooper 2000)

Sometimes the vendor could simply be concealing information to enhance the website, as could be seen in the above websites, although to what extent is concealed and to what extent the consumer investigates also leads to varied depths of deception (Cohen 1998).

Thailand

Tapachai and Waryszaks (2000) stated that

> '...although Thailand is depicted in websites as a relaxing destination, travel consumers perceptions of Thailand found that Thailand was a rushing, busy, noisy and polluted place.'

Information available to travel consumers before they visit a tourist region is usually supplemented by their own mental image of that region. In Tapachai and Waryszaks (2000) research this could be the respondents individual stereotype perception of Bangkok, Thailand's capital, and not the country as a whole.

DOING THE MASKAROVA

Trust is the basis for both positive and negative interactions and exchanges occurring between humans (Valli 2000). Use of the Internet by consumers is contributing to "blind faith" according to Valli (2000). This trust has led to increased Internet travel transactions (McKee 1999). The geographical location of an Internet travel site diminishes the ability of the consumer to gather tacit behaviour from the vendor. For example, the consumer cannot see the body language, voice innotation, eye movements or the excessive sweating (Valli 2000) as one would with a bricks and mortar vendor. The increased use of the Internet can also be associated with the numerous discounted products available online, no global limitations and the 24/7 availability of the Internet to the consumer (O'Neill 2000).

Pictures and detailed information relating to travel products are not the only items used by fraudulent e.travel vendors. Information regarding secure sites for payments and contact names and addresses can also be listed on an Internet site, although this information could be a ruse to gain the trust of the consumer and support the vendor hypothetically as a reliable travel organization [Level 2&3]. The Russians call this type of tactical deception, Maskarova, (Infowar.com 1999) the art of camouflage. The e.travel vendor gains the upper hand on the e.travel consumer by getting them to believe what the e.travel vendor wishes them to believe, causing the e.travel consumer to act and respond the way the e.travel vendor wishes, either by booking accommodation at the e.travel vendors establishment or by giving payment details on line so the e.travel vendor can gain money through credit card fraud.

ABOVE THE LAW

An additional implication to fraudulent travel sites is the use of photographs, drawings and words without the approval of the original owner. Not only is the use of digital manipulation available to fraudulent vendors but plagiarising original photographs is easily captured via tools on the Internet. Copyright laws, used to protect an author, creator or maker's work so no one is allowed to copy or reproduce that work (Stoney & Stoney 2000), are not enforced globally.

Digital photographs. They are easy to modify and, if a digital camera is out of your financial scope, photographs are easily copied from one website to another. Images of travel destinations play an important role in travel decision-making, dishonest Internet travel vendors use misleading information and pictures to entice consumers to purchase their products, but so do the old fashioned paper brochures, as Colaco (2000) on his website the Goa Travel Advisory states:

'Most beach resorts are quite good and reasonable, but some are great only in the brochures that travel agents display.'

It is easy to manipulate digital photographs as subtle changes can disproportionately change the meaning of an image (Hutchinson et.,al 2000(a)). A polluted beachside can change into a tropical paradise or an old hotel can be restored to its original splendor. The dishonest e.travel vendors' objective is to create an illusion to entice the consumer to purchase products. Today creating an illusion digitally is incredibly easy. Hutchinson et.,al. (2000 (b)) states that;

'The presentation of data either in picture or words can often be much more important to the consumer than the actual content. The use of colour, shade, scale, thickness of lines, and voice creates impressions and will add to any illusion.'

You could also add music to the list, this would give the vendor all the ingredients for developing a successful travel website.

Online users who book and research travel online generally locate travel websites through search engine links, online travel buyers are not loyal, two in three online travelers click from one travel site to another to find the information they want (Nua 2001). Meta-tags and the use of keywords are also being used to both mislead the consumer, and defraud organizations (Stoney et.,al. 2000). If a trusted, known metatag or keyword is used within a fraudulent website, the consumer searching could be deceived into thinking that the site found is the site requested. This was clarified by McKee (1999) when he stated, at a conference to American Travel Agents, that a website with carefully chosen keywords will draw thousands of consumers to it. Stoney and Stoney (2000) suggest that this type of Internet fraud leads to increased profitability and ultimately the saleability of products on this website.

According to Stoney and Hutchinson (2000) legalities relating to information use differ worldwide. When there is doubt and uncertainty, individuals, corporations and countries will inevitably seek to take advantage, to the detriment of others. Currently laws differ throughout the world, with a majority of countries having no Internet laws at all. Individual rights may be impossible to enforce when a fraudulent company or individual is halfway around the world (McKee 1999). Future effective enforcement mechanisms should not be confined to geographical boundaries (Hutchinson et.,al 2000(b)), although even with these precautions fraud is a crime which is difficult to stop, this is confirmed in a statement by Lasry (2000), a Melbourne barrister when he said:

'Of all the activities attracting the sanction of criminal law, the offences which are usually the most complex, difficult to investigate, difficult to prosecute, difficult to defend and difficult to generally understand, are offences which might be drawn under the general heading of fraud.'(p23)

CONCLUSION

Although the idea of the Internet taking consumers into an almost virtual world is a perception, the reality is that it can seduce the consumer into purchasing products that may not be real. It eludes the consumer into trusting the vendor without knowing if the vendor is honest or if the product actually exists. As technology advances, the use of real-time, interactive, video conferencing, may diminish the lack of trust gained, as the ability for consumers to gather information about the vendor would increase.

Due to the difficulty of investigating fraud, personal research into travel destinations should be of a high priority prior to any consumers purchasing travel products over the Internet. Payments should only be made via credit card over the Internet if the vendor can provide a secure site. Once the consumer reaches their travel destination and finds that the hotel, vehicle or guide do not exist, alternative arrangements may be hard to come by especially in some remote places, so care is the best policy.

In the immediate future there will be little legal control over the misuse of the Internet, there are currently no associations or international regulations controlling the industry globally online. Affirmative action and enforcement needs to take place internationally regarding Internet law, until this happens deception and fraud on the Internet relating to travel will continue.

The vulnerability of using Internet sites for booking of travel requirements must be clearly and completely understood by the consumer to enable them to deduct the truthfulness of the product they are purchasing. E.commerce can be a safe and convenient method for conducting travel arrangements, with care and common sense being the key to any online transaction.

One of the limitations of this preliminary study was the small number of travel websites examined. However even with so few, a pattern did emerge which verified the researchers supposition that there is a perception problem with travel consumers and that fraudulent behaviour relating directly to travel web pages can easily occur.

From this preliminary study it is clear that there are certain issues relating to perception and fraud. Further investigation, in the form of a quantitative study, will therefore be undertaken in this area and the results of which will be published.

REFERENCES

Cohen, F. (1998) *A Note on the Role of Deception in Information Protection.* Strategic Security Intelligence [On-line]
http://all.net/journal/ntb/deception.html

Colaço, J. (2000 Dec) *Travel Advisory – Goa* [On-line]
http://www.colaco.net/1/gta.htm.

Cooper, A. (2000 Dec) *Personal Comments on Langkawi.*

Frew, A., J. (2000 Nov) *Information and Communication technology research in the Travel and Tourism Domain: Perspective and Direction.* Journal of Travel Research. Vol 39. Iss.2. Pp 136-145.

Hussey, J., Hussey R. (1997) *Business Research: A Practical Guide for Undergraduate and Postgraduate Students.* MacMillan: London.

Hutchinson, W., Warren, M. (2000(a)) *Information Warfare: Illusion and Reality in the Information Age.* Australia.

Hutchinson, W., Warren, M. (2000(b)) *Concepts in Information Warfare.* Proceedings of the 1st We-b Conference Working for e-business: Challenges of the New Economy. 30th Nov–1st Dec. Perth Western Australia.

Infowar.com (1999 May 3) *Tactical Deception in Information Warfare – A New Paradigm for C4i* [On-line]
http://www.infowar.com/mil_c4i_030599a_j.shtml

Knight, W (2001 Jan) *Are bogus Web sites becoming latest dot-com trend?* [On-line]
www.zdnet.co.uk/news/2001/0/ns-19954.html

Lasry, L. (2000 January/March) *Fraud Have You Got It Right?* Investigator: Australia's Journal for the Investigation Industry. Issue 1. Pp 22-26.

MacKay, K., J., Fesenmaier, D., R. (2000 May) *An Exploration of Cross-Cultural Destination Image Assessment.* Journal of Travel Research. Vol.38. Iss.4. Pp 417-423.

McCormick, B. (2001 February) *Make Money, Not War: A Brief Critique of Sun Tzu's The Art of War.* Journal of Business Ethics. Vol.29. Iss.3. Pp285-286.

McKee, P.C. (1999) *Remarks to the Annual Conference of the American Society of Travel Agents.* National Consumers League. 8th October 1999. America.

Nua Internet Surveys (2001 April) *Online Travel Sites to Thrive in Slow Economy* [On-line]
http://www.nua.net/surveys/index.cgi

O'Neill, L (2000) *Survival of the Fastest: Natural Selection For Small and Medium Enterprises (SMEs) on the Internet.* Proceedings of the 1st We-b Conference Working for e-business: Challenges of the New Economy. 30th Nov–1st Dec. Perth Western Australia.

Ramsden, J. (2000) *Protecting Copyright.* Investigator: Australia's Journal for the Investigation Industry. January/March. Issue 1. Pp 36-39.

Sawyer, R.D. (1994) *Sun-tzu The Art of War.* Barnes and Noble: New York.

Spinney, l. (2000 Nov) *Blind to Change.* New Scientist. No.2265 Pp 27-32.

Stoney, M., Hutchinson, W. (2000) *Information Warfare and Developing Nations: Opportunities and Threats.* Proceedings from the BITWorld Conference 2000. Mexico.

Stoney, M., Stoney, S. (2000) *Meta Tags and Keywords: Their Use and Misuse in E.commerce. Proceedings of the 1st We-b Conference Working for e-business: Challenges of the New Economy.* 30th Nov–1st Dec. Perth Western Australia.

Tapachai, N., Waryszak, R. (2000 August) *An Examination of the Role of Beneficial Image in Tourist Destination Selection.* Journal of Travel Research. Vol. 39. Iss.1. pp37-44.

Tierney, P. (2000 Nov) *Internet-based Evaluation of Tourism Website Effectiveness: Methodological issues and Survey Results.* Journal of Travel Research. Vol. 39. Iss.2. Pp212-219.

Weber, K., Roehl, W., S. (1999 Feb) *Profiling People Searching for the Purchasing Travel Products on the World Wide Web.* Journal of Travel Research. Vol 37. Iss.3. Pp291-298.

Valli, C. (2000) *Achilles is Alive and Well – Trust and Virtual Organisations.* Proceedings of the 1st We-b Conference Working for e-business: Challenges of the New Economy. 30th Nov–1st Dec. Perth Western Australia.

The Need for In-depth Cyber Defence Programmes In Business Information Warfare Environments

Stephen Edwards[1] and Mark C. Willimas[2]

[1] *University of Western Australia*

[2]*School of Management Information Systems*
Edith Cowan University
Email: m.williams@ecu.edu.au

ABSTRACT

Many organisations have overlooked their security strategies by entering the increasingly inter-connected world of electronic environments. These organisations often still rely on the traditional strategies of security. With increasing information warfare risks, organisations need to reconsider their security strategy within a multi-layered framework that integrates all points of interconnectedness and reflects the rapid changes in technology. In this paper we take the stand that organisation's e-security strategy should be a continuous, comprehensive process of adding, removing, and managing layers of actions based upon balanced risk management. A merit of in-depth defence strategies is that they begin from inside the organisation and extend outward creating defensive webs to withstand information attack.

INTRODUCTION

The objective of this paper is to argue a need for a comprehensive in-depth cyber defence strategies for organisations. Firstly, the paper describes the business risks rapidly evolving in the electronic marketplace widely known as the new battlefield. Secondly, the paper discusses how some cyber attacks take place. Thirdly, the paper discusses a strategy organisations employ to protect themselves from attack and ways to respond to these attacks to avert further damage. Finally, this paper explores the ways information warfare can prompt organisations to evolve in-depth cyber defence strategies to meet new information security challenges and defend against new enemies on the e-battlefields of the future.

RESEARCH AREA

At the turn of the millennium, one would be hard-pressed to find a competitive organisation that does not rely upon communications and information technologies (CIT) as an enabler of its activities. CIT are integral part of any business today. However, these enabled digital technological systems can create enormous new risks, many of which organisations have overlooked or considered superficially (Gates 1998).

The complexity of modern organisations and their reliance on CIT and the heightened interconnectivity among organisations are rapidly increasing. These CIT systems can create diverse opportunities for theft, fraud, and other forms of exploitation by offenders both outside and inside in an organisation (Beer 1999). With the growth of e-business, internal and external perpetrators can exploit traditional vulnerabilities in seconds and they can take advantage of new weaknesses in the software and hardware architectures that now form the backbone of most organisations. For example, in a networked environment, such crimes can be committed from any location in the world (Armstrong 2000a).

As organisations grow, their systems are becoming increasingly sophisticated and less dependent on human intervention. Subsequently monitoring individual behaviour becomes more difficult and vulnerability to electronic intrusion grows as organisations are increasingly connected to, and rely on, individuals and systems they do not directly control. Most organisations are generally alert to the risks posed by electronic viruses such as the May 2000, "I Love You virus" which is estimated to have cost organisations and governments in excess of $US 10 billion dollars (Talleur et al., 2000, p. 2). However, many organisations still remain unaware of the extent to which they can be harmed by cyber intrusion (Arquilla & Ronfeldt 2000).

RESEARCH QUESTION AND RELEVANCE

The research question considered in this paper is "what strategic issues compel organisations to develop plans to counter information warfare threats, and what information security programs should be used."

This paper is considered to be timely, relevant, and interesting to both industry and academic audiences because of the obvious dangers posed by information warfare.

The research methodology employed is the presentation of a sustained point of view, written from an interpretivist perspective. The author's use a third personal impersonal writing style because it is considered to best match the subject matter of the paper.

STRATEGIC BUSINESS CONCERNS IN INFORMATION WARFARE ENVIRONMENTS

Popular misconceptions often attribute cyber attacks to mischievous teenagers or social misfits. Experience indicates that these individuals represent a small number of the diverse group who perpetrate such intrusions. These attackers sometimes commission intrusions for their own objectives or make their skills and services available for hire (Armstrong, 2000b).

The purpose of strategic information warfare is to induce your opponent to make decisions which benefit your organisation's goals (Libicki, 1998) and to gain your organisation a competitive advantage. information warfare is becoming 'an obvious way to win a war' (Berkowitz, 2000:9) by striking your opponents' information networks, whether they be military or business opponents. As competitive advantages can impact an organization's success or failure, it is important to understand factors which can affect the organisation, and the framework created by the new technologies and paradigms (Cramer, 1997) which are capable of winning or taking away competitive advantages.

The object of information warfare in this secondary sense is to penetrate competitors' processing systems and influence key decision making processes in ways that are beneficial for the attacking organisation (Saarelainen, 1996). Many commentators consider that information warfare is an integral part of a business strategy for defending and advancing an organisation's goals and market domination. Furthermore, as in war, surprise can be a powerful strategic weapon – and the use of information warfare can provide a competitive edge in achieving the pre-empting surprise in the commercial marketplace (Cronin et al 1999).

As organisations develop their e-business strategies, they need to consider the issues that influence the confidentiality, integrity, and availability of their data. In this context, they need to know how they can be affected by the new risks of electronic intrusion, how inadequate preparation leaves them open to an attack, and how they can protect their weaknesses and exploit their strengths in this cycle of attack and defence in the new world of information warfare.

Organisations are increasingly incorporating technologies into their infrastructures without understanding how they can be exploited and used. Cyber intruders can divert financial assets, shut down communications, steal intellectual property, damage an organisation's reputation, or bring e-commerce to a halt. Computers can be used as weapons, as storage devices to harbour evidence of crimes and they can even be the objects or victims of the war (Gasser 1988).

As organisations increasingly integrate their systems with those of their vendors, suppliers, customers, and others, the risks they face multiply exponentially. The shift toward self-service systems within and among organisations also makes their host organisations increasingly vulnerable (Nevis 1995).

Another strategic business concern is that there is a lack of cyber security awareness among many organisations. Many do not realise that the same technological advancements that have enabled business growth and innovation are equally available to facilitate cyber intrusion. Indeed, many organisations have not yet understood that protecting assets in the virtual world is a more complex and exacting endeavour than protecting them in the physical world (Talleur, 2000).

External attackers include sophisticated crackers who develop and use technology based tools that facilitate illegal entry into an organisation's network. Once they have achieved their objectives, they distribute their tools anonymously, via the Internet, to mask their association with either the tools or the exploitation of the organisation. Cookbook crackers who lack the knowledge, skills, and abilities to create and use sophisticated intrusion tools but who seek out such tools to launch attacks (Talleur, 2000).

Internal attackers often include dissatisfied current employees working alone or with other insiders or with disgruntled ex-employees It is believed that organisations face a greater risk from their own employees than they do from external threats (Armstrong, 2000b). Employees who exceed their authorised access to the organisation's systems and facilities perpetrate internal attacks. For example:

1. Internet Trading Technologies Corporation in New York suffered three days of disruption to its business when a disgruntled employee transmitted data to intentionally cause damage to the network (Johnson, 2000).

2. Three Internet-only radio stations went off the air after they were actually deleted from the computer server they were hosted on by a disgruntled former employee (Creed , 2000).

If information warfare is extrapolated to the business arena and assimilated into an organisation's business plan, information warfare can then be defined as a metaphor (Libicki, 1995) for achieving and maintaining an information advantage over competitors or adversaries. This type of information warfare is emerging as the threat of physical military confrontation decreases and as business competition increases (Kruczek, 1998). Furthermore, as there has been a proliferation of commercial off the shelf technology on a global scale, more and more individuals and organisations have (McHale, 1999). Accordingly, nations losing their monopoly on the ability to wage warfare – criminals, disgruntled employees, commercial competitors and terrorists are now potential threats (Barker, 2000).

Today many organisations outsource desktop, Internet and network support services. Most are also developing e-business alliances with customers, suppliers, and employees. Improperly managed and controlled, however, these new alliances can be as problematic as they are beneficial because by their very nature they entrust partial and sometimes complete control of an organisation's information assets to an external party (Nathan, 1998).

Cyber intruders conduct reconnaissance of their targets first. They will often use publicly available information about the technical vulnerability of network systems coupled with inside information to develop their attack methods (Byrne, 1993). Both external and internal intruders look for weaknesses in their targeted systems to gain access to them. However, not all attacks begin in cyberspace. Indeed, the physical security of systems and facilities is a vital component of a cyber defence program.

Organisations need to ensure that their physical security systems appropriately control and monitor their facilities to prevent unauthorised installation of system software that facilitates intrusion.

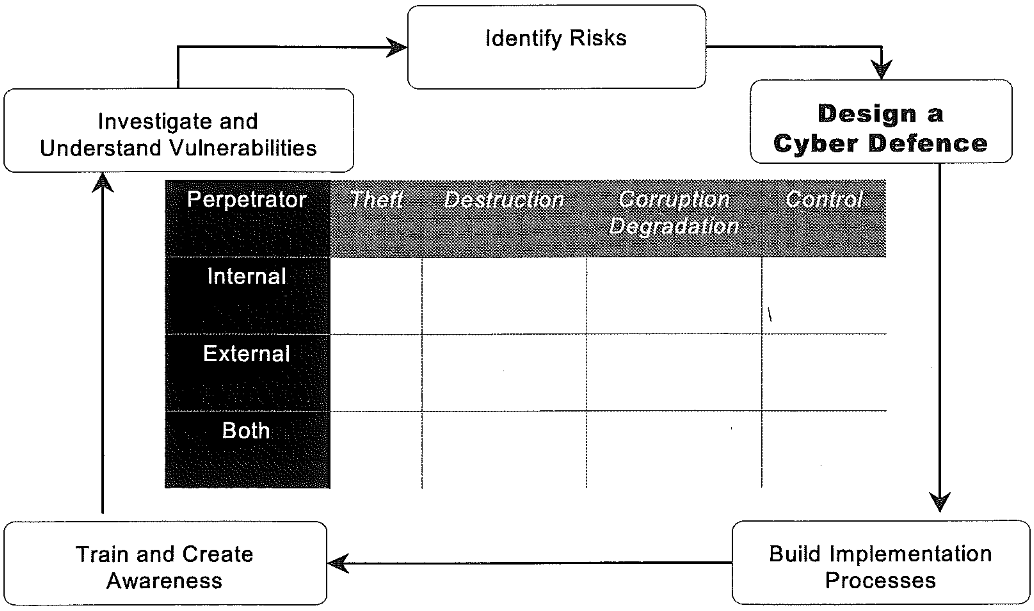
If information warfare is extrapolated to the business arena and assimilated into an organisation's business plan, information warfare can then be defined as a metaphor (Libicki, 1995) for achieving and maintaining an information advantage over competitors or adversaries. This type of information warfare is emerging as the threat of physical military confrontation decreases and as business competition increases (Kruczek, 1998). Furthermore, as there has been a proliferation of commercial off the shelf technology on a global scale, more and more individuals and organisations have (McHale, 1999). Accordingly, nations losing their monopoly on the ability to wage warfare – criminals, disgruntled employees, commercial competitors and terrorists are now potential threats (Barker, 2000).

While these general definitions of information warfare are a starting point, it is important to consider the various elements which constitute information warfare in order to be able to integrate them into cyber defence programmes.

IN-DEPTH CYBER DEFENCE PROGRAMS

The consequences of the above factors underscore the need for organisations to develop cyber defence programmes that weave preventive measures into the fabric of e-business operations. Along with a strong emphasis on prevention, a cyber defence program must also focus on detection (Nevis 1995). In an information warfare environment, organisations are constantly repelling numerous attacks each day. Such assaults are part of doing business in today's interconnected world and often how prepared an organisation is to respond to these attacks will ultimately determine its success or failure.

Organisation e-security is a continuous, comprehensive process of adding, removing, and managing layers of actions based upon holistic risk management strategies. During times of war, this concept is referred to as defence in depth. A strategy based on this concept of protection begins from the inside and extends outwards to create defensive webs (Arquilla & Ronfeldt 1995).


Identify Risks
Design a Cyber Defence
Build Implementation Processes
Train and Create Awareness
Investigate and Understand Vulnerabilities

Perpetrator	Theft	Destruction	Corruption Degradation	Control
Internal				
External				
Both				

Figure 1: Defence in-depth Cyber Defence Strategy
(Talleur, 2000)

Today's organisations are providing greater access to their computer networks and subsequently they must integrate their cyber defence to encompass all points of interconnectedness, from the inside out. If they fail to do so, they leave themselves vulnerable to attacks. Many organisations, however, have not adapted their security strategies to the inter-connectedness of the electronic world; consequently, they tend to think about security and risk management solutions in a disjointed fashion (Armstrong 2000b). They rely on the aging and limited one-size-fits-all strategies. In the face of escalating information warfare risks, organisations need to avoid one-dimensional, uninformed behaviour and instead, develop a holistic strategy for a cyber defence (see Figure 1).

Talleur (2000) asserts that leading organisations in implementing cyber defence programs:

- Establish clear, focused, integrated security policies.
- Provide employees with appropriate awareness and technical training.
- Employ trained personnel and support them in maintaining an integrated response to attacks.
- instil awareness of electronic threats and risks throughout the organisation.
- Pursue the perpetrators of e-crimes against the organisation to the fullest extent of the law

A holistic cyber defence system offers innumerable benefits both in helping to deter attacks and in reducing the effects of an intrusion. Preparedness can become a strategic advantage in a business environment increasingly dependent on the security and reliability of computer networks (Nathan, 1998). A holistic cyber defence system should include both offensive and defensive strategies.

An enterprise-wide cyber defence includes integrated strategies, established in the form of philosophies, policies, procedures, and practices that are implemented through defined action plans. It also needs to encompass technical, legal and business strategies that consider all key stakeholders. In creating a cyber defence, organisations need to consider what they have to lose, especially new-economy business assets that can be removed with ease from their virtual setting (Arquilla & Ronfeldt, 1995). Once organisations know what they need to protect, they need to develop a strategy for implementing their cyber defence program, integrating it into daily operations while striking a balance between the demands of accountability and privacy (Armstrong, 2000a). Such a defence plan would encompass enterprise wide planning, enterprise policy development and implementation, and training programs on threat awareness.

When a cyber attack occurs, failure to respond often exposes the organisation to further operational risks. Yet, experience has shown that many organisations have little or no understanding in responding to cyber attacks (Talleur, 2000). They often underestimate the scope of the intrusion and then fail to take actions that would deter further loss of assets. Organisations can lose assets in nanoseconds on the e-battlefields of virtual commerce. When an organisation believes it is under cyber attack it must react instantly following established incident response plans to minimise further losses, assess damage, affix responsibility, and then implement the appropriate and planned counter measures (Nathan, 1998).

Today's organisations have accepted the need to recognise the value of skilled personnel in information technology (IT). However, most IT professionals are trained to establish and maintain specific technology services. Typically, they are not trained to address attacks on those technologies. But a few IT security professionals have the experience to effectively construct defensive measures to mitigate threats and some of them are capable of establishing potent counter measures (Arquilla &Ronfeldt 1995). Organisations need recruit these specialist IT personnel and use their extensive experience and knowledge of computer networks, applications and operating systems to develop counter measures that protect the organisations assets while exploiting the full capability of the organisation's cyber defence program (Anderson 1999).

DISCUSSION AND CONCLUSION

With the passing of the immediate threat posed by Y2K, many organisations have begun to focus on cyber network defences. Organisations are beginning to understand that as technology changes so to do the risks. New technologies will pose new risks and demand new responses to those risks (Armstrong, 2000b; Talleur 2000).

In the future, for example, new technologies such as holograph memory, nanotechnology, wireless communication protocols, and biomechanical technologies will be introduced and embedded into new core products that organisations will use to facilitate productivity in their organisational infrastructures (Talleur, 2000). Detecting exploitation of these technologies will need to become embedded in the core mission of many organisations, particularly those with extensive virtual assets. Issues related to the protection and storing of intellectual property developed in a network environment will also create concerns, and cyber protection methodologies will be paramount in this context.

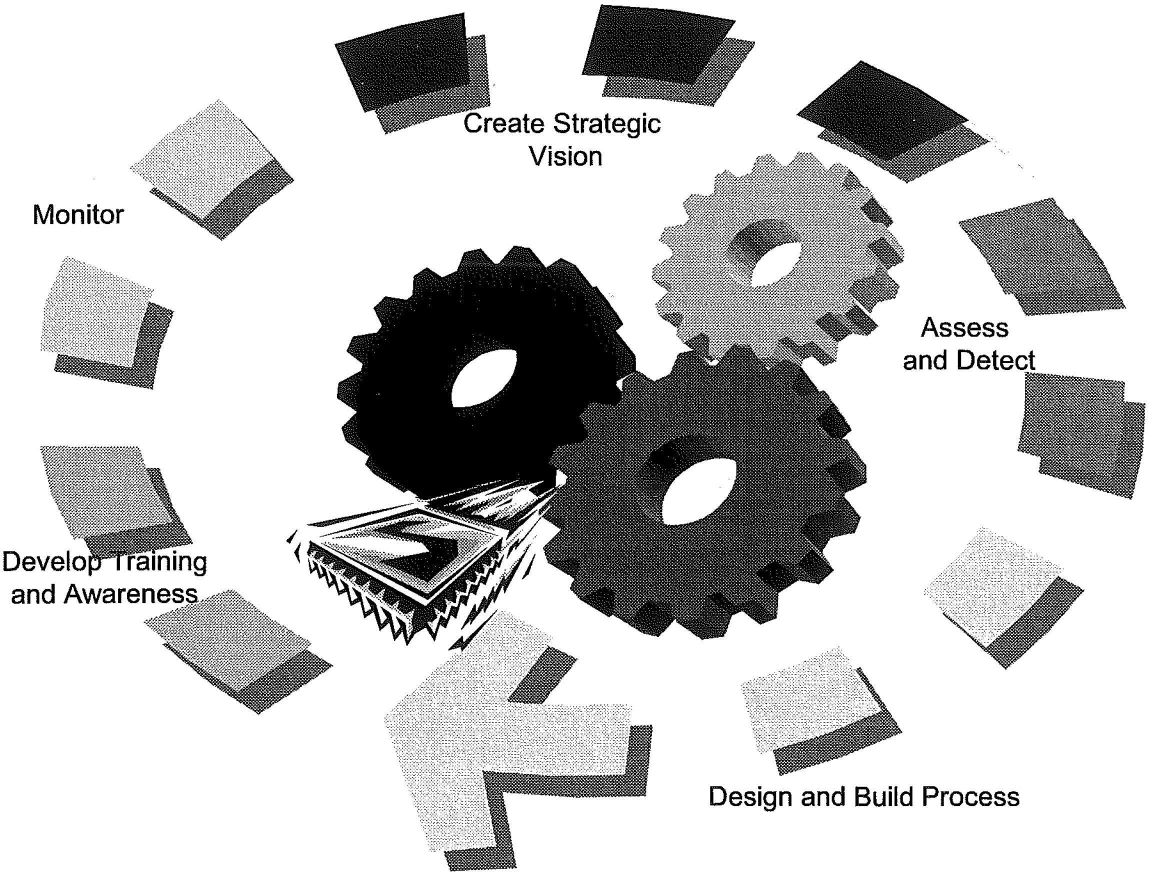


Figure 2. Organisational Preparedness is a Continuous Process

As the technology continues to evolve, organisations must actively understand the related risks this evolution brings. They must understand how they will be affected by these risks and ensure that their cyber defence processes and controls are continually improved to meet evolving needs (Anderson, 1999).

The explosive growth of Internet-based open networks has paved the way for instantaneous and devastating trans-national electronic incursions that often deny victims the ability to operate their organisations or control their assets. These exploitations will multiply as technology change and as attackers' methods inevitably become more sophisticated. Indeed collectively these cyber attacks represent the information warfare that has become an indelible fact of an organisations operating environment.

Subsequently organisations need to develop a comprehensive program of cyber defence initiatives, as schematically outlined in figure 2, that take specific measures to defend their assets against electronic incursions.

Organisations, to secure themselves, should also establish a plan of how they will respond should an intrusion take place. Properly implemented, an integrated in-depth cyber defence program will mitigate the risks of attack while becoming a strategic advantage in a world increasingly dependent on the security and reliability of computer and communication networks.

REFERENCES

Anderson, K. (1999). *Intelligence Based Threat Assessments for Information Networks and Infrastructures. Global Technology Research Inc.,* January.

Arquilla, J. & Ronfeldt, D. (1995). *Cyberwar and Netwar: New Modes,* Old Concepts, of Conflict. *Rand Research Review,* 19(2), Fall.

Armstrong, I. (2000a). *Computer Forensics: Investigators Focus on Foiling Cybercriminals.* SC Magazine, April.

Armstrong, I. (2000b). *Computer Crime Spreads*, SC Magazine, April.

Beer, S. (1999). *What price security?* The Australian Financial Review, January 32-36.

Byrne, J. A. (1993). *The digital corporation*, Business Week, December, 778, 76-81.

Creed, A. (2000). *Former employee steals radio stations.* Daily News Computer User.com. 18 April 2000 [On-line]
www.currents.net/newstoday/00/04/18/news2.html

Gates, W. (1998). *Speech by William (Bill) Gates, at Press Conference during Australia-Asia Tour.* March 16-20 1998[On-line]
www.microsoft.com/BillGates/news/icontrip.htm.

Gasser, M. A. (1988). *Building a secure computer system.* New York: Van Nostrand Reinhold.

Holder, E. H. (2000). *Speech by U.S. Deputy Attorney General Eric H. Holder*, Jr., at the High-Tech Crime Summit. 12 Jan. 2000 [On-line]
www.usdoj.gov/criminal/cybercrime/dag0112.htm

Johnson, D. (2000). *The hackers are coming; the hackers are coming*, Security Portal. 10 April 2000. [On-line]
www.securityportal.com/cover/coverstory20000410.html

McWilliams, B. (2000). *Shopping Cart Program Leaves Back Door Open*, Internet News.com. 13 April 2000 [On-line]
http://www.internetnews.com/ec-news/article/0,2171,4_340591,00.html

Nathan, R. (1998). *The secure organisation, Research Technology Management*, July-August. 46, 4-8. [On-line]
http://www.infosecuritymag.com/2000survey.pdf

Nevis, E. C. (1995).*Understanding organisation security.* Sloan Management Review, Winter, 73-85.

Peters, T. (1997). *Thriving on chaos*. New York: Knopf.

Reno, J. (2000a). *Speech by U.S. Attorney General Janet Reno to the National Association of Attorneys General*. 10 Jan 2000 [On-line] www.usdoj.gov/ag/speeches/2000/011000naagfinalspeech.htm.

Reno, J. (2000b). *Speech by U.S. Attorney General Janet Reno to the Virginia Journal of International Law, University of Virginia Law School*, Charlottesville, Virginia. 1 April 2000 [On-line] www.usdoj.gov/ag/speeches/2000/4100aguva.htm

Talleur, T. (2000). *E-Commerce and Cyber Crime,* KPMG Forensic and Litigation Services [On-line] http://www.kpmg.com/.

Tzu, S. (translated Griffiths, S. G.) (1963). *The art of war*. London: Oxford University Press.

Using the Techniques of Internet Advertising for a Perception Offensive in Information Warfare

Dragan Velichkovich

Edith Cowan University, Western Australia.
Email: d.velichkovich@ecu.edu.au

ABSTRACT

The topic of Information Warfare is currently focussed on networks and information systems as applied within the realm of military conflict. When mounting a Perception Management offensive the military are still reliant on a broadcasting model. The military, currently, do not take into account the effectiveness of Internet technologies, and the Internet.

There are parallels to be drawn between implementing a Perception Management offensive during military conflict and the development of a traditional advertising campaign for a product or service. In both instances, the focus is on the development of the message content by the Perception Moulder and the delivery of messages in a "one-to-many" or broadcasting format.

However, the techniques used in Internet advertising implement a process defined as narrowcasting to deliver the message. Internet advertising has the ability for the advertising message to be customized and pinpointed (narrowcast) to an individual, thus operating via a "one-to one" method.

Using the Internet as a medium, and in particular, the techniques used in Internet advertising, can, in turn, deliver an efficient Perception Offensive within the Information Warfare paradigm. This was proven by the Serbian Military's perception management offensive deployed during the Bosnian and Kosovo conflicts.

Key Words: Information Warfare, broadcast, narrowcast, perception moulder, perception management and interactivity.

INTRODUCTION

Information Warfare (IW) is used predominantly in military circles. In fact, IW has become a major issue within the United States military, and in particular, within the Pentagon. There are now IW offices within the United States' Army, Navy and Air Force divisions (Washington, 1995).

The term IW can be interpreted in a number of differing contexts. In fact, IW is rather a generalised term that could be viewed as either meaning hacker war, electronic war, cyberwar, soft war, cyberwarfire or low intensity warfare (DiCenso, 2000).

IW takes a different view of warfare and has revolutionized the battlefield by using as the weapon, information, executed by information technology. Currently, the concentration point of IW is on networks and information systems.

The literature analyzed for this paper are predominantly United States Military and Academic journal articles. They indicate that the focus of IW is on the offensive, defensive and exploitive strategies that can be implemented on networks and information systems. However, this is a concern due to the fact that there is very limited research conducted on the role of the Internet in IW. In particular, the use of the Internet for attack.

The paper will concentrate on the offensive category. Boni and Kovacich (2000, p.223) define the offensive category as one that can "deny, corrupt, destroy, or exploit an adversary's information, or influence the adversary's perception."

In particular, this paper is focussed on the efficient implementation of perception management, within the realm of IW. Perception management, as a tool, cannot only be implemented within the realm of IW; it is also implemented in traditional military combat as well as being integral to the operations of the advertising industry.

A perception management offensive is dependent upon delivering an appropriate message via a medium. The media used currently in IW, is the same that has been used in traditional military conflict for over 30 years. The media is radio, television and print. This is the same that is also used by the Traditional Advertising Agencies (TAAs). The medium that is not efficiently used, by these two groups, is the Internet.

Perception Management can basically be described as the function to manage people's perception (Driscoll, 2000). Perception Management is not only a term employed within military circles, it has now taken over the function that used to be called Public Relations within commercial, business and advertising circles. So much so, advertising companies now employ Perception Managers to carry out the duties of branding and public relations for their customers (Synder, 2001).

The roles of Perception Management in business, the advertising industry, as well as traditional warfare and IW have similar motives. However, it is within the realms of the advertising industry where Perception Management is perceived to be favorably and appropriately implemented. According to Dearth (2000, p.154); " Perception Management is an advertisement agency sort of thing."

The United States Department of the Army has identified six "steps" to effectively carry out an effective perception management campaign. These are also the procedures used by the TAAs. The steps are (1) identify the target, (2) obtain information about the target audience, (3) develop friendly messages, (4) identify pressure points, (5) measure effectiveness, (6) evaluate the programme (Craig, 1999).

In current times, one of the major concerns of the TAAs has been the growth of the specialist, Internet Advertising Organisations (IAOs). This growth has been due to TAAs not being able to understand the functions of the Internet. The TAAs approach the use of the Internet in the same way that they approach traditional media. That is, implementing broadcasting techniques. On the other hand, the IAOs understand the workings of the Internet and its unique technologies, thus implementing narrowcasting techniques, which have delivered appropriate returns for their customers and has led to their phenomenal growth (Hyland, 2000).

This paper will identify that Perception Management, as a methodology in IW, is not fully utilized or effectively instigated. This is due to the fact that major "players", the military, in this paradigm are still using traditional methods and not using, or not understanding, the effectiveness of the Internet as a medium or the underlying Internet technologies. This is the same problem that the TAAs are having. This is also the reason why the instigation of the six-point plan is extremely hard to implement when using a broadcasting method, and easily implemented when deploying narrowcasting.

In turn, this paper will set out to prove why the techniques employed by the IAOs can be extrapolated to the IW paradigm so as to launch an effective perception campaign as an offensive attack. As proof, the Bosnia and Kosovo tactics will be presented highlighting that the Serbian's implementation of narrowcasting via the Internet was much more effective than NATO's broadcasting perception offensive.

PERCEPTION, PROPAGANDA AND PERCEPTION MANAGEMENT

The use of perception within traditional Military circles, as well as within the newer domain of IW, comes under the heading of "Pysops" or Psychological Operations". Wall and Fulghum state (2001, p.64), "...perception or Pysops is focused on identifying and exploiting any messages that will resonate in a targeted society to help shape the view of people."

Perception Management is characterised by a message or what is being communicated (the content); through a means of communications (the media), leading to interpretation by the receiver. This is best illustrated in Figure 1.

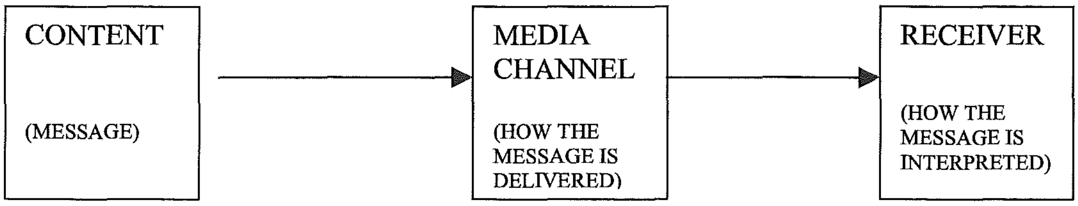

CONTENT
(MESSAGE)
MEDIA CHANNEL
(HOW THE MESSAGE IS DELIVERED)
RECEIVER
(HOW THE MESSAGE IS INTERPRETED)

Figure 1: The communication process

Driscoll (2000) asserts that what a piece of information might mean to a receiver (the perception that is conveyed), is dependent upon not only on the content, but also upon the vehicle and the context that the message is delivered. Driscoll (2000, p.170) has stated that perception is based on; " What is said, by whom, when and to whom."

James (1999, p.1) from the United States Army Command and General Staff College defines Perception Management as; "... all the actions that convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives."

Perception Management is about shaping information to achieve the environment that is intended. It has nothing to do with firepower or mass. Its elements are psychology, artistry, and imagination; this is the notion of propaganda. Winter (2001, p.181) defines propaganda as; "The deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist."

Some argue that all persuasive communications is propaganda, while others argue that only dishonest messages are propaganda. All definitions have one central theme, and that is basically the dissemination of information for the purposes of persuasion and advocating an agenda.

Propaganda is thus an integral tool to be used in Perception Management. Delwiche (1995) asserts that the general populace associates propaganda with advertising.

Prior to the advent of the Internet, delivering messages that are broadcast "on mass" could carry out Perception Management. In fact, the broadcasting approach is still implemented and is dominant within IW, traditional military conflict, and the traditional advertising industry.

According to Kennedy (2001, p.22), "Perception Management uses a wide array of communications media-including radio and TV broadcasts, loudspeakers, leaflets, newspapers and magazines."

When delivering messages via traditional media (television, radio, and print) there is employed a "one to many" approach. The message is not interactive, it is not personalized, nor can it be customized, nor targeted to an individual. In addition, it is difficult to ascertain whether the message has had the appropriate affect.

On the other hand, when using the Internet for message delivery, the message can be targeted to an individual, customized, personalized and judged whether the message has had the appropriate affect via the level of interactivity. Holbert (2001, p.182), states that:

"Perception management as an interactive process raises the notion that the nature of the new media technologies may offer a new form of communication that is particularly suited relative to existing print or broadcast media."

THE MEDIA

Due to Internet technologies, the message diffusion method moves from the traditional broadcasting to narrowcasting. In other words, moving from a "one-to-many" scenario to a "one-to-one". Or moving from a mass communication approach to one that can be personalised and customised to the individual.

Figure 2 exemplifies the message diffusion process under the traditional method of broadcasting. Here the same message is broadcast, on mass, to a mass market. This particular process is used when diffusing messages via the traditional channels of television, radio, and print.

Figure 2: Broadcasting Method (Source: Hoffman & Novak, 1995)

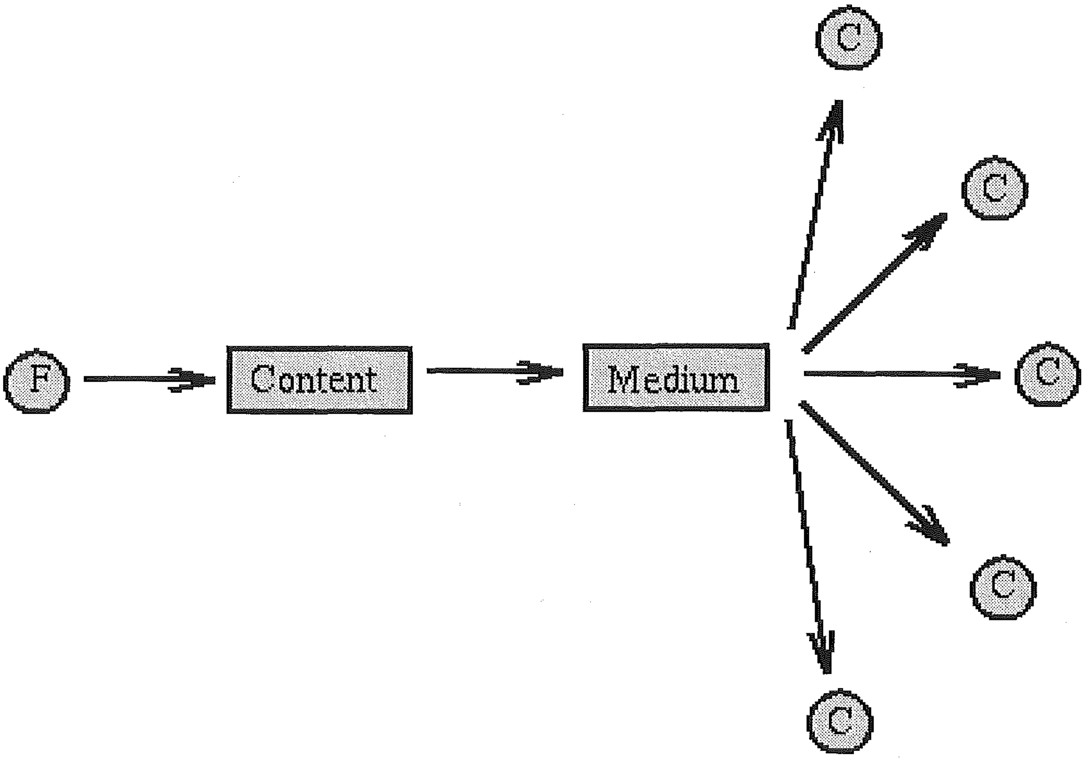


Figure 2 highlights the message (F) being sent to individuals(C), which make –up the mass market. The message is unidirectional thus not being interactive. There is no measure to guarantee whether each individual will receive the message, or more importantly, if the message has had the desired affect.

However, when using the Internet, narrowcasting can be deployed. Messages cannot only be directed to an individual, but can also be personalised and customised to the needs and tastes of that individual.

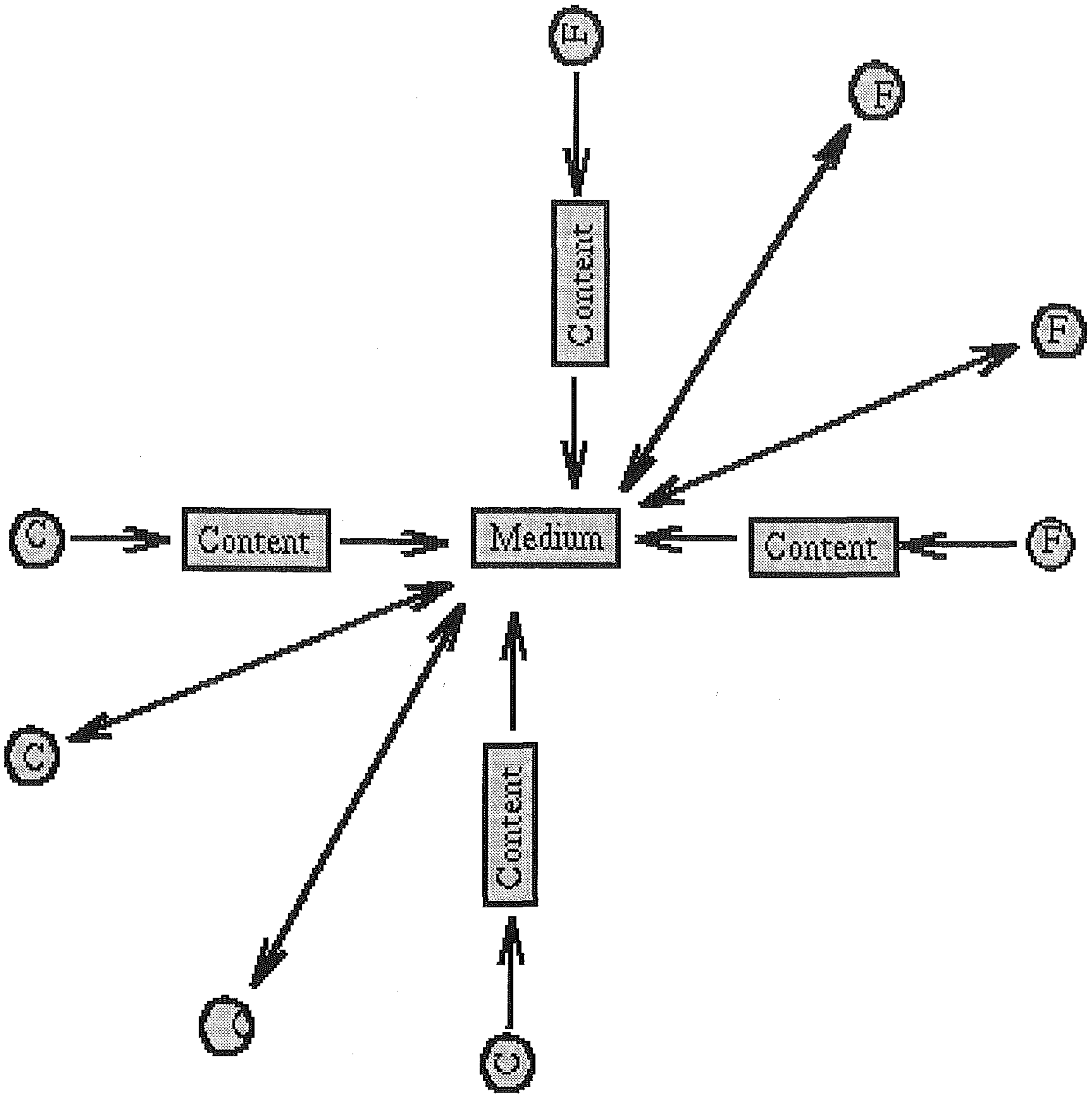


Figure 3: Narrowcasting Method (Source: Hoffman & Novak,1995)

Narrowcasting, as shown in Figure 3, highlights the changed dynamic between the message (F) and the individual (C). The major points being that the individual can respond to the message; the message can be personalized, and targeted to an individual.

The Internet is an ideal medium to commission for an IW offensive strategy which is focussed on perception, that can deliver customised propaganda based messages to a target audience.

THE MEDIA USED IN IW

It seems that the United States military could be viewed as being somewhat preoccupied with traditional broadcasting methods, and not really aware of the power of narrowcasting via the Internet, to achieve adequate effectiveness for a perception offensive.

The United States Department of Defense via the U.S. Special Operations Command (SOCOM) and its Pysops Division predominantly focuses the Perception Management strategy via using the traditional communication media of TV broadcasts, radio, loudspeakers, newspapers, magazines, and leaflets. In fact, the U.S. military have been using the broadcasting method ever since the U.S. Revolutionary War. George Washington distributed leaflets to British soldiers in the hope that they would desert. In World War II the Allies, Germany and Japan used radio broadcasts and loudspeakers to broadcast their message.

In more current times, Pysops' main means of implementing a perception offensive is by disseminating radio and television broadcasts, via aircraft, that are able to broadcast in standard and military frequency bands. The U.S military have operated their perception management campaign, in this fashion, in every military engagement, for the last two decades. Kennedy (2001, p.22) states, " Broadcasts can be used to inform and influence both military and civilian audiences. In Grenada, they warned civilians about the impending invasion. In the Persian Gulf, they encouraged Iraqi soldiers to surrender."

However, with the broadcasting there can only be a limited method of targeting or pinpointing of an audience. For example, during the "Pysops' campaign against Haiti's military, the U.S. targeted certain urban areas and distributed their message to the residents. This is still an example of broadcasting, because it is still a distribution of a message in the one-to-many format. The message was not personalised, nor customised, it was predominantly targeted to a demographic.

Within the military's six-step plan it is extremely difficult to gauge or gather the information to ascertain whether the campaign was successful, purely due to the fact that a broadcasting method has been instigated. Under traditional Perception Management campaigns there is no interactivity. In other words, it is difficult to ascertain who is watching, listening, or even reading the message. More importantly, whether the intended participants have responded to the call for action.

It is through the Internet and in particular the use of Internet technologies, that will propel Perception Management, and in particular its usage, into a new phase of effective IW outcomes. It is through this technology and network that will deliver the military's six-step plan on Perception Management. The proof can be found in the techniques used in the Internet advertising industry.

It is the Internet advertising industry that has grasped the effectiveness of narrowcasting. The United States Internet advertising industry has grown from US $268 Million in1994 to US$8 Billion for the year 2000 (PWC, 2000).

THE INTERNET AND INTERNET ADVERTISING

The birth of Internet Advertising and the instruments that are used to deliver messages, on the Internet, happened in 1994 (Hyland, 2000). The benefits that can be derived from Internet advertising are based on being able to access a sophisticated audience, precisely target customers, offer interactivity with the audience, and offer advertisers a quick-response capability to terminate ineffective advertising (Krishnamurthy, 2000).

Implementing an Internet advertising or Online Perception Management strategy enables the advertiser, or generally speaking the Perception Moulder, to customise an effective one-to-one strategy via the leveraging of technology. Creating individualised response messages, based on a participant's direct and immediate feedback, brings about this one-to-one strategy.

In its simplest form, the Internet Perception Moulder sets out to communicate a message that can be instantaneously responded to by the audience or the person that is targeted. Once there is a response, the Perception Molder archives the action and the recipient can be further categorised via a process called "profiling", which can lead to customisation of future messages.

However, with current IW techniques and traditional advertising, the audience is, in a general sense, passive, and may wish to participate at a later date. In fact, if the audience is passive, then this could mean that the medium employed is passive. Swett (1995, p.8) quoting Snider states, "The importance of today's passive media is likely to diminish greatly over coming decades. Passive media will be replaced by a new type of interactive media."

Both Gillette and Douwe Egberts (multinational consumer goods corporations) implemented Internet advertising campaigns (in the United Kingdom), focussing on customer interaction via a one to one narrowcast process. These are traditional "bricks and mortar" businesses, and large users of traditional advertising methods.

They made the decision to use Internet advertising to launch new products or "re-badge" existing product lines. The campaigns were launched purely online, and took the form of banner ad placements and online competitions, both with editorial tie-ups. The aim was to drive customers to purchase the products, as well as creating a database of current, new and potential customers. It not only led to identifying the customers, but also to keep them informed of products. The campaigns were aimed at obtaining the customers' details and to tailor future campaigns on an individual basis (Reed, 1999).

The essence or crux of the Internet advertising campaigns was the development of customer databases, that is, the obtaining of information on current, prospective and new customers. With Internet advertising once a person "clicks"- customer information can be obtained by the advertiser, and most importantly, further advertisements can then become personalised and customised.

Both campaigns where highly successful, and provided Gillette and Douwe Egberts with personalized, targeted information on their customer base, information that they never had before.The actions of Gillette and Douwe Egberts can be extrapolated to the IW realm quite easily, and most importantly, quite quickly. A case in point was the IW efforts of Serbia during the Kosovo and Bosnian conflicts. Satchell (2000, p1) has termed it, "... a cyberspace clickskrieg by the Serbians and a World War II-style leaflet drop by NATO planes. The greatest irony is that the Serbs have seized the Internet initiative from the wired up Americans."

The Serbian military carried out their Perception campaign by disseminating their messages no differently to Gillette and Douwe Egbert's Internet advertising campaign. They created banner advertisements to be placed on selective sites, created databases from the participants who accessed the banners, then personalised additional messages, via email, to be forwarded to the audience. The Serbian military could identify who their target audience was and what was needed to get a response from that audience, not only within Serbia, but also to audiences outside their country.

In complete contrast to the Serbians, the NATO forces relied on broadcasts from Voice of America, Radio Free Europe and the "dropping" of 19 million leaflets from aircraft. These traditional methods had problems such as weak frequencies and changing weather patterns that hindered the message delivery process. More importantly, under these methods, it was extremely difficult to ascertain whether the message was delivered to the right audience or even gauge the audiences' response (Satchell, 2000).

A post-conflict analysis by the Pentagon showed that the use of television and radio broadcast was largely ineffectual. According to Wall and Fulgham (2001, p.64); "...the art of massaging the views of locals was not as successful as it might have been".

The above is re-iterated by Levien (1999) who describes that broadcasts where hindered by the terrain (mountains). As well as the wind and weather conditions which affected the airdrop of leaflets.

The point that has to be made is that the messages that are delivered via the Internet, within an IW paradigm, can deliver the six-step IW objective. As in the campaign by the Serbians they:

Identified the targets via the specific websites where they placed their banners.
Obtained information about the audience that participated, more importantly on an individual basis.
Developed appropriate message themes that where applied individually.
Identified pressure points that resonated with the audience, individually.
Measured the level of effectiveness via interaction levels.
Could evaluate the program via the level of responses, participation and interactivity.

Under the NATO campaign, the effectiveness or delivery of the six-point plan, would have been extremely difficult to ascertain.

CONCLUSION

Internet advertising is not just banner serving and button placement. It can involve the development of sponsorships, creation of insitertials, placement of classifieds, e-mail marketing, the diffusion of Simple Message Services (SMS) via the Web, and Wireless Application Protocol (WAP).

In turn, it would be deemed quite logical that some of the beforementioned Internet advertising techniques could be applied, within the genre of Perception Management, in IW.

The concentration on network and information systems within the IW paradigm, by the United States military, is a major concern. It seems that the military are more concerned with "hacking" and electronic broadcasting devices rather than the benefits that can be attained from the technologies of the Internet. In particular, the benefits that can be derived by implementing Internet advertising techniques for efficient perception offensives.

REFERENCES

Boni, W. & Kovacich, G.L (2000). *Netspionage: The Global Threat to Information (1st Edition).* Butterwoth-Heineman, Woburn, MA.

Craig, S.J. (1999). *The Perception Management Process.* Military Review, US Command and General Staff College, LXXVII, 6: 1-6.

Dearth, D.H. & Campen A.D. (2000). *Cyber War 3.0. (1st Edition).* Fairfax, Virginia, AFCEA International Press.

Delwiche, A. (1995). *Propaganda Analysis.* Washington University Journal, 52, 3: 95-123.

DiCenso, D.J. (2000). *The Legal issues of Information Warfare.* Law Technology, 33, 2: 1-25.

Fulghum, D.A & Wall, R. (2001). *Putting the Spin On Modern War.* Aviation Week & Space Technology, 154, 9: 64-65.

Fulghum, D.A. & Wall, R. (2000). *Infowar Improves, But Psywar Stumbles.*Aviation Week & Space Technology, 152, 18: 67-68.

Hoffman, D. L., Novak, T. P. and Chaterjee, P. (1995). *Commercial Scenarios for the Web: Opportunities and Challenges.* Journal of Computer Mediated Communication 1 (3) [On-line] http://www.ascusc.org/jcmc/vol1/issue3/hoffman.html

Holbert, R.L. (2001). *Propaganda and Persuasion.* Southern Communication Journal, 66, 66: 181-182.

Hyland, T. (2000). *Why Internet Advertising?* Internet Advertising Bureau [On-line] www.iab.net/advertise/content/adcontent.html

Kennedy, H. (2001). *Pysops units encouraged to modernize their units.* National Defense, 85, 567: 22-24.

Krishnamurthy, S (2000). *Deciphering the Internet Advertising Puzzle.* Marketing Management, 9, 3: 34-40.

Levien, F.H. (1999). *Kosovo: An IW Report Card.* Journal of Electronic Defense, 22, 8: 41-51.

Reed, M (1999). *Going Beyond the Banner.* Marketing, London, April, 1999, Haymarket Publishing.

Satchell, M. (1999). *Captain Dragan's Serbian* Cybercops. U.S. News.

Swett, C. (1995). *Strategic Assessment: The Internet.* Federation of American Scientists, Project on Government Secrecy, 1-32.

Snyder, B. (1999). *Bess Tries "Crosstraining", Moves to Madison Avenue.* Advertising Age, 70, 51: 60.

Washington, D.W. (1995). *Onward Cybersoldiers.* Time Magazine (August 21, 1995), 168, 8.

Winter, D.L (2001). *Propaganda: Demons, Atrocities, and Lies.* Washington University Journal, 128, 55: 23-85.

An Intelligent Agent-based Security Management Architecture for Enterprise Networks

K. Boudaoud[1], Z. Guessoum[2] and Charles McCathieNevile[3]

[1] *University of Geneva, Switzerland*
E-mail: Karima.Boudaoud@cui.unige.ch

[2] *University of Paris 6, France*
E-mail: Zahia.Guessoum@lip6.fr

[3] *World Wide Web Consortium*
E-mail: charles@w3.org

ABSTRACT

The openness of enterprise networks towards the Internet, for business purposes, is achieved at the price of high security risks that cannot be overlooked. These networks are becoming very complex (in terms of services offered, number of users) which expose them to various kinds of complex security attacks. Therefore, security management of enterprise networks requires more sophisticated models. To deal with these requirements, intelligent agents and multi-agent systems are well adapted. They provide a powerful paradigm for the modeling and development of complex systems. This paper proposes an intelligent agent-based security management model to adapt to enterprise networks' evolution.

Keywords: Enterprise Network Security Management, Security Policies, Security Attacks, Intelligent agents, Multi-agent System.

INTRODUCTION

Enterprise networks are becoming more complex, particularly in terms of services offered. Moreover, the number of users is continuously increasing. Networks are therefore more subject to various kinds of complex security attacks. So security management of these new networks requires more intelligence and sophistication. However, existing solutions are developed for well-defined networks and systems (Balasubramaniyan et al. 1998)(Mukherjee et al. 1994)(White et al. 1996). Thus, they are not adapted to dynamic environments, nor to the increasing complexity of user behaviors. Particularly some recent aspects like mobility of users enhance this complexity. Classical security solutions cannot easily deal with these aspects. What is needed is a solution that is flexible and adaptable to variations and non-predictive complex evolution of networks. These characteristics have been the subject of many works, particularly in the network management domain (Oliveira 1998)(Conti 2000). Recent solutions (Oliveira 1998)(Guessoum 1996) have shown that multi-agent system (MAS)-based approaches are well-suited to resolve complex problems. MAS are based on the decomposition of systems into several interacting and autonomous entities called agents. An agent refers to an entity that acts continuously and autonomously in a dynamic and unpredictable environment. Therefore, in order to provide security solution for actual networks as well as for the next generation, we apply the multiple agents paradigm to the area of security and propose a new generation of security management architecture based on a MAS to model and implement an *intelligent* security system.

This paper is organized as follows. We first give an overview about our security model. Then, we describe our security policies management model. Afterwards, we present our agent-based security management model. Finally, we conclude with some remarks and future work.

A NEW MODEL FOR SECURITY MANAGEMENT

To model the problem of security management, we have to deal with:

- the distributed nature of networks to secure,
- the network variation and complexity in terms of application and services offered,
- the increasing number of users and diversity of their profiles that change continuously, particularly in the case of mobility,
- the diversity and complexity of security attacks,
- the variation of security policies.

To fulfill these requirements, we propose an *intelligent agent*-based solution. Moreover, to manage the security of a network, we need to:

- manage *security policies* specified by the administrator,
- analyze *security events* characterizing security attacks occurring in the network.

Based on these elements, we decompose security management in three plans:

- The *user plan* that represents the *security policy-based model.* It involves the administrator and *the security policies.* The administrator defines and specifies security policies to apply to the network. He modifies them when the network configuration changes or when he would like to detect new attacks. Moreover, he receives security reports.
- The *intelligence plan* that represents the *intelligent agent-based* model, which involves the MAS.
- The *kernel plan* that represents the *security event-based model.* It is constituted by: the network to secure and the *security events* occurring in it. These events are analyzed to detect attacks and to make sure that security policies are respected.

In this paper, we focus on the user and intelligence plan.

SECURITY POLICY-BASED MANAGEMENT MODEL

The aim of our security policy management model is:

- to permit the administrator to specify security policies (i.e. security rules) of the enterprise network and define what is authorized and prohibited,
- to implement these policies and to ensure that they are respected.

Attacks, which are a violation of these policies, must be detected by the MAS when they occur. Thus, security policies guide the MAS' behavior and act at three levels (Figure 1) by:

- selecting and instantiating security attack schemas to detect,
- creating goals to send to the agents concerned for detecting these attack schemas,
- selecting events to filter for recognizing instantiated attack schemas.

In order to be interpreted by the MAS, security policies must be formalized by identifying the different abstraction levels and specifying them in a formal language. Based on existing works (Heilbronner 1999)(Lupu et al. 1997)(Mariott 1999)(Moffet et al. 1993)(Wies 1995)(Yialelis et al. 1995), we have proposed a new model for a hierarchy of security policy, where we have identified three abstraction levels for security policies (Figure 1):

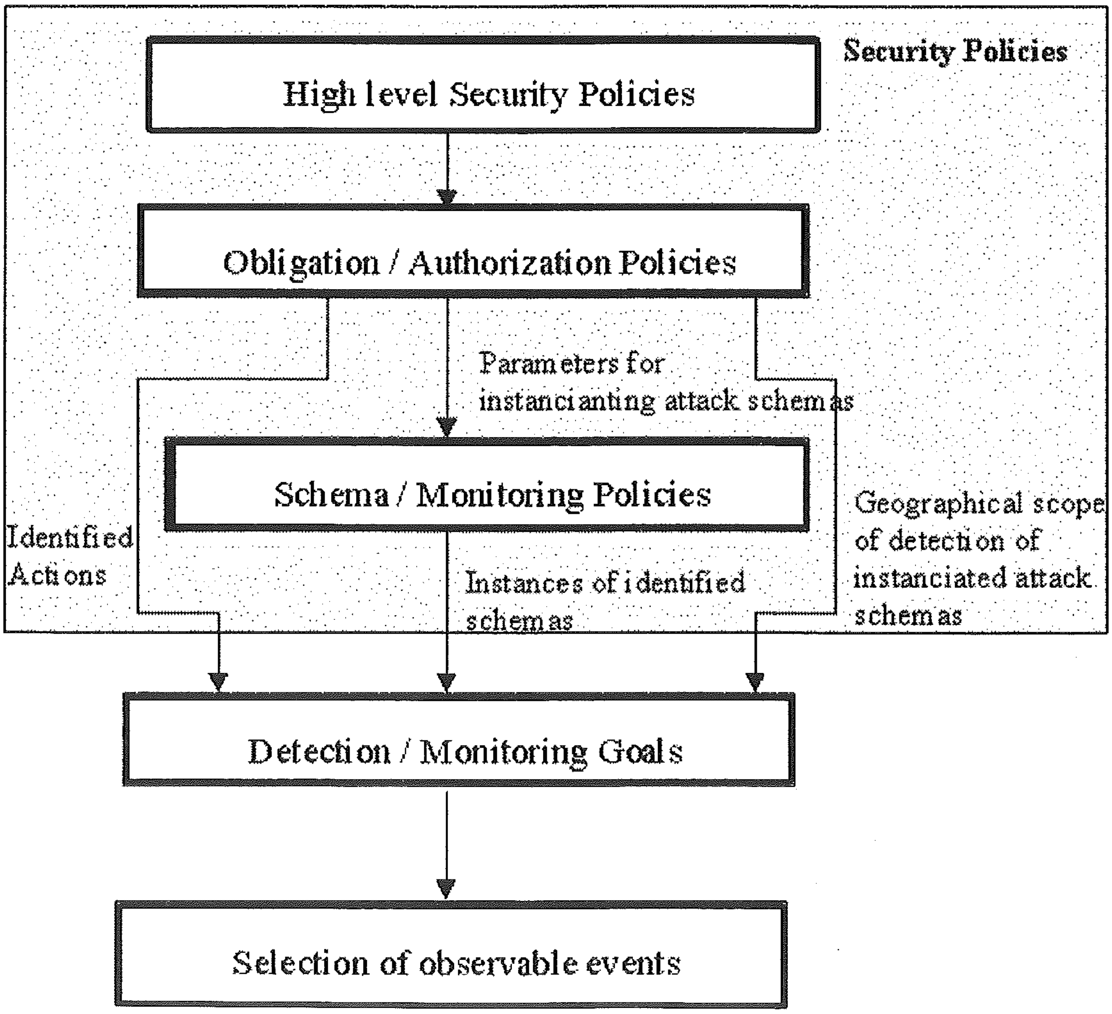
1. The **high level security policies** that specify the general enterprise security rules,

2. The **obligation/authorization policies** that specify the obligation and authorization rules. In this level of abstraction we define:
   - the different entities (workstations and domains to protect, internal or external users) to which these rules are applied.
   - the authorized/denied actions and the temporal/geographical constraints.

3. The **schema policies** that specify the attack schemas to detect. We focus on this policy level because they represent the policies that are finally implemented in our system. In the same level, we have the **monitoring policies** that specify the monitoring tasks. They permit the administrator to monitor specific activities concerning a part of the network or a particular user.

The aim of a policy hierarchy is to automate the best possible refinement process between the different abstraction levels of a security policy.

Figure 1: Security policy role


Security Policies
High level Security Policies
Obligation / Authorization Policies
Parameters for instancianting attack schemas
Schema / Monitoring Policies
Identified Actions
Instances of identified schemas
Geographical scope of detection of instanciated attack schemas
Detection / Monitoring Goals
Selection of observable events

To automatically derive *obligation/authorization policies* in *schema policies,* they must be expressed into further details. This means that from the formalism used for the obligation/authorization policies, the different operators used for defining an attack schema must be deduced. Therefore, security policies must allow us to identify:

- what we want to protect, and against what we want to protect it,
- what we want to do when an attack is detected.

Indeed, we define two *schema policies*: **schema instantiation policies** and **response to attack schemas policies.**

The *schema instantiation policies* define attack schemas. The instantiation of the attack schema is not always done in the same manner, but depends on whether the superior level policy is an obligation or authorization policy.

The *authorization policies* define what it is authorized or denied in a network (or part of a network) with regard to persons, network entities and/or geographical places. Moreover, they permit us to define and to create new attack schemas. An authorization policy could be *positive* or *negative,* and the process for each is different:

- from a positive authorization, we must deduce the attack schemas denying the authorized actions,
- from a negative authorization, we must deduce the attack schemas defined directly in the authorization policy.

The *obligation policies* enable the system to detect specific attacks by instantiating existing schemas in order to specify what we really want to deny. The instantiation of a schema is done either:

- nominatively, i.e. with regard to a user, a particular source/destination network, or
- anonymously without specifying the source and/or destination.

Moreover, the detection zone of an attack can be delimited by the administrator, to either:

- the whole enterprise network, or
- a part of the network, when he wants to protect strongly this zone.

Thus, the obligation policy acts on either:

- the instance itself of an attack schema, or
- the schema instance and the geographical detection zone.

The *negative* or *positive* mode of an obligation policy has no influence on the instantiation process. The mode acts precisely on the *response to attack schemas policy* to specify to the system how to react against an attack.

The *response to attack schemas policies,* which are specified by *obligation policies* in the superior level, allow the system to implement system reactions when an attack is detected. They define the actions that the administrator and the agents must do or not in this case such as:

- closing or not a connection,
- filtering source or destination addresses by modifying the parameters of a filter or a firewall.

For specifying a securitcan specify obligation/authorization policies, that create and instantiate attack schemas and schema policies.

To create an attack schema, we:

- identify the attack schema,
- specify the list of event types that represent the attack schema,
- specify the constraints on these events.

Moreover, to instantiate an attack schema, we:

- select a schema,
- parameterize the schema by forcing the free parameters (non specified attributes), for example the source or the destination of the event defined in the schema,
- specify new constraints in case of modification of some attributes, such as the number of repetitions of an event or an event series,
- define the detection zone of the attack schema. This information is used to select the group of agents that have to detect this attack schema.

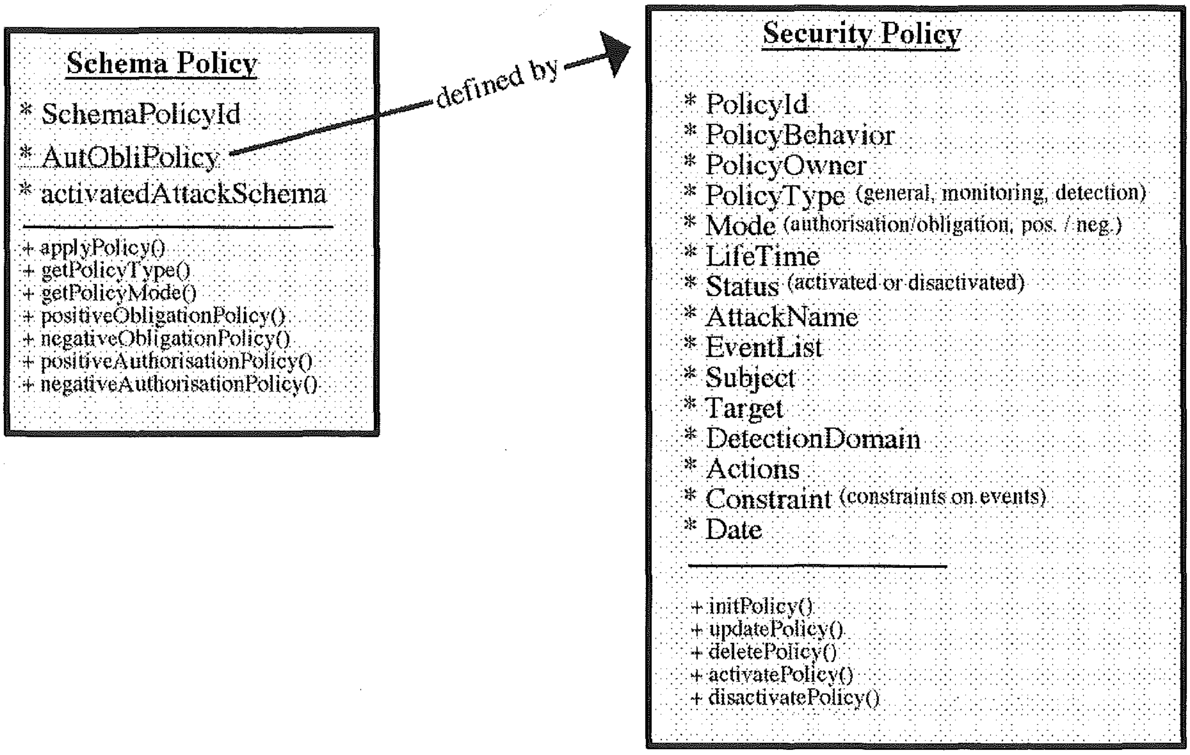


Figure 2: Security policy classes

To define a schema policy, we:

- use the reference of the obligation/authorization policy from which the schema policy derives,
- select the attack schema to create or instanciate.

Consequently, obligation/authorization and schema policies are defined by a set of attributes, which we regroup respectively in 'SecurityPolicy' and 'SchemaPolicy' classes (Figure 2).
An example of derivation of schema policies is illustrated in (Boudaoud 2001b).

Now, we describe the MAS driven by security policies.

AGENT-BASED SECURITY MANAGEMENT MODEL

To design our MAS, we have used existing design methodologies (Gutknecht et al. 199)(Kinny 1997a)(Wooldridge 1999) that allow us to describe:

- the organizational model of the MAS by defining roles and groups,
- the agent model by defining its internal architecture.

The organizational model of the proposed multi-agent system for intrusion detection

For defining the agent's roles, we have to identify the functions that our security management system must fulfill, independently of the agent technology. We have identified the following functions:

- to specify security policies in order to instantiate *attack schemas* to detect,

- to distribute the detection of *attack schemas* to several entities distributed in the network. Each entity will have to monitor a specific domain (network elements grouped with regards to the enterprise organization and/or by geographical zone). The distribution of *attack schemas* is done with regards to:
  - □ the *detection scope* of an *attack schema*, which defines the domain where it must be detected,
  - □ the type of activities (extranets, intranets, internal and local) to monitor for detecting the *attack schema*s,

- to detect attack schemas by:
  - □ filtering security-relevant events to recognize instanciated *attack schemas*,
  - □ analyzing filtered events,

- to act against detected attacks by executing actions specified in security policies when *attack schemas* are instantiated. We note that, in prototyping this work, the actions implemented were limited to informing the concerned entity.

Each of the first process steps is functionally represented by one or several entities that fulfill a role:

- to instantiate *attack schemas*, we define the role of ***security policy manager*** ,
- to realize the distribution of *attack schema*, we define the role of ***extranet manager***. According to the size and the geographical distribution (several regions in a country or several countries) of the network enterprise, we propose to define a supplementary role: the ***intranet manager***,
- to ensure the detection of distributed attack schemas, we define three roles: **extranet local monitor, intranet local monitor, internal local monitor**.

The role of *security policy manager* is to ensure the following functions:

- interaction with the administrator,
- management of security policies (creation, updating, activation,),
- instantiation of *attack schemas* from the security policies,
- translation of *attack schemas* in terms of *goals*.

The entity with the role of *extranet manager* has a global view of the enterprise network. The functions fulfilled by this entity are:

- security management of the enterprise network with regards to external networks and between the different local networks constituting the enterprise network,
- reception of *goals* that express the *attack schemas* to detect in the enterprise network,
- detection of coordinated and global attacks,
- distribution of *attack schemas* to the different entities distributed in the network and that fulfill the role of *intranet manager.* This is achieved by translating goals received into sub-goals which are sent to the distributed entities,
- management and control of the distributed entities,
- reception of pertinent analysis done by the distributed entities,
- correlation of these analysis. Other analyses are then done on suspicious events in order to confirm or not the detection of an attack. According to the results, other analysis could be requested and new *attack schemas* could be sent in form of new *goals* to reach.

The entity with the role of *intranet manager* has a local view of the enterprise network. It fulfills the same functions as the previous entity but at the local network of the network enterprise, which is summarized as:

- security management of a local network constituted of several domains,
- detection of coordinated attacks produced inside a local network and between its different domains,
- management and control of the entities distributed inside the local network that fulfill the role of *extranet local monitor, intranet local monitor* or *internal local monitor.*

The entity with the role of *extranet local monitor* has to detect *attack schemas* that are characterized by *extranet* activities. This means that this role is associated to the function of detection of attacks coming from or going to an external network.

The entity with the role of *intranet local monitor* has to detect *attack schemas* that are characterized by *intranet* or *local* activities. This means that this role has the mission of detection of:

- attacks coming from or going to other local networks of the same network enterprise,
- attacks that are internal to the local network (i.e.: coming from or going to one or several domains of the same local network).

The entity with the role of *internal local monitor* has to detect *attack schemas* that are local to a domain

Having described the agent's roles, we now regroup them in two group structures: a *manager group structure* and a *local monitor group structure* (Figure 3).

The *manager group* manages the global security of a network, that could be local or distributed. It is defined by the roles of *security policies manager, extranet manager* and *intranet manager.* It has two functions: control and data processing. On one hand it controls the *local monitor group* and on another hand, it ensures a high level correlation of the analysis results made by the local group. It also supports the recognizing of global attacks including the coordinated attacks that are internal to a network enterprise i.e.: that occur between local networks of the same distributed network. We can say that the *manager group* operates at the enterprise level by correlating the results produced by the different sub-networks (intra-domains).

The *manager group* interacts with the administrator by: 1) receiving specified security policies to respect; and 2) sending security reports and/or alarms. This group has a hierarchical structure of agents where we distinguish three levels of agents that have a manager role:

- The **security policies manager agent** that fulfills the *security policies manager* role,

- The **extranet manager agent** that ensures the *extranet manager* role. The number of agents to which this role is attributed depend on the size of the enterprise network and its geographical distribution. For example one might choose to have one *extranet manager agent* for each country represented in a network.

- The **intranet manager agents** (IMAs) that have the *intranet manager* role. The IMAs cooperate and interact in order to ensure security of the distributed network. In fact, an IMA could receive analysis conclusions or suspicions messages from other IMAs. It correlates then these suspicions with the analysis made by the agents of the lower level. It can also, depending on these suspicions, ask to its sub-agents for specific information (suspicion level of a particular user, services used by a user, etc.) in order to go thoroughly into the analysis of its homologues and to confirm their suspicions. This communication between IMAs permits a cooperative detection of coordinated attacks that occur at different points of the distributed network.

The *local monitor group* is responsible for security management of a domain. It has a local view restricted to the monitored domain. This group is composed of a group of *local agents* (LA) that fulfill the role of *extranet*, *intranet* or *internal local monitor* and that are distributed in the local network . These agents detect *attack schemas* that are local to their domain. Domains are distributed to the LAs by the IMAs. This group operates at a domain level by correlating the results of its different LAs. When an agent suspects one or several activities, it notifies the other agents to confirm whether or not an attack happened.

The LAs interact with the network, either passively by looking at log files and/or observing network traffic, or actively by using specific network probes. Thus, they collect security-relevant events produced in the network and analyze them for detecting intrusive behaviors.

According to the roles of *local monitors* identified previously, this group contains three kinds of *local agents*:

- the **extranet local agents** that fulfill the *extranet local monitor* role,
- the **intranet local agents** that ensure the *intranet local monitor* role,
- the **internal local agents** that have the *internal local monitor* role.

The *local monitor group* ensures a first detection level whereas the *manager group* performs a second, more detalied level of detection.

The hierarchical organization of agents allows us to ensure a global analysis and detection as well as a local one. The aim is to try to detect attacks as soon as possible. In fact, each agent, at its level, has its own vision of the network which is limited by the domain that it has to monitor and whose security it has to manage.

Domains are defined by the agents of the *manager group*. In the *local monitor group*, a domain is an enterprise local sub-network, which represents a group of network resources, which are gathered either according to the organization of the company in terms of departments or according to security levels specified by the security policies of the company. In the *manager group*, a domain represents either a distributed network or a local network of this same enterprise network.

The *manager group* interacts with the *local group* by:

- sending messages in form of goals to reach, derived from security policies. These goals concern detection of specific attacks parameterized in security policies,
- delegating specific functions of monitoring and/or detection,
- asking for particular information such as the security state of a host or the suspicion level of a specific user.
- specifying the various domains to monitor, which must be distributed to the different LAs, receiving the relevant analyses results and alarms.

THE SECURITY AGENT MODEL

To model security management, agents must combine cognitive abilities (knowledge-based) to reason about complex attacks with reactive capacities (stimulus-response) to react rapidly to changes in the environments. So an agent has three main functions: *event collection*, *interaction* and *deliberation*. The first one filters security-relevant events produced in the agent environment, according to event classes specified to the agent when it receives a detection goal derived from a security policy. The *interaction* function allows agents to communicate their analysis and decisions. It also permits the administrator to interact with the *SPMA*. Thanks to the *deliberation* function the agent is able to reason and extrapolate by relying on its mental attitudes, built-in knowledge and experience, in a rational way, to find the adapted answers. The information model is based on BDI (Beliefs, Desires and Intentions) concepts (Rao et al. 1991). The agent uses its beliefs resulting from the filtered events for reaching its specified goals. When a goal is reached (an attack is detected), it executes appropriate actions.

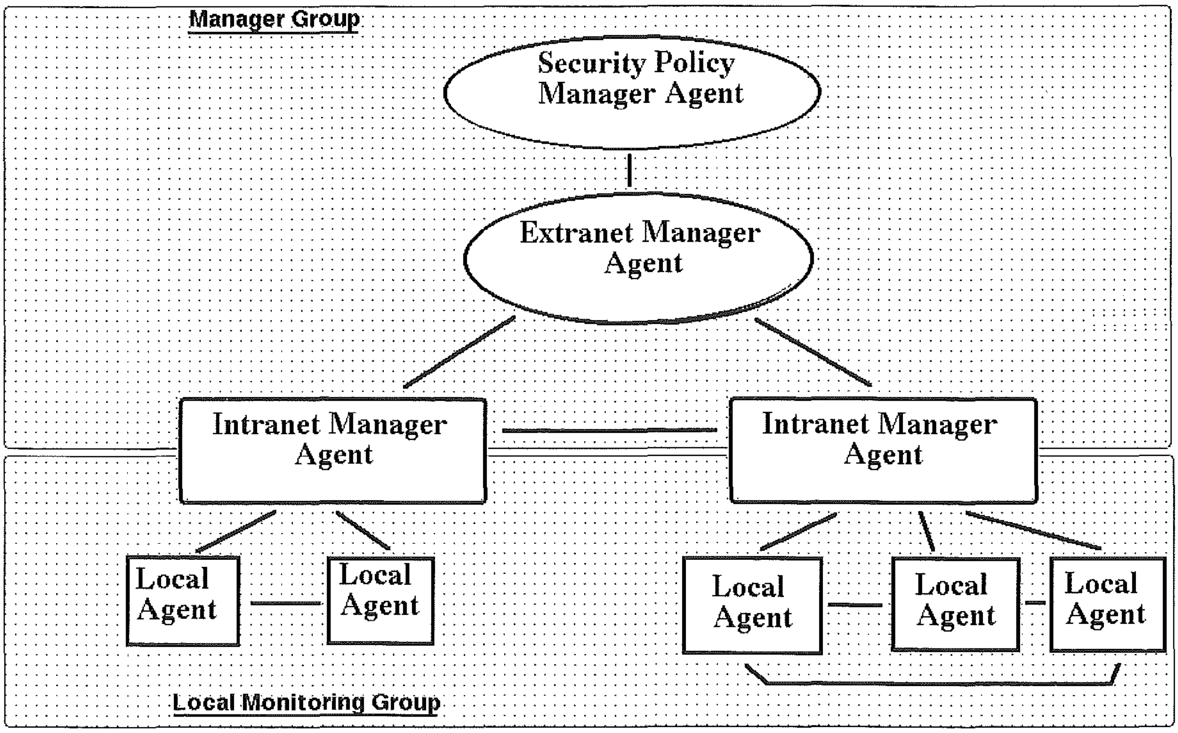


Figure 3: Functional architecture of the multi-agent system

CONCLUSION

We propose a new generation of flexible and adaptable systems for efficient security management. This intelligent agent-based approach is innovative because it allows a security management system to adapt to unpredicted complex evolution of both enterprise network environments and security attacks. The proposed approach is currently implemented using the DIMA platform (Guessoum 1996). The prototype enables detection by the agents of known attacks. Presently, we are working on the adaptation of agents' behaviors to new kind of attacks.

REFERENCES

Balasubramaniyan J. S., Garcia-Fernandez J. O., Isacoff D., Spafford E. H. and Zamboni D. (1998). *An Architecture for Intrusion Detection using Autonomous Agents*. Technical Report, Coast-TR-98-05, Computer Sciences Department, Purdue University.

Boudaoud K. (2001a). *Intrusion Detection: a New Approach using a Multi-Agent System*. Ph.D. thesis, Institut Eurecom/ EPFL, Sophia Antipolis, France.

Boudaoud K. (2001b). *Policy-based Security Management using a Multi-agent System.* Eight Workshop of the HP Openview University Association (HP-OVUA'99), Berlin, Germany.

Conti P. (2000). *Intelligent Agents: Emergence of a new technology for Network Management. Ph.D.* thesis, ENST, Paris, France.

Damianou N., Dulay N., Lupu E. and Sloman M. (2000). *A Language for Specifying Security and Management Policies for Distributed Systems.* Imperial College Research Report, Doc 2000/1, Department of Computing, Imperial College of Science Technology and Medicine, University of London, England, 2000.

Guessoum Z. (1996). *An Operational Environment of Conception and Realization of Multi-Agent Systems.* Ph.D. thesis, University of Paris VI, France.

Gutknecht O., Ferber J. (1999). *Towards an Organizational Methodology of Design of Multi – Agent system.* Research report, LIRMM 99073, University of Montpellier, LIRM.

Heilbronner S. (1999) *Requirements for Policy-Based Management of Nomadic Computing Infrastructures.* Sixth Workshop of the HP Openview University Association (HP-OVUA'99), Bologna, Italy.

Kinny D. and Georgeff M. (1997). *Modelling and Design of Multi – Agents Systems.* In J. P. Müller, M. Wooldridge and N. R. Jennings editors, Intelligent Agents III, (LNAI Volume 1193), pp. 1-20, springer-verlag, Berlin, Germany.

Lupu E. and Sloman M. (1997). *Conflict Analysis for Management Policies. Fifth IFIP/IEEE* International Symposium on Integrated Network Management (IM'97), San Diego, USA.

Mariott D. A. (1997*). Policy Service for Distributed Systems*. Ph.D. thesis, Department of Computing, Imperial College of Science Technology and Medicine, University of London, England.

Moffett J. D. and Sloman M. (1993). *Policy Hierarchies for Distributed Systems Management.* IEEE Journal on Selected Areas in Communications, 11 (9), pp. 1404-1414.

Mukherjee B., Heberlein L.T., and Levitt K.N. (1994). *Network Intrusion Detection.* IEEE Network Journal, pp. 26-41, May/June.

Rao A. S. and Georgeff M. P. (1991). *Modelling Agents within a BDI – Architecture.* Technical report, 14, Australian AI Institute, Carlton, Australia.

Teixeira de Oliveira R. F. (1998). *Network Management with Knowledge of Needs: Use of software agents.* Ph.D. thesis, ENST, Paris.

White B., Fisch E. A., and Pooch U. W. (1996). *Cooperating Security Managers: A Peer-Based Intrusion Detection System.* IEEE Network Journal, pp. 20-23, January/February.

Wies R. (1995). *Using a Classification of Management Policies for Policy Specification and Policy Transformation.* Third IFIP/IEEE International Symposium on Integrated Network Management, Santa Barbara, CA, USA.

Wooldridge M., Jennings N. R., and Kinny D. (1999). *A Methodology for Agent Oriented Analysis and Design.* Third International Conference on Autonomous Agents (Agents 99), Seattle, WA, pp. 69-76.

Yialelis N. and Sloman M. (1995). *A Security Framework Supporting Domain Based Access Control in Distributed Systems.* Imperial College Research Report, Doc 1995/14, Department of Computing, Imperial College of Science Technology and Medicine, University of London, England.

On Wireless Network Security

J.K. Fawcett [1] and W.R. Sowerbutts [2]

[1] *Laboratory for Communications Engineering*
University of Cambridge, UK,
E-mail: jkf21@cam.ac.uk

[2] *Laboratory for Communications Engineering*
University of Cambridge, UK,
Email: will@sowerbutts.com

ABSTRACT

We discuss practical security of 802.11b wireless networks through three anecdotal case studies. The dangers facing a university faculty, a small business and a home user are explored. Information Burglary—industrial espionage against telecommuters—is introduced. We investigate the underlying causes of security holes, spanning theoretic algorithmic flaws, deployment errors and end-user naivety. Failures to appreciate the range of radio coverage are highlighted and features interactions with other technologies are explored. Technical and ethical suggestions for improvements by the industry and network administrators are made.

Keywords: wireless network, 802.11, practical security, Information Burglary.

INTRODUCTION

Security is a buzzword in today's hi-tech society. Companies must be mindful of Information Warfare and safeguard their commercial futures against onslaughts of anonymous hackers, crackers and script kiddies. Wireless networks offer high bandwidth, low latency, mobile networking and the current generation of products—those conforming to IEEE802.11b (IEEE 1999)—are forging ahead, despite concerns, as system administrators face pressure from user groups to deploy fashionable technologies.

Wireless networks are not without problems: flaws in the link-layer encryption algorithm—Wired Equivalent Privacy (WEP)—make it susceptible to analytic attacks (Borisov 2001, Walker 2000, Walker 2001). Cryptanalysis work by Fluhrer et al. (2001) on weaknesses in the schedule of initial values used by the RC4 block cipher has lead to passive ciphertext-only attacks on WEP. AirSnort (http://airsnort.sourceforge.net) requires as little as 100 Mb of encrypted traffic to discover keys. Furthermore, case studies have revealed that many customers remain unaware of security concerns and serious issues with deployed networks have been highlighted. The motivation for this work is to address these issues by drawing the attention of both end-users and industry professionals to practical security of wireless networks.

The contributions made by this paper are twofold: in addition to highlighting problems introduced by inadequate 802.11 installations and offering remedial advice, we explore grounds for improvement in the computer industry. The range of radio coverage and interactions with wired networks and network services are exemplified by a university faculty in the next section. A small business illustrates commonly held misbeliefs concerning WEP encryption and MAC address filtering, and demonstrates unpleasant interactions with Unix permissions and file sharing, in the second case study. A home users' network shows, in the final case study, how Information Burglary may soon become a corporate headache. It should be emphasised that *a priori* permission was sought by the authors in each case.

CASE STUDY 1: A UNIVERSITY FACULTY

A university faculty must preclude unauthorized use of its high-bandwidth Internet connection—an attractive foothold for laundering traffic and launching further attacks. Routers direct IP traffic between the departmental Ethernet and the global Internet; the game is to ensure each traffic source on the private segment is authorized. Selective usage tolls on external links provides financial pressure to ensure all traffic is valuable. A private meeting room had been equipped with an 802.11b access point (AP) for the convenience of research staff. The AP was patched onto the Ethernet and performing only network address translation (NAT) to bridge the wired and wireless domains. Staff observed laptops 'could see' the AP if located in the meeting room or any of the immediately adjacent offices but signal attenuation prevented communication if the user roamed further. Encryption had not been enabled to avoid problems of key dissemination.

Range

It was a widely held belief that the wireless network had highly localised availability and was thereby no less secure than the wired Ethernet since physical access to the building was a prerequisite of connecting to either. It came as a shock that we were able to communicate with their AP from our office window a quarter mile across town using a directional Yagi antenna providing 12 dBi gain (net of cable losses). Furthermore, the equipment required is commercially available and retails for only US$120, placing this attack in the domain of the casual hacker or even script kiddie. Indeed, a recent SlashDot article (a popular online news site focussing on hi-tech stories, http://www.slashdot.org/) introduced 'War Driving': a modern-day version of war-dialling involving driving through cities with a laptop and high-gain antenna seeking insecure wireless networks. Although we took care not to exceed effective isotropic radiated power (EIRP) regulations applicable in the UK, hackers may be less conscientious and could work over longer distances as a result. EIRP regulations are less restrictive in countries where FCC regulations apply. Figure 1 gives the broader picture: the authors completed a practical investigation into achievable ranges using Lucent Technologies' *ORiNOCO* 802.11b cards and range-extending Yagi antennae. Lucent quote ranges of 25 km for 1 Mbps traffic with symmetric antennae 'in ideal conditions' for the Fresnel bulge.

	Yagi—Yagi		Yagi—unassisted 802.11 card	
Range (km)	Mode (Mbps)	RTT (ms)	Mode (Mbps)	RTT (ms)
0.25	11	2.0	11/5.5	2
0.5	11	2.0	5.5/2	2.4
1	11	2.0	1	2.4
2	11	2.0	-	-
4	11	2.0	-	-
7	11/5.5	2.1	-	-
10	5.5/11	2.2	-	-

Figure 4: Outdoor long-range 802.11 connections

APs house unassisted 802.11b cards so anyone within 1 km of the faculty meeting room and with line-of-sight can communicate with their network; a similar installation in Manhattan would be open to 65000 people. In common with TEMPEST attacks (van Eck 1985, Kuhn et al. 1998) snoopers may listen to network traffic from afar with little fear of being detected. Microwave sources are difficult to localise; even active attacks may go unnoticed or untraced. The situation is "unproportionate" (Overill 2001)—the cost of defence greatly exceeds that of attack.

Overwhelmingly, consumer 802.11b NICs do not feature external antenna connection jacks. The possibility of attaching external aerials does not occur to most users yet the security ramifications are grave. For fear of damaging sales or undermining market confidence, most product's documentation avoids mentioning signal range attacks. The consumers, who are not expected to hold radio-engineering qualifications and rarely do so, remain naïve to the properties of the underling radio frequency (RF) technology and consequently unaware of the hazards. Mistakes in deployment assumptions are inevitable. There is clear scope for improvement within the industry. Accredited courses for administrators would help reduce the general susceptibility of large organisations to electronic attacks on their radio networks by teaching relevant radio and systems engineering. An alternative course of action might recommend professional installation but this may jeopardise sales, which is hardly feasible in an industry with such fierce competition.

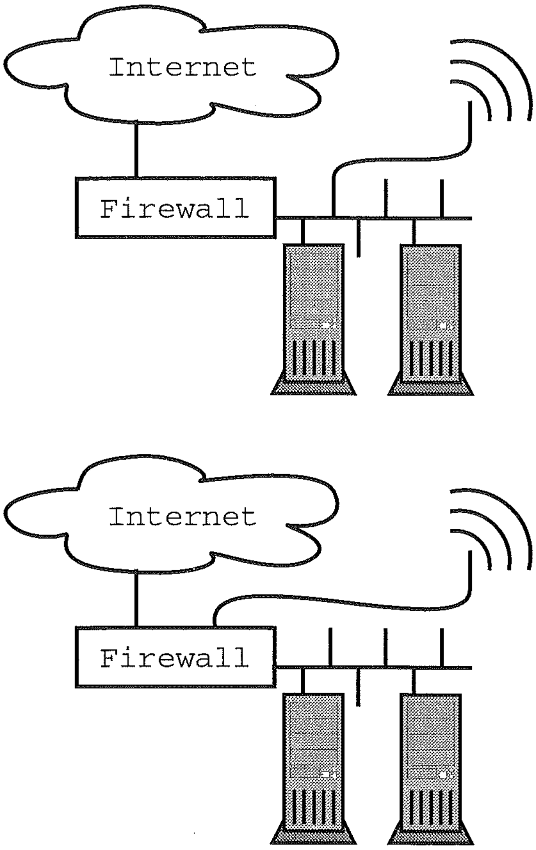


Figure 5: Wired/wireless interconnections: above, (a), the more common; below, (b), the more secure

Wired/wireless interconnection

The AP was connected to the faculty's internal Ethernet, allowing us to roam around their private network from our remote location. Traffic arriving via the AP should be trusted no more than that from an Internet ingress. Figure 2a illustrates the arrangement typical of current deployments and 2b a more secure configuration. A sound deployment should follow the latter and tunnel authorized connection through the firewall using IPsec or Virtual Private Networking (VPN). Windows and Unix clients are mature; versions for PDAs are becoming available.

Installation instructions rarely distinguish the situations shown in Figure 2, preferring to describe their own mechanisms to control access to the radio channel or packet forwarding hardware. Any secure system should put in place periphery access control mechanisms and design the core as though they were not present or rendered ineffective. Professional advice should have made this clear initially but only now are we seeing effective use of firewalls and VPN.

Short of constructing a Faraday cage around the building, there is little administrators can do to prevent outsiders communicating with their APs. The first line of defence is WEP encryption, the second MAC filtering; we return to these in the next section. With both disabled on the faculty's AP there were no barriers preventing further exploration of their private, internal network.

INTEGRATION WITH INTERNET PROTOCOL (IP) AND SUBNETTING

The faculty ran a dynamic host configuration protocol (DHCP) server offering (dynamically allocated) IP addresses to machines on the Ethernet. Continuing to use the antenna in our office window we leased an IP addresses and thereby achieved use of their network—which they were keen to protect—without even running a script! IP addresses in the DHCP pool were assumed trustworthy in the configuration of their proxy server, permitting it to launder our HTTP traffic. Their webserver similarly served us intranet pages, including a live webcam view of the administrator's office which we watched when telephoning to explain our findings! Other intranet pages list the home and mobile telephone numbers of research staff. Possessing an address deemed trustworthy by their mail exchanger, we were able to relay e-mail through their server. If exploited by spam mailers embarrassment would ensue and their mail exchanger could be appended to victim's barred host lists.

The problems here exemplify unpleasant interactions among several technologies and can only be the responsibility of the end-users. Most systems are built or installed with certain assumptions in mind; these become the preconditions for successful operation of the system. Violating the preconditions of a software system renders inapplicable any intuition or proof about its runtime behaviour. Pair-wise interactions among network services increase as the square of the number of services—suppressing the undesired combinations, and adding new services, becomes ever more intricate. A dynamic DHCP daemon leasing addresses from a pool is 'safe' under the assumption that only requests from authorized machines can ever reach the server process, static DHCP is safe provided clients cannot change their Ethernet address. Attaching an AP to the same Ethernet segment as a DHCP server (or relay) demonstrates a violation of the preconditions for safe use and lead to our being able to exploit the intranet. Thorough system documentation is essential if these errors are to be detected. Various automation attempts have used Prolog horn clauses to express properties of a system of interconnected components. A goal then succeeds if and only if none of a set of undesired properties can be proven. Although technically elegant, those systems used by the authors have been cumbersome and expressing the behaviour of a network as horn clauses is unintuitive and error-prone.

CASE STUDY 2: A SMALL BUSINESS IN NORTH ENGLAND

It is essential to assure the integrity and privacy of internal ordering and personnel databases, in addition to any source code and company-confidential documentation held on corporate fileservers. The potential consequences of a security breach are far-reaching: leaking employment information would be embarrassing and public acquisition of internal documents could erode corporate advantages or affect patent applications. Lawsuits and lost revenue caused by either could threaten the future of the business; security is therefore imperative. Our work found administrators were unaware of the range of radio coverage and were guilty of connecting APs directly to their Ethernets but also heard claims of security through WEP encryption and MAC address filtering, which we now consider.

Encryption

802.11b makes provision for link-layer encryption to protect traffic in the air from eavesdroppers using the Wired Equivalent Privacy (WEP) protocol and a 40-bit shared key. However, controlled key dissemination presents a logistic challenge—the motivation for disabling encryption in the university faculty—and users find key changes highly disruptive. Moreover, numerous flaws in the WEP encryption algorithm have been identified, many leading to constructive attack strategies taking fewer steps than brute force. The business' key had not been changed for 11 months—too infrequently for the level of security desired. Wireless LANs are perceived to be a 'fit-and-forget' technology whereas diligent attention is required to manage encryption keys. Automated key variation techniques can lighten the administrative load without bombarding users with inconvenient key change notifications. Updated product documentation to reflect recent research into WEP vulnerabilities has yet to reach the marketplace.

All radio traffic should be regarded as potentially dangerous and additional encryption applied to bona-fide frames at another level in the network hierarchy. End-to-end secure sockets layer (SSL, application-layer) protects individual connections and suits a single host using a wireless network card, for example, to collect e-mail; LAN-to-LAN IPsec and VPN (network layer) secure all communications between two networks or a host and a network using a key shared by the egress routers of each. It is of best use on backhaul 802.11b networks such as fixed broadband connections to individual houses, and for connecting laptops to corporate networks through a firewall as described above. Medium- and long-term connections can benefit from frequent WEP key hopping which increases the effort required of an attacker. Manual key changing is highly disruptive; Fawcett et al. (2001) describe an automated approach based on the Advanced Encryption Standard (AES) in which a daemon regularly changes WEP keys in synchrony with other wireless hosts.

MEDIUM ACCESS CONTROL (MAC) FILTERING

In common with wired counterparts, wireless network interface cards (NICs) contain a unique 48-bit ID known as the MAC address. Authorized MAC lists stored in an access point (AP) are a means of controlling access to a wired/wireless bridge: APs will not forward Ethernet frames emanating from unrecognised MAC addresses. For reasons of cost-effective manufacture device firmware allows the MAC address to be written after product assembly. Unfortunately the value can be assigned repeatedly so an authorized address can be found merely by passively monitor traffic and assuming the MAC addresse involved in any 2-way communication (to avoid noting the MACs of unsuccessful, active attackers). Harvesting MAC addresses by this approach requires cracking WEP keys if encryption is enabled, which is a substantial undertaking notwithstanding algorithmic flaws. The necessity for a little MAC-layer snooping presents an insignificant barrier to a seasoned attacker compared to cracking keys, although to a novice or under-informed script kiddie it may prove sufficient. Duplicate MAC addresses cause Ethernet segments to go awry and thus to the attackers' detection so, to reduce the risk of being caught, attackers simply wait until the victim has taken their laptop away before assuming the MAC address of its network card.

Network File System (NFS)

The business' NFS servers were configured under the assumption that a firewall would block RPC requests issued by external (unauthorised) hosts. The wireless network provided second ingress to their network and a means of bypassing the firewall. The latter invalidates the preconditions of the NFS configuration. NFS is trusting with respect to user IDs (UIDs) so reading and even altering files is unhindered on directories exported for read-write. The difficulty here is another interaction-between-technologies issue but is poignant nonetheless. We demonstrated the ease of copying files off their NFS servers from afar: using an external antenna we listened to traffic, 'borrowed' a MAC address and made up a suitable IP address for their private subnet then ripped documents over NFS from a location too distant for their security camera coverage.

Without MAC filtering, and provided the intruder does not alias their MAC address to a recognised value, invisible thefts of this nature can be detected by watching traffic at the Ethernet frame level using tools such as ARPwatch. Log processing tools are required in practice because the bulk of data would soon overwhelm a human operator.

CASE STUDY 3: A HOME NETWORK

Home users face familiar privacy issues: personal communications and finances are increasingly managed with computer assistance. Cookies saved by web browsers can contain private information, credit card numbers and credentials for on-line retailers. Identity theft is increasingly common but personal details are of low monetary value. Attacks on home PCs with cable modems often seek a foothold from which to launch more sinister attacks on banks or on-line traders. Home users are early-adopters for new technologies and software revisions with the effect of increasing the susceptibility of their PCs to attack. They also tend to be lax in the installation of service packs and security hot-fixes, and virus defence software is often out-of-date.

Our final case study concerns a home wireless network with an analogue modem dial-up connection to an ISP. In common with most home users, any IT support was lacking. The owner frequently telecommutes and is not a computer expert making him a prime Information Burglary target. Large corporations have tightened their electronic security measures in recent years, forcing attackers to seek alternative means of acquiring confidential information. Recent copies of their employer's confidential documents can often be found on Teleworkers' laptops hard disks and intranet pages are cached in their web browser's cache. Their lack of expertise in securely configuring a network often leads to this data being easily accessible to intruders. We saw root directories shared with no password on Windows 98, leaving files open for copying or alteration by Information Terrorists in the neighbourhood. Files were also copied between machines using unencrypted 802.11b, allowing straightforward eavesdropping. Little thought had been paid to computer viruses: it would have been trivial, for example, to insert a macro virus into a document which, when activated in the office, copied files from the corporate network on to the laptop hard drive ready for the virus writer to read when the laptop returned home—a covert sneaker-net!

The easiest and quickest industrial espionage techniques focus on the homes of teleworkers where defences are likely to be low compared to their employer's office building. However, despite the evolution in work practices, network administrators consider the extent of their responsibility to be that of the office network. Companies must invest in support for distance workers if their files and intellectual property are to be continually subject to adequate security measures. Supporting home PCs represents a considerable undertaking with significant financial implications. Mixing trusted and untrusted computing environments is hazardous.

The onus of protecting personal data and financial records always rests with the homeowner. The computer industry could provide clear advice to these non-expert users on all aspects of data security. Relying on magazine articles to fill this task is not sufficient. Cross-manufacturer working groups might standardise practical security info-packs to be sold or included with relevant hardware.

CONCLUSION

We have discussed practical security of wireless networks with reference to three examples. Radio coverage zones were demonstrated to be significantly larger than users believed. We saw wired/wireless gateways facilitating the circumvention of firewalls, and unintended interactions between radio networks and DHCP, mail exchangers and NFS yielding vulnerabilities. We considered WEP and MAC filtering as deterrents and stronger ciphers as defence.

System administrators and users often lack the knowledge required to formulate informed security policies. In the workplace, enhanced product documentation may improve the situation in part and training courses would go further. Telecommuters often need the qualified support available from their employer's IT department.

ACKNOWLEDGEMENTS

John Fawcett is a PhD student at the Laboratory for Communications Engineering. He receives an EPSRC grant and a CASE award from AT&T Laboratories, Cambridge, Limited. Thanks are due to Martin Brown for providing some of the equipment and to Ian Wassell and Alastair Beresford for their assistance with Radio Authority power emissions compliancy. Thanks are also due to the faculty, small business and home user for their co-operation.

REFERENCES

Borisov N, Goldberg I and Wagner D (2001). *Intercepting mobile communications: the insecurity of 802.11 (draft).* [On-line]
http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

Fluhrer S, Mantin I and Shamir A (2001). *Weaknesses in the Key Scheduling Algorithm of RC4.* Proceedings of Selected Areas of Cryptography (SAC), August 2001.

IEEE (1999). *IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher speed Physical Layer (PHY) extension in the 2.4 Ghz band.* Designation 802.11b-1999.

Kuhn MG and Anderson RJ (1998). *Soft tempest: hidden data transmission using electromagnetic emanations.* Proceedings of the 2nd Workshop on Information Hiding, Portland, Oregon, April 1998.

Overill, RE (2001). *Information warfare: battles in cyberspace.* IEE Computing & Control Engineering Journal, June 2001, pp 125—128.

Van Eck W (1985). *Electromagnetic radiation from video display units: an eavesdropping risk?* Computers & Security 1985(4), pp 269-286.

Walker J (2000). *Unsafe at any key size; An Analysis of the WEP encapsulation.* 802.11 committee, October 2000.

Walker J (2001). *An Inductive Chosen Plaintext Attack Against WEP/WEP2.* Presented at 802.11 subgroup on security meeting, Orlando, May 2001.

The Autonomous Locksmith

J.K. Fawcett [1] and W.R. Sowerbutts [2]

[1] *Laboratory for Communications Engineering*
University of Cambridge, UK,
E-mail: jkf21@cam.ac.uk

[2] *Laboratory for Communications Engineering*
University of Cambridge, UK,
Email: will@sowerbutts.com

ABSTRACT

In the age of Information Warfare protection from hackers and industrial espionage can determine commercial futures. We discuss a flexible strategy involving frequently changed keys to combat the theoretic flaws of the Wired Equivalent Privacy link-layer encryption algorithm used by 802.11 wireless LANs. WEP keys are generated autonomously by encrypting the current time under a long, shared, cryptographically random master key. Automated network joining and key dissemination issues are addressed. The duration of privacy offered by this technique and the effort required by attackers are quantised. Lessons learned from the deployment of a prototype implementation are presented.

Keywords: wireless network, WEP, 802.11b, practical security, information warfare, key windowing, key changing.

INTRODUCTION

Wireless networks offer high bandwidth, low latency and extremely convenient mobile networking. The current generation of products, those conforming to IEEE802.11b (IEEE 1999), are enjoying explosive take-up in worldwide markets for both domestic and business use.

The widely deployed 802.11b "WiFi" interoperability standard defines the Wired Equivalent Privacy (WEP) mechanism for link layer frame encryption. The WEP algorithm was designed to provide both secrecy and authenticity. Unfortunately WEP, and the underlying RC4 algorithm, have recently been shown to exhibit numerous weaknesses (Borisov et al. 2001, Walker 2000, Walker 2001, Fluhrer et al. 2001). These weaknesses allow tools such as AirSnort (http://airsnort.sf.net/) to determine a WEP key given 100-1000Mb of encrypted packets in under a second.

This paper contributes a practical approach to counteract the analytic weakness of WEP by frequently changing keys. The advantages of the approach demonstrated here are that no hardware modification is required and both user convenience and compatibility are maintained.

The cipher used by generals during a battle to protect plans sent to their infantry must withstand a few hours of the enemy's attempts to crack it; that protecting ATM transactions need hold up against only a few minutes since session timeouts are short. The process of selecting a suitable cipher and key length for an application must consider the time period for which the ciphertext is to withstand determined analysis. Although design flaws have rendered WEP less secure than originally intended, it nevertheless takes nontrivial time to brute force a key. More intelligent attacks such as AirSnort require a minimum number of "interesting" packets to succeed. By changing the shared secret key frequently, communicating hosts can claw back durations of secrecy. Although an attacker can spool to disk the encrypted traffic and ultimately brute force each key used, the computational complexity of doing this means that she will never be able to perform the task in real-time, and will always fall behind. Clearly there is merit in changing encryption keys; we now explore methodologies.

INSECURE CONFIGURATIONS

Consider a group of hosts using just 15% of the bandwidth of an 11Mbit 802.11b network. An attacker armed with suitable but modest tools could determine their shared secret key in around ninety minutes. On a fully loaded 11Mbit network, this attack would take under 15 minutes. Once the key has been compromised the attacker may decrypt any previously spooled encrypted frames, as well as embark on interactive attacks by interjecting malicious messages. Therefore it is important to choose a key schedule that replaces keys rapidly enough to cause any attackers to fall hopelessly behind. Note that the most common key schedule currently employed involves key changes only at the administrator's decision; key lifetimes in excess of a year are not uncommon. To ensure lasting secrecy, an automated approach is required.

A naïve strategy might arrange for a trusted machine to periodically generate a new WEP key and broadcast it to active hosts in a frame encrypted under the previous key. However, after cracking a single WEP key, an attacker needs simply to post-process a journal of subsequently transmitted encrypted messages to find the next key update, and in this manner walk along the chain of key changes up to the current moment. She is now in a position to decipher encrypted traffic, inject her own traffic and follow key updates in real time. Moreover this scheme inconveniences authorised users; whenever a laptop is returned to the wireless network after a period away the device will be unaware of the current key and thus unable to inter-operate. The user must acquire the current correct key, perhaps using a wired workstation to interrogate the key server, and enter it into the mobile device manually.

AUTONOMOUS LOCKSMITH KEY VARIATION

In order for a cohort of machines to synchronously change keys without using the radio medium to distribute cryptographic information it must be possible for each participant, in isolation, to fabricate the shared WEP keys. One approach would be to provide each user with a CD containing a large number of pre-generated keys, along with a corresponding schedule for their use in the future. This requires the distribution of a considerable bulk of data, which will eventually be exhausted. Thus the user must periodically refresh the key material. The moderate storage capacity of a PDA would mean that the key material would require refreshing irritatingly frequently.

The Autonomous Locksmith algorithm operates using a single secret master key, with length on the order of 256 bits, generated from a cryptographically random source and known to each wireless device. This master key is then used to generate WEP keys. The WEP key is changed at regular intervals; our prototype implementation switches keys every minute. Each WEP key is generated by encrypting the Unix timestamp for the start of each interval under the master key using a block cipher such as AES (Daemen et al. 1999). Each device can independently determine this WEP key using only the master key, which is secret, and UTC, which is common knowledge.

The Autonomous Locksmith avoids necessitating atomic key changes, and the associated tight coupling of local clocks, by using the ability of commonly deployed 802.11b hardware to simultaneously decrypt frames using four keys. We set the decryption keys as follows:

Slot 1: make_wep_key(interval + 1)	transmitter's clock is faster than receiver's
Slot 2: make_wep_key(interval)	transmitter's and receiver's clocks match
Slot 3: make_wep_key(interval - 1)	transmitter's clock is slower than receiver's
Slot 4: make_wep_key(interval - 2)	transmitter's clock is much slower than receiver's

Transmitted traffic is always encrypted under what the transmitter believes to be the correct current key (slot 2 in our example), while frames may be received from peers who are either still using the previous key, or have already switched to the next interval's key. Individual devices may therefore asynchronously change keys; clock skew of up to an entire interval is acceptable. This key-windowing greatly simplifies implementation and removes packet loss that would otherwise occur at interval boundaries. Once connected, devices can rectify local clock drift using NTP (Mills 1992) against the local stratum.

Devices with highly erroneous clocks joining the network may require the user to type in the current time from an accurate wristwatch, or may use a Navstar GPS (NATO 1991) or other method of wireless UTC distribution to determine the correct time unaided. In practice if the clock is slightly skewed it would not take long to scan backwards and forwards from the best available estimate of UTC in an attempt to join the network.

Analogous to military IFF challenge/response protocols (1973), an attacker may crack as many WEP keys as they desire, thus accumulating sample {interval_time, WEP_key} tuples, without being able to predict future WEP keys. WEP keys can be predicted only by cracking the underlying block cipher—AES—to reconstruct the 256 bit secret master key. Furthermore, since the 256 bit key is good for extended periods it need not be changed in the lifetime of the wireless network; users can simultaneously enjoy increased security and reduced administration. Kerkhoff's "memorability" requirement (Kerkhoff 1883) is satisfied, since just 64 hexadecimal characters suffice to express the master key—it is not unwieldy.

This technique does not tackle problems arising from a compromise of the master key: the network administrator must then promptly issue a new master key. It is essential that the master key is not distributed over the wireless network; in practice it takes very little time to enter 64 hex digits on a keyboard. The Autonomous Locksmith provides greatly improved long-term secrecy over WEP; however it does not increase the security of any individual packet, since it is still possible to brute-force a given WEP key.

The Autonomous Locksmith is simple enough to be implemented on a smart-card. This would increase the security of the master key, since the 802.11b hosts would simply use the smart-card as an oracle to compute keys for any given time interval and would never know the secret master key themselves. To compromise the key one would have to compromise the smart-card; this reduces the Trusted Computing Base significantly.

An example implementation of the Autonomous Locksmith is available for Linux:
http://sowerbutts.com/locksmith/

CONCLUSIONS

Motivated by the desire for long-term secure communications using the commodity 802.11b hardware already deployed, a practical technique to strengthen WEP secrecy through frequent key changes was developed. A 256 bit shared secret master key seeded an AES block cipher and the current time was encrypted to generate WEP keys at periodic intervals. Our prototype deployment proved key windowing to be a valuable technique in tolerating clock skew and removed packet loss due to loosely coupled clocks.

In the age of Information Warfare protection from casual crackers and industrial espionage can determine the commercial futures of small- and medium-sized businesses. Attacks on wireless networks are "unproportionate" (Overill 2001)—the cost of defence greatly exceeds the cost of attack—and, like TEMPEST attacks (van Eck 1985, Kuhn et al. 1998), can be highly damaging and difficult to detect. The technique presented here is a useful defence in a war over access to information.

ACKNOWLEDGEMENTS

John Fawcett receives an EPSRC grant and CASE award from AT&T Laboratories, Cambridge to study for a PhD at the Laboratory for Communications Engineering. The authors are grateful to Frank Stajano for his advice and comments.

REFERENCES

Borisov N, Goldberg I and Wagner D (2001). *Intercepting mobile communications: the insecurity of 802.11 (draft).* [On-line]
http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

Daemen J and Rijmen V (1999). *AES Proposal: Rijndael* AES Algorithm Submission, September 1999.

Fluhrer S, Mantin I and Shamir A (2001). *Weaknesses in the Key Scheduling Algorithm of RC4.* Proceedings of Selected Areas of Cryptography (SAC), August 2001.

IEEE (1999). *IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*: Higher speed Physical Layer (PHY) extension in the 2.4 Ghz band. Designation 802.11b-1999.

Kerkhoff A (1883). *La Cryptographie Militaire,* Journal des sciences militaries, vol. IX, pp. 5–38, Jan. 1883, pp. 161–191, Feb. 1883.

Kuhn MG and Anderson RJ (1998). *Soft tempest: hidden data transmission using electromagnetic emanations.* Proceedings of the 2nd Workshop on Information Hiding, Portland, Oregon, April 1998.

Mills, D.L. *Network Time Protocol (Version 3) specification, implementation and analysis.* Network Working Group Report RFC-1305, University of Delaware, March 1992, 113 pp

North Atlantic Treaty Organisation (NATO, 1991). *Technical characteristics of the Navstar GPS (public release).* June 1991.

Overill, RE (2001). *Information warfare: battles in cyberspace.* IEE Computing & Control Engineering Journal, June 2001, pp 125—128.

Van Eck W (1985). *Electromagnetic radiation from video display units: an eavesdropping risk?* Computers & Security 1985(4), pp 269-286.

Walker J (2000). *Unsafe at any key size; An Analysis of the WEP encapsulation*. 802.11 committee, October 2000.

Walker J (2001). *An Inductive Chosen Plaintext Attack Against WEP/WEP2*. Presented at 802.11 subgroup on security meeting, Orlando, May 2001

In-depth Analysis on the Web Server Behavior

Shu Wenhui[1], and Tan T H, Daniel[2]

[1] *Information System Research Lab, School of EEE*
Nanyang Technological University, Singapore
E-mail: P149115018@ntu.edu.sg

[2] *Center for Education Development*
Nanyang Technological University, Singapore
E-mail: ethtan@ntu.edu.sg

ABSTRACT

With the growing concerns of confidence with today's web-based information, effective methods are needed to secure web content. This paper applies the "correlation-digging' method into access log provided by the web server. It makes an in-depth analysis of the web server behavior and properties. We present a solution by extending ripple effect analysis into a two-layer intrusion detection system architecture. Experiment results have shown that by digging the correlation between all the abnormalities, rate of the false positive can efficiently be decreased.

Keywords: Security, Intrusion Detection, Ripple Effect Analysis, False Positives

INTRODUCTION

As a window opened to the public, web server may be that single point that outsiders glimpse the corporation network. It can become the focal point of a threat. When that entry point is compromised, the corporation network can become vulnerable. With the growing concerns and confidence in today's web-based information, effective methods are needed urgently to secure web content.

Since 1980, the research on intrusion detection (ID) has produced a wide range of solution strategies to check the violations against security policy. As a preventive method, ID monitors the events occurring in a computer system or network, analyzing them for signs of security problem. The ad hoc presumption for and IDS is that normalcy and anomaly will be accurately manifested in the chosen set of these events.

Till now, Many models have been proposed and implemented. Wenke Lee et al (1999) used data mining techniques to discover consistent and useful patterns of system features that describe program and user behavior. Association rules and frequent episodes algorithm were adopted to compute the intra- and inter-audit record patterns.

Calvin Ko et al (1999) developed a formal framework for specifying the security relevant behavior of programs, on which they based the design and implementation of a real-tem IDS for a distributed system. Such an approach can detect attacks caused by monitored programs, including security violations caused by improper synchronization in distributed programs.

Specially, some ID models have been dedicated to the security of the web server. "Web-safe" models the security-relevant behavior of a typical web server through static and dynamic profiling (Zhu & Tan, 2000). These include reading files, writing files, executing programs or processes. The mismatch between the pre-constructed profile and real-time behavior will be regarded as abnormality.

Nevertheless, ID is still a young and immature technology and a gulf exists between theoretical and practical aspects. One of the biggest problems facing IDS (Intrusion Detection System) is the number of false positives and false alarms. It has the effect of de-sensitizing alarm notifications.

Based on this understanding, a two-layer mechanism was proposed (Shu & Tan, 2001) to secure web-based database systems. The first layer models the behavior for each kind of data source and the pre-alarm is triggered when abnormal behavior is occurred. The second layer is dedicated to "digging" the correlation between the pre-alarms.

By integrating the pre-alarm with alarm content, such a mechanism can efficiently lower the false positives and lessen the conflict between the scope of monitoring and memory requirements. Preliminary experiments have shown its efficiency on the profiling and also resulted in the investigation of an efficient solution to find the correlation between the abnormal events.

This paper applies a 'correlation-digging' method into the access log provided by the web server. It makes an in-depth analysis of the expected and defined web server behavior. Not only can it act as an independent method to protect the web server against malicious intrusions, it can also provide a basis of an efficient implementation of a correlation digging method for the two-layer mechanism.

In this paper, a brief overview of the main threat towards the web server is given. Multiple features in the profiling steps are described. Experimental data and results are then presented. They show that simple feature-based profile can easily lead to high rates of false positives. The ripple effect analysis algorithm to dig for the correlation existing in the different abnormalities is applied. The observed result shows that the false alarm rate was efficiently lowered.

MULTIPLE FEATURE PROFILING

A Solaris-based Apache Web Server is used for the case example. The Apache server is a very popular choice for the provision of web services. Raw data in its *access.log* reflects detailed information of requests such as remote IP address, time of activity, request method, URL path requested, connection status when response is completed, etc. These related fields will be extracted from each record. The IDS is designed to, automatically, first profile the behavior and properties of web service based on these multi features extracted from log file. The selected features would aid in identifying characteristic of future attacks against the web service.

Threat Towards Web Server

Generally, software-based threats against a web server can be classified in three categories:

- Exploiting vulnerabilities of the host, including bugs of other system services running on the same hardware system;
- Exploiting vulnerabilities of the web service *per se*, such as sending malicious HTTP requests to mount denial of service (DOS) attacks, exploiting the buffer overflow bug of the web service, etc;
- Exploiting vulnerabilities of scripts, which are executed by the web service in response to user requests, including CGI (Common Gateway Interface) and Server Side Includes (SSI), etc.

Typically, most web server exploits are based on CGI attacks (Rubin & Geer, 1998). CGI vulnerabilities may appear in the HTTP service, HTTP protocol, and environment variables or data input using 'GET' and 'POST'. Unsafe use of input data is the main source of CGI security holes, usually encountered in combination with improper use of the shell. Errors of this nature can be made in nearly any language, on any platform.

Feature Extraction

Based on the understanding of the threats, the following three features to generate behavior profile for the web server is done.

- Collect status codes
  HTTP status codes are represented by three-digit code. The first digit classifies the message into a class of response; the last two digits are used to identify a specific error within a message group. These status codes provide the information of the status of the web service. Accordingly, anomalous behavior can be reflected by such error messages.

  For example, if the web server starts returning multiple '404 Unauthorized' messages, the site might be experiencing a search for vulnerable (non-existent) CGI's. Any failed 404 (actually 40*) could also indicate a broken link or a web probe, and could possibly be an indicator of potential attacks or an overloaded server.

- Monitor multiple requests from the same IP address
  An interesting activity to observe is sustained browsing activities from a single IP address over a relatively short period of time. If a host connects to the web server and engages in unusual activities (including the exploring of multiple links), it can be a precursor indicator of an impending attack. Information-gathering through non-malicious means is a good way to stage a preliminary assessment of a target while staying 'buried in the noise'. The 'same host' feature is examined by the count of the connections to the web server.

  In addition, this can be extended to multiple IP addresses that are either related by sub-nets (such as 155.69.223.x), or by blocks (such as multiple Class C's assigned to one ISP), or by geographic location.

- Look for '200' status codes, and search for /etc/passwd (or similar) in the URL/URI.
  Looking for successful connections (200's) can yield interesting insights. This feature may consider looking for readable directories, for example, or a successful URL which referenced /etc/passwd, /etc/shadow, or some system control file.

Also as another example, normal logs would not usually expect *.asp* and *.dll* requests for sites using Netscape servers operating under Unix. Such instances could indicate that possible CGI vulnerability scanners which did not bother checking first the web server type; instead it “bashes” the Unix servers with such requests.

A crucial issue here is the tradeoff between model accuracy and model cost. Knowing which kind of feature to extract to build the profile model is essential. Some current work is to develop on the automatic feature extraction through a learning stage.

Multiple Feature Profiling

Based on the NIDES statistical component (Javitz & Valdes, 1994), a relatively simple monitor technique was deployed. NIDES uses the idea of 'decay' to generate long-term and short-term profiles with minimal calculation and memory resources.

According to the captured features, frequency distribution vectors are formulated. Assume that a vector in n classes is scaled. The k th measure for a frequency distribution vector v_k is defined as v_k=$[v_{k1},v_{k2,...,}v_{kn}]$. Suppose m measures are adopted to generate a profile, then the overall monitored characteristics of the data module will be described in the matrix:

$$V=\begin{pmatrix} v_1 \\ v_2 \\ \\ v_m \end{pmatrix}=\begin{pmatrix} v_{11} & \cdots & v_{1m} \\ \cdots & \cdots & \cdots \\ v_{m1} & \cdots & v_{mn} \end{pmatrix} \qquad [1]$$

Consider the contribution of previous data, the aging rate r is introduced into the profile generation as follows:

$$V_{new}=rV_{old} \qquad [2]$$

The long-term and short-term profiles will be then generated respectively. Long-term profiling, based on a period like a 24-hour day, describes the expected probability distribution. Short-term profiling, performed on an audit record basis, acts as the observation.

For the i th day and the k th record, the updating of the profile matrix is given by

$$LP_{i+1}=r_l LP_i+M_i \qquad [3]$$

$$SP_{k+1}=r_s SP_k+M^{'}_{k+1} \qquad [4]$$

where LP_i denotes the long-term profile matrix till the i th day. SP_k is the matrix described the short-term profile after receiving the k th record. r_l and r_s are the aging rates for the long-term and short-term profiling. M_i reflects the frequency distribution matrix after the analysis on the whole day's audit records. $M^{'}_k$ denotes the frequency distribution matrix for the single record.

After the analysis on each record, the difference between two profiles will be determined. The traditional way is χ^2 testing. The formula for testing the goodness of fit is as follows:

$$D_i=\sum_{j=1}^{n}\frac{\left\{s_{ij}-\sum_{k=1}^{n}s_{ik}\frac{l_{ij}}{\sum_{m=1}^{n}l_{im}}\right\}^2}{\sum_{k=1}^{n}s_{ik}\frac{l_{ij}}{\sum_{m=1}^{n}l_{im}}} \qquad [5]$$

Such a statistical analysis method evaluates the deviation of the recent behavior with the expected pattern recorded in the history profile. If the deviation is significant, the corresponding data source will generate a pre-alarm. When enough and/or the correct combinations of pre-alarms are set, a trigger will be activated to report the suspicious behavior.

Experimental Data

For the performance test, some 'clean data set' was prepared – these data describe routine and normal behavior profile activities. Then, real world traffic was simulated – this included some artificial 'abnormal data' in the test set to indicate anomalous web service behavior. In the setup, as the set of abnormal data was quite small in proportion to the larger set of normal training data, the former was duplicated and distributed. In the test data set, it ultimately had a collection of 995 records, including 47 records for web scanning, 3 records which successfully snatch the sensitive info from the server through a designed malformed CGI scripts, 134 records simulating DOS behavior, and 7 records for the false positive test.

Figure 1: Deviation Score Observed Based on Multiple Features

Figure 1 shows the deviation score observed during our test. Fig 1a represents the status code monitoring. The activities of the 'web scanning' are represented in the data range 383 to 414 (on the axis). The graph exhibits a sharp spike when this malicious behavior was encountered. The top of the spike increases to 1.7369, a value far above the norm. Spikes were also observed between data points 180 and data 741 – these indicated the false positive test. By applying the threshold-judge method, these two fields will be labeled as an intrusion candidate.

In these tests, we took advantages of security holes in a malformed CGI to transfer several sensitive files through web server. Fig 1b shows a peak to indicate its presence. The results from sourceIP request monitoring are displayed in Fig 1c. From record 860, a DOS attack against Apache server was simulated. It can be seen that requests from the IP address escalating than usual.

In a large network, relying on the feature profiling can lead to high false positive (see Fig 1a). False positive (or the 'cry wolf' phenomenon) is a serious problem facing IDS today. It has the effect of de-sensitizing alarm notifications. The 'correlation digging' method in Shu & Tan (2001) the proposed two-layer system, a ripple effect algorithm is applied that has a pre in-depth analysis stage. Such novel architecture has the effect of lowering such false alarms.

RIPPLE EFFECT ANALYSIS

Yau (1999) considered inherent security relations among multiple network nodes to achieve accurate result. SDR (security dependency relation) is defined to describe these relations. Ripple effect analysis (or REA) is used to detect, assess, and prevent intrusions based on SDRs. The ripple effect analysis is extended here, and it defines CF (correlation factor) to describe the correlation among suspicious behavior existing in different features. CF is automatically constructed when abnormal behavior occurs in the access log.

POI (probability of intrusion) is used to denote how probable an intrusion may have occurred. It is calculated by normalizing the deviation score in each feature profiling. Ripple effect analysis algorithm will extract all the affected subjects and collect their POIs. All subjects to be checked will be stored in a set Q. All affected subjects found will be stored in another set AF.

From profiling based on multiple features, the POI is computed for each feature. If POI is smaller than a lower boundary, it will be labeled as *normal* behavior. If the POI value is greater than or equal to an upper boundary, the record is regarded as indicated of *intrusive* behavior. If the POI is greater than or equal to the lower-boundary but smaller than the lower-boundary, it will be assigned *suspicious*. Such an approach will effectively lowered the number false positive.

For the ripple effect analysis, the CF engine will put all the abnormal subjects into Q and store the abnormal relation in CF library. REA will select one subject from Q, and determine all elements that contain this subject from the CF library. For each new subject found, if the corresponding POI has the *suspicious* label, it will add it into Q. This process is repeated till the Q is empty.

The final step for by REA is to calculate the final POI of the whole web service:

$$POI_{system} = 1 - \prod_{for\ each\ affected\ subject\ S} (1 - POI_s) \qquad \text{- [6]}$$

where POI_s denotes the POI of the subject S.

Experiment

The REA algorithm was applied in the above experiment. The parameters are define as:

lower-boundary=0.3, upper-boundary=0.5

From the multiple feature profiling, the POI from each feature is:

Feature 'Status Code': $IP\ A : POI_{A1} = 0.45$
$IP\ A : POI_{A2} = 0.4$
$IP\ B : POI_{B} = 0.3$

Feature 'File Stolen': $IP\ A : POI_{A} = 0.45$

Feature 'Same Source Request': $IP\ A : POI_{A} = 0.2$
$IP\ B : POI_{B} = 0.25$
$IP\ C : POI_{C1} = 0.5$
$IP\ C : POI_{C2} = 0.6$
$IP\ D : POI_{A} = 0.3$

Web probing from an IP address A was conducted, and allowed to steal sensitive files via the web service. In IP B, false positives were tested, while DOS intrusion was simulated on IP C.

For the REA algorithm, the final POI was calculated as:

$$IP\ A : POI_{SYSA} = 1 - (1 - 0.45)(1 - 4)(1 - 0.45)(1 - 0.2) = 0.8548$$

$$IP\ B : POI_{SYSB} = 1 - (1 - 0.3)(1 - 0.25) = 0.475$$

$$IP\ C : POI_{SYSC} = 1 - (1 - 0.5)(1 - 0.6) = 0.8$$

$$IP\ D : POI_{SYSD} = 1 - (1 - 0.3) = 0.3$$

Thus, the values of POI in IP address A and C are higher than their initial individual scores from the multiple feature profiling and also much higher than the upper boundary. The IDS can conclude that an intrusion has occurred. In the case of IP B where the false positive test was conducted, the POI score was lower than the upper boundary – thus no (false) alarm to indicate an intrusion instance.

CONCLUSION

This paper describes a generic IDS model for in-depth analysis of web server behavior. The design and architecture of such a model is proposed to simulate the two-layer mechanism of an earlier work. It can be usefully applied to detect both misuse intrusion and anomaly intrusion.

Behavior profiling based on multi-feature can lead to high false positives. To achieve accurate results, ripple effect analysis is applied to dig the correlation among the various abnormal behaviors. It has been shown that REA is very useful to improve the performance of the traditional feature profiling method, and thus improve IDS performance

However, there are challenges to be addressed in a large networks with heavy traffic in collecting and categorizing all POIs – this is due to the numerous clients visiting the web server. A big CF library may introduce the high overhead to the system. An alternative would be to track only identified or danger-profiled users.

Other possible limitations include smart intrusions that does not leave a trace or abnormal trail in the web server log. Also, as such methods are based on the log file, a 'store and forward' approach might not result in real time detection-response.

REFERENCES

Calvin Ko, M.Ruschitzka , K.Levitt(1999). *Execution Monitoring of Security-Critical Programs in Distributed Systems: A Specification-based Approach.* In Proceedings of the 1997 IEEE Symposium on security and privacy.

Javitz H S and Valdes A, (1994). *The NIDES Statistical Component: Description and Justification.* Technical Report, SRI International, California.

Rubin A D and Geer D E (1998). *A Survey of Web Security.* IEEE Jr. Computer .Volume: 31 Page(s): 34 -41.

Shu W and Tan D T H (2001). *A Novel Two Layer Mechanism for Securing Web based Database Systems.* Computer Software and Applications Conference, 2001. COMPSAC '01. Proceedings. The Twenty-Fifth Annual International.

Wenke Lee, S.J.stolfo, and K.W.Mok(1999). *A data mining framework for building intrusion detection models.* In Proceedings of the 1999 IEEE symposium on security and Privacy.

Yau S S and Zhang X (1999). *Computer Network Intrusion Detection, Assessment and Prevention Based on Security Dependency Relation.* Computer Software and Applications Conference, 1999. COMPSAC '99. Proceedings. The Twenty-Third Annual International, Page(s): 86 -91.

Zhu H and Tan D T H (2000). *Secure Web Server through Behavior Modeling.* In Proceedings of the 1st International Conference on Internet Computing, Las Vegas, US.

ID Based Key Distribution Protocols for Mail Systems

Wei-Chi Ku[1] and Sheng-De Wang[2]

[1]Department of Computer Science and Information Engineering
Fu Jen Catholic University, Taipei 242, Taiwan, R.O.C.
E-mail: wcku@csie.fju.edu.tw

[2]Department of Electrical Engineering
National Taiwan University, Taipei 106, Taiwan, R.O.C.
E-mail: sdwang@hpc.ee.ntu.edu.tw

ABSTRACT

To use the secret key cryptosystem for efficient message protection, a key distribution protocol is required for dispatching secret keys to the communicants. The ID based key distribution protocol for mail systems is a protocol that can dispatch the secret keys without on-line key centers and interaction between the communicants. A family of three similar ID based key distribution protocols for mail systems are reviewed. We show that even the most secure protocol of the family remains vulnerable to the replay attack and the unknown key share attack. Then, we describe an improved protocol that has better security.

Keywords: Key distribution, cryptanalysis, replay attack, unknown key share attack.

INTRODUCTION

To use the secret key cryptosystem for efficient message protection, it is required to dispatch the secret keys to the communicants. A key distribution protocol is the protocol that can solve this problem, i.e., it can be used to provide the basic security infrastructure for secure communications, and can also be referred to as the key exchange protocol, the key establishment protocol, or the digital envelope protocol. The key distribution protocol can be either centralized or distributed. The centralized key distribution protocol needs the help of on-line key centers while the distributed key distribution protocol doesn't require on-line key centers. The ID based key distribution protocol is a distributed protocol that can efficiently establish a secret key between the communicants, and can be categorized into two classes (Tanaka 1991): interactive and non-interactive. Since the non-interactive ID based key distribution protocol does not require the interaction between the communicants, it can also be applied to mail systems and thus is also referred to as the ID based key distribution protocols for mail systems. The non-interactive ID based key distribution protocol can be further classified into two types, one that doesn't need user's public information, e.g., (Tanaka 1991, Okamoto 1986, Okamoto 1987, Okamoto1989a, Shieh 1997), and the other one that requires user's public information, e.g., (Tanaka 1991, Okamoto 1989b, Tsai 1990). This research focuses on the second type of protocols because the first type of protocols is vulnerable to the conspiracy attack (Tanaka 1991).

Okamoto and Tanaka (Okamoto 1989b) proposed the first ID based key distribution protocol for mail systems. A key center constructs an RSA cryptosystem (Rivest 1978), in which p and q are two secret large prime numbers, $n = p\cdot q$ is the modulus, e is the public exponent, and d is the private exponent, i.e., $e \cdot d \equiv 1 \bmod \phi(n)$, where $\phi(n) = (p\text{-}1) \cdot (q\text{-}1)$. The key center then publishes n, e, and g, which is a primitive element in both GF(p) and GF(q). The key center computes:

$S_i = \mathrm{ID}_i^{-d} \bmod n$ *(Equation 1)* for each user i and delivers S_i to the user i through a secure channel. The key center computes the user i's public information x_i as in the following:

$x_i = g^{e \cdot Si} \bmod n$ *(Equation 2)*
and puts x_i into the public directory.

Let A and B denote the sender and recipient of a secret mail. To send the mail to user B, user A retrieves x_B from the public directory, selects r_A (an integer $\in [1, n\text{-}1]$), and computes y_A and his mail key K_A as in the following:

$y_A = S_A \cdot g^{rA} \bmod n$ *(Equation 3)*
$K_A = x_B^{rA} \bmod n.$ *(Equation 4)*

User A then encrypts the mail with key K_A ($= g^{e \cdot rA \cdot SB} \bmod n$), and sends ID_A, y_A, and the encrypted mail to user B who computes his mail key K_B as in the following:

$K_B = (y_A^{e} \cdot \mathrm{ID}_A)^{SB} \bmod n,$ *(Equation 5)*
and then decrypts the mail with key K_B ($= g^{e \cdot rA \cdot SB} \bmod n$).

However, the Okamoto-Tanaka protocol is vulnerable to the forgery attack (Tsai 1990). Additionally, the key center can easily compute K_B since he knows S_B. Tsai and Hwang (Tsai 1990) revised the Okamoto-Tanaka protocol, by modifying x_i and K_A as in the following:

$x_i = S_i \cdot g^{Si} \bmod n$ *(Equation 6)*
$K_A = (x_B^{e} \cdot \mathrm{ID}_B)^{rA} \bmod n.$ *(Equation 7)*

Unfortunately, the Tsai-Hwang protocol remains vulnerable to the key center attack since the key center can easily compute K_B. Tanaka and Okamoto (Tanaka 1991) proposed a protocol (the Tanaka-Okamoto protocol) that modified x_i, K_A, and K_B of the Okamoto-Tanaka protocol: x_i is generated by user i as in the following equation:

$x_i = S_i \cdot g^{Ri} \bmod n$ *(Equation 8)*
where R_i is an integer $\in [1, n\text{-}1]$ chosen by user i, K_A is generated according to *(Equation 7)*, and K_B is generated as in the following equation:

$K_B = (y_A^{e} \cdot \mathrm{ID}_A)^{RB} \bmod n.$ *(Equation 9)*

Consequently, the mail key ($K_A = K_B$) is $g^{e \cdot rA \cdot RB} \bmod n$. As explained in (Tanaka 1991), the Tanaka-Okamoto protocol can prevent against the key center attack. In this paper, we will show that the Tanaka-Okamoto protocol remains vulnerable to two attacks. Then, an improved protocol will be described.

CRYPTANALYSIS OF THE TANAKA-OKAMOTO PROTOCOL

We first illustrate how the Tanaka-Okamoto protocol (Tanaka 1991) is vulnerable to the *replay attack*. Let K_A^{*} denote an old mail that user A employs to encrypt an old mail for user B, y_A^{*} represent the data used by user B to compute the corresponding mail key K_B^{*}. The attacker can replay y_A^{*} to user B so that user B will falsely use K_B^{*} as his new mail key. Therefore, the attacker can fool user B into believing the replayed old mail, and can also impersonate as user A to forge any mail if he knows K_B^{*}.

Next, we illustrate how the Tanaka-Okamoto protocol (Tanaka 1991) is vulnerable to the *unknown key share attack* (Yen 1999). Since the equation $(x_B)^e \equiv (S_B)^e \cdot (g^{RB})^e \bmod n$ always holds, the attacker can easily compute $g^{e.RB} \bmod n$, and $u_1 = (g^{e.RB})^k \bmod n$ for any integer k. The attacker can replace x_B with $x_B \cdot u_1 \bmod n$ while user A retrieves x_B from the public directory so that user A will compute $K_A' = (g^{e.rA.RB})^{(e.k+1)} \bmod n = K_A^{(e.k+1)} \bmod n$ and falsely take K_A' as his mail key. Similarly, the attacker can easily compute $g^{e.rA} \bmod n$ since the equation $(y_A)^e \equiv (S_A)^e \cdot (g^{rA})^e \bmod n$ always holds. The attacker can compute $u_2 = (g^{e.rA})^k \bmod n$ and replace y_A with $y_A \cdot u_2 \bmod n$ when user A sends y_A. Subsequently, user B will compute $K_B' = (g^{e.rA.RB})^{(e.k+1)} \bmod n = K_B^{(e.k+1)} \bmod n$ and falsely take K_B' as his mail key. Hence, users A and B share a mail key that is not the one supposed by them. Although this mail key is unknown to the attacker, it reveals a weakness that may be employed to carry out other attacks against the protocol (Yen 1999).

THE PROPOSED PROTOCOL

The RSA system is constructed the same as in the Tanaka-Okamoto protocol except that the public exponent e is fixed at three to reduce computational overhead. The key center selects and publishes a constant integer c that is larger than all the possible timestamp values but is smaller than n. The system clocks are assumed to be synchronized and the mail servers are assumed to be trust in verification of the timeliness of the received messages. In addition, the channel between the user and his mail server is assumed secure. The user generates his public information according to (*Equation 8*). To send a secret mail to user B, user A retrieves x_B, selects r_A (an integer $\in [1, n\text{-}1]$), and computes y_A according to (*Equation 3*). User A computes K_A as follows:

$K_A = (x_B{}^3 \cdot \mathrm{ID}_B)^{rA.xB.(c-t)} \bmod n$ (*Equation 10*)
where t denotes the time user A performs the computation. User A encrypts the mail with key K_A (= $g^{3.rA.RB.xB.(c-t)} \bmod n$), and sends ID_A, t, y_A, and the encrypted mail to user B's mail server. User B's mail server relays the received message once it successfully verifies the timeliness of t. After user B receives the relayed message from his mail server through a secure channel, he computes K_B as follows:

$K_B = (y_A{}^3 \cdot \mathrm{ID}_A)^{RB.xB.(c-t)} \bmod n$,   (*Equation 11*)
and then decrypts the mail with key K_B (= $g^{3.rA.RB.xB.(c-t)} \bmod n$).

CRYPTANALYSIS OF THE PROPOSED PROTOCOL

Resistance to the Forgery Attack

The attacker must find two integers y and r that satisfies the following equation if he wants to impersonate as user A to send mail:

$y^3 = \mathrm{ID}_A{}^{-1} \cdot g^{3.r} \bmod n$.   (*Equation 12*)

Given y, to solve (*Equation 12*) for r is equivalent to solve a discrete logarithm problem. Given r, to solve (*Equation 12*) for y is equivalent to break RSA. Because there is only one RSA constructed, the use of low public exponent ($e = 3$) will not degrade the security of the protocol (Shieh 1997).

Thus, the proposed protocol can resist the forgery attack.

Resistance to the Replay Attack

Let K_A^* (= K_B^*) denote the old mail key employed by user A to encrypt a mail for user B, while t^* represents the corresponding timestamp. The attacker must find a timestamp $t > t^*$ that satisfies the equation $K_B = K_B^*$ if he wants to fool user B into believing the corresponding old mail when t^* is smaller than the smallest timestamp acceptable by user B's mail server. The proposed protocol can resist the simple replay attack because no attacker could derive t without r_A^* and R_B. Additionally, if the attacker knows K_B^*, he must find a timestamp t that satisfies $(c - t) = k \cdot (c - t^*)$, where k is an integer ≥ 1, so that he can fool user B into believing a forged mail encrypted with key $(K_B^*)^k$ mod n. However, it contradicts the fact that $(c - t^*) > (c - t)$. On the other hand, it is infeasible for the attacker to find t that satisfies $K_B \equiv (K_B^*)^k$ mod n without knowing r_A^* and R_B.

Hence, the proposed protocol can resist the replay attack even if the attacker knows an old mail key.

Resistance to the Key Center Attack

(*Equation 10)* and (*Equation 11*) demonstrate that the key center can compute K_A (= K_B) only if he knows r_A or R_B. However, the difficulty of either computing r_A from y_A or computing R_B from x_B is equivalent to the difficulty of solving the discrete logarithm problem.

Therefore, the proposed protocol can resist the key center attack.

Resistance to the Unknown Key Share Attack

If the attacker chooses an integer k and replaces x_B with $x_B' = x_B \cdot g^{3.k.RB}$ mod n, user A will compute $K_A' = ((x_B')^3 \cdot \mathrm{ID}_B)^{rA.xB.(c-t)}$ mod n, which yields $g^{(3.k+1).rA.RB.xB'.(c-t)}$ mod n. If the attacker replaces y_A with $y_A' = y_A \cdot g^{3.k.rA}$ mod n, user B will compute $K_B' = ((y_A')^3 \cdot \mathrm{ID}_A)^{RB.xB.(c-t)}$ mod n, which yields $g^{(3.k+1).rA.RB.xB.(c-t)}$ mod n.

The proposed protocol can resist the unknown key share attack since it is infeasible for the attacker to find k that satisfies $K_A' = K_B'$.

CONCLUSION

This study illustrated that the Tanaka-Okamoto protocol (Tanaka 1991), the most secure protocol of a family of three similar ID based key distribution protocols for mail systems, remains vulnerable to the replay attack and the unknown key share attack because it doesn't guarantee the freshness and integrity of mail keys.

We have proposed an improved ID based key distribution protocol for mail systems. The proposed protocol can also be applied to interactive systems by using the mail key as the session key for subsequent communications between the communicants. In this application, the timeliness verification of the received message is performed by the recipient himself because there is no mail server involved. Additionally, the secure channel between the user and his mail server is not required.

REFERENCES

Okamoto E. (1986). *Proposal for Identity based Key Distribution Systems.* Electronic Letters 22, pp. 1283-1284.

Okamoto E. (1987). *Key Distribution Systems based on Identification Information.* Proc. Crypto '87, pp. 194-202.

Okamoto E., and Tanaka K. (1989). *Identity-based Information Security Management System for Personal Computer Networks.* IEEE Journal on Selected Areas in Communications 7, pp. 290-294.

Okamoto E., and Tanaka K. (1989). *Key Distribution System based on Identification Information.* IEEE Journal on Selected Areas in Communications 7, pp. 481-485.

Rivest R.L., Shamir A., Adleman L. (1978). *A Method for Obtaining Digital Signatures and Public Key Cryptosystems.* Communications of The.ACM 21, pp. 120-126.

Shieh S.P., Yang W.H., and Sun H.M. (1997). *An Authentication Protocol without Trusted Third Party.* IEEE Communications Letters 1, pp. 87-89.

Tanaka K., and Okamoto E. (1991). *Key Distribution System for Mail Systems using ID-related Information Directory.* Computer & Security 10, pp. 25-33.

Tsai Y.W., and Hwang T. (1990*). ID Based Public Key Cryptosystems based on Okamoto and Tanaka's ID Based One Way Communication Scheme.* Electronics Letters 26, pp. 666-668.

Yen S.M., (1999). *Cryptanalysis of an Authentication and Key Distribution Protocol.* IEEE Communications Letters 3, pp. 7-8.

Intelligent Agents and Their Information Warfare Implications

T. B. Busuttil [1]and M. J. Warren[2]

[1] *School of Computing and Mathematics*
Deakin University, Australia.
E-mail: tbb@deakin.edu.au

[2] *School of Computing and Mathematics*
Deakin University, Australia
E-mail: mwarren@deakin.edu.au

ABSTRACT

Research into Intelligent Agent (IA) technology and how it can assist computer systems in the autonomous completion of common office and home computing tasks is extremely widespread. The use of IA's is becoming more feasible as the functionality moves into line with what users require for their everyday computing needs. However, this does not mean that IA technology cannot be exploited or developed for use in a malicious manner, such as within an Information Warfare (IW) scenario. This paper will discuss the current state of malicious use of IA's as well as focusing on attack techniques, the difficulties brought about by such attacks as well as security methods, both proactive and reactive, that could be instated within compromised or sensitive systems.

Keywords: Information Warfare, Intelligent Agents, Computer Security, Risk Management.

INTRODUCTION

The growing need for information technology users to work more efficiently has been the driving force behind the development of agent technology. Agents are entities that act on our behalf. "Software agents perform tasks for us, learn about our wants and needs and let us carry on with our everyday tasks whilst they complete some of our tasks autonomously" (Vitek & Castagna 1999). Due to the immense amount of information, both formatted and unformatted, which resides across the Internet, agents have a seemingly boundless workplace where tasks such as collection, matching, choosing and sorting of information and data are being started or completed constantly (Sharpe 1997).

Information warfare attacks have also continued to increase in both frequency and effectiveness as new IT and methodologies surface (Black 1996). Just as agent technology can be helpful in the completion of tasks it can also be programmed to act maliciously (Goldschlag et al 1998, Hunter 1999). Agents may be developed from the beginning of the lifecycle to behave in a damaging manner on certain systems (Washington 1995).

Few agent systems have been blatantly attacked and exploited (Wilder & Dalton 1997), however vulnerabilities are apparent within existing systems and the exploitation methods required to cause disruption within agents and agent systems are being reviewed and researched currently (Hohl 1998).

TAXONOMIES OF AGENT TECHNOLOGY

Agents can be deployed across different schemas to complete a required task to a high level of effectiveness and efficiency. There are a number of predominate taxonomies that exist in the field of agents. These are:

- Single static intelligent agents;
- Single mobile intelligent agents;
- Collaborative mobile intelligent agents and
- Multiple-intelligent agent systems.

Single Static Intelligent Agents

A single agent employed to complete user tasks on a commercial system that it is installed on is schematically described as being a single static agent. This is a simple taxonomy where a user provides input, the agent completes its designated task and some output is produced. Security is an issue but in this case the agent tends to be isolated from networks and therefore less prone to IW-based attacks.

The most prevalent use of the single static agent in a commercial environment is within a database as a search agent shown in Figure 1. The user would input a query, the agent then seeks information regarding the query, and outputs information based on the query search.

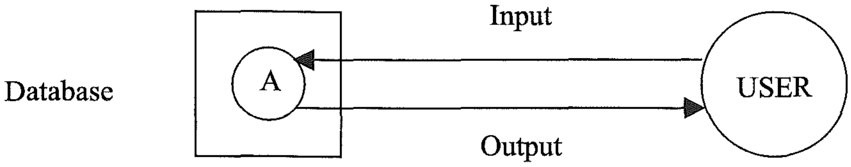


Figure 1: Single Static Intelligent Agent

Single Mobile Intelligent Agents

Mobile agents are useful at finding things that are stored across distributed systems such as the Internet. A single mobile agent can be deployed with the agenda of searching for information distributed across web servers. As the agent is mobile, it is capable of transporting itself from one networked system to the next completing any allocated tasks. Inherently, security is a greater problem than with static agents as the mobile agent may interact with many hosts on many systems (Tschudin 1999) possibly leading to malicious attack toward or from the mobile agent.

Web spiders or Web indexing agents are the most popular uses for single mobile agents. These agents tend to hop from networked system to networked system searching and return indexes of the documents store on servers as shown in Figure 2.

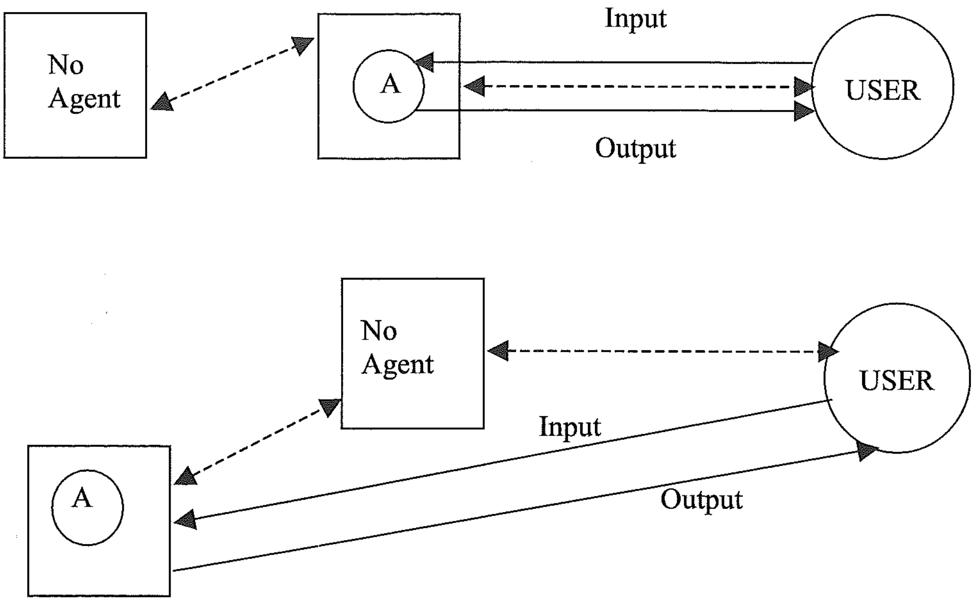


Figure 2: Cycle of a Single Mobile Intelligent Agent

Collaborative Mobile Intelligent Agents

Singular mobile agents have many uses; however, when mobile agents are grouped to complete more complex tasks, such as Internet shopping, the abilities of agent technology are truly seen. The ability of agents to share and learn from information means that the decision making process followed by agents can be refined autonomously. This information exchange and sharing can also lead to security problems within the commercial environment as agent or host sabotage is possible.

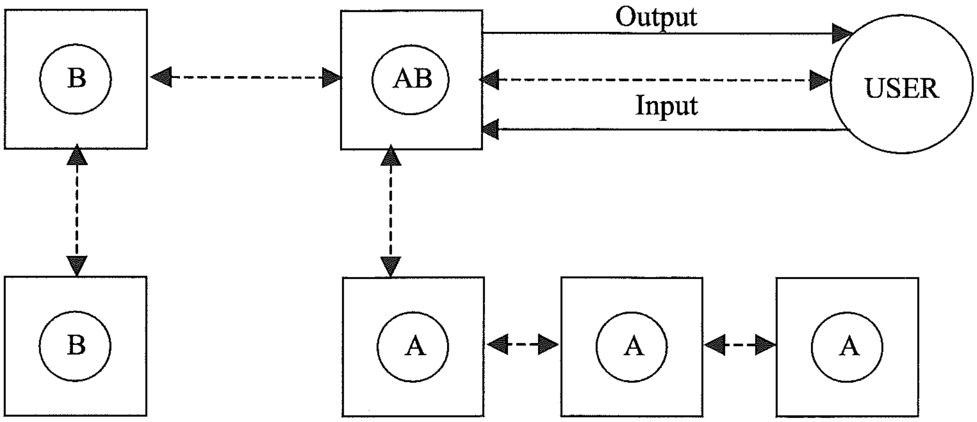


Figure 3: Cycle of Collaborative Mobile Agent System

Multiple Intelligent Agent Systems

Multi-agent systems are similar in schematics to a collaborative agent system, however, in this case the system exists in a more logically and physically secure arrangement where network hosts and agents are all trusted entities or are at least authenticated and certified as being trustworthy. Despite the increased security of this agent taxonomy there are still risks involved with the use of multi-agent systems (Wooldridge & Jennings 1998).

An example of a multi-agent system is a financial investment package. This system searches trusted exchanges and brokerages to find investments for clients, which coincide with customer spending limits and preferred investment type within a secure trade circle as depicted in Figure 4.

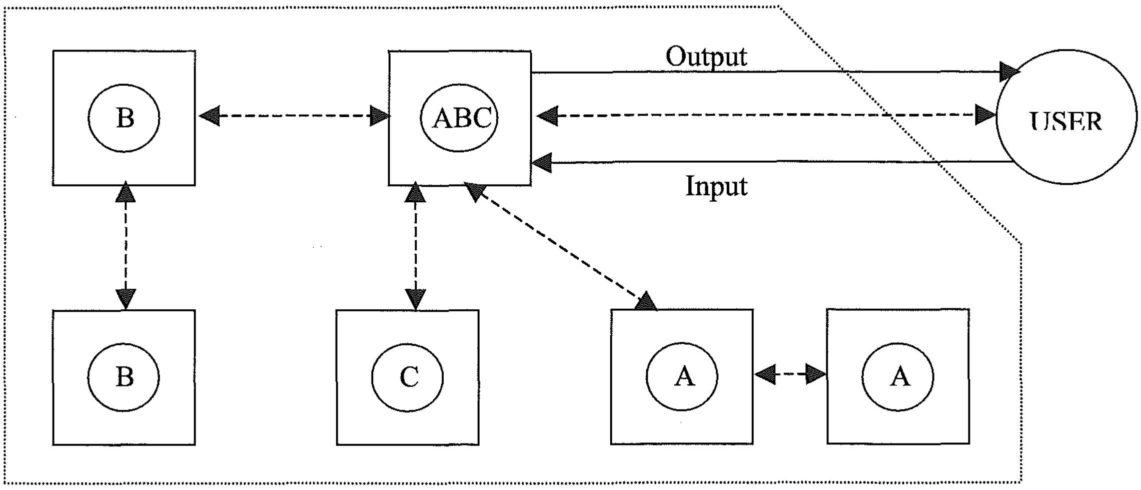


Figure 4: Cycle of a Multi-Agent System

ATTACK TARGETS OF INTELLIGENT AGENTS

Attacks can occur based on when and where processing is taking place. In the following sections this paper will cover the different stages in the information system-IW taxonomy discussed by Cramer (1998) and will also look at the physical stages within an agent schema where an attack may occur.

Information Action Stages

The information systems-IW taxonomy as drafted by Cramer (1998) is made up of the following six categories:

- Information Acquisition;
- Information Protection;
- Information Processing;
- Information Transport;
- Information Management and;
- Information Denial.

These events are tightly coupled to actual occurrences within an agent system and attacks related to agent system-IW would tend to fall into these six categories:

Information Acquisition Attack

An attack that occurs during the information acquisition stage involves disrupting or sabotaging the agent system during the transfer of information from one agent/host to another agent/host (Cramer 1998). One example of this technique of attack would be the addition of a malicious host into an agent system for the prime purpose of deleting, changing or transferring misleading or incorrect information to an insecure agent within the system.

Information Protection Attack

The protection of information is important to the value of the agent system. If information can be tainted then the reliability of data provided by the system is compromised. An attack using a host or agent that renders a system component subject to security vulnerabilities is an information protection attack. This type of attack would normally be associated with the inclusion of remotely accessible, malicious code, which attacks a system entity causing system security failure.

Information Processing Attack

An attack during the information-processing phase within an agent system is would tend to be aimed at a host target or the user system where the agent was originally deployed. If a host is attacked, the information being processed may be compromised. These sorts of attacks could also stem from an outside entity presenting malicious code to either the host or user systems that is then executed, causing processing sabotage or failure (Cramer 1998). The use of agents to actually process data on other hosts as they traverse a MAS can also cause problems as hosts must be stable during processing or data will be lost.

Information Transport Attack

The information transport attack can happen during agent travel across networks or at a malicious host or user. This type of attack is aimed at causing data or agents to be sabotaged or destroyed whilst in transit. The main technique involved in this type of attack is for a host to insert code into an insecure agent with the goal of agent failure. Other techniques exist also, such as the commandeering of a mobile agent so that attacks can be mounted against hosts that are visited by the malicious agent.

Information Management Attack

The management of information is an extremely important process within an information system. An information management attack focuses on creating problems within the databases and other information management software and hardware involved with the storage and organisation of information (Cramer 1998). This method of attack can cause many difficulties for organisations as staff often depends on system reliability. In the case of system failure, working hours, sensitive information and company reputation may be lost. The period for information recovery may be lengthy and costly and in the worst case may never be possible.

Information Denial Attack

This form of attack involves stopping users of a system from accessing a particular piece of information that is required for completing a certain task. The denial of information can be brought about using a number of different attack techniques including use of viruses and other malicious code based attacks (Cramer 1998). The denial of information can be a very inhibitive form of IW as many systems and people are often waiting for access to the same files and data, such as during a login procedure with a single encrypted password file. This type of attack could leave organisations with no option but to shutdown as the organisations information is often the only asset, especially in some e-business models.

Agent System Attack Scenarios

Within agent systems there are three major concerns when looking at security issues. The first is obviously attacks targeting or being waged from outside the system. The other two possibilities are that the host and/or agent could be solicited as either a target or and attacker (Jansen 1999). The Following sections will detail each of the scenarios that can occur in IW situations involving agents.

Agent-to-Agent

An agent-to-agent attack consists of one or more agent within a particular system attack another agent from the local system. This does not mean there is a limit on the size of the agent system, however, the locality of the system is implied by the agent's relation to the current system (Jansen 1999). This type of attack can be directly via agent communication or through use of a host as a method of attacking the target agent.

Agent-to-Host

An agent-to-host attack relies on host vulnerability for success. A scenario for this type of attack is an agent that visits a vulnerable host and executes code that damages or disrupts the deliverable host services. The vulnerability of the host is extremely important as hosts may have proactive or reactive security strategies in place, which could lead a path to the origin of the offending mobile agent. The agent may also be destroyed if it does not interact in the predetermined correct fashion with a protected host.

Host-to-Host

Hosts within agent systems will tend to communicate mainly via the agents within the system. A host may receive directives to insert code within a vulnerable agent which inturn could pass this code to a vulnerable host. The vulnerable host could then be attacked by some payload, which may also travel across communications channels with the vulnerable agent. Another scenario could exist wherein a vulnerable agent may place some sort of triggered code fragment on the vulnerable host so as to perhaps collect information or deny services at a later though still designated date (Jansen 1999).

Host or Outside System-to-Agent

A Host-to-agent attack will on most occasions require the agent to have at some stage interacted with at least one host. The host that attacks the agent does not necessarily have to be malicious. The host could perhaps have been infected with some virus which inturn attacks subsequent visiting agents. Use of hosts to attack agents is possibly the easiest form of attack due to the fact that the vulnerable agent actually resides on the system (Jansen 1999) and can therefore be controlled either manually by a user or autonomously by a system.

PROBLEMS CAUSED BY ATTACKS ON INTELLIGENT AGENTS

The actual damage or disruption caused when agents are used in a commercial IW scenario can vary greatly depending on:

- The size and importance of the agent system being attacked (Gray 1996);
- The amount of disruption and/or damage the attacker wants to cause (Etzioni & Weld 1995) and;
- The security involved with the system being targeted (Tschudin 1999).

Information and Data Manipulation

As information within agent systems is used, perhaps many times per agent execution, the changing of information to some non-preferred value is an attack method that can be used effectively and without extreme risk of apprehension to the perpetrator. The changing of information in the commercial IW sense could lead to incorrect business decisions, such as poor investment, as well as loss of privacy depending on the vulnerability being targeted by the attack.

Information and Data Destroying

This case involves the same parties and problems as information change attacks, however, In this case rather than the information being changed to reflect another value, the information is just deleted or totally obfuscated so that the user is unable to take away any opinion from analysis of the data. Although this attack sounds more dangerous to an organisation than an information change attack, it is often the information change attack that can be more damaging as wrong decisions are more likely to be made based on incorrect complete data rather than incomplete data (Meadows 1997).

Misuse or Overuse of Resources

Software agents are often used as a method of selecting, organising and using web-based services and resources. The autonomy of agents means that difficulties can arise if agents are exploited in a way which allows them to use too many or misuse some of the resources and services they must interact with. This attack technique can cause problems not only within a particular agent system but also to other systems that require interaction with the problematic agent system or other systems that in some way make contact with a vulnerable agent from the compromised systems.

Misinformation

A misinformation attack is a way of confusing an enemy user or system into believing or using some tainted data within a normal execution procedure. This information may be skewed data sets, incorrect news reports etc. The use of agents to maliciously misinform other systems is a method that could be extremely destructive in current world situations where peace can be dependant on comments made by world-leaders. If details of speeches were to be misreported this could lead to disruptive behaviour on the world stage (Black 1996), which shows the importance of protection from this method of attack.

Disabling Agents

The disabling agents within systems can cause major disruptions or may go unnoticed. This form of attack is heavily dependent on the reliance an organisation has on the particular agent that is destroyed. In a system where there are many threads and many agents all completing similar tasks the loss of a single agent would cost very little in efficiency. In the case of a business being heavily reliant on a single agent-system the results of an attack of this nature could be catastrophic as information regarding business transaction and other sensitive data could be rendered lost and unrecoverable.

Disabling Hosts

The disabling of hosts is more costly than the disabling of agents. The loss of hosts may lead to host system failure. The loss of a host may also mean that agents are destroyed or discontinued, as they are unable to meet a particular system goal. The disabling of a host can be in two forms. The first loss could be from the agent system point-of-view only so that the host computer may still operate. The second and more severe host attack would leave the host computer totally unusable.

Actual Security Breaches Involving Agents

Software Agents that damage other systems and software have been around for many years, however, they have commonly been referred to as viruses (Goldschlag et al 1998). It has been evidenced since Cohen (1984) put forward early research on viruses, that the virus is basically an agent with varying degrees of intelligence and mobility. The major issue with viruses being regarded as agents is that viruses are, for the most part, created for malicious and/or disruptive purposes. We have seen the Code Red/Code Red II worm cause disruption and damage to many systems as the polymorphic denial of service attack payload forwards itself to remote systems (CERT 2001). “Viruses and worm programs carry out the bidding of their designer autonomously by creating duplicates of itself among many computers” (Denning 1990). The use of the words intelligent and mobile when discussing agent technologies does not imply that the agent is to be used for perceived good or bad they are only characteristics of said programs.

Aside from the issue of viruses there are also more complex agent systems that have been and are being developed currently (Cramer 1998) which could be greatly compromised if security measures, both proactive and reactive, are not built into systems. Any of the aforementioned attacks are possible, as agents, by design are merely *computer programs* that are not only designed to work together, derive intelligent solutions to problems and be mobile but also to have the same vulnerabilities that can be found in most common programs.

DEALING WITH INTELLIGENT AGENT-BASED ATTACKS

Information Warfare threats can be dealt with in a number of ways. These methods tend to fall into two categories shown in Table 1:

Handling Method	Definition
Proactive Handling	Where agent technology is built to prevent attacks occurring
Reactive Handling	Where agent technology is used and problems dealt with as they arise

Table 1: Risk Handling Methods and Definitions

Agent-Based IW is no different to other IW techniques in the sense that proactive and reactive methods can still both be used for risk management (Pellissier 2000).

Risk Management - Proactive or Reactive?

The major differences between proactive and reactive risk management strategies when dealing with agent-based IW are still those of cost in time, money and efficiency. The decision involved in this case is whether to prevent attacks from occurring or to detect them and then deal with them as they arise. Major questions exist as to whether or not mobile-agent systems can be made totally secure as a proactive measure and if so is it still more efficient to solve problems as they occur considering the youth of some of the newer agent technology advances.

Agent or Host as Platform for Security Features?

Another major decision to make is whether to develop security at the host or within the agent. The development of host security is more expensive and difficult to implement as one agent could visit many hosts therefore meaning every host would need to be updated or developed with new security in mind. Developing agent security is seen as a more efficient method of building security into agents. The major problem with this approach is that excess agent code to deal with security may make the agent slow and costly to use on a large scale and therefore less efficient as an information collection solution. The current methods of security being developed or currently in use are shown in Table 2 (Jansen 1999).

Countermeasure	Technique	Security Platform
Signed Code	Reactive	Host
State Appraisal	Reactive	Host
Path Histories	Reactive	Host
Partial Result Encapsulation	Reactive	Agent
Mutual Itinerary Recording	Reactive	Agent
Itinerary Recording with Replication and Voting	Reactive	Agent
Execution Tracing	Reactive	Agent
Software-Based Fault Isolation	Proactive	Host
Safe Code Interpretation	Proactive	Host
Proof Carrying Code	Proactive	Host
Environmental Key Generation	Proactive	Agent
Computing with Encrypted Functions	Proactive	Agent
Obfuscated Code	Proactive	Agent

Table 2: Risk Countermeasure and Handling Table (Jansen 1999)

CONCLUSIONS

This paper has highlighted the current state of agent technologies and how they can be exploited in terms of information warfare attacks. A number of conclusions were reached. Initially there was confirmation from review of literature that IA technology can be exploited for use within an IW campaign. There are also a number of both proactive and reactive security methodologies either in use or being developed currently. The development of host-based security is more expensive but is also more secure. The use of proactive security methods is more expensive to initially develop but provides a more reliable agent system. Despite this fact moves toward proactive security are slow due to the fact that overheads involved with proactive security, especially built within agents, are extremely high and does remove functionality and efficiency from the system. There are a number of possible vulnerabilities and methods of attack associated with agent technology. This is due mainly to the novelty of the technology at present. The new security methods being developed do go a long way toward attempting to deny some of the existing attack methodologies and vulnerabilities within certain agent systems.

REFERENCES

Black, Lt. Col. S. K. (1996). *Information Warfare in the Post Cold-War World.* Ridgway Viewpoints 96-1 USAF, USA.

CERT (2001). *Code Red / Code Red II Worms.* CERT Advisory CA-2001-13, June 19, 2001, CERT/CC.

Cohen F. (1984). *Computer Viruses Theory and Experiments.* DOD/NBS 7th conference on Computer Security.

Cramer M. (1998). Intelligent Agents in Information *Warfare.* InfowarCon '98, Washington DC, USA.

Denning P. (1991). *Computers Under Attack – Intruders.* Worms and Viruses, ACM Press, New York, USA.

Etzioni O.and Weld D.S. (1995). *Intelligent Agents on the Internet.* Department of Computer Science and Engineering, University of Washington, USA.

Goldschlag D., Landwehr C., Reed M. (1998). *Agent Safety and Security.* Naval Research Laboratory, Washington DC, USA.

Gray R. S.(1996). *Mobile-Agent Security.* Dartmouth College, New Hampshire, USA.

Hohl F. (1998). *A model of Attacks of Malicious Hosts Against Mobile Agents.* Institute of Parallel and Distributed High-Performance systems (IPVR), University of Stuttgart, Germany.

Hunter P. (1999). *Spies on Your Hard Drive.* Computer Weekly, United Kingdom, September 1999.

Jansen W. (1999). *Countermeasures for Mobile Agent Security.* National Institute of Standards (NIST), USA.

Jennings N. R. and Wooldridge M.(1998). *Applications of Intelligent Agents.* Queen Mary & Westfield College, University of London, United Kingdom.

Meadows C. (1997). *Detecting Attacks on Mobile Agents.* Center for High Assurance Computing Systems, Naval Research Laboratory, Washington DC, USA.

Pellissier S. V.(2000). *A Brief Overview of Software Agent Applications and Risks.* SANS Institute.

Sharpe R.(1997). *Interrogating the Software Agents.* Computer Weekly, United Kingdom.

Tschudin C. F. (1999). *Mobile Agent Security.* Department of Computer Systems, Uppsala University, Sweden.

Vitek J.and Castagna G. (1999). *Mobile Computations and Hostile Hosts.* Journees Francophones des Langages Applicatifs, February-JFLA99, France.

Washington D.W.(1995). *Onward Cyber Soldiers.* Time Magazine, Volume 146 - No.8, USA.

Wilder C. and Dalton G. (1997). *The World Wide Web Watch – Using Web Agents.* Information Week, Issue 652, CMP Media, USA.

Wooldridge M. and Jennings N.R. (1998). *Pitfalls of Agent-Oriented Development.* Department of Electronic Engineering, Queen Mary & Westfield College, University of London, United Kingdom.

Towards a Framework for Analyzing Information - Level Online Activities

Christopher Lueg

Department of Information Systems
Faculty of Information Technology
University of Technology Sydney, Australia
lueg@it.uts.edu.au

ABSTRACT

Global communication systems allowing virtually unlimited information dissemination have enabled novel ways to affect companies and organizations. Compared to network-level threats, such as Denial-of-Service attacks or break-ins into corporate computer systems, information-level online activities and their threat potential are little understood. In this paper, we look at what can be learned from research on network-level attacks and we discuss first steps towards a better understanding of information-level activities. In particular, we discuss criteria that can be used to analyze information-level activities by example of some actual incidents reported in the literature.

Keywords: Online Activities, Information Dissemination, Characteristics, Framework.

INTRODUCTION

It is now widely acknowledged that computer security is an important topic and the state-of-the-art in computer security provides some protection against threats ranging from hackers trying to break into corporate computer systems to Denial-of-Service (DoS) attacks. Apart from such technically constrained ways to attack corporate systems and networks, evidence exists that it becomes more and more important to be aware of potentially threatening activities that are based on the virtually unrestricted dissemination of certain information. So-called information-level attacks have been defined as attacks that are based on the dissemination of information in such a way that companies, their operations, and their reputations may be affected (Lueg 2001). The primary lever of an information-level attack is the content of a message rather than its form. For example, sending faked but meaningful inquiries to service accounts to eat up human resources would qualify as information-based attack as it is the content of the messages that would provide the lever for the attack. To the contrary, an attack where the content does not matter as in flooding an account with randomly generated messages would qualify as network-level attack.

Compared to network-level activities, information-level activities are little understood. In this paper, we describe work that has been done to help analyze information-level activities. We proceed as follows. First we briefly discuss work on network-level activities and lessons to be learned from this research area. Then we focus on information-level activities and discuss criteria that can be used to analyze incidents by example of actual incidents reported in the literature. Finally, we draw our conclusions and outline future research directions.

ANALYZING NETWORK-LEVEL INCIDENTS

Typically, computer security is associated with what we call network-level incidents. It is an area that is well researched and where comprehensive information is available in the literature. Boulanger (1998), for example, provides a detailed analysis of the stages involved in break-ins. A detailed analysis of DoS attacks can be found in Moore et al. (2001).

In order to assess appropriate reactions once incidents have been detected, it is necessary to be able to distinguish severe incidents from less severe ones. Yasin (1998) quotes a network security specialist claiming that 80% of `intrusions' occur inside an organization and 65-70% of these incidents were due to mistakes. Smith (1998) looked at reports on security accidents used to justify investments into cyber warfare and found that the report of 250,000 hacker intrusions into US Department of Defense (DoD) computers in 1995 seems to be quite an exaggeration. Smith explains that the figure has never been a real number; rather, the figure was an estimate based on 500 actual incidents in 1995 and the assumption that only 0.2 percent of all intrusions are reported. Furthermore, it seems that the figure was inflated by instances of legitimate user screw-ups and unexplained but harmless probes sent to DoD computers. Some of the `DoS attacks' have been compared by security specialists to graffities; hackers attacking the DoD in 1998 have been called the virtual equivalent to a`kid walking into the Pentagon cafeteria' (Smith, 1998).

The most comprehensive approach to classifying security incidents so far can be found in Howard (1997) which is based on an in-depth analysis of incidents reported to CERT between 1989 and 1995. Howard describes an alarming trend in the way how attacks were performed: `the sophistication of intruder techniques progressed from simple user commands, scripts and password cracking, through the use of tools such as sniffers (1993) and toolkits (1994), and finally to intricate techniques that fool the basic operation of the Internet Protocol (1995)'. A second trend was that `as intruder tools became more sophisticated and the size of the Internet grew, the severe incidents involved more attackers operating in many different locations. The newest and most sophisticated techniques allowed the attackers to obtain nearly total obscurity.'

In particular, Howard's (1997) work indicates that it is hard to estimate the severity of an Internet security incident:

> '[...] there is not one obvious measure of the severity of an Internet security incident. Two examples will make this point more clearly. In one incident reported to the CERT/CC, the number of sites involved was 1,563. This incident also involved root break-ins. Using these measures, this was the most severe incident in the CERT/CC records. Closer examination reveals, however, that this incident was actually relatively minor. The incident's duration was only 8 days, while the average duration for all CERT/CC incidents was 16.5 days. The 23 messages to and from the CERT/CC for this incident was only slightly above the average for all incidents (and well within the 54.4 standard deviation). The primary reason for this unusual set of numbers was that this incident involved a sniffer and the sites involved were recorded in the sniffer logs, but apparently not actually attacked. The incident was also quickly resolved.
>
> A second example illustrates a more severe incident. This incident was characterized by the following data: 712 days duration, 383 sites, 158 messages to/from the CERT/CC, and root-level break-ins. This incident had the longest duration of any incident in the CERT/CC records, but all of the measures for this incident were also more than one standard deviation above their respective means. The intruders used numerous methods of operation including password cracking, Trojan horse login programs, deleting files, exploitation of open servers, social engineering, trusted hosts attacks, exploitation of sendmail bugs, mail spoofing and software piracy. It is the combination of all of these measures that makes this incident more severe than the first example given.'

Howard's (1997) analysis indicates that significant domain knowledge may be required to understand an incident 's severity and to determine measures that could be used to assess severity. Moreover, it may be difficult to find precise measures that can be used to assess the severity of an incident.

ANALYZING INFORMATION-LEVEL INCIDENTS

Compared to network-level incidents which happen on well-defined technical levels, information-level attacks are harder to analyze and to address. Information-level threats differ from network-level attacks in several important aspects:

1. Information-level activities happen outside (secure) corporate environments and attackers do not have to get into contact with corporate computer systems in order to launch an attack. This means that *internal* security approaches, such as company policies, intrusion detectors and usage profilers, are hardly applicable.

2. Often, companies are affected only indirectly as information may influence the environment in which companies operate (e.g., reputation, shares price).

3. Information-level attacks may manifest on a variety of levels. The level on which an attack can be observed (i.e., where information dissemination takes place) is different from the level on which the attack unfolds.

4. Even if information-level activities are witnessed by employees it may be difficult for them to identify the activities as attacks as significant domain knowledge may be required to understand the threat potential (e.g., fake sales figures).

5. Only a limited number of electronic communication channels can be monitored as monitoring has to be (technically) possible and (ethically) appropriate. Examples for open communication channels are public mailing-lists, Usenet newsgroups and large parts of the World Wide Web. Contrary, email is almost always private, many mailing-lists are for closed user groups and many Web servers have password-protected areas. Even in the case of the publicly accessible Web, it is simply impossible to monitor all traffic for resource reasons (bandwidth, storage capacity, processing power).

6. Sometimes, network-level attacks may also be used to launch an information-level attack. For example, the Microsoft hack (Bridis and Buckman 2000) and the DoS attack against Microsoft's domain name servers (Yasin 2001) could be interpreted as attacks on the company's reputation as the company is a major player in the security business.

In order to understand how information-level attacks may apply their lever, the information warfare literature provides some interesting material. As Cronin (2000) outlines, misinformation has long been staples of conventional warfare. Cronin provides an information warfare (IW) typology. Level I IW seeks to damage or destroy the equipment associated with command, control and communication functions through the use of brute force. Cronin notes that this is not really an instance of `soft' warfare or information warfare. Level II seeks to prevent the selected targets from operating effectively by, for example, launching a DoS attack. Level III IW seeks to degrade or corrupt the contents of a target's information systems. Examples would be malicious code or hacks that cause damage. Level IV IW involves infiltrating a target's information resource base in order to conduct espionage and support intelligence-based warfare. Level V IW is based on the silent penetration of a target's systems to shape opinions, manage perceptions, etc. What we call network-level activities would match levels II IW and III IW of Cronin's typology. A significant part of information-level activities would be located on level V IW but the typology does not really meet our requirements.

Hutchinson and Warren (2000) discuss strategies in information warfare and mention, among other things, two specific techniques in information warfare that are related to the activities addressed in this paper: flooding a target organization with information, thereby slowing stopping effective processing or analysis of the incoming information, and exposing confidential or sensitive information, thereby embarrassing or in other ways harming the organization.

Our approach is to start from threatening online activities reported in the literature. We have listed a variety of incidents that are based on the active or passive dissemination of certain information elsewhere (e.g., Lueg 2001). These and other incidents reported in the literature indicate that the range of potentially threatening activities is rather broad ranging from urban legends (Ulfelder 1997, Brauer 1998) and hoaxes promising certain benefits (Park 2000) to web sites deliberately providing false information about products of competitors (Fumento 1999) to fake business announcements (Neue Zürcher Zeitung 1999) to information that were subject to a libel case (`McLibel'). Search engines are fed with specific information so that online customers using the search engines are directed to other web sites than they were looking for. Recently there was an incident where information describing a popular web site were used to direct customers to a porn site (Chai 1999). Some years ago, the cyber artist group eToy used a similar technique to `capture' about one million surfers.

Online communities have shown to be places where effective knowledge and information sharing happens. An example is an online community that shares information about internal quality standards set by a particular fast food company and how these quality standards are sometimes ignored in the company's own restaurants (Lueg 2001). The information are circulated in a particular Usenet newsgroup but can be found even by casual Internet users when using regular search engines, such as Google (URL http://www.google.com).

There is some evidence that `joe jobs' are increasingly used to silence opponents as well as competitors on the Internet. A `joe job' means hiring a spammer to spam under the name of another person's domain, or web pages. The effect is that lots of people complain to the Internet service provider (ISP) hosting the domain or the web page advertised in the spam as they mistakenly assume they know the source of the spam.

It is reasonable to assume that incidents reported in the literature are just the tip of the iceberg. Companies may not be aware of threatening information circulated online or they may have chosen to deliberately ignore these information. An example for the latter is an US-based car manufacturer who decided not to go online to combat a certain revenge web site as the company was afraid that anything they would do on their own web site would validate what is described on the revenge web site (Ulfelder 1997).

While working on a better understanding of information-level incidents we found the following criteria helpful:

Active vs. passive dissemination of information

Active: the attacker herself actively posts threatening information to dissemination channels, such as mailing lists or Usenet newsgroups.

Passive: the attacker sets up a (revenge) web site that provides information and waits for others to find or disseminate the information.

Direct vs. indirect attack:

Direct: the attacker herself targets a company's resources. An example would be sending meaningful but faked inquiries to service accounts in order to overload human resources dealing with the inquiries.

Indirect: joe jobs (abusing an opponent's identity for spamming so that the apparent sender is blamed and kicked off the Internet by his or her ISP).

True vs. false information:

True: the attack is based on information that is probably true but nevertheless well suited to affect a company's reputation. Examples are Nike's controversial salaries which are published on the `living wages' Web site (URL http://www.nikewages.org) and MIT student Jonah Peretti's email exchange with Nike when ordering personalized running shoes with the word `sweatshop' (sic!) as personal ID (MediaGuardian, 2001).

False: the attack is based on false information as in the case of urban legends.

Small scale vs. large scale dissemination:

(initial scale; further dissemination is difficult to control as demonstrated by the `lover' email exchange between British lawyers that was circulated round the world within a few hours)

Small: information initially sent to individuals by personal email or posted to Intranet web sites / protected web sites / internal newsgroups, etc.

Large: initial posting to a large mailing list / widely disseminated newsgroup / regular web site.

Further criteria to be considered are, for example, the number of communication channels used (single channel or multiple channels), the level on which the attack unfolds, scope of an attack and intent (intended vs. unintended). In the end, unintended `attacks' may be as powerful as intended attacks but is not clear whether an activity that was not intended as attack should be treated as such. This is especially relevant if corporations consider launching counter-attacks or involving lawyers. In any case, such criteria indicate the need to involve disciplines, such as law which has a long tradition of distinguishing between intended and unintended activities.

CONCLUSIONS AND FUTURE RESEARCH

In this paper, we have used example of information-level incidents reported in the literature to identify criteria that can be used to analyze incidents. Typically, more than one criteria applies. `Joe jobs', for example, meet the `indirect' criteria, the `false' criteria (as the sender's identity is faked), and the `large scale' criteria. We are working on extending and refining the list of criteria.

The ultimate goal of this research is the development of a comprehensive framework that helps analyze means, scope and severity of information-level activities. Future work includes researching measures for assessing the severity of incidents as well as the development of a taxonomy for information-level activities.As Howard (1997) outlines, a satisfactory taxonomy should have classification categories with the following characteristics:

1. Mutually exclusive - classifying in one category excludes all others because categories do not overlap,
2. Exhaustive - taken together, the categories include all possibilities,
3. Unambiguous - clear and precise so that classification is not uncertain, regardless of who is classifying,
4. Repeatable - repeated applications result in the same classification, regardless of who is classifying,
5. Accepted - logical and intuitive so that they could become generally approved,
6. Useful - can be used to gain insight into the field of inquiry.

One of the next tasks is to investigate how the criteria we identified relate to Howard's (1997) work on classifying security incidents and how a taxonomy for information-level online activities may look like.

ACKNOWLEDGMENTS

The author would like to thank one of the anonymous reviewers for his or her enormously helpful comments on the draft version of this paper, Robert James Steele for valuable discussions and Jim Underwood for his ongoing support.

REFERENCES

Boulanger, A. (1998). *Catapults and grappling hooks: the tools and techniques of information warfare*. IBM Systems Journal, 37(1):106-114.

Brauer, M. (1998). *Net spreads lies far and wide*. Detroit Free Press. [On-line] http://www.freep.com/tech/qblarn30.htm (last visit 31 August 2001).

Bridis, T. and Buckman, R. (2000). *Microsoft hacked! Code stolen?* Wall Street Journal Interactive Edition. [On-line] http://www.zdnet.com/zdnn/stories/news/0,4586,2645850,00.html (last visit 31 August 2001).

Chai, J. (1999). *Search engines point to porn*. ZDNet. [On-line] http://www.zdnet.com/zdnn/stories/news/0,4586,2317225,00.html (last visit 31 August 2001).

Cronin, B. (2000). *Strategic intelligence and networked business.* Journal of Information Science, 26(4):131-136.

Fumento, M. (1999). *Tampon terrorism. Forbes Global*. [On-line] http://www.forbes.com/global/1999/0517/0210033a.html (last visit 31 August 2001).

Howard, J. D. (1997). *An analysis of security incidents on the Internet 1989 - 1995*. PhD thesis, Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, USA.

Hutchinson, W. and Warren, M. (2000). *Concepts in information warfare*. In Proceedings of the First Conference on Challenges in the New E-conomy.

Lueg, C. (2001). *Information dissemination in virtual communities as challenge to real world Companies. Proceedings of the First IFIP Conference on E-Commerce.* E-Business, and E-Government (I3E 2001), Zurich, Switzerland, October 2001.

MediaGuardian (2001). *Jonah Peretti and Nike*. [On-line] http://www.mediaguardian.co.uk/news/story/0,7541,440022,00.html (last visit 31 August 2001).

Moore, D., Voelker, G. M., and Savage, S. (2001). *Inferring Internet Denial-of-Service activity*. In Proceedings of the 2001 USENIX Security Symposium.

Neue Zürcher Zeitung (1999). *Internet-Missbrauch für Kursmanipulationen*. Falschmeldung über eine Fusion. Nr. 81. April 9, p. 33.

Park, B. (2000). *Free mobile phones offer a hoax, says Ericsson*. IT News from The Age and the Sydney Morning Herald. [On-line] http://it.mycareer.com.au/breaking/20000407/A54797-2000Apr7.html (last visit 31 August 2001).

Smith, G. (1998). *An electronic Pearl Harbor? Not likely*. Issues in Science and Technology, Fall. [On-line] http://205.130.85.236/issues/15.1/smith.htm (last visit 31 August 2001).

Ulfelder, S. (1997). *Lies, damn lies and the Internet.* Computerworld. [On-line] http://www.computerworld.com/cwi/story/0,1199,NAV47_STO6800,00.html (last visit 31 August 2001).

Yasin, R. (1998). *The enterprise strikes back.* Internet Week. [On-line] http://www.internetwk.com/news1298/news120498-12.htm (last visit 31 August 2001).

Yasin, R. (2001). *Tools stunt DoS attacks.* Monitors dam packet floods at ISP routers. Internet Week. [On-line]
http://www.internetweek.com/newslead01/lead020501.htm (last visit 31 August 2001).

Swarming: A New Paradigm for Agent Management

Leigh Watson

School of Management Information Systems
Edith Cowan University, Australia,
E-mail: l.watson@ecu.edu.au;

ABSTRACT

Using "swarming" techniques it is feasible to create a methodology for use in an agent management environment. There are many factors operating upon the use of swarming, some of these allow for autonomous, networked and dispersed agent resources to interoperate with centralised resources. With the use of agent "objects, a model may be created, with this model a methodology and subsequent simulation may also be developed.

Keywords: Swarming, Agent Management, Information Warfare

INTRODUCTION

The permeation and use of modern Information Technologies (IT) throughout the world has meant an increasing reliance upon electronically stored and accessed information. This information is increasingly becoming the target and facilitator of aggressive action. The potential for attackers with a limited physical presence to effect an attack upon opponents of larger resources is becoming evident with recent waves of "hacker" style attacks. These attacks may become part of a strategy based upon the concept of "Information Warfare".

The potential focus for an "Information Attack" to be one of a logical, rather than physical, nature means that any system of logical management may be susceptible. In this light, a new adaptation to Agent Management systems may be feasible. This adaptation is the use of "swarming techniques" to create an effect upon attackers, while maintaining dispersed system functionality.

AGENTS AND AGENT MANAGEMENT

For the purposes of this paper and its associated methodology, the term "agent" shall be defined as "any autonomous entity operating within the confines of the agent management system, be they either human or computer based". This definition provides the basis of assumption by which these agents and their interaction may be modelled.

One of the difficulties to be overcome with this modelling methodology involves the simultaneous mapping of both human and computer agents. Essentially the capabilities and functionality of these two classes of agents may vary widely. Therefore this model will attempt to focus upon some of the common ground between the two groups. The common ground focussed upon will be the collection and interchange of information, decision making processes and relationships with other decentralised and centralised resources.

The collection and interchange of information gathered by computer agents is restricted to the pre-programmed capability and functionality of the agent, coupled with its ability to determine new means of collecting information, or learning. The functionality of the computer based agents will be dictated by the ability and functionality of the hardware upon which the agents software is operation upon, and the software itself. On the other hand, human agents are restricted by their natural capacity to learn and make deductions based upon the information they are receiving. Additionally, human agents are restricted in functionality by their range of senses. For example a human agent typically will not be able to sense in the infra-red spectrum without assistance, whereas this mode of operation may be the sole functionality of a specialised computer agent. Furthermore to replicate the natural ability of human agents to recognise and predict new patterns within their environment, computer agents require sophisticated software, and often hardware.

The dissemination of information between agents and their associated resources is not a new discussion topic. There exist many types information security models dealing exclusively with the implementation of procedure for information dissemination. This model will focus more heavily upon the requirements for a decision making methodology for agents.

The decision making process to be outlined in this model will be of two types. The first is Analytic Decision Making (ADM) the second is Naturalistic Decision Making (NDM). Traditionally, ADM is seen as advantageous for many reasons, however research has been conducted into the actual decision making process used when, in certain situations, an observation of the breakdown and subsequent non-use of the ADM techniques was made. This has lead to an understanding of a decision making process known as NDM.

While the ADM approach has many advantages, it neglects to capitalise on some of the most useful aspects of human decision making abilities. Essentially ADM type approaches are capable of managing the decision making requirements for situations, and for measures of logistics which are far beyond the capacity for a single human decision maker. However, the chief disadvantages of the ADM approach are the time required to undertake an ADM approach to a point of completion where a decision may be selected, and the frequent lack of scope in the ADM methodology for producing unusual or unexpected decisions. In many situations, particularly in a crisis, combat or other situation involving fast rate of change and opposing forces, the ADM approach becomes unworkable, thus the NDM approach is adopted. This is due to the advantages gained from taking an unusual or unexpected decision, in addition to the ability to work within the expected decision cycle time of an opponent utilising ADM.

A more formal presentation of the factors which allow for successful utilisation of ADM or NDM has be presented by Bergstrand (1998).This list is as follows:

ADM

- Time is not a factor
- Decision makers lack the experience needed for sound intuitive judgements.
- The computational complexity renders intuition inadequate – (e.g. mobilization planning)
- It is necessary to justify a decision to others or resolve internal disagreements over which course to adopt.
- There is a choice among several clearly defined and documented options.

NDM

- Time is critical
- Decision-makers are knowledgeable and experienced in the given situation.
- There is a high degree of uncertainty.
- There is a high degree of risk
- There is ambiguous or changing direction.
- There is a requirement for innovative, original or creative thought. (Bergstrand, 1998)

An important aspect for the success of any NDM based decision is the knowledge and experience of the decision maker. For this reason, in many cases the ADM approach is favoured by decision makers for the capacity to audit the decision process and the responsibility the process adopts for any decision acted upon. Conversely, the NDM approach is not effectively able to be audited and the decision maker accepts full responsibility for the success or failure of the decision. However, some decisions, particularly in critical situations, require the NDM approach. For this reason, several researchers have presented formalised models and subsequently more formalised training of NDM approaches. This work has been largely based upon the perception of change in decision making process in "field" situations. Kuhaneck and O'Malley (2000) sum this perception up when they stated the "initial impetus behind the NDM movement was to describe what people do, whereas the motivation behind traditional decision research was to improve the way people make decisions".

Some of the formalised mechanisms for NDM have been presented as various models. Some of these models include Klein's Recognition-Primed Decision (RPD) model, Endsleys Situation Awareness model, the Recognition / Metacognition (R/M) model, Rasmussen's Skills/Rules/Knowledge model, and Beach and Mitchell's Image Theory. Perhaps the most widely recognised of these models is Klein's RPD model. In his description of how and why the RPD model can be used to create a higher quality NDM process, Klein (1997) states these reasons as:

1. Classical methods do not apply in many naturalistic settings.
2. Experienced decision makers can be used as standards for performance.
3. NDM tries to build on the strategies people use.
4. Experience lets people generate reasonable courses of action.
5. Situation awareness may be more critical than deliberating about alternative courses of action.
6. Decision requirements are context specific. (Klein, 1997)

Aspects of these decision making considerations may be reflected in the area of electronic agents and their capacity for decision making. Traditionally, electronic or computerised agents require some form of task specification requiring singular completion or continual monitoring and reaction. Effectively these decision making processes would be implemented in some form of programmed action or activity, followed by monitoring and response. There are several key problems with decision making for computerised agents, in particular, in environments where NDM is required.

A commonly and widely used modern example of a computerised agent is the network mechanism known as an Intrusion Detection System (IDS). IDS systems typically behave in a reactive fashion, monitoring all traffic passing through their network point, detecting and reacting to known attack traffic patterns or contents. These attack patterns are stored in a template within the IDS system and are referenced to provide a match for detection. Some work has begun in the use of heuristic attack detection within IDS systems, however this work further highlights the shortfall of this essentially ADM based technology.

In order to provide continued undated capability for an IDS, there exists a large community of computer security professionals whom monitor, detect and analyse attacks via various means. When a new attack is recognised a signature for the widespread IDS software installations is generated and uploaded by their various system administrators. While heuristic attack detection is successful at detecting previously unknown attacks, these attacks are generally of a form previously known, with altered technical specifics and therefore a unique signature. The chief problem with this system is the reliance on the constant updating of attack signatures and heuristic model for the IDS systems. A potentially better system would be the use of more programmed intelligence in IDS system agents to use a "learning and activity" approach based upon NDM methods.

A further point for investigation in the research for this model will be the relationship between centralised and decentralised resources in an agent management environment. The use of a swarming methodology necessarily implies a dispersed base of activity, however, due to the nature of agent management, there is potential for the use of centralised resources for activity which is not easily mobilised or dispersed. For example such activity may be analysis of cryptography or generation of new access and communication tokens and mechanisms for distributed agents. Discussion of a methodology via which the use of swarming could be utilised for agent management requires the discussion of swarming itself.

SWARMING

The study of swarming has essentially evolved from a general concept of behaviour by certain types of insects, and expanded within the field of natural science in order to provide some form of explanation. The term "swarming", in a military context, has been described as being "seemingly amporhous, but it is a deliberately structured, coordinated, strategic way to strike from all directions, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions" (Arquilla & Ronfeldt, 2000, p. vii). This presentation of the swarming concept is expandable to include logical information based swarming, not only physical force based swarming.

The implications of utilising a swarming force may be derived from an examination of the use of swarming over history, particularly in human use, as this is where history is most abundant. It should be noted however that the use of the term "swarming" firstly conjures images of bees, and secondly a numerically large mass of these insects. This image is not altogether incorrect for use in an agent management methodology, however, further explanation of the details for the potential structure, coordination and strategy of a swarm is required.

In terms of how a swarm structures itself, there are four basic categories outlined by Arquilla and Ronfeldt (2000). These are;

1. Hive Organisation
2. Pack Organisation
3. Opportunistic Mobbing
4. Other (Arquilla & Ronfeldt, 2000, p. 25)

The "Hive Organization" centers around a "nesting" type of activity. For example bees, ants and other social insect are of this category. Taking the example of bees, each individual "drone" autonomously conducts its own activity within an adopted range of the nest. This activity includes foraging for food and defence of the nest. In a normal manner of operation, these drones will spread out, each individually seeking the maximum coverage of territory, or gathering of food. When a large food source or potential threat to the nest is identified, a signal is given by several "source" bees. This communication is quickly transferred to all bees within the proximity of the source, and the bees take action. This action is typified by individual efforts, multiplying the effect of a mass of bees in the same place.

The "Pack Organisation" focuses upon another type of activity, based upon the roaming type of activity. An example of this classification of swarming is the wolf pack. Wolves will roam in a pack together, assuming a hierarchy for most other activities other than the active hunt, where the pack will adopt swarming tactics for maximum individual and group gain. When a wolf pack detects and tracks a herd of prey to within striking distance, the pack will split up and surround the herd. Upon a given signal the wolves will simultaneous attack the herd, each operating upon the best of their ability, both individually and in cooperation with other wolves the "chase" will bring together.

The third type of swarming is the classification of "Opportunistic Mobbing". This type of activity is found in mosquitoes, flies and certain breeds of shark. Essentially this style of swarming has no obvious group gain operation and is purely generated by the action of one individual within the vicinity of other individuals of the same requirements, causing interest from them, and thus activity. This type of swarming appears to have no group communication, even competition between individuals operating within the same swarm, each operating autonomously for maximum individual gain.

The fourth category of swarming is labelled "Other". This classification includes many examples of swarming which are either a combination of the other types of swarming, in manner which classifies them apart, or are a type of swarming which is beyond current technique for description and classification. For example viral, bacterial and antibody swarming fits into this category, particularly as in these cases swarming may be analysed as growth of organisms within an infected body, or as growth of the number of infected organisms within a population.

These classifications provide a mechanism via the construction of formal activity patterns for swarming agents to be developed. This construction may focus upon the identification of recognisable patterns of activity, behaviour and environmental conditions, being monitored by the agents. This may be followed by the generation of activity of two kinds. This activity may be of the reactive or proactive description. This would allow for both quick reactive and longer term proactive development of the agent management capability.

However, in terms of human swarming activity in a military historical perspective, three key factors have been identified. These factors are:

1. Elusiveness – Either through mobility or concealment
2. A longer range of firepower – Standoff capability
3. Superior situational awareness (Edwards, 2000, p.53)

These factors may be adapted for use in the field of developing a methodology for use in agent management. Although the use of an agent management system may indicate greater reliance upon managing actions, activity and information operations of the agents, there is both a logical and a physical necessity for these three factors. Although arguably a "longer range of firepower" is dependant upon the notion of armed conflict, an adapted factor for agent management may be the ability or capability to affect the operations of a target.

The autonomy of an individual within the dynamics of an organised group is central to the operation of swarming. Additionally, central to the distinction between "Opportunistic Mobbing" and the other forms of swarming is the use of communication. This communication may come in many topological forms and be implemented in a myriad of technologies. These communication techniques and technologies provide for mechanisms of effective and secure communication between swarming agents, and their centralised resources. These communications techniques may become both facilitators and targets for any swarming agent system, particularly in a modern IW arena.

NETWORKING THE SWARM

There are many existing communication technologies which may easily be adapted to provide for a swarming agent management system. Many of these high speed connection oriented technologies, operating in a wireless environment, are already being adapted for civilian use, some of the behaviour of which closely replicates swarming activity. This is particularly evident in the mobile telephone technology development area.

A key element in the use of a swarming methodology is "Elusiveness". One way to achieve this is via secure communications, and more generally, security of the agent and management system. One agent management system proposal, the MASIF proposal, details a list of considerations for security of an agent management system:

- Transfer
- Tracking
- Monitoring and auditing
- Intermittent connection
- Fault Tolerance
- Time, location, itinerary, ownership, security, resources
- Types of Mobility (Code, state, thread) (Fox, 1998)

If all these considerations are to be built into an agent management system communications, a complex and redundant system would be required. One mechanism for creating a communications system such as this is to create cells, chains and operations centres for a swarming population. This style of networking is achievable by the use of three simple network topology types. Figure 1, taken from Arquillla and Ronfeldt (2000), displays a logical chart of three types of topology;

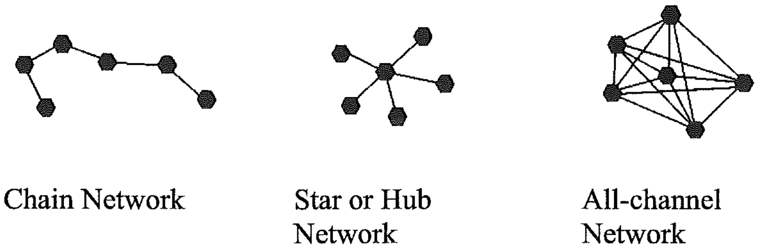


Figure 1: Network topologies for use in swarming
(Arquilla & Ronfeldt, 2000, p. 58)

Each of these types of network suits different purposes and situations. In many cases the ability for adaptation of one existing network connection into a connection of another type may be necessary, therefore any agent management system utilising a swarming methodology should address the requirement for communications and decision making mechanisms which are adaptable to a rapidly changing environment. For example, an agent operating within a cell may have "all-channel" access to their cell, while at the same time having access to a "chain network" with other cells and another member of their cell with access to a "Hub network" operating with centralised resources.

The potential for a swarming agent management system to utilise modern communications is large, however, this potential is likely to become a requirement for success. In this scenario, an attacker of the agents and/or the agent management system may be likely to target the information and the information infrastructure upon which the agents and their management system is reliant.

A PROPOSED METHODOLOGY FOR TESTING AND SIMULATION

The methodology being proposed is for an exercise in generating, testing and simulating an agent management system utilising "swarming". The definition of agents as autonomous entities operating within the influence of the agent management system allows for the development of "generic" agent objects. These agent objects may either be human or computer based and range from hostile to friendly, and capable through to incapacitated. There are many more variables and relationships to be defined, some of these will be based upon the decision making processes, information gathering and transfer and logistical requirements of agents. Furthermore these considerations will be used to create variables for use with the agent objects. These objects may be adapted for use in a exercise of modelling the management of agents, utilising swarming theory.

The use of swarming theory will require that agents become dispersed and operate autonomously, within the confines of strategic directives given by centralised (or non-dispersed resources). The use of a swarming method allows for many different network topologies to be utilised to create highly functional, secure and effective communication of information, between agents themselves and their associated centralised resources.

The operating environment for the agent management system will be the rapidly changing and information attack driven world of IW. The use of a defensive IO directive for the agent management system will allow for the creation of a methodology via which the agents and centralised resources may interact and cooperate. Additionally, this environment is required due to the inclusion of "computer agents" and modern communications and computing technologies, which are the reality of any modern agent management system.

The creation and modelling of these "objects" will lead to the development of a methodology. This methodology may consist of several competing lines of investigation and deduction, therefore it will be necessary to simulate the operation of the model and the methodology. The simulation process to be developed will allow for the manipulation of individual objects, or of groups of objects to effect environmental and situational effects. Additionally it may be feasible to overlay object variable influencing effects, for example the effect of a new technology for communication.

The simulation process will allow the model and methodology to be tested against scenarios, both historic and potential, to test the legitimacy and the capability of this research. The legitimacy of this research will also be affected by the continual reliance upon verification of each stage of the process by relevant experts in each field.

In this way an agent management methodology, utilising "swarming" may be created and simulated.

REFERENCES

Arquilla, J. & Ronfeldt, D. (2000). *Swarming & The Future of Conflict.* Santa Monica: RAND.

Bergstrand, B. (1998).*Situating the Estimate: Naturalistic Decision-Making as an Alternative to Analytical Decision-Making in the Canadian Forces.* Canada: Canadian Forces Colledge.

Edwards, S.J.A. (2000). *Swarming on the Battlefield: Past, Present and Future.* Santa Monica: RAND.

Fox, R. (1998) *Output of the MASIF clean-up.* [On-line]
http://cgi.omg.org/cgi-bin/doc?orbos/98-03-09.pdf

Klein, G. (1997). *An Overview of Naturalistic Decision Making Applications.* In C.Zsambok & G Klein (Eds), Naturalistic Decision Making. (pp. 49-59). New Jersey: Lawrence Erlbaum Associates.

Kuhaneck, T.S., Heggers, A. M. & O'Malley, M. P. (2000). N*aturalistic decision making and training the incident commander.* Chicago: Marine Safety Office.

Automaton Hackers - The New Breed

Alice Voeten-Lim[1] and Craig Valli[2]

[1] Alice Voeten-Lim
MDIS, Singapore

[2] Craig Valli
Edith Cowan University, Western Australia
E-mail: c.valli@ecu.edu.au

ABSTRACT

This is a case outline of a computer security novice creating an attack profile and testing a proposed on-line system for an organisation. Consequently, the tools used were gathered from Internet sites and the testing while not overly rigorous discovered several significant problems. The unsettling part of this case is that the same steps and procedures that have applied to the testing of this facility can equally be applied by an external novice hacker to gain access to the systems.

Keywords: hacker, attack, insider, security, tools

INTRODUCTION

This paper is a case outline of a real world risk analysis and subsequent security testing of networked systems for an emerging application service provider. It was completed by the co-author Alice who is a Masters student, she had not had previous exposure to risk analysis and security testing of networks until undertaking this task. Consequently the tools used were gathered from Internet sites and the testing while not overly rigorous discovered several significant problems. The unsettling part of this case is that an external novice hacker can equally apply the same steps and procedures that have applied to the testing of this facility.

Alice conducted a risk analysis of the existing web infrastructure for the organisation that we will call Another.com as part of her Masters assessment and there were several serious risks identified for the existing infrastructure. Another.com had recently developed a proprietary program Plan-B and planned to offer this tool as a business-to-business service to conference organisers. The risk analysis was then used to do some attacks on the proposed infrastructure.

PLAN-B

Plan-B allows conference organisers to create and host customised databases on Another.com's servers. By using the service, an organiser would be able to offer information-on-demand to their customers, that is the event participants or visitors. All relevant information about the events and exhibitions being marketed would be available online to their registered customers.

The service includes the licensed use of the proprietary software, database hosting, and online payment facilities. The Plan-B organisation was in its beta-testing phase of the software and project. As Another.com planned to launch this new service by June 2001, it was suggested to the management to include security testing during this beta testing phase, to ensure the integrity of the intended Plan-B service.

The security test was to identify potential security holes on the system and propose appropriate protective countermeasures. The management approved the testing with a 2 week completion and reporting deadline. Full access to the internal network was given and approval to use widely available penetration and testing tools was given.

The internal network infrastructure was as follows (see Figure 1)

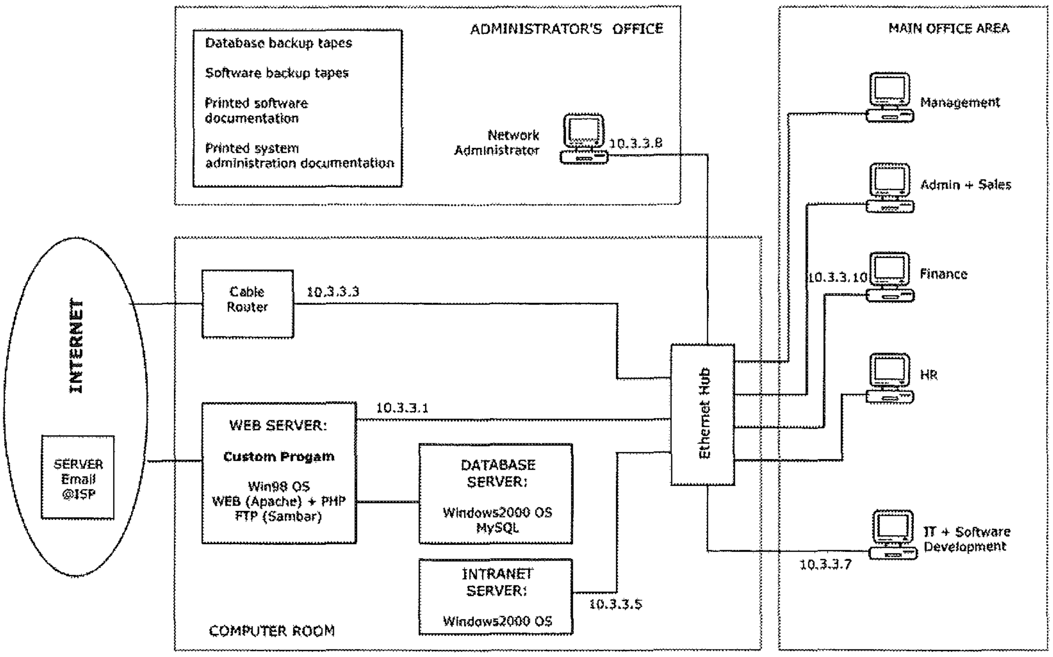


Figure 1: Network Layout & Plan

Security Test Objectives

The purpose of the security evaluation was to ensure that the network's vulnerabilities were reduced to the minimum, and that recommended security measures from a recent risk analysis would be able to protect the organisational assets adequately against the commonly known exploits.

After analysis of the network layout, the web server and the Intranet server had been identified as the most vulnerable assets prone to attack. Therefore these servers would be tested for vulnerabilities to attack from intruders.

Password Attack

According to the existing security policies of Plan-B all network equipment including PCs and workstations would require passwords to gain access. The goal of this test is to find a username and password to gain access to one of the servers. The author devised an 'Attack Tree' (see Figure 2) that can "provide a methodical way of describing threats against, and countermeasures protecting, a system." (Schneier, 2000, p.318). This figure illustrates nine alternatives to getting the usernames and passwords.

By analysing this tree, it was possible to identify the vulnerabilities that the passwords were being exposed to. From this analysis the author identified the two most likely attacks. Firstly, password sniffing directed specifically at the servers from across the network. The existing computer room has an Electronic Access Control System installed, and is monitored by a 24-hour security camera linked to a video recorder, gaining physical entry into the computer room would be a tougher choice for the potential attacker. However, there is still a possibility that if someone does manage to get into the computer room would be able to install a password sniffer program directly on the servers to gather usernames and passwords.

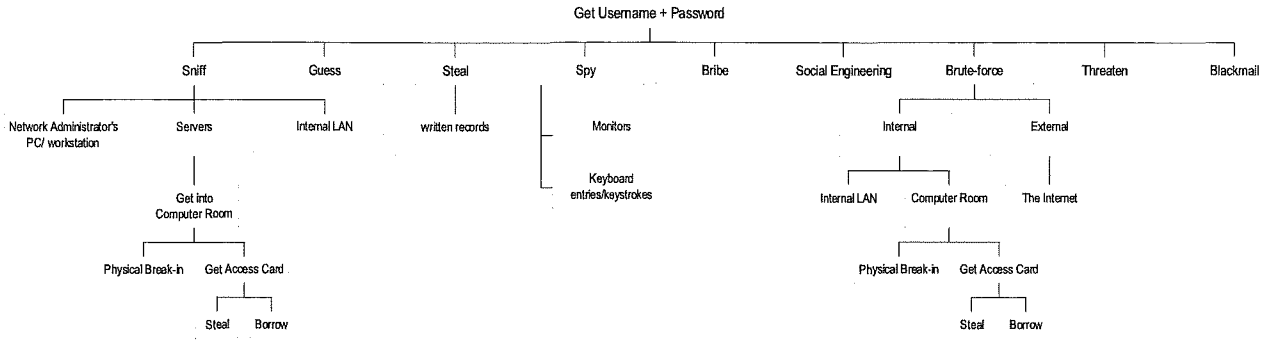


Figure 2: Password Attack Tree

The second alternative is compromise a machine on the internal LAN and install a password sniffer program to capture usernames and passwords. This attack would be more open to a brute-force approach as a dictionary attack program could be installed on any PC or workstation on the internal LAN.

Computer Security Institute (CSI) and the FBI have conducted an annual survey and found that "dishonest and disgruntled employees top the list at about 80% as the most likely source of attack". As such, the author decided to focus tests on the internal LAN and a brute-force password attack to evaluate the possibilities of internal attacks.

TECHNIQUES AND TOOLS USED IN THE INVESTIGATION

Ping Sweepers

Ping allows us to see which PC's and servers are active and thus potentially vulnerable to attacks. This is achieved by sending a small packet to an IP address if it is active the packet will return a result.

NetBIOS Information Discovery programs

These are programs that scan entire networks and provide NetBIOS information for each computer such as hostnames, IP addresses, open shares and usernames. The usernames provided can then provide the basis attacks on passwords.

Port Scanners

Port scanning programs allow us to detect "security weaknesses in a remote or local host". (Hacking Techniques. April 3, 2001. Security Watch.) Port scanners simply scan all ports to see what ports are open and what services are potentially running. This then allows for hackers to target available ports for compromise on these systems.

Sniffing Utilities

The Security Watch web site also suggested using sniffer devices to gather "information travelling along a network" such as "usernames, passwords, addresses, ports, or just the content of e-mails, etc.". (Hacking Techniques. April 3, 2001. Security Watch.) These are only really effective against plain text or unencrypted data traversing a network.

Password Cracking

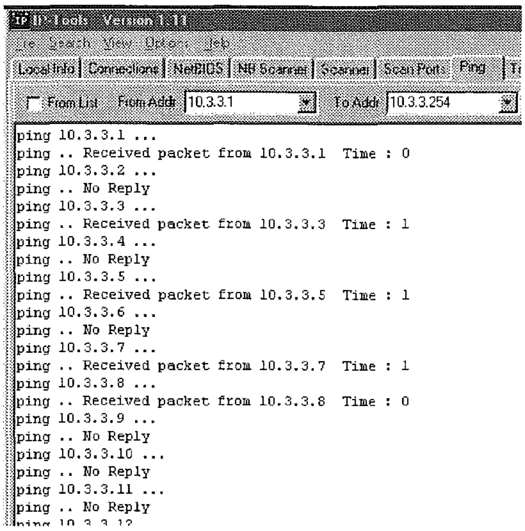
The "FAQ: Network Intrusion Detection Systems" article from the Technical Incursion Countermeasures web site describes some common password cracking methods, such as brute-force and dictionary-based techniques. (Section 1.4.3 Password cracking. FAQ: Network Intrusion Detection Systems. March 21, 2000. Technical Incursion Countermeasures.)

ACTUAL TESTS PERFORMED ON THE NETWORK

A battery of tests was performed on the 2 servers in question utilising tools and information downloaded freely off the Internet. The following is an outline of the testing undertaken.

Step One – Ping

The first step taken was to identify which servers were online. The tool used was IP Tools, a ping sweeper from KS-Soft (www.ks-soft.net). The ping result of the network is as follows. As this test was done on a Friday evening, only five machines were on-line at that time



□ From List From Addr 10.3.3.1 To Addr 10.3.3.254

```
ping 10.3.3.1 ...
ping .. Received packet from 10.3.3.1  Time : 0
ping 10.3.3.2 ...
ping .. No Reply
ping 10.3.3.3 ...
ping .. Received packet from 10.3.3.3  Time : 1
ping 10.3.3.4 ...
ping .. No Reply
ping 10.3.3.5 ...
ping .. Received packet from 10.3.3.5  Time : 1
ping 10.3.3.6 ...
ping .. No Reply
ping 10.3.3.7 ...
ping .. Received packet from 10.3.3.7  Time : 1
ping 10.3.3.8 ...
ping .. Received packet from 10.3.3.8  Time : 0
ping 10.3.3.9 ...
ping .. No Reply
ping 10.3.3.10 ...
ping .. No Reply
ping 10.3.3.11 ...
ping .. No Reply
ping 10.3.3.12
```

Figure 3: Screendump from ping program

Step Two – Network Scan

The author then used LANguard Network Scanner (www.languard.com) to get NetBIOS information, mainly to find out what the IP addresses and the usernames of all the PCs and servers on the network.

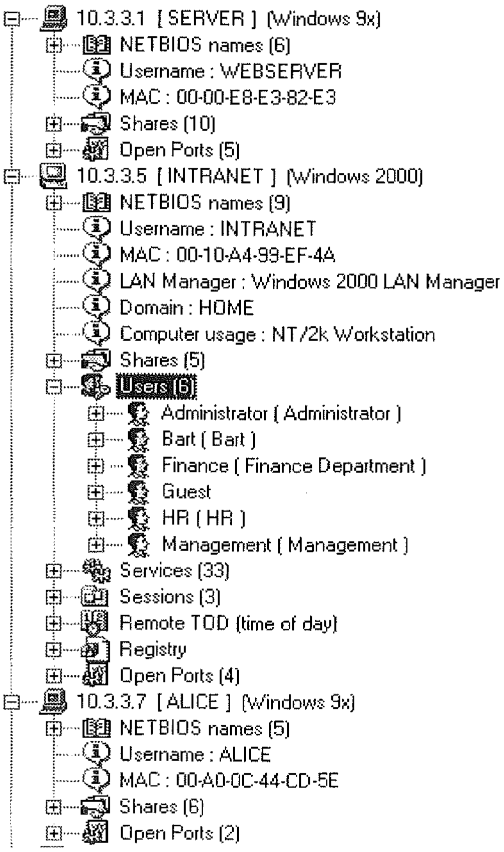
From this result, it can be seen:

The Network Administrator's IP address is "10.3.3.8" and username is "Administrator".

The web server's IP address is "10.3.3.1" and username is "webserver".

The intranet server's IP address is "10.3.3.5".

There are six usernames defined on the intranet server, i.e. "Administrator", "Bart", "Finance", "Guest", "HR", and "Management".

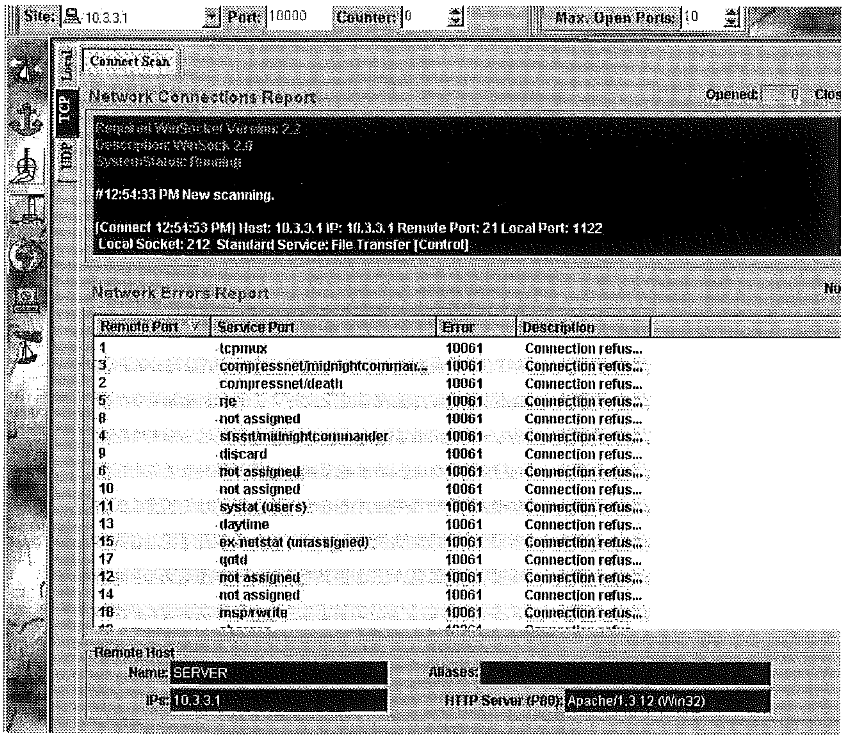


```
⊟ 10.3.3.1 [ SERVER ] (Windows 9x)
    ⊞ NETBIOS names (6)
      Username : WEBSERVER
      MAC : 00-00-E8-E3-82-E3
    ⊞ Shares (10)
    ⊞ Open Ports (5)
⊟ 10.3.3.5 [ INTRANET ] (Windows 2000)
    ⊞ NETBIOS names (9)
      Username : INTRANET
      MAC : 00-10-A4-99-EF-4A
      LAN Manager : Windows 2000 LAN Manager
      Domain : HOME
      Computer usage : NT/2k Workstation
    ⊞ Shares (5)
    ⊟ Users (6)
        ⊞ Administrator ( Administrator )
        ⊞ Bart ( Bart )
        ⊞ Finance ( Finance Department )
        ⊞ Guest
        ⊞ HR ( HR )
        ⊞ Management ( Management )
    ⊞ Services (33)
    ⊞ Sessions (3)
    ⊞ Remote TOD (time of day)
    ⊞ Registry
    ⊞ Open Ports (4)
⊟ 10.3.3.7 [ ALICE ] (Windows 9x)
    ⊞ NETBIOS names (5)
      Username : ALICE
      MAC : 00-A0-0C-44-CD-5E
    ⊞ Shares (6)
    ⊞ Open Ports (2)
```

Figure 4: Screendump from NETBIOS scanner program

Step Three – Port Scan

Next, the Atelier Web Security Port Scanner (www.atelierweb.com) was used to find out what are the open ports on the servers. These are the results:



Network Connections Report

```
Requested WinSocket Version 2.2
Description: WinSock 2.0
SystemStatus: Running

#12:54:33 PM New scanning.

[Connect 12:54:53 PM] Host: 10.3.3.1 IP: 10.3.3.1 Remote Port: 21 Local Port: 1122
 Local Socket: 212  Standard Service: File Transfer [Control]
```

Network Errors Report

Remote Port	Service Port	Error	Description
1	tcpmux	10061	Connection refus...
3	compressnet/midnightcomman...	10061	Connection refus...
2	compressnet/death	10061	Connection refus...
5	rje	10061	Connection refus...
8	not assigned	10061	Connection refus...
4	sfsst/midnightcommander	10061	Connection refus...
9	discard	10061	Connection refus...
6	not assigned	10061	Connection refus...
10	not assigned	10061	Connection refus...
11	systat (users)	10061	Connection refus...
13	daytime	10061	Connection refus...
15	ex-netstat (unassigned)	10061	Connection refus...
17	qotd	10061	Connection refus...
12	not assigned	10061	Connection refus...
14	not assigned	10061	Connection refus...
18	msp/rwrite	10061	Connection refus...

Remote Host

Name: SERVER

Aliases:

IPs: 10.3.3.1

HTTP Server (P80): Apache/1.3.12 (Win32)

Figure 5: Port Scanner Output

Figure 5 shows the interface of this tool. The upper window shows the "Network Connections Report" indicating all the open ports. The lower window "Network Errors Report" shows the unsuccessful connection attempts, indicating that those ports are not in use.

Network Connections Report – Intranet Server

TCP port open:
110 (Post Office Protocol)
135 (Location Service)
139 (NetBIOS-ss)
445 (Microsoft-DS)
1025 (blackjack)
1026 (nterm)
1028 (????)
1030 (iad)
1801 (Microsoft Message Que)
2103 (????)
2105 (????)
2107 (????)
3372 (????)

UDP ports open:
135 (Location Service)
137 (NetBIOS-ns)
138 (NetBIOS-dgm)
445 (Microsoft-DS)
500 (isakmp)
1027 (????)
1029 (????)
1031 (iad)
3527 (????)

Network Connections Report – Web Server

TCP ports open:
21 (File Transfer Protocol)
25 (Simple Mail Transfer Protocol)
80 (Hyper Text Transfer Protocol)
110 (Post Office Protocol)
139 (NetBIOS)
3306 (MySQL)
8888 (backup web server)

UDP ports open
137 (NetBIOS-ns)
138 (NetBIOS-dgm)

Step Four – Network Sniffer

From the previous steps, the following was learned:

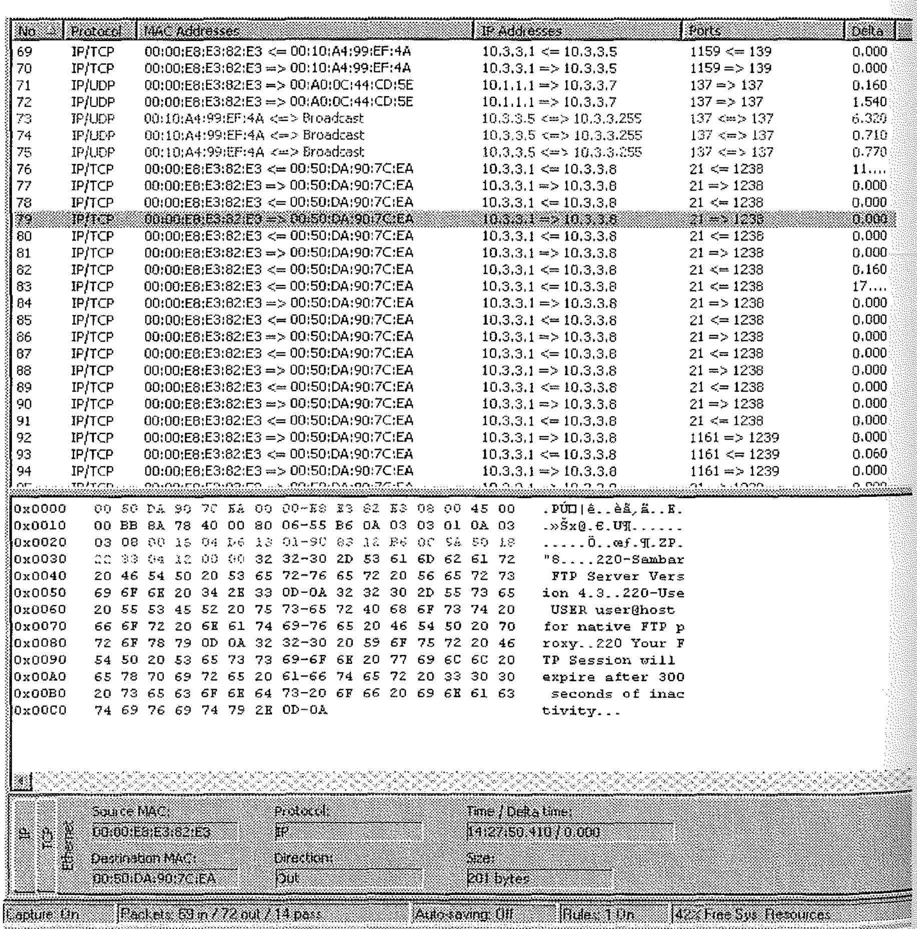
- IP Address of the web server is 10.3.3.1
- IP Address of the Network Administrator's PC is 10.3.3.8
- FTP (port 21) is open on the web server

In this step, a network sniffer program was used to try and get the FTP username and password of the Network Administrator on the web server. CommView (www.tamosoft.com) was the sniffer used to capture all packets on the network. What CommView showed is displayed in Figure 6.

The upper window displays all packets occurring on the network (Protocol, MAC Address, IP Address, Ports, Time).

The lower window shows the detailed content of the highlighted packet on the upper window.

To identify an FTP session from the Network Administrator, search was made through the complete list (as shown below) for packets with IP Addresses 10.3.3.1 and 10.3.3.8, and port 21.



```
No  Protocol  MAC Addresses                             IP Addresses               Ports          Delta
69  IP/TCP    00:00:E8:E3:82:E3 <= 00:10:A4:99:EF:4A    10.3.3.1 <= 10.3.3.5       1159 <= 139    0.000
70  IP/TCP    00:00:E8:E3:82:E3 => 00:10:A4:99:EF:4A    10.3.3.1 => 10.3.3.5       1159 => 139    0.000
71  IP/UDP    00:00:E8:E3:82:E3 => 00:A0:0C:44:CD:5E    10.1.1.1 => 10.3.3.7       137 => 137     0.160
72  IP/UDP    00:00:E8:E3:82:E3 => 00:A0:0C:44:CD:5E    10.1.1.1 => 10.3.3.7       137 => 137     1.540
73  IP/UDP    00:10:A4:99:EF:4A <=> Broadcast           10.3.3.5 <=> 10.3.3.255    137 <=> 137    6.320
74  IP/UDP    00:10:A4:99:EF:4A <=> Broadcast           10.3.3.5 <=> 10.3.3.255    137 <=> 137    0.710
75  IP/UDP    00:10:A4:99:EF:4A <=> Broadcast           10.3.3.5 <=> 10.3.3.255    137 <=> 137    0.770
76  IP/TCP    00:00:E8:E3:82:E3 <= 00:50:DA:90:7C:EA    10.3.3.1 <= 10.3.3.8       21 <= 1238     11....
77  IP/TCP    00:00:E8:E3:82:E3 => 00:50:DA:90:7C:EA    10.3.3.1 => 10.3.3.8       21 => 1238     0.000
78  IP/TCP    00:00:E8:E3:82:E3 <= 00:50:DA:90:7C:EA    10.3.3.1 <= 10.3.3.8       21 <= 1238     0.000
79  IP/TCP    00:00:E8:E3:82:E3 => 00:50:DA:90:7C:EA    10.3.3.1 => 10.3.3.8       21 => 1238     0.000
80  IP/TCP    00:00:E8:E3:82:E3 <= 00:50:DA:90:7C:EA    10.3.3.1 <= 10.3.3.8       21 <= 1238     0.000
81  IP/TCP    00:00:E8:E3:82:E3 => 00:50:DA:90:7C:EA    10.3.3.1 => 10.3.3.8       21 => 1238     0.000
82  IP/TCP    00:00:E8:E3:82:E3 <= 00:50:DA:90:7C:EA    10.3.3.1 <= 10.3.3.8       21 <= 1238     0.160
83  IP/TCP    00:00:E8:E3:82:E3 <= 00:50:DA:90:7C:EA    10.3.3.1 <= 10.3.3.8       21 <= 1238     17....
84  IP/TCP    00:00:E8:E3:82:E3 => 00:50:DA:90:7C:EA    10.3.3.1 => 10.3.3.8       21 => 1238     0.000
85  IP/TCP    00:00:E8:E3:82:E3 <= 00:50:DA:90:7C:EA    10.3.3.1 <= 10.3.3.8       21 <= 1238     0.000
86  IP/TCP    00:00:E8:E3:82:E3 => 00:50:DA:90:7C:EA    10.3.3.1 => 10.3.3.8       21 => 1238     0.000
87  IP/TCP    00:00:E8:E3:82:E3 <= 00:50:DA:90:7C:EA    10.3.3.1 <= 10.3.3.8       21 <= 1238     0.000
88  IP/TCP    00:00:E8:E3:82:E3 => 00:50:DA:90:7C:EA    10.3.3.1 => 10.3.3.8       21 => 1238     0.000
89  IP/TCP    00:00:E8:E3:82:E3 <= 00:50:DA:90:7C:EA    10.3.3.1 <= 10.3.3.8       21 <= 1238     0.000
90  IP/TCP    00:00:E8:E3:82:E3 => 00:50:DA:90:7C:EA    10.3.3.1 => 10.3.3.8       21 => 1238     0.000
91  IP/TCP    00:00:E8:E3:82:E3 <= 00:50:DA:90:7C:EA    10.3.3.1 <= 10.3.3.8       21 <= 1238     0.000
92  IP/TCP    00:00:E8:E3:82:E3 => 00:50:DA:90:7C:EA    10.3.3.1 => 10.3.3.8       1161 => 1239   0.000
93  IP/TCP    00:00:E8:E3:82:E3 <= 00:50:DA:90:7C:EA    10.3.3.1 <= 10.3.3.8       1161 <= 1239   0.060
94  IP/TCP    00:00:E8:E3:82:E3 => 00:50:DA:90:7C:EA    10.3.3.1 => 10.3.3.8       1161 => 1239   0.000
```

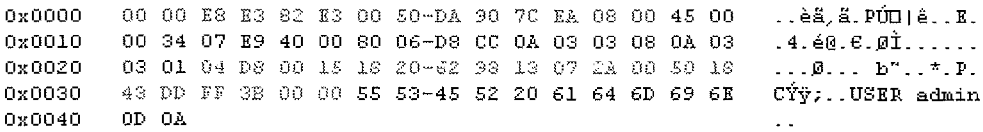
```
0x0000   00 50 DA 90 7C EA 00 00-E8 E3 82 E3 08 00 45 00   .PÚ□|ê..èã,ã..E.
0x0010   00 BB 8A 78 40 00 80 06-55 B6 0A 03 03 01 0A 03   .»Šx@.€.U¶......
0x0020   03 08 00 15 04 D6 13 01-9C 83 12 B6 0C 5A 50 18   .....Ö..œf.¶.ZP.
0x0030   22 38 04 12 00 00 32 32-30 2D 53 61 6D 62 61 72   "8....220-Sambar
0x0040   20 46 54 50 20 53 65 72-76 65 72 20 56 65 72 73    FTP Server Vers
0x0050   69 6F 6E 20 34 2E 33 0D-0A 32 32 30 2D 55 73 65   ion 4.3..220-Use
0x0060   20 55 53 45 52 20 75 73-65 72 40 68 6F 73 74 20    USER user@host
0x0070   66 6F 72 20 6E 61 74 69-76 65 20 46 54 50 20 70   for native FTP p
0x0080   72 6F 78 79 0D 0A 32 32-30 20 59 6F 75 72 20 46   roxy..220 Your F
0x0090   54 50 20 53 65 73 73 69-6F 6E 20 77 69 6C 6C 20   TP Session will
0x00A0   65 78 70 69 72 65 20 61-66 74 65 72 20 33 30 30   expire after 300
0x00B0   20 73 65 63 6F 6E 64 73-20 6F 66 20 69 6E 61 63    seconds of inac
0x00C0   74 69 76 69 74 79 2E 0D-0A                        tivity...
```

Source MAC: 00:00:E8:E3:82:E3
Protocol: IP
Time / Delta time: 14:27:50.410 / 0.000
Destination MAC: 00:50:DA:90:7C:EA
Direction: Out
Size: 201 bytes

Capture: On | Packets: 69 in / 72 out / 14 pass | Auto-saving: Off | Rules: 1 On | 42% Free Sys. Resources

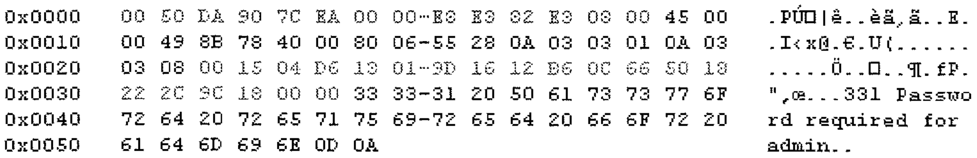
Figure 6: CommViewPacket Sniffer

From the highlighted packet, we can see that the FTP server identified itself to the Network Administrator. The next packet showed that the Network Administrator identified himself as "admin".



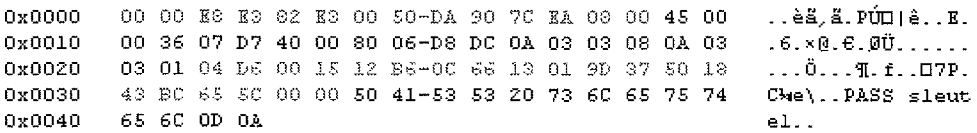
```
0x0000   00 00 E8 E3 82 E3 00 50-DA 90 7C EA 08 00 45 00   ..èã‚ã.PÚ□|ê..E.
0x0010   00 34 07 E9 40 00 80 06-D8 CC 0A 03 03 08 0A 03   .4.é@.€.ØÌ......
0x0020   03 01 04 D8 00 15 18 20-62 98 13 07 2A 00 50 18   ...Ø... b˜..*.P.
0x0030   43 DD FF 3B 00 00 55 53-45 52 20 61 64 6D 69 6E   CÝÿ;..USER admin
0x0040   0D 0A                                             ..
```

The server then asked for a password for user "admin".



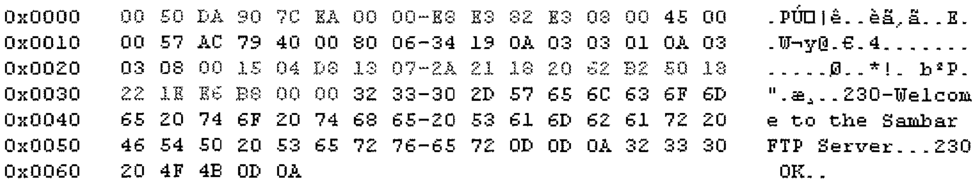
```
0x0000   00 50 DA 90 7C EA 00 00-E8 E3 82 E3 08 00 45 00   .PÚ□|ê..èã‚ã..E.
0x0010   00 49 8B 78 40 00 80 06-55 28 0A 03 03 01 0A 03   .I‹x@.€.U(......
0x0020   03 08 00 15 04 D6 13 01-9D 16 12 B6 0C 66 50 18   .....Ö..□..¶.fP.
0x0030   22 2C 9C 18 00 00 33 33-31 20 50 61 73 73 77 6F   ",œ...331 Passwo
0x0040   72 64 20 72 65 71 75 69-72 65 64 20 66 6F 72 20   rd required for 
0x0050   61 64 6D 69 6E 0D 0A                              admin..
```

This packet now tells us that "sleutel" is the password entered by the user "admin".



```
0x0000   00 00 E8 E3 82 E3 00 50-DA 90 7C EA 08 00 45 00   ..èã‚ã.PÚ□|ê..E.
0x0010   00 36 07 D7 40 00 80 06-D8 DC 0A 03 03 08 0A 03   .6.×@.€.ØÜ......
0x0020   03 01 04 D6 00 15 12 B6-0C 66 13 01 9D 37 50 18   ...Ö...¶.f..□7P.
0x0030   43 BC 65 5C 00 00 50 41-53 53 20 73 6C 65 75 74   C¼e\..PASS sleut
0x0040   65 6C 0D 0A                                       el..
```

The last packet confirmed that the login was successful, confirming that the username and password had been accepted by the server.



```
0x0000   00 50 DA 90 7C EA 00 00-E8 E3 82 E3 08 00 45 00   .PÚ□|ê..èã‚ã..E.
0x0010   00 57 AC 79 40 00 80 06-34 19 0A 03 03 01 0A 03   .W¬y@.€.4.......
0x0020   03 08 00 15 04 D8 13 07-2A 21 18 20 62 B2 50 18   .....Ø..*!. b²P.
0x0030   22 1E E6 B8 00 00 32 33-30 2D 57 65 6C 63 6F 6D   ".æ¸..230-Welcom
0x0040   65 20 74 6F 20 74 68 65-20 53 61 6D 62 61 72 20   e to the Sambar 
0x0050   46 54 50 20 53 65 72 76-65 72 0D 0D 0A 32 33 30   FTP Server...230
0x0060   20 4F 4B 0D 0A                                     OK..
```

Now that the "admin" user name and password are known the upload and download files from the web server via FTP is possible. It would be possible to do this within the internal LAN as well as from the Internet.

It was also discovered that the e-mail is not encrypted and that all e-mail messages, complete with headers, can be read by using this CommView tool. Upon further investigation it also clearly shows all e-mail accounts and their corresponding passwords. Therefore, anyone on the internal LAN or for that matter an external attacker could be able to read someone else's e-mails, or simply steal their identity by configuring their email client program using the relevant account name(s) and password(s) gleaned from the CommView tool.

Step Five – Password Cracking

In this step, the author chose the Finance account on the intranet server as the target account. From step two, the author learned the following:

IP Address of the intranet server is 10.3.3.5
Usernames on the intranet server: Administrator, Bart, Finance, Guest, HR, Management

The author downloaded some dictionaries and dictionary generators from HNC Network (www.hack-net.com) for these tests. The 'Dict Make' generator was tried but it was stopped after 24 hours as a result of time constraints of the test. The generated dictionary although incomplete was used for this test. The author also downloaded the 'Big Dict' dictionary file but due to time constraints again it was not actually possible to run a password cracking tool. However, the Finance department was asked for their actual password in order to check against the dictionaries used by these programs. The author managed to find the password in the 'Big Dict' dictionary, but not in the 'Dict Make' generated dictionary. This means that any password cracking tool using "Finance" as username, and a password from the 'Big Dict' dictionary, would be able to get into the Finance account.

SECURITY SCAN FINDINGS

The tests have shown that it is very easy to get detailed information about the network and the servers by using publicly available tools from the Internet. After discussing the test results with the Network Administrator and management the following course of action was outlined.

Web Server

There are too many open ports on the web server. Ports 21 - File Transfer Protocol (FTP) and 80 - Hyper Text Transfer Protocol (HTTP) to be open. Ports 25 - Simple Mail Transport Protocol (SMTP) and 110 -Post Office Protocol (POP3) are meant for e-mails, they should not be open on a web server. The MySQL database has been moved to another server, this port 3306 should also be closed.

Intranet Server

The intranet server shows a lot of open ports. Port 110 (POP3) certainly should not be open since we do not use this server for e-mails. Ports 135, 139, and 445 are used for Microsoft networking and should allow connection only from the Internal LAN. The Network Administrator could not identify yet why the other ports are open and what they are used for.

Other Issues

Due to the shared nature of the network (Ethernet hub), it is easy for anyone on the internal LAN to use a sniffer tool to get the login names and passwords. Although the list of 'sniffed' packets can be very long, it is still relatively easy to identify packets with the relevant IP Address and Port Number (this search can be easily automated).

Since e-mails are not encrypted, anyone can read e-mail content directly from the network using a sniffer program.

The password for the Finance department is too straight-forward. Many password crackers would be able to break it easily. It is assume that many of the staff are using very simple passwords.

It would be difficult to prevent spoofing and denial-of-service attacks. We will have to rely on the proposed Intrusion Detection Systems (IDS) to monitor and detect such attacks.

Since it is easy to obtain usernames and passwords, it is also easy to gain unauthorized access to, and modify data files.

PROPOSED SECURITY MEASURES

In addition to the Recommended Security Counter-Measures, and Security Policies and Procedures from the recently conducted risk analysis, the following additional recommendations were also made:

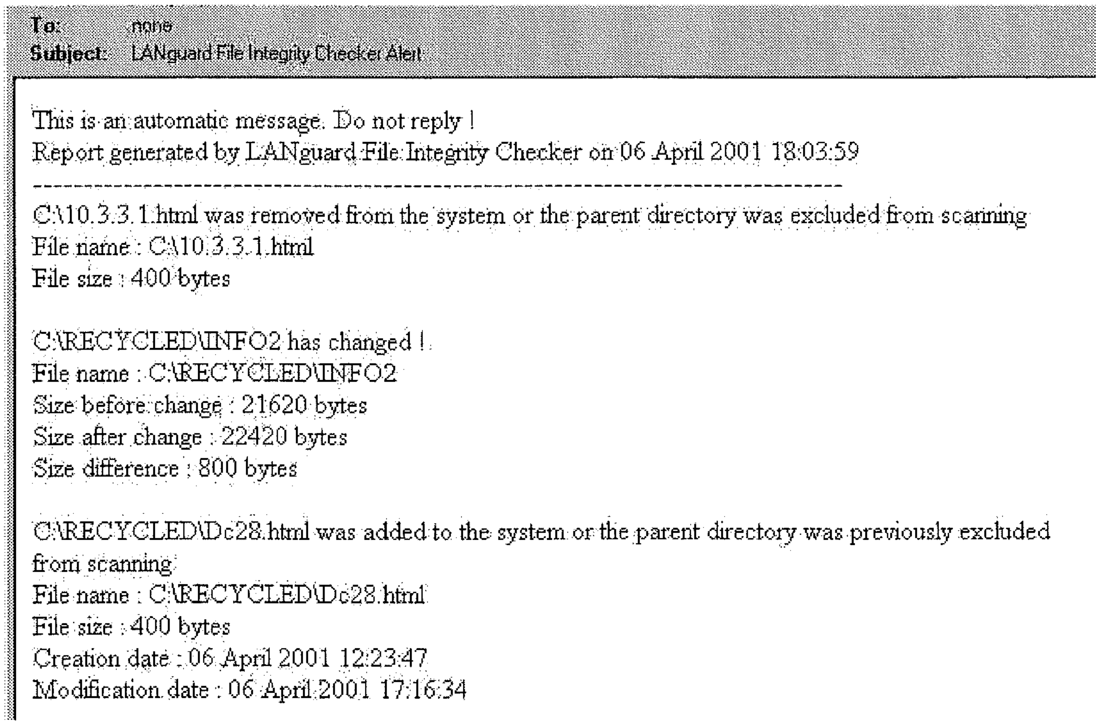
All unneeded ports and services on the network and servers must be disabled.

To replace the Ethernet hub with an Ethernet switch to prevent unauthorized monitoring of the network.

To use PGPi, an international variant of PGP (Pretty Good Privacy) to encrypt all our emails. We can obtain a commercial use license for PGP 6.5.1i Windows 95/98/NT from Network Associates Inc. at (www.pgpinternational.com).

To enhance the Password Policy and include the following:
Must contain at least 2 numbers
Must not begin or end with a number

To install a file integrity check software, to provide baseline intrusion detection by checking whether files have been changed, added or deleted on all servers. The author tested the LANguard File Integrity Checker (www.languard.com) see Figure 7. After deleting file C:\10.3.3.1.html, an e-mail alert was received about the event:



```
To:       none
Subject:  LANguard File Integrity Checker Alert

This is an automatic message. Do not reply !
Report generated by LANguard File Integrity Checker on 06 April 2001 18:03:59
------------------------------------------------------------------------------
C:\10.3.3.1.html was removed from the system or the parent directory was excluded from scanning
File name : C:\10.3.3.1.html
File size : 400 bytes

C:\RECYCLED\INFO2 has changed !
File name : C:\RECYCLED\INFO2
Size before change : 21620 bytes
Size after change : 22420 bytes
Size difference : 800 bytes

C:\RECYCLED\Dc28.html was added to the system or the parent directory was previously excluded
from scanning
File name : C:\RECYCLED\Dc28.html
File size : 400 bytes
Creation date : 06 April 2001 12:23:47
Modification date : 06 April 2001 17:16:34
```

Figure 7: File Integrity Checker

Lastly, there is a need to check on the security measures taken by our Internet Service Provider (ISP) to ensure that DNS exploits will be prevented.

CONCLUSION

This case outlines some serious implications for existing networked installations. The level of sophistication and ease of use of the network intrusion tools as demonstrated in this case is now such that a novice can effectively use them to compromise a network. The threat type for persons capable of attacking your systems has widened greatly as these intrusion and attack tools have become more sophisticated. The implication is here that the myth of the archetypal bespectacled, myopic, adolescent male, nerd, aka hacker is fast becoming an anathema.

The programs and information used in this case was largely acquired from Internet sites and sources which any Internet connected user has access to. Managers of Internet connected systems should now have these style of tests deployed against their existing systems before another network user does whether that be external or an internal attack. Only by closing and hardening the network defences by incorporating these tools into a network security program can we start to effectively repel the automaton hacker.

REFERENCES

Atelier Web Security Port Scanner v4.04. Evaluation copy. José Páscoa. [On-line] http://www.atelierweb.com/pscan/index.htm

CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks. (November 29, 2000). CERT Coordination Centre. [On-line] http://www.cert.org/advisories/CA-1996-21.html

CommView v2.5. *Evaluation copy.* TamoSoft, Inc. [On-line] http://www.tamosoft.com/products.htm

Controlling Internal Abuse Through The Process Of Security. (January 12, 2001.) EarthWeb by Internet.com Corporation. [On-line] http://networking.earthweb.com/netsecur/article/0,,12084_625611,00.html

Critical Patches. (April 3, 2000). Active Network. [On-line] http://www.activewin.com/win2000/patches.shtml

Dict Make generator and Big Dict dictionary. HNC Network. [On-line] http://www.hack-net.com/archives/browseCategory.php?cat=Dictionary%20Genorators

Hacking Techniques. (April 3, 2001). Security Watch. [On-line] http://www.securitywatch.com/EDU/ency/hacking_techniques.html

IP Tools version 1.11. Evaluation copy. KS-Soft. [On-line] http://www.ks-soft.net

LANguard File Integrity Checker v1.0. Freeware. GFI Software Ltd. [On-line] http://www.languard.com

LANguard Network Scanner v1.0. Freeware. GFI Software Ltd. [On-line] http://www.languard.com

Password cracking. Section 1.4.3. FAQ: Network Intrusion Detection Systems. (Version 0.8.3, March 21, 2000). Technical Incursion Countermeasures. [On-line] http://www.ticm.com/kb/faq/idsfaq.html

SYN Flood. Section 1.10.2. FAQ: Network Intrusion Detection Systems. (Version 0.8.3, March 21, 2000). Technical Incursion Countermeasures. [On-line] http://www.ticm.com/kb/faq/idsfaq.html

Voeten-Lim Alice. Risk Analysis. (April 15, 2001). Section 3. Recommended Security Counter-Measures And Contingencies. MIS5292 Assignment 1.