

Fall 2002

ACUTA Journal of Telecommunications in Higher Education

Follow this and additional works at: <http://digitalcommons.unl.edu/acutajournal>

"ACUTA Journal of Telecommunications in Higher Education" (2002). *ACUTA Journal*. 24.
<http://digitalcommons.unl.edu/acutajournal/24>

This Article is brought to you for free and open access by the ACUTA: Association for College and University Technology Advancement at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in ACUTA Journal by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

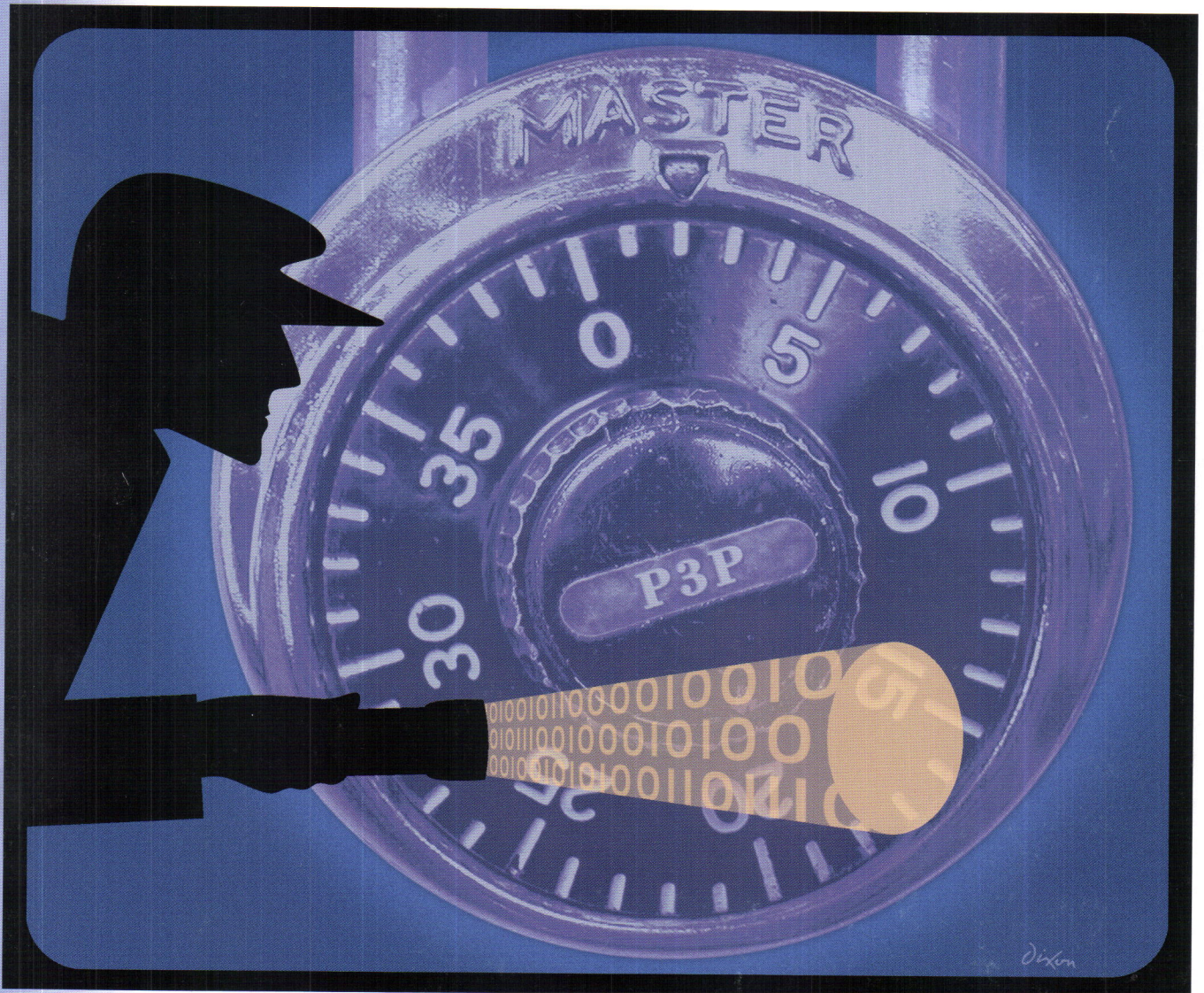
Fall, 2002
Vol.6, No.3

acuta

Journal

of Telecommunications in Higher Education

Published by The Association for Communications Technology Professionals in Higher Education



This Issue: Privacy and Security Issues

Beautiful on the outside. Tough as nails on the inside.



The new B series from Teledex. The shape of things to come.

Don't let looks fool you. This is a real workhorse. It just looks like it'll steal your heart.

The new Teledex B series features six distinct models, from the no-frills B100 single-line set, to the full featured B450D four-line display set. Each built Teledex tough. Which means that the years of expertise we've gained from being the world's



Innovative, World-Class Telecommunications Solutions

leading supplier of terminals to the hospitality industry, where telephones suffer unbelievable abuse on a daily basis, has resulted in durable, elegant sets that enhance any campus setting. All at a price that will make even the toughest bean counter smile. See all the new Teledex B series telephones now at www.teledex.com.

Events Calendar

Event	Date	Place
Fall Seminars	October 20 – 23, 2002	Marriott City Center Denver, Colorado
Winter Seminars	January 12 – 15, 2003	Wyndham Buttes Resort Tempe, Arizona
Spring Seminars	April 27 – 30, 2003	Sheraton Norfolk Waterside Norfolk, Virginia
Annual Conference	July 27 – 31, 2003	The Westin Diplomat Resort and Spa Hollywood, Florida

ACUTA's Core Purpose is to: Support higher education institutions in achieving optimal use of communications technologies.

ACUTA's Core Values are to:

- Share information, resources and insight,
- Respect the expression of individual opinions and solutions,
- Maintain our commitment to professional development and growth,
- Advance the unique values and needs of higher education communications technologies, and
- Encourage volunteerism and individual contribution of members in support of organizational goals.





Colleges and universities face the additional challenge of protecting themselves from accidental and intentional threats posed by an exceptionally intelligent and curious internal community.”

Ted Udelson
Integrity Computing
page 6

THE ACUTA JOURNAL OF TELECOMMUNICATIONS IN HIGHER EDUCATION

Published Quarterly by

ACUTA: The Association for Communications Technology Professionals in Higher Education
152 W. Zandale Drive, Suite 200
Lexington, KY 40503-2486

PHONE 859/278-3338
FAX 859/278-3268
E-MAIL pscott@acuta.org

Publisher

Jeri A. Semer, CAE, Executive Director

Editor-in-Chief

Pat Scott, Communications Manager

Contributing Editor

Curt Harler

Advertising Sales

KCS International, LLC
717/397-7100 or www.kcsinternational.com

Submissions Policy

The ACUTA Journal welcomes submissions of editorial material. We reserve the right to reject submissions or to edit for grammar, length, and clarity. Send all materials or letter of inquiry to Pat Scott, Editor-in-chief. Author's guidelines are available upon request or online at www.acuta.org.

The opinions expressed in this publication are those of the writers and are not necessarily the opinions of their institution or company. ACUTA, as an association, does not express an opinion or endorse products or services.

The ACUTA Journal is published four times per year by ACUTA, a nonprofit association for institutions of higher education, represented by telecommunications managers and staff.

Contents of this issue of *The ACUTA Journal* are copyrighted: © 2002, ACUTA, Lexington, Kentucky.

ISSN 1097-8658

POSTMASTER, send all address changes to:

ACUTA
152 W. Zandale Drive, Suite 200
Lexington, KY 40503-2486
Postage paid at Louisville, Kentucky.

Visit the ACUTA site on the World Wide Web:
<http://www.acuta.org>

Membership and Subscriptions

Subscriptions are provided as a benefit of membership. The publication is available to nonmembers for \$80 per year or \$20 per issue. For information, contact Kellie Bowman, Membership Development Manager, 859/278-3338, ext. 22, or e-mail, kbowman@acuta.org.

ACUTA

2002-2003 Board of Directors

President

Jeanne Jansenius, University of the South

President-Elect

Walter L. Czerniak, Northern Illinois University

Secretary/Treasurer

John Bradley, Rensselaer Polytechnic Institute

Immediate Past President

Maureen Trimm, Stanford University

Directors-at-Large

Dave Barta, University of Oregon

William A. Brichta, DeSales University

Tamara J. Closs, Georgetown University

Mary L. Pretz-Lawson, Carnegie Mellon University

Patricia Todus, Northwestern University

Publications Committee

James S. Cross, PhD, Michigan Technological University, *Chair*

Felecia Flack, Northern Michigan University

Angela Imming, Southern Illinois University at Edwardsville

Ron Kovac, PhD, Ball State University

Walt Magnussen, Texas A & M University

Barb Renner, University of Cincinnati

Jon VanderMeer, Western Michigan University

Ex Officio

Jeanne Jansenius, University of the South

Jeri Semer, CAE, ACUTA Executive Director

Board Advocate

William A. Brichta, DeSales University

Staff Liaison

Pat Scott, ACUTA Communications Manager

Editorial Review Board

Diane Blake, University of California, Los Angeles

James S. Cross, PhD, Michigan Technological University

Larry Farmer, Drew University

Jay Gillette, PhD, Ball State University

Ray Horak, The Context Corporation

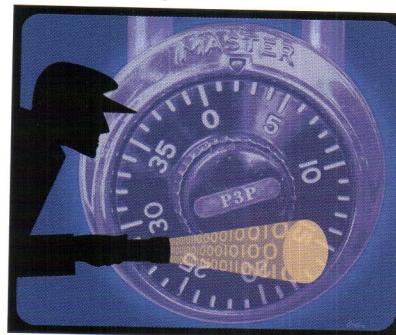
Angela Imming, Southern Illinois University, Edwardsville

Mick McKellar, Michigan Technological University

Dave Metz, Compass Consulting International, Inc.

Contents

Fall 2002 • Volume 6, Number 3
Privacy & Security Issues



Cover design by John Dixon

FEATURES

6

System Security Policy: What It Is and Why Every Campus Needs One

Ted Udelson

This article introduces the concept of security as a process which results in a policy, describing characteristics and features of a security policy as well as rights and responsibilities of those to whom it applies.

10

Missouri Integrates Firewall and VPN Technology for Added Security

Nathan Eatherton

Firewalls and VPN technologies are no guarantee that the network is completely secure, but they are valuable pieces of the security plan at the University of Missouri-Columbia.

14

College-Based Programs Boost Computer Security

Curt Harler

Programs and organizations such as CERT, CIP, and CSDS are helping network administrators practice safe computing. Read about these as well as some campuses that prefer to handle security themselves.

20

Privacy on Today's Electronic Campus

Tracy Mitrano

Electronic communications have raised a wide range of new questions and concerns about liability, governance, surveillance, and privacy in general. From the perspective of Cornell University, Mitrano looks at these and other privacy-related issues.

24

Current Trends in Information Security at UW-Madison

Kim Milford and Jeffrey Savoy

To reduce risks to departmental computing resources at the University of Wisconsin at Madison, Information Security provides a variety of tools, training, and services.

36

Watching the Network

Earl Carter

Yesterday's security standards are no longer sufficient to guard networks that are accessible by faculty, staff, and students. An intrusion detection system may be the best hope for protecting your campus resources.

42

Cybercrime: Are You Ready?

Megan Statom

For those who feel unprepared to meet the security challenges of the 21st century, training is available at every level from a host of sources.

SPECIAL: SECURITY AGENDA

32

Privacy Bills Before Congress

Amy Worlton

38

Design and Operations Criteria: Trust No One

Ron Walczak, RCDD

44

Managing the Threat from Within

Tad Deriso

INTERVIEW

28

with David Safford

Manager, Global Security Analysis Lab, IBM

COLUMNS

4

President's Message

Jeanne Jansenius, University of the South

48

From the Executive Director

Jeri A. Semer, CAE

BOOK REVIEW

41

Information Security Best Practices

by George L. Stefanek

Reviewed by *Justin M. McNutt*

BILL D. MORRIS AWARD

45

Corinne Hoch

Columbia University

ADVERTISERS' INDEX

46

Thanks to the companies who support ACUTA by advertising in our Journal.

PRESIDENT'S MESSAGE



Jeanne Jansenius
University of the South
ACUTA President
2002-2003

Locking the Doors

When I was growing up and until my 20s, it was not uncommon to leave the doors to the family home and car unlocked. Security was not an issue in most neighborhoods, and there was always the unofficial neighborhood watch (that delightful well-informed neighbor). Yes, times have changed. Communications technology must now cope with trap doors, worms, hoaxes, Trojan horses, and thousands of viruses.

While recently planning for the renovation to my home, even in the remote location of Sewanee, Tennessee, I included the cost of installing a state-of-the-art home security system. I justified it by telling everyone that it was for fire protection, but like everyone I am beginning to worry about security. The point being, the good ole days are long gone. Security is an issue regardless of what medium you are trying to protect. It is no longer a simple means of protection by locking the data center doors as we could 20-plus years ago when most applications were run in batch mode with no remote access. The Internet has brought everyone to our back door. Computer networks have revolutionized the way we do business, but the risks involved can be fatal due to loss of funds, time, and—thank goodness in rare cases—life.

One of the major issues of network security is to keep information that is key to the organization confidential and assure privacy to protect the organization from damage or loss that could occur from the disclosure of the confidential information. The integrity and accountability of the information is also key to the success of the organization. As in any business, upper

management makes decisions based upon sound financial analysis. While it is important to keep information confidential and accountable, information must be accessible on the network for prospective students, employees, and administration in order to make appropriate decisions. How can a business feel secure while at the same time providing accessibility to its assets?

Since September 11, whom or what to trust has become a key concern. How do we protect ourselves from danger and provide the services that our employees and customers expect? How do we protect our identity? Identification, authentication, authorization, and cryptography continue to be developed and improved. The revolution of e-commerce is transforming personal data into a commodity. This privacy drain will continue.

According to Dr. Lance Hoffman, a professor of computer science at George Washington University and director of the School of Engineering's Cyberspace Policy Institute, "We will also see increased use of screening browsers built into handheld devices, such as PDAs. Starting with the Platform for Internet Content Selection (PICS) for content control, we will proceed to filter interaction rules as well as content rules using mechanisms like the Platform for Privacy Preferences (P3P), which enables Web sites to express their privacy practices—and users to exercise (automatically, if desired) preferences over those practices. P3P will support digital certificate and digital signature capabilities and can be incorporated into browsers, servers, or proxy servers."

On May 25, 2000, Richard D. Pethia, director of the CERT® Centers Software Engineering Institute at Carnegie Mellon University, testified before the U. S. Senate Judiciary Committee: "[T]he recent rash of attacks on the Internet demonstrates how quickly automated attacks can spread across the network and hints at the kind of damage that can be done. Incident response organizations are able to limit damage by working effectively together to analyze the problem, synthesize solutions, and alert the community to the need to take corrective action ... The long-term solutions to the problems represented by new forms of automated attack will require fundamental changes to the way technology is developed, packaged, and used. It is critical that system operators and product developers

recognize that their systems and products are now operating in hostile environments ... As new forms of attack are identified and understood, developers must change their designs to protect systems and networks from these kinds of attacks." (http://www.cert.org/congressionaltestimony/Pethia_testimony25May00.html)

The popularity and ease of installation of wireless technology is only making security breaches easier. Wireless access point devices are plugged directly into an enterprise network. Employees are bringing access points through the back door without the communication technology folks even knowing they are on the premises. With a \$99 wireless LAN card someone can transmit sensitive data while sitting in an adjacent parking lot. Serious hackers can even use long-range

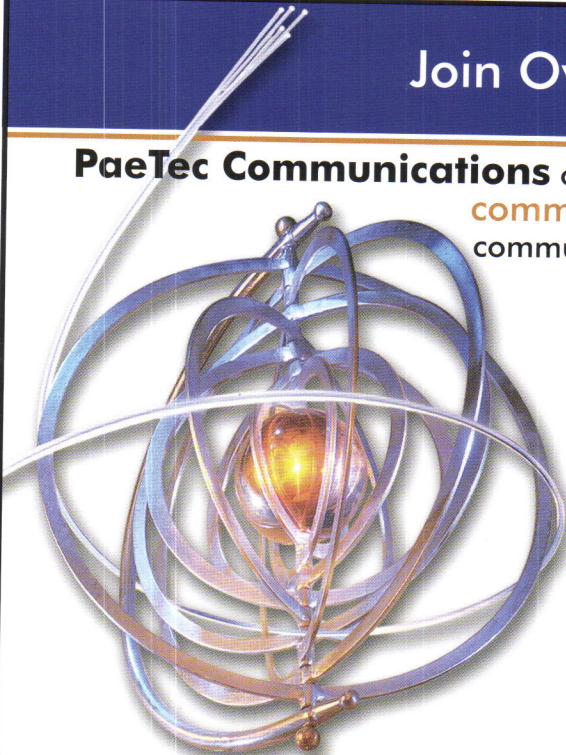
antennas from a distance of 1,000 to 2,000 feet.

It is never too late to plan and implement security and privacy policies and practices. The articles in this issue of the journal are intended to provide experience and guidelines on security and privacy issues. As communication technology networks grow more complex, no one person can be expected to control all aspects relating to security. It is also more effective if the process of security and privacy issues start from the top. Offense seems to have significant advantages over defense in most cases as it is more effective to identify and try to manage security risks up front than to implement damage control later.



Join Over 275 Fellow Colleges and Universities

PaeTec Communications offers our Higher Education customers the most **comprehensive communications solution** in the business. We provide an integrated communications offering, tailored specifically for colleges and universities.



- Advanced **voice** services: local and long distance
- Enhanced high-speed **data**: Internet, Email and VPN
- **PINNACLE** Communications Management System*
- **Campuslink** Student Billing and Management Services
- Unique **revenue-sharing** programs
- Unparalleled customer service

***PINNACLE** provides billing and operations management tools for **convergent voice, data and video networks**. Enjoy the benefits of this comprehensive web-based solution as either a PaeTec-hosted (**ASP**) or in-house implementation.



877.7PAETEC

WWW.PAETEC.COM



System Security Policy: What It Is and Why Every Campus Needs One

by Ted Udelson
Integrity Computing

Our concerns about system security continually increase—and not without justification. Crimes reported to the Computer Emergency Response Team (CERT) more than doubled in each of the last three years, increasing from 252 in 1990 to 52,648 in 2001. And if the security threats from the outside aren't enough, colleges and universities face the additional challenge of protecting themselves from accidental and intentional threats posed by an exceptionally intelligent and curious internal community. The academic world promotes curiosity, fostering an environment conducive for inquiring minds to peek, poke, peer, and penetrate. Clearly, a system security policy is essential.

What Is a System Security Policy?

A system security policy is a document that establishes our priority for securing our systems. It prevents the loss of assets, identifies and mitigates our risks, and minimizes the impact of security breaches on organizational assets. A security policy identifies the assets we're trying to protect, documents the vulnerabilities posed against those assets, and plots a strategy to protect those assets, including hardware, software, intellectual property, private information, documentation, goodwill and reputation, people and skills.

The security policy is a living document that organizations must modify as information assets change and as the threats against those assets change. It provides a framework for which we select, implement, and configure our systems and networks. Finally, the security policy provides standards of use for the organization's resources, removing excuses for unacceptable behavior. A security policy is more than just a document that specifies rules and concepts of how to protect our systems. It's a process. The security policy is a series of decisions balancing the need for

security versus cost, capability, and convenience.

The security policy provides a vehicle for us to make decisions with regard to other important policy matters:

- It affects budgeting for security-related measures and all IT projects
- It affects how we select, configure, back up, and manage our systems
- It determines how we react to a security breach

Why Do We Need a Security Policy?

The security policy serves as a blueprint for our security architecture. We need to make sure that our policies are followed, so we must document them. After all, an unwritten policy is no policy at all. We further need to audit practice against policy to ensure adherence, so we know our security practices are effective. Lastly, we can review the written policy to ensure that our protection is up-to-date and relevant.

How do we know our systems are secure without defining what *secure* means? An organization can say, "We've never been attacked," but how do we know? Digital assets are so extensive that there is no practical way to check them individually. Without a policy and procedures to implement it, we can't really know if we've been attacked. The security policy doesn't just define what *secure* means—it identifies how it's measured.

The security policy process requires us to decide our institution's tolerance for risk. We then determine the resource commitment we're going to make to ensure we reach that level of acceptable risk. As part of this process, we balance the need for security with the need for capability; the cost of securing systems versus the cost associated with security breaches; the need to keep private

information confidential, systems available, and data sources reliable versus the inconvenience and practicality of our security policy ramifications.

As part of the security policy process, we ask, "What are we trying to protect?" Do we have sensitive data such as credit card numbers, ACH (direct deposit) numbers, patient records, social security numbers, financial records, student records, donor history, and investment information? Do we have proprietary research data or other intellectual property we must protect? Do we have information that health insurance portability and accountability act of 1996 (HIPAA) mandates us to protect?

Lastly, in a crisis, unprepared staff can make precipitous and inappropriate decisions. The security policy process not only reduces such opportunities, it also should dictate who has the autonomy to make which decisions under what circumstances.

What Are the Characteristics of a Security Policy?

Most important is that the policy be both accepted and enforceable. Security breaches inevitably follow if our systems' users don't follow the rules. Furthermore, if we can't enforce policy, what makes us think that people will follow the rules?

The security policy must be useful and easy-to-understand. We want to structure the security policy so that we can easily locate important information. Top-level management must sanction the document as official. The document must be carefully worded to avoid confusion. The policy should have definitions included to eliminate ambiguity from the document. The policy's wording can determine criminality should someone violate its precepts. The document should provide guidelines rather than procedures. (Often procedures follow naturally from the guidelines). Each revision of the security policy should have a version number and date of revision.

One feature often forgotten by security administrators is that the policy should be well advertised and well understood. We can accomplish this through publicity and training. The policy itself should document how the document should be publicized. We publish applicable sections to those entities for which those sections apply. We can do this because we have organized the policy into discrete sections.

One important component of advertising is to mandate a log-on banner. A log-on banner mandating appropriate use of systems eliminates the "I didn't know" excuse for security breaches. In many states, lack of a log-on banner prohibiting unauthorized use limits criminal prosecution.

We should review our security policy at least once per year to ensure that it is up-to-date. We should also specify other times that would be appropriate for review—for example,

it would only follow that we mandate a review of our security policy after a major security incident occurs. Of course, in our tightly worded policy, the term *major incident* would be well defined!

Who Should Get Involved?

To start, organizational leaders must embrace the concept of a security policy. Without leadership from the top, the resources and commitment necessary to implement the policy will not follow. People won't adhere to the guidelines set forth in the policy without the clout of your organization's leadership. Departmental leaders must get involved because individual departments have their individual technology requirements and their individual security requirements. Students and faculty must get involved because they too have a stake in those security decisions.

Lastly, we need the organization's counsel to review and bless the



VIBES
TECHNOLOGIES

Here for you...

Telecommunications and data networking products with exceptional service, value, and reliability

- Save up to 70% with a 2 year warranty on VIBES certified remanufactured telecom products
- Save an additional 10% on your first online order at www.vibestech.com
- VIBES buys and sells new and remanufactured equipment. We also repair and advance replace products within 24 hours

VIBES is now a direct premium partner of

NORTEL NETWORKS™

Let us buy your old, out-of-service products

www.vibestech.com
1-877-237-0948 (toll free)

**NORTEL
AVAYA/LUCENT
CISCO
PLANTRONICS
EXECUTONE
ASPECT
POLYCOM
ADTRAN**

document to ensure that it is both legal and consistent with the institution's other policies. Once final, our security policy must be distributed to and understood by all levels of the organization.

Rights and Responsibilities

For each group involved, we need to specify rights and responsibilities. For users, we need to specify account use and software and data access. Users must also know the rules about passwords (not sharing them, not writing them down, etc.). Users should also know their rights, such as their right to privacy, and under what circumstances they will lose those rights. They should also know which individuals may revoke those rights.

For system managers or network administrators, we must specify backup procedures, system configuration guidelines, authentication requirements, and auditing and monitoring requirements. Someone must be responsible for overseeing users to make sure that they live up to their responsibilities—and we must also specify who will oversee the overseers.

What Do We Put in Our Security Policy?

Our security policy must first inventory our systems and assets. For each asset, we need to discuss the four phases of security: vulnerability, prevention, detection, and recovery.

1. Vulnerability

Appropriate parties should discuss, in detail, the vulnerabilities that pose threats against each system. Knowing the threats, we then need to determine the methods to prevent intrusion. Normally we try to protect ourselves in the following areas:

- **Authenticity:** to ensure that whoever accesses our systems is who we think they are
- **Privacy:** to make sure that only authorized individuals can access confidential information
- **Integrity:** to make sure that the information is not tampered with or otherwise altered

- **Availability:** to ensure that authorized individuals can access systems they need

For each threat, the security policy will address the probable impact and the maximum impact of each kind of event.

As part of our vulnerability assessment, we need to identify the value of each asset and indicate what the loss of that asset would represent as well as how it would be replaced.

2. Prevention

Knowing the vulnerabilities, we can then prescribe preventive measures. We should give preference to technology for preventive measures because technology is consistent in how it will deal with an issue. Then again, humans always set up technology, so there is that point of contention. We need to prescribe measures to authenticate users and systems. Notice that the other three phases of security depend on authenticity, so we must pay particular attention to authenticating our users. Passwords have become almost trivial to crack or intercept, and one day soon they'll be outdated altogether in favor of one of the following:

- **Security tokens**—synchronized, ever-changing passwords through password token devices
- **Biometrics**—authentication by use of some unique biological characteristic like fingerprints, retina scans etc.
- **One-time passwords**—passwords used but one time and changed after each log-in. This makes it nearly impossible to guess passwords

As part of the prevention process, we need to specify acceptable use. Much damage is done to systems through inappropriate use. Without specifying acceptable use, universities invite unnecessary damage to their computer systems. As implied earlier, our policies must be adhered to and enforced. Our policy must specify who will audit adherence and what

penalties apply to each kind of infraction. We must always make the penalties proportionate to the infraction. We must treat accidents differently from malicious conduct, and we must define terms such as *malicious* and *accident*.

3. Detection

Network administrators often forget that detection is just as important as prevention. If someone is in the process of attacking our systems, what will we do? If we determine that someone has already compromised our systems, what will we do to limit the damage? Once damage is mitigated, how do we prevent further damage? How will we prevent future attacks? None of these questions can be answered, or even asked, without detection methods. We should define how we monitor our systems.

System logs are critical to detecting security breaches. Logging of exceptional events will allow system administrators to determine "normal" patterns of use, so that when abnormal patterns start, a security breach might have occurred. The security policy must specify how detection is to be accomplished, usually through logging and alerts. Furthermore, the policy must specify who is responsible for monitoring the logs and the alerts. Lastly, we should add fail-safes to ensure that those responsible are monitored as well.

4. Recovery

We must be prepared for times of crisis. Our security policy dictates how we handle these crises. First of all, whom should we notify and by what means? Have we documented important personnel's home and mobile phone numbers?

Some of the questions we must ask ourselves include the following:

- Do we let an event continue in order to catch the culprit?
- Have we secured the log files to preserve an audit trail of what happened? Better yet, do we ensure that an attacker cannot destroy log files?

- Do we shut down some critical services to prevent further damages?
- Do we contact legal authorities?
- What type of backups must be maintained to ensure a full (or at least acceptable) recovery? Better yet, have we tested our recovery procedures to ensure acceptable recovery?

Answering these questions is part of the process that the security policy takes us down. Having prepared the answers avoids precipitous, if not inappropriate, action during the time of a crisis.

Once we recover from an incident, we need to use the information gathered in the recovery and detection phase to improve our understanding of the vulnerability phase. As part of this feedback loop, we need to ask if the policy was followed and how the policy can be changed to prevent similar events in the future.

What Are the Special Challenges Facing Academic Institutions?

Academic institutions face special challenges not faced by commercial or government entities, including:

- They comprise many autonomous entities that have complex trust relationships with each other.
- They have difficulty in controlling end users.
- The culture cultivates free thinking and “open” access to information.
- They have a *network anarchy*—that is, just about anyone can attach to the network at any time. Furthermore, students have little organized supervision to control inappropriate behavior.
- The university serves as a research body, corporation, and Internet service provider. Colleges and universities must analyze each of these functions to determine the proper stance to take with regard to security.

Resources on the Web

http://www.brown.edu/Research/Unix_Admin/cuisp/: A compilation of computer policies from institutions of higher education—a “must” resource for colleges and universities.

<http://www.sans.org/newlook/resources/policies/policies.htm>: from the System Administration, Networking and Security Institute—probably the best resource for security policies. Provides dozens of resources and links to sites that instruct on how to write an effective security policy.

<http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2196.html>: An official Internet request for comment, a guide to developing computer security policies and procedures for sites connected to the Internet.

<http://secinf.net/info/policy/netsec1.htm>: How to develop a network security policy.

<http://secinf.net/info/policy/AusCERT.html>: Site security policy development—outlines issues one *should consider when writing a security policy*.

http://downloads.securityfocus.com/library/Why_Security_Policies_Fail.pdf: A white paper from Control Data Corporation, “Why Security Policies Fail,” or better named, the characteristics of successful security policies.

On top of all that, most universities have pretty rigid security requirements. Answering the questions involved in developing a sound security policy that balances security with cost, capability, and convenience is easier in less complex organizations.

Conclusion

The security policy is both a journey and a destination, and this journey leads to the destination of more secure systems. The security policy process involves everyone, especially top management, and all levels of the organization. It must be adhered to

and enforceable. It lists our information assets through four phases of the security process: vulnerability, prevention, detection, and recovery. It protects our assets in the areas of authenticity, privacy, integrity, and availability.

Ted Udelson, president of Integrity Computing, can be reached at TedU@IntegrityComputing.com. Integrity Computing, Inc., is a technology firm that provides technology strategic planning, needs assessments, network consulting, and security.



Mizzou Integrates Firewall and VPN Technology for Added Security

by Nathan Eatherton
University of Missouri, Columbia

The commodity Internet has changed how many college and university departments conduct research, interact with students and other affiliates, and share information both internally and around the world. With new laws and regulations being passed (i.e., the Children's Internet Protection Act and the Health Insurance Portability and Accountability Act) and with heightened security requirements for e-business and credit card transactions, schools must take the proper measures to ensure compliance and protection.

At the University of Missouri-Columbia (MU), the department of Information and Access Technology Services (IAT Services) has implemented both firewall and virtual private networking (VPN) services to help protect the campus network, its systems, and the data stored within.

Firewalls

First, a little about why firewalls are needed, exactly what they do, and how IAT Services manages this technology at MU.

Almost every mid-to large-size business or organization uses a local area network (LAN) to effectively share resources and communicate with others on its local network. Many of these LANs have a connection to the Internet, extending these benefits outside the local network and around the world. Unfortunately, this

connection to the Internet presents an exponentially increased security risk.

Internet connections allow both inbound and outbound traffic; on the plus side, LAN users can access an abundance of information and resources outside their local network. The associated risk, of course, is that they simultaneously open up their network to incoming Internet traffic.

Sometimes this incoming Internet traffic is desirable, as is the case when providing services across the Internet. Other times, Internet traffic takes the undesirable form of hackers who are looking to compromise the LAN as well as the systems and data resources contained within. Firewalls can help protect against these actions.

A firewall is a network device that serves as a checkpoint between multiple networks. It is configured with specific rules specifying exactly what can and cannot be passed between the networks. These rules can be based on IP subnets, specific IP addresses, MAC addresses, and TCP/IP ports among others. A firewall examines the traffic being passed from one network to another and routes (or denies) the traffic accordingly. The typical firewall design includes a minimum of two security zones. One is very secure, restricting most, if not all, access from the outside networks. Others are less restrictive than the first but still maintain a base level of security. Firewall administrators tend to place servers containing nonpublic or sensitive data, such as credit card information, medical records, or research, in the secure zone while providing baseline protection for staff workstations in the less restrictive security zones.

Sometimes this incoming Internet traffic is desirable, as is the case when providing services across the Internet. Other times, Internet traffic takes the undesirable form of hackers who are looking to compromise the LAN as well as the systems and data resources contained within.

There are two methodologies used to deploy firewalls at MU. The first is to strategically place them on the enterprise network to help protect MU from the outside world. Currently there are two firewalls on the enterprise network: one in front of the departmental network and another in front of the residential student network. These firewalls are used to apply general security rules based on preapproved policies that are appropriate for each of these networks. Since the restrictions applied to these firewalls are general in nature, another level of firewall security may be needed.

This second level of firewall protection is positioned on individual building or departmental networks. Because many MU departments have unique network security requirements, these firewall restrictions are customized per the departmental needs, offering multiple zones of varying security levels.

Beyond the obvious security need, there were other reasons for IAT Services to offer a centralized firewall service to departments. Before the departmental firewall service was offered, a handful of departments had bought and were self-maintaining their own firewalls. Since these departments didn't purchase the same firewall product, different knowledge bases were required to manage each firewall device. Many of these departments had only one or two technology experts, so there was a risk involved with the depth of support, and there were inefficiencies since firewall management was not the primary responsibility for these individuals. Seeing this trend, IAT Services adopted the Cisco Secure PIX 500 Firewall Series as the campus standard, based on its feature set and scalability, and leveraged the preestablished network security group to specialize on, manage, and support this product line. This decision increased the efficiency involved with

The Call Center... ...that Connects



Higher education deserves the highest level of call center efficiency. And STARTEL's Call Center Solutions make the grade. They include a full range of operator services for everything from an Intelligent Console and Online Directories to Centralized Attendant, Help Desk, even Facilities/Security Monitoring. STARTEL also gets an A+ for keeping your staff in touch — on and off campus. Features like Operatorless Paging, Automated Dispatch, Web-Enabled & Wireless Interfaces and more bring your college or university into the 21st century of communications.

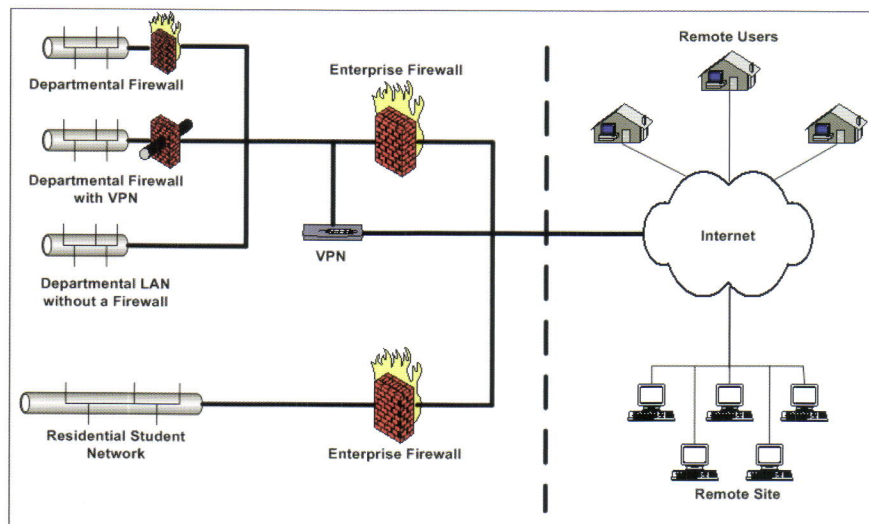
- **Directory & Information Services**
- **Campus Security**
- **Help Desk**
- **Reverse 911 Response**
- **Web-Enabled & Wireless Interfaces**



Call Center Solutions

Call (800) 782-7835 for more information
www.startelcorp.com

Figure 1: MU Network Infrastructure: Firewalls and VPN



firewall management and enabled IAT Services to provide a cost-effective service. Departments pay the purchase price of the firewall box, an initial setup fee, and monthly maintenance. The maintenance cost includes the manufacturer's maintenance and routine maintenance tasks performed by IAT Services, like code upgrades and maintaining backup copies of device configurations. Additionally, IAT Services maintains a baseline level of spare firewall equipment should a box fail and need immediate replacement. Subsequent firewall configuration changes and/or in-depth consulting services are billed on a time-and-materials basis.

Virtual Private Networking (VPN)

VPN technology offers several benefits revolving around a variety of remote access services, network and data security through authentication and encryption, and potential cost savings. At MU, VPN is used in conjunction with firewalls to enhance the overall security of the campus network infrastructure. VPN serves as a method for legitimate users to access MU-specific applications and re-

sources by allowing access around firewall-imposed restrictions that may be in place to block outside Internet service providers (ISPs) and untrusted sources.

There are four varieties of VPN services being implemented at MU: general, group, and LAN-to-LAN access, and direct VPN access to a departmental firewall.

The general access VPN service offering is a no-charge service designed for all MU faculty, staff, and students needing to access specific resources that are restricted at the enterprise firewalls. This service provides an encrypted tunnel to the campus network via an outside ISP connection at the end user's point of origin. Since accessing campus resources is the sole purpose of this service and the users already have an ISP, access from campus to the Internet is restricted to save on bandwidth consumption and to limit the VPN connection times, effectively freeing up resources for others to use.

The group access VPN service is similar in structure to that of the

general access service; however, it's geared toward departmental users who need guaranteed access and the same IP address each time they connect. This service is ideal for system administrators to securely manage their systems from a remote location. There is a monthly charge associated with this service since address space and VPN resources are allocated to a specific department.

The LAN-to-LAN service offering is hardware based, whereas the general and group services establish connections via client software. With a LAN-to-LAN connection, remote sites can establish a VPN connection through a VPN concentrator for their entire site, eliminating the need for each workstation to have a client running. This service is very cost effective for connecting remote sites because a dedicated WAN connection such as T1 or frame relay can potentially be eliminated. Instead, remote sites can purchase local ISP connections and use VPN to secure their communications with MU. A monthly charge is associated with the hardware maintenance and VPN connection since the service requires the allocation of specific VPN resources.

Finally, the departmental firewalls that are used at MU are capable of serving VPN connections to the specific network they protect. This VPN service is offered on a case-by-case basis and is configured at the time of the initial firewall implementation. Unless the department has a specific security concern whereby it needs remote connections encrypted across the campus network in addition to the Internet, departments are encouraged to use the general or group access VPN service. Departments are charged on a time-and-materials basis for IAT

Services to administer VPN on a departmental firewall.

Like many schools, MU provides remote access to its network in the form of dial-up modem pools, which can be expensive to maintain. With ISPs offering more competitive rates for high-speed broadband services such as DSL and cable, VPN may in some cases eliminate the need for colleges and universities to provide remote access in the form of dial-up and leased-line connectivity.

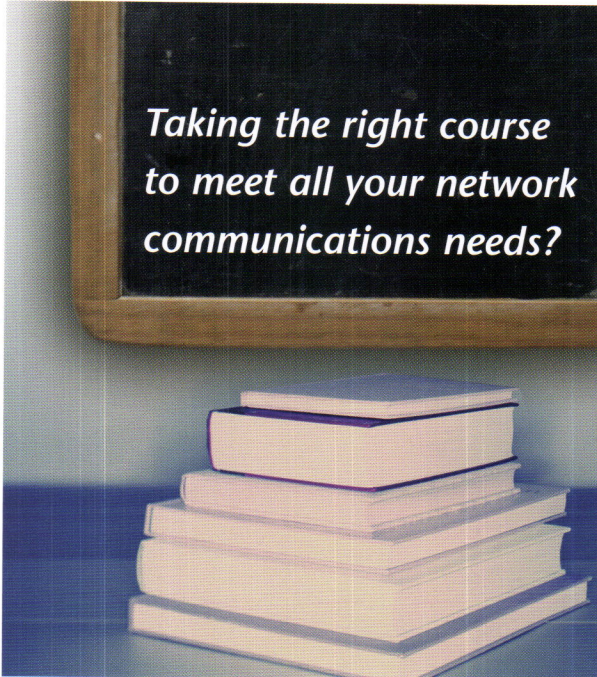
The combination of firewall and VPN services can help eliminate

trade-offs associated with implementing one service or the other. Firewalls can restrict all outside access to a system or its resources, allowing only authorized VPN connections if desired. VPNs can effectively extend a network wherever its users are located, be it in their homes, in their travels, or on sabbatical, offering security in the form of encryption back to the campus network. Additionally, by centrally managing these services, schools can take advantage of cost savings received from promoting internal efficiency.

Firewalls and VPN technologies are no guarantee that the network is completely secure—the SANS security forum identifies over-reliance on firewalls as part of the problem in their list of top 10 security mistakes businesses make—but they are valuable pieces of a security plan. It's a good idea to continually reevaluate the security requirements for a network, modifying the firewall and VPN rules along the way.

Nathan Eatherton is a business technology analyst at University of Missouri–Columbia. Contact him at eathertonn@missouri.edu.

III



*Taking the right course
to meet all your network
communications needs?*

At Daycom Systems, we partner with our customers to take a "big picture" view of their communications network challenges and organizational needs by offering total telecommunications solutions. Through our industry-leading services, we help our customers plan, design, install and maintain voice and data networks tailored to their specific requirements.

Contact us today to learn more about how our top-branded products and industry expertise deliver the solutions you need to support your educational institution now and in the future.

- Avaya voice & data systems for organizations of any size
- Enterprise class IP solutions (ECLIPS)
- CRM Enterprise solutions
- Call Center/CRM applications and equipment
- Carrier & Data Services Consulting
- Nationwide installation, project management and maintenance
- Avaya certified technicians
- 24-hour Help Desk
- Remote Diagnostics
- Customized maintenance contracts
- Conferencing equipment for video and voice

1.800.824.1661
www.daycomsystems.com

College-Based Programs Boost Computer Security

From music schools to software labs, colleges lead security endeavors

by Curt Harler
Contributing Editor

Universities are on the cutting edge of innovation in many fields, including computer security. While colleges are frequently—and justifiably—slammed both as being the source of and the incubators for distribution of computer worms and viruses, the fact is that colleges are among the leaders in protecting computer networks.

Safe computing is usually considered an individual responsibility: If you don't look out for your own network's health and safety, you deserve whatever bugs infect your system. However, many programs are available to help network administrators practice safe computing.

CERT, the Computer Emergency Response Team

The best-known and most active university-based security project is the CERT Coordination Center (CERT/CC). CERT, the Computer Emergency Response Team, is a center of Internet security expertise located at the Software Engineering Institute (SEI), a federally funded research and development center operated by Carnegie Mellon University in Pittsburgh.

CERT provides a reliable, trusted, single point of contact for Internet-related emergencies 24/7. In just the first quarter of 2002 a whopping 26,829 incidents were recorded by CERT. That's up from six incidents in 1988 and 132 in all of 1989. In fact, this year's January–March total represents about one-fifth of all the incidents (127,198) ever reported since the group began record keeping in 1988.

An incident may involve one site, hundreds, or even thousands of sites. Some incidents involve ongoing activity over long periods of time. Do these

statistics mean that hackers are becoming more obnoxious or that CERT is getting better at tracking incidents? History says it may be both.

Following the Morris worm incident, which brought 10 percent of Internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency charged SEI with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents. Since then, the CERT/CC has helped to establish other response teams. CERT's incident-handling practices have been adopted by more than 90 response teams around the world.

CERT lists what it calls "security practices." These are concrete, practical tips and guidance to help colleges and other organizations improve the security of networked computer systems. These practices address the most pervasive problems, as reported to the CERT/CC. They are technology-neutral for broad application. A complete list of the practices can be found on the CERT/CC Web site at <http://www.cert.org/security-improvement/>. Every network administrator should have that site bookmarked.

CERT/CC also has books available on security. Some of the CERT staff members teach courses in the Information Security Management specialization of the Master of Information Systems Management program in the H. J. Heinz III School of Public Policy and Management at Carnegie Mellon.

CERT's Forum of Incident Response and Security Teams (FIRST) is a coalition of individual response teams around the world. Each response team builds trust within its constituent

community by establishing contacts and working relationships with members of that community. These relationships enable response teams to be sensitive to the distinct needs, technologies, and policies of their constituents. FIRST members collaborate on incidents that cross boundaries, and they cross-post alerts and advisories on problems relevant to their constituents.

Toward Secure Software: CSDS

The Idaho State Board of Education established its Center for Secure and Dependable Software (CSDS) at the University of Idaho in response to the overwhelming need for computer-related security education and research. Dr. Liz Wilhite, program manager at the center, says the program's vision is to become a leader in the field of computer forensics.

"In five years, we will have our own program, with majors at all levels (undergrad, masters, and doctoral) in computer forensics," Wilhite says. That's an aggressive schedule for a program just three years old.

In May 1999, the National Security Agency (NSA) designated the University of Idaho as one of the initial seven Centers of Excellence in Information Assurance Education, partly in recognition of CSDS's efforts in promoting information security education and research.

Where CERT focuses on response to computer incidents, CSDS looks at designing software to prevent incidents in the first place.

CSDS is made up of 10 computer science faculty, three business faculty, two accounting, one law faculty, associates in the College of Education at INEEL and PNNL, a full-time program manager, over 30 students, and 3,000 square feet of laboratory and office space, Wilhite says. The program is adding a computer engineer, as well. "A well-rounded staff is necessary to do our job," Wilhite says.

INEEL is the Idaho National Engineering and Environmental Lab, a multipurpose national laboratory delivering science and engineering solutions to the world's environmental, energy, and security challenges. PNNL is the Pacific Northwest National Laboratory, Richmond, Washington (www.pnl.gov).

Completely self-funded, CSDS brings together collaborative research efforts and serves as an educational focal point for the design, development, analysis, and use of technologies that result in secure and dependable computing systems.

The program involves both students and faculty, often working together on research with commercial impact. In addition, they work with Idaho State as part of the National Alliance for Information Assurance, with Idaho State focusing on the business and human side of the equation.

An intelligent phone for very intelligent people.

"Because FonSystems understood the university's cutting-edge technology needs and Scitec's innovative engineering abilities, we were able to provide the desired solution. This was possible in no small part to Scitec's custom software programming of 14,000 Scitec 5S-c sets to meet the school's unique switch and call feature preferences."



Mike Paulda
Vice President
FonSystems, Inc.
Dallas, TX



The line-powered Scitec 5S-c with smart, programmable voice/data features, certainly does appeal to intelligent people. After all, it requires no AC adaptor or batteries, maintains function during power outage, and is suitable for migration to IP switch analog port Caller ID applications!

If you're not specifying smart, Centrex/PBX/IP-compatible Scitec sets, join FonSystems, the University of Minnesota and dealers, schools, businesses, hospitals, hotels and call centers nationwide...who do. Call 800-451-4035 or write acuta@scitecinc.com.

SCITEC

www.scitecinc.com

Telecom solutions for a global marketplace.™

Copyright © 2002, Scitec, Inc. All rights reserved 453-0702AJ

when reviewing a firewall product that interfered with Netscape (the vendor now says the product has been fixed).

Tech's Web site is for "family members" of the Georgia Tech community only. However, it does not stop any visitor from noodling around the Web site and getting an idea of how the school's network usage policies are outlined, looking at its security awareness policy, or checking out several other useful features.

Info Security Institute

As they do in Idaho, the Johns Hopkins University Information Security Institute (ISI) takes a comprehensive approach to information security.

Located in Baltimore, Maryland, ISI is an information security partnership across the divisions of Johns Hopkins that addresses all of information security's major concerns. "The idea is to take a holistic perspective on

information security. We don't want to duplicate programs like CERT's, says ISI Founding Director Dr. Gerald Masson. "They do what they do exceedingly well. Our goal is to take students with an information technology background and develop their technology, policy, management, and applications components."

An anonymous donor gave \$10 million to establish ISI. ISI blends educational, research, business relationship components, and a mixture of academic, business, and government involvement.

ISI will combine concerns from its school of advanced international studies, public health, and even the Peabody Music Conservatory (which will deal with intellectual property rights and MP3 types of issues) and the civilian bio-terrorism defense strategy group. ISI outlines its goals as follows:

1. To create an interdisciplinary and cross-divisional environment for research and study of issues related to information security, including technology, privacy, strategic management, and a number of other emerging fields.
2. To establish effective feedback loops with organizations outside of academia to sharpen research and education and to create new opportunities for programs and projects.
3. To establish JHU's eminence in the field in the eyes of both researchers and practitioners by developing programs of the highest quality.

ISI will confer a master's degree in security informatics starting this fall (2002). Eventually, an undergraduate minor will be added to the program.

While it will not track viruses and physical disasters, the program looks at



**Lots of people are accessing your campus wireless LAN,
make sure only the right ones do.**

Find out how the Vernier Networks System can help you.
www.verniernetworks.com/acuta or call 1-866-Vernier

other relevant issues. "While technology is at the core of the whole information security field," Masson says, "there are other relevant issues—privacy, copyright, digital rights, and other regulations that are equally significant. This degree touches every component and division of the university," Masson says.

A six-page introductory white paper on ISI is available at www.jhuisi.jhu.edu/About/JHUISI>DescriptionPaper—060101.pdf.

New Jersey's New Program

The newly formed Center for Wireless Networking and Internet Security, based at the New Jersey Institute of Technology (NJIT), Newark, in collaboration with Princeton University, is a new think tank designed to develop technologies that can identify and block hacker intrusions.

NJIT claims to be "America's most wired public university." The joint program hopes to develop technologies to protect the Internet from cyber attacks. It will also work on protecting and improving computer network management.

The center, funded by a \$2.6 million grant from the New Jersey Commission on Science and Technology, will complement two others already at NJIT: the Center for Communications and Signal Processing, run by Yeheskel Barness, NJIT distinguished professor of electrical engineering, and the New Jersey Center for Telecommunications, run by Alexander Haimovich, NJIT associate professor of electrical engineering.

Atam Dhawan, Ph.D., the center's director, is a professor of electrical and computer engineering at NJIT. He oversees the operation of the center, working with a team of researchers from NJIT and Princeton. Those researchers are allied with a host of corporate technology leaders from firms such as AT&T, Mitsubishi, NEC, and Spirent Communications. A

representative from the U.S. Army is also on the advisory board as is an employee from the New Jersey Commission on Science and Technology.

Students at both NJIT and Princeton benefit from the center's guiding research projects in accordance with industry need. About 20 doctoral candidates from both schools will work on solving problems such as how to make wireless networks more secure. The research will train the students to work for high-tech firms after they graduate.

"The center will forge a synergistic relationship between academia and industry," says Dhawan. "The universities are key to knowledge dissemination, and the center will allow academics to develop technology they understand best, such as protecting the Internet from hackers and transferring that technology to industry. That will in turn create jobs and have a significant economic impact on the state."

Based at the Electrical and Computer Engineering building at NJIT, the center already has two computer labs, and more computers and equipment are to come, Dhawan says. He expects the center will receive additional funding from both corporations and the federal government.

Researchers use grant funds to work on myriad technologies. One planned technology will allow the military to instantly recognize a cyber attack and trace its source. The center will also design computer systems that can predict, and thus prevent, a cyber attack, especially attacks on wireless multimedia networks. Researchers will also upgrade network management security. Wireless systems are especially vulnerable since hackers can exploit their very nature: providing location-aware services and location-sensitive modes of access to information services.

Wireless networks must deal with unauthorized detection and tracking of location users. The center also will

work to safeguard the Internet from consumer fraud.

"The Internet was first conceived to be an information highway with access to all," says Dhawan. "Because of that, we now have few standards to protect information. Classified information about healthcare, banking, e-commerce, online shopping, our personal lives, and our military safety can all be in jeopardy. There's no better environment than the academic one to work in and solve these problems, and that's what the Center for Wireless Networking and Internet Security will do."

Critical Infrastructure Protection Project (CIP)

One of the newest programs is the Critical Infrastructure Protection Project (CIP), a collaborative effort led by George Mason University School of Law's National Center for Technology and Law in Arlington, Virginia, in conjunction with James Madison University. CIP got rolling in mid-May this year. CIP is funded by a \$6.5 million National Institute of Standards and Technology grant.

"Our intent is for the CIP Project to generate real solutions that address the complex legal, policy, and technology issues associated with an increasing number of cyber attacks and cyber failures affecting government agencies, military, private-sector businesses, and even individuals," says John McCarthy, executive director of CIP.

"By working together, George Mason University and James Madison University will develop a nationally recognized program that fully integrates the disciplines of law, policy, and technology for enhancing the security of cyber networks and economic processes supporting the nation's critical infrastructures," McCarthy says. "The consideration of all three disciplines is what will make the CIP Project unique and valuable."

Among the hurdles CIP faces are impediments involving intricate questions of law, policy, and business

processes and their relationship to technological applications. Some examples include tort liability, information sharing among competitors for security purposes, and exchange of information between business and government to improve cooperation for managing national security risks.

The CIP Project's four program elements include the following:

- Providing education and outreach – seminars and workshops, professional education and training, and facilitated government-industry-academic discussions.
- Serving as a repository of expertise for government and industry – Because cyber-security issues are not generally well understood, there is a need for expertise in a range of issue areas. Government support includes developing model legislation covering cyber-security issues and testifying on

complex issues of law, policy, and technology.

- Sponsoring research – While there is no single source of excellence in cyber-security law and policy, both George Mason University and James Madison University are recognized by the National Security Agency as Centers of Excellence for Cyber Security. CIP will develop a one-stop shop for information on cyber security law and policy and support applied research as well as long-term endeavors in law, policy, and technology.
- Developing special programs – by focusing resources on certain special areas of interest, such as guidance to small business, directing cyber-security knowledge and expertise directly into the homeland security discussion, integrating technological expertise with legal and policy insights to support creation of a viable underwriting

market for cyber risks, and information sharing and analysis center modeling.

Down the Road

The job of keeping networks secure is not getting easier. McCarthy notes that senior leaders in business, government, and academia are struggling with a variety of technological and nontechnological impediments to managing cyber-related risks.

“Clearly, September 11 has changed the game. There is a national and international concern relative to the use and exchange of information on the Internet. Universities of the stature of Johns Hopkins and others feel an obligation to address this area,” concludes Masson.

Curt Harler is a contributing editor for the ACUTA Journal. He can be reached at curtharler@adelphia.net.



Teamwork



Talent



Technology

213-622-4444

www.wtc-inc.net

wtc@ix.netcom.com



*Consulting In Telecommunications
And Networks In Higher Education*

Privacy on Today's Electronic Campus

by Tracy Mitrano
Cornell University

New technology generates new anxieties—often with good reason. The trade-offs of one generation are not always the same for another generation with different historical circumstances or different expectations of efficiency, privacy, and social order. The popularization of the transportation and communications industries—from trains to planes and telegraphs to telephones—produced a long litany of contract and tort cases, not to mention reams of regulations and volumes of administrative law.

In light of the remarkable technologies that have made electronic communications a popular and significant component of the American economy, it is no wonder that electronic communications have raised a wide range of new questions and concerns about Internet service provider liability, Internet governance, legal strictures for government surveillance, and privacy in general. Perhaps the main reason is that people feel so personal about their computer usage.

The psychological intimacy between people and their computers sharply contrasts with the fact that network operators can see electronic communications, governments with proper authorization can intercept transmissions or obtain stored data, and snoops or hackers can all too easily *sniff* communications or trespass into an individual's computer. For those who have used electronic data or communications to express personal emotions or political thoughts, it is a shock to learn that their message has been posted on the Web or widely circulated as the result of easy forwarding. Electronic diaries and wills have been sent out as documents as the result of a computer virus. The sniffing out of a credit card or social security number produces obvious credit problems. Harassing or defamatory messages put on the Web for the entire world to see can be a

psychic blow that leads to questions of trust and privacy and strikes the mystic cords that bind people to their society.

Technology

So what are the rules—technical, legal, and ethical—that shape this very uncertain reality of the privacy of electronic communications? Technically, people should be prepared to accept that network operators can see virtually any unencrypted communication. In cases where the operators are performing necessary business functions, they do, in fact, sometimes see such communications. Notwithstanding the common analogy that an e-mail is like a postcard going through the United States Postal Service, the more accurate comparison would be telephone operators or technicians who could break into live communications in the course of their duties.

One distinction to make between both of these analogies and electronic communication is that in neither the postal nor telephonic world are backups or network logs maintained that provide yet another avenue for retrieval of communications and/or data after the fact. People are often surprised to learn that their own computers contain records of every Web site visited. The capacity and volume of information that network communications contain constitute a quantum leap of trace and tracking ability that understandably makes people nervous. And even if it could be established that no social or political entity conspired to make this technology so transparent, it simply feels unnerving to discover that the privacy of communications is not what it used to be.

Law

Two federal criminal laws speak directly to the legal and ethical concerns regarding electronic privacy. First, the Computer

Abuse Act, Title 18 of the criminal code, section 1030 specifically, renders computer trespass—not just rattling the doorknobs but actual penetration, retrieval, or damage—and destructive programs such as worms and viruses illegal. Second, the Electronic Communications Privacy Act (ECPA) establishes privacy of electronic communications at a standard similar to the wiretapping act of the late 1960s. In short, the disclosure of any information by an Internet service provider to the public is actionable. Since Congress amended ECPA in 1994 to include wireless communications, sniffing is uncharted legal territory, given that the spectrum in which wireless communications operate is public.¹

Almost certainly reading the text of a communication would support at least a cause of action, especially if that communication was disclosed to the public. Disclosure is regulated even for those who fall under some of the exceptions to ECPA, such as network operators who access communications in the normal course of business or law enforcement with an administrative, executive, or court order to access transmissions and data. If a network operator working in the usual course of business uncovers the extramarital affair of a famous person, for example, it is against the law to disclose it. Likewise, if in the course of an investigation, law enforcement discovers legal but potentially damaging information about an individual, say the homosexuality of a closeted person (in a state with no sodomy laws), it may not disclose that information. The singular exception to the exception is when consent is given by one party to a communication to disclose information of the second party; such disclosure is not actionable.

State tort laws offer another dimension to this issue. Claims such as defamation, misappropriation of likenesses, or invasion of privacy—together with state sexual harassment laws—offer opportunities for ambitious attorneys to carve out a specialized niche in tort and civil plaintiff Internet law. Actions in this area are still very sparse and have yet to yield a clear direction of the law, and so remain speculative at best. Such speculation leads to another question, however: What about the ethical dimensions of exposure on the World Wide Web? I have a personal example.

I was teaching my 10-year-old son how to do a search when he suggested that we search my name. To my surprise there appeared as a title, “The shit hits the fan ...” In my role as copyright agent for the university under the Digital Millennium Copyright Act of 1998, I had sent a student a form notice of copyright infringement. He had sent it on to a friend at another university who posted the

Shaping the Way You Communicate Today and Tomorrow...



...with a Proven Track Record.

Integrissys Communications Group, Inc. is a full-service IT provider of voice, data, video and broadband. Our expertise in integrating diverse communication needs across campuses has solidified our partnership with many educational institutions.

In fact, we have a proven track record with educational institutions in developing customized IT solutions that include:

State-of-the-art broadband systems that allow students access to cable TV, campus intranet, e-learning programs, campus-dedicated and proprietary local/long distance telephone systems, surveillance and security systems, and long-term maintenance contracts –

Integrissys is your single-source IT provider.

Integrissys is a Corporate Sponsor of ACUTA.



Shaping How You Communicate TomorrowSM

Voice, Data, Video, Broadband:
Products & Services Built with Integrity

545 Lafayette Road, Portsmouth, NH 03801



Call 1-877-277-7101 today or visit our web site at www.integrissysgroup.com

The capacity and volume of information that network communications contain constitute a quantum leap of trace and tracking ability that understandably makes people nervous.

notice on the Web with that opening phrase. Since the recipient consented to the posting, I have no cause of action in criminal law, and since it does not allege anything defamatory about me, I have no private claim either. (It most certainly would have been a violation of the Buckley Amendment, or the Family Education Records Privacy Act, for me as an agent of the university, to post the information.) But still, it is a gratuitous posting. I acted as an employee of the university, yet the search turned into something personal about me.

I decided to contact the student, not as an employee of the university but as a private individual on my home computer and with my private e-mail address. I asked him to redact my name and the name of another employee. He never did. Given the minor significance of this incident, I present it as an example of an ethical question. In lieu of law, how do we, as citizens of the United States and of the world of Internet users, articulate an ethics of electronic media?

Cornell University Policy

Where law treads, policy is sure to follow. Law—from Middle English, “to lay down”—represents the floor of acceptable behavior, a level of performance beneath which an individual or institution courts liability. Policy—from the ancient Greek, “polis” or “citizen”—speaks to higher principles that incorporate foundational social and political notions of rights and responsibilities of the individual to the group, and of the group to and for the individual. To be sure, policy does not fill the gap between the law and ethics completely. To draw upon the example explored above, it is important to note that not even policy would have addressed my concerns. The fan material is not posted on the Cornell University network, but even if it were, the university does not have a policy against posting it. To the contrary, the university’s Policy on Responsible Use of Electronic Communications holds forth on free speech that does not violate law or policy in such a way that it would have been a violation of policy for

me, as an officer of the university, to use my authority to remove it!

Such strictures define the obligations that the university undertakes to protect its constituents. Conversely, intervening in cases where individual students interfere with the activity of others and establishing ground rules of responsible use and security are obligations the university exercises to maintain order and to teach responsible use. Such intervention prohibits bandwidth hogging, e-mail bombing, and sharing passwords. To adhere to those rules is the obligation of individuals who enjoy the privilege of network usage. Those rules are not codified in American law but they could potentially bring sanction upon constituents of the university who use the network in violation of them, which illuminates precisely how policy raises expectations of an individual’s behavior. The policy reasons why those rules exist: to promote fairness, respect, and dignity—if not a relative concept of privacy—comport with the lofty mission of the university.

A note on the term *privacy* is worth making at this juncture. The concept of privacy in American law is largely a 20th-century phenomenon and has come to revolve around the debate over abortion or reproductive rights as they took shape in the civil rights movement of the 1960s. However much ridiculed, Justice Goldberg’s famous statement that the First, Third, Fourth, Fifth, and Ninth Amendments to the Constitution amount to a “penumbra” of privacy rights, otherwise not articulated as such by name in that august document, represent to date the best summary of how American constitutional law considers this nebulous area. It is equally important to remember that the Constitution protects against government action and not private entities. Thus, while privacy may have become the catchword for personal rights in the last half of the 20th century, those rights do not translate to all areas of experience and certainly not to private entities such as Cornell University.

Policies on Privacy

The University Counsel’s Office has made it clear to policy advisors across campus that their policies had best steer clear of the term *privacy*, lest it suggest or infer a set of rights to which the university is not obliged, and to which the university would not want to associate itself in policy as a matter of potential litigation. Nuanced terms such as *fair information practices* fill the gap that privacy policies might well play in state universities or other governmental institutions.

Another example of how the *public* and *private* distinction plays out is in the area of privacy rights for employees of any private network. Employees enjoy no privacy whatsoever. Every case that has asked questions about monitoring, snooping, sniffing, and consciously and intentionally looking at either transmissions or stored data

of employees has found squarely for the employer, not the employee.

To its credit, Cornell, while reserving its right to monitor communications, has nonetheless stated in policy that it will not adopt those practices as a matter of normal business. The University Policy on Responsible Use states that while it reserves the right to control and access systems, it does not as a practice monitor data or usage. Important distinctions must be made among three discrete points. Technologically, systems operators can see, for example, e-mail or URLs passing through as transmissions. Yet, the equally true fact that more than 1 million e-mail messages pass through the Cornell network on average every day means that it is impossible to monitor them, even if the university did not hold itself to a higher ethical standard in policy. Thus, there is a difference between the technological ability to see e-mail and the practice of reading it. It is important to note, however, that as a matter of policy, in the course of standard business procedures, should system operators observe content of e-mail, they are obliged to maintain the confidentiality of it unless the content of what they observe violates law or policy or is evidence of immediate danger of life and limb, in which case they are obliged to report it.

Another variation on the theme of privacy of an individual's data on an electronic network is the question of how third parties can gain access to it. The Office of Information Technologies is sponsoring a policy on this matter, called Fair Information Practices for the Access of Data about Individuals Transmitted or Stored on Cornell Information Technologies Systems. Until such time as the university policy office issues it, it is the practice of the Office of Information Technologies and Cornell Information Technologies to provide information to third parties only on the request of the head of the subject's constituency (i.e., the vice presidents of Human Resources, or Student Affairs or the dean of faculty) or to law enforcement with proper authorization. Individuals may retrieve logging information about themselves if they present reasonable cause in a formal request to the policy advisor of Information Technologies. And then there is the question of sniffing. It may be murky in the law, but it is clear in policy. Cornell Information Technology interprets the Cornell University Policy Regarding Abuse of Computers and Network Systems to make "sniffing" a violation.² And there are other matters too, such as the selling of e-mail addresses or the use of cookies for the collection of personal information about users—neither of which is a practice of Cornell Information Technologies, nor, in my humble opinion, should they ever be.³

Conclusion

Each generation will define *privacy* in the electronic world by setting the concept beside an array of external realities such as prevailing custom and law, technologies and

practices, institutional policies, and ethical ideals. The tensions between the dual human impulses to preserve a personal environment and to accommodate the demands of society for survival inform that effort. Indeed, the electronic world will not change that dynamic, but will add to its many dimensions. We could choose to ignore the debate, but only with the most contemporary notions of privacy as this generation knows them hanging in the balance. Awareness, political discourse, and policy discussion will not eliminate the tension but animate it with creativity.

Tracy Mitrano is policy advisor and director of computer policy and law, Office of Information Technologies at Cornell University. Reach her at tbm3@cornell.edu.


Notes

¹ "Sniffing" is a slang term for interception of data communications. In telephonic communications the analogous term is "tapping."

² <http://www.cit.cornell.edu/computer/responsible-use/abuse.htm>


³ Cornell Information Technologies does use cookies for network tracking information, but not personal information—content—about users. It does not sell e-mail addresses either, but, like so many institutions, has fallen prey to commercial interests harvesting addresses from its directories.








ENTERPRISES, INC.


We would like to thank all those who visited ATL at The Annual ACUTA Tradeshow in Reno, NV, as well as, congratulate the winners of our drawings.



Joseph Nell of University of Alaska Southeast
Winner of Antique Candlestick Phone

We Answer All of Your Telecom Needs...


-  We Sell New & Refurbished
-  We Repair Telecom Equipment
-  We Buy Excess Equipment



Tom Holt of Pittsburgh State University
Winner of Polycom SoundPoint Unit

AVAYA/LUCENT NORTEL MITEL
TIE/NITSUKO NEC TOSHIBA ASPECT

FORUM TRISYS MCK ADTRAN
PLANTRONICS TELECORP POLYCOM



Angie Fernandez of Norwich University
Winner of Polycom SoundPoint Unit

888.285.9777
www.buy-atl.com

Current Trends in Information Security at UW-Madison

by Kim Milford, CISSP, JD
and Jeffrey Savoy, CISSP
University of Wisconsin–Madison

At the University of Wisconsin–Madison, the Information Security department within the Department of Information Technology (DoIT) plays an integral role in providing IT services to campus. Our responsibilities run the gamut, from responding to someone whose computer has been hacked to providing guidance on developing security controls in new applications.

What is Information Security?

Information security is the protection of the confidentiality, integrity, and availability of information technology assets, including hardware, software, and the institutional information stored therein. To implement protection and reduce risks, information security controls are applied. These controls can be categorized in three areas:

- Administrative controls
 - Policies and procedures
 - Rotation of duties
- Technical controls
 - Firewalls
 - Virus protection
- Physical controls
 - Locks
 - Alarms

A well-known security concept is *security in depth*. Security in depth can be achieved by applying a mixture of various administrative, technical, and physical controls.

While the term *security* tends to denote absolute protection, information security is actually more of a continuum. The achievement of a fully secured IT environment is rarely possible, but controls, such as intru-

sion detection systems, backups, password criteria, etc., may help to place you closer to the secure end of the spectrum. As you implement security in depth, you tend to increase your security position on the continuum.

There are often external factors that affect decisions about security controls—primarily cost and convenience. For instance, a firewall may help to protect users from outside threats, but it reduces the ease with which users can access the Internet and can be costly. As more security controls are implemented, costs generally increase and access to the IT resource may be less convenient.

An important aspect in the implementation of controls is risk management: assessing what risks an organization encounters and determining whether to accept the risk or take steps to reduce the risk. Another important determination in assessing the level of security that an organization needs is checking in with what peer organizations are doing. Do other universities deploy firewalls at the campus level? Are they offering e-mail encryption for sending confidential data across the Internet? What are their password controls? This sort of peer review essentially sets the standard of due care for IT security, an important legal consideration.

What Are the Threats?

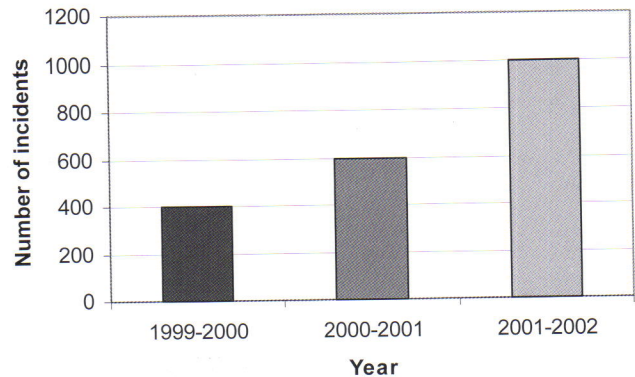
Hacked servers (sometimes just hours after connecting to the Internet!), copyright infringement viruses, denial-of-service attacks, misuse of institutional information and the loss of reputation that goes with it ... The list of possible security breaches goes

on and on. It's probable that every university has seen its share of exposures in recent years. The Computer Security Institute and the FBI produce an annual survey on computer crime and security and publish the results. This survey, available at www.gocsi.com, shows a growing trend in both the number of security breaches and the cost of the breaches. According to the 2002 CSI/FBI survey, 90 percent of respondents detected security breaches. Of those who reported security breaches, 80 percent acknowledged financial losses due to the breaches.

Incident tracking at the University of Wisconsin-Madison substantiates this growth trend in the number of security incidents, as illustrated in Figure 1. The graph in Figure 2 (page 26) shows a breakdown of the types of cases reported to UW-Madison's Incident Response Team:

Complaints about spam received and spam relaying together constitute the majority of cases reported. Reports of virus infections continue to grow, especially after recent Klez virus outbreaks. Copyright infringement and unauthorized access, which includes hacked machines, continue to make up a large number of the cases we see as well. Tracking these statistics allows us to strategically place our security controls and tools to

Figure 1: Incidents reported to BadgIRT



better meet the needs of our environment now and to anticipate potential services in the future.

The Challenge of Security in Today's Environment

Remember the mainframe days? A user's only responsibility was to know the password—one password. Application developers merely had to notify the appropriate mainframe administration staff when a new system went live and voila!—security was built right in.

It's not quite so simple in today's decentralized environment. At the University of Wisconsin-Madison,

Picture Perfect Communication

No other distributor offers you the variety, quality and satisfaction that 1 Nation Technology does. We stock a multi-million dollar inventory of the latest telecommunications, networking and conferencing equipment, service what we sell and back it all with the most comprehensive warranty in the nation.

Whether your need is a single item or a complete system, 1 Nation has the gear you need to make it happen.

We also house a complete technical facility to handle all your repair and refurbishing needs.

What's more, 1 Nation offers a competitive Buy Back program allowing you to turn your excess inventory into dollars.

Contact us today for details on our complete range of new and refurbished equipment. Let the professionals at 1 Nation Technology put savings and quality into the picture for you.

nortel avaya
plantronics
polycom orinoco
cisco repair maintenance

800-998-9862 www.1nationtech.com

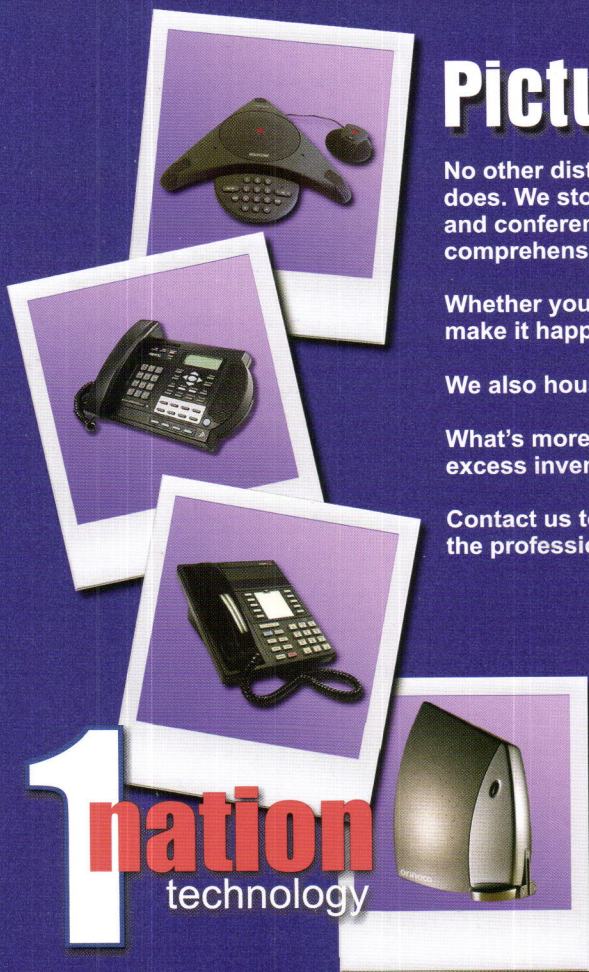
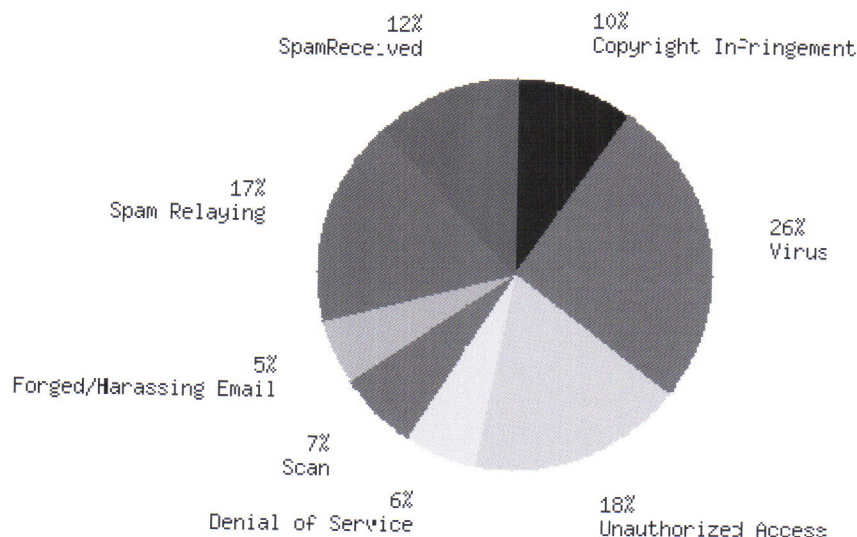


Figure 2: Types of cases reported to UW-Madison's Incident Response Team



everyone has a responsibility in information security. Managers assist by setting policy and direction. Application developers consider security throughout development and implementation of new applications. As systems become increasingly integrated, developers need to consider more global security needs instead of focusing on specific applications. System administrators keep current on exploits and patches, turn off unused services, and provide access control privileges. Network managers watch for suspicious network activity that may indicate an attack. End users have a responsibility to protect an increasing number of passwords and credentials across various applications.

How UW-Madison Information Security Helps to Address These Challenges

In order to meet the challenges of today's computing environment, UW-Madison Information Security coordinates the following services for campus:

- Awareness and training

Awareness is an ongoing effort for the Information Security department, with campaigns targeting students and

employees. Based on current trends we're tracking in student computing, the two main areas where we need to increase education among students are the unauthorized sharing of copyrighted materials and the use of virus protection. Thus our awareness campaign will focus on these areas. Outreach to students is accomplished primarily through information screens provided during the account activation process, posters, and videos posted on our Web site.

Awareness to faculty and staff focuses on tools, training, and services that provide campus departments with ways to reduce the risk to departmental computing resources. One of our main ways of providing security awareness to faculty and staff is through Lockdown, an annual computer security seminar for campus employees.

- Incident response and investigations

Through the UW-Madison Incident Response Team (BadgIRT) we provide a centralized collection point for tracking information security incidents, analyzing trends, and collaborating with other incident response

teams, such as FIRST (the Forum of Incident Response and Security Teams). In addition to collecting and responding to incidents, we provide investigative services, such as investigating reported violations of UW-Madison's appropriate-use guidelines, and assisting law enforcement agencies with investigations and forensics, that is, the preservation and analysis of computer evidence such that it is admissible in court.

- Expert consulting

By providing expert security consulting services, we collaborate with other IT staff. Expert consulting, a growing area of business for the Information Security department, includes providing assistance in assessing current security risks and suggesting controls to reduce risks in a particular application, across several integrated applications, for the computing environment, or for a specific operating system.

- Security tools and services

Another way we collaborate with other IT staff is by providing tools that assist them in improving their own security. These tools include vulnerability scanning, antivirus protection, and security best practices.

We offer campus administrators a vulnerability-scanning tool that allows administrators to run their own comprehensive scans of potential security weaknesses on their network. We plan to enhance scanning services by providing centralized, campuswide scans looking for well-known, high-risk vulnerabilities, such as Windows Web server exploits. Other possible enhancements include offering additional scanning tools as well as running comprehensive scans for departments and assisting them in interpreting the results and taking corrective action.

We offer the enterprise version of antivirus protection software to departments at a volume discount. This allows departments to deploy antivirus on all desktops and manage

it centrally. In addition, an antivirus solution is available to students on CD for a nominal fee or free of charge for a downloadable version.

We offer SANS (System Administration Networking and Security) "Step-by-Step Security" guides to campus. In addition, we have various information security best-practice documents and other resources available to campus on our Web site, www.doit.wisc.edu/security.

- Access control and security administration

Another way we assist campus is by providing centralized access control to many campus enterprise business systems, including the student information system, payroll, budgeting, and financials. In this way, the security concept of least privilege, that is, the minimum level of access needed

to complete work functions, can be enforced.

Future Directions

As we look at current trends, we try to forecast future issues that concern information security. Some of our current areas of research and development include firewalls, intrusion detection systems, and virtual private networks to help provide more secure networking. While these technologies are not new, there is a significant challenge to implementing them in a decentralized environment. Our current efforts in addressing these challenges will lead to a more robust network now and in the future.

In addition, we are investigating the deployment of public key encryption and strong authentication to enhance the protection and verifiability of confidential data being ex-

changed over the Internet. Our work in this area has found that these technologies, used in combination with existing controls, offer great potential for the future of securing information resources.

There will always be some inherent risk to IT assets. As we deploy tools to mitigate the risk, new threats and weaknesses are discovered that require additional controls. Also, as IT shifts to encompass emerging technologies, UW-Madison's Information Security department must stay ahead of the developments by keeping basic security concepts in mind.

Kim Milford, CISSP, JD, is the information security manager, and Jeffrey Savoy, CISSP, is information security officer at the University of Wisconsin-Madison. Reach Kim at kim.milford@doit.wisc.edu and Jeff at jrsavoy@doit.wisc.edu

III

2009 Dewberry Court Westlake Village, CA 91361
Phone: (805) 496-8053 Fax: (805) 497-3606



Ethernet
10/100/Gigibits

Video/Audio/Data

RS232, RS422, RS485
T1, E1, T3, E3, MUX
Multidrop & Telephone

Sharp Video

Crisp Audio

Fiber Optic Communications

High Reliability

Low Cost

Military Installation

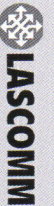
Broadcast Quality

Data Network

Financial Route Protection

Distance Learning

Security Surveillance



Email: eds@lascomm.com
<http://www.lascomm.com>

Interview

Dave Safford, PhD

Manager, Global Security Analysis Lab, IBM

Dave Safford is the manager of the Global Security Analysis Lab for IBM. He holds a PhD in computer science from Texas A & M University. Dave can be reached at safford@watson.ibm.com.

Walt Magnussen is the associate director of telecommunications at Texas A & M University in College Station. He is also a member of ACUTA's Publications Committee. Reach Walt at wmagnussen@ppfs4.tamu.edu.

Magnussen: In view of security concerns that have come to light in recent weeks regarding the vulnerability of our nation's infrastructure (including utilities, water systems, dams, telecommunications switches, and other critical systems) to cyberattack, how can universities best protect infrastructure systems on their campuses? Where are the key vulnerabilities in these systems, via the Internet or other channels, and what precautionary or corrective measures should campuses be taking over the short and long term?

Safford: A few years back I was director for supercomputing and networks at TAMU. Back in 1992 A & M was attacked by a very persistent hacker. In fact, the incident was written up in a book called *At Large* by Friedman and Mann. That's what got me started in this field, trying to understand the vulnerabilities and defenses in a university environment. The basics remain the same nine or ten years later.

There are three main things that universities should be doing: firewalling, intrusion detection, and security auditing or vulnerability assessment. We developed at Texas A & M the TAMU tools, which basically had (1) a firewall, context sensitive, or a packet filter that was oriented toward university environment, (2) intrusion detection that was oriented toward the university environment, and (3) security auditing tools that were oriented toward the university environment. Those three basically provide your front line of defense.

Magnussen: All the tools that were initially developed are still in use here today: The firewall is Drawbridge

which is UNIX based. This program is open source and is used at several other universities. Along with Drawbridge, you wrote an application that tests hosts against known threats. These tests check to ensure that the machine's been kept secure and reliable

Safford: One thing I might add to the answer, too, is that it was very important at A & M that we had very strong support from the provost and higher level management who agreed that security was important. And in some cases that can be the hardest thing to get. The technical issues can be dealt with fairly easily, but getting the world to recognize that there is a problem and to do something about it in some cases can be the hardest step.

Magnussen: As wireless and mobility continue to emerge as an expected network service rather than an add-on option, what challenges and future problems might we encounter? What advice and guidance do you offer to those planning wireless and mobility projects? How will initiatives such as the Wireless NYC Project be made secure given the current limitations of technologies?

Safford: We've got two different types of wireless: the wide area wireless or the cell-phone based connections and the local area network wireless, like the 802.11 technologies. They're two different environments. The wide area wireless actually started out to be the one with the most problems, and the good news is that they're finally actually converging on something that's semi-reasonable, as the third generation or 3G phones start rolling out the data services on these have

much better protection. They're based on native TCP. They can use IPSEC. The technology is a definite improvement from the first generation that didn't have anything and the second generation that had a relatively new thing called WAP [a protocol that extends Web information to wireless devices]. Basically the 3G phones are doing the right thing.

The local area networking is kind of a repeat of the same thing, although they are now kind of stuck in the second stage. When they first rolled out, they had absolutely terrible security. The 802.11B was fundamentally flawed and in some cases unfixable when it first started out. It was terribly insecure.

The second generation is adding another protocol, 802.1x, which is good enough for second generation. This helps, but it's not perfect. For most institutions, particularly the university, we think that this is quite

adequate. I would not hesitate to go with this in the university environment. But it's not a complete, long-term fix. Probably 18 to 24 months out we're looking at 802.11i which should actually be a complete rewrite, third generation, and will actually have pretty decent security. For now I think the 802.11B with the 802.1x protocols is reasonably good for the university environment.

For the longer term, this kind of gets back to one of my strategies, which is basically in the long term we shouldn't be trusting the network anyway. All of these technologies try to make the network perfect, and the better long-term perspective is to say that the networks aren't going to be secure. We have to harden our hosts and harden our connections between the hosts with something like IPV6 [IP version 6]. I think we will see a shift away from these temporary or near-term measures of firewalls and intrusion detection and move on to

actually trying to solve the underlying problem which is hardening the individual hosts and connections from host to host.

Magnussen: It sounds like what you're saying is that security needs to be more on the end nodes than on the network itself.

Safford: Absolutely. What you see right now with the firewalls and intrusion detections is actually kind of a band-aid approach. We have to protect insecure hosts from their own vulnerabilities. State-of-the-art in the operating systems and applications isn't there yet for the kind of Internet threat we're seeing, so you put on these protective barriers like firewalls and intrusion detection and vulnerability scanners to get the posture good enough to protect them against the Internet. That's certainly something that works now, but longer term we'd like to move to something that doesn't



CBi is a **national invoice billing service provider** focused on offering **colleges, universities** and **secondary schools:**

- Campus student telephone billing
- High volume invoice billing...
- Cable TV, Internet access, medical bills, etc.
- Cellular telephone billing

CBi provides these services via turnkey, individually tailored, flat fee or commission structured web-based solutions.

Call us at **866.523.8400**

or visit **www.cbibilling.com**
to learn more today!

CBi

Serving your needs.

GOLD AFFILIATE



have firewalls, that a host is able to withstand attack.

Magnussen: As advantageous as NAS/SAN convergence can be, it has drawbacks. Most vendors' NAS/SAN gateways only let arrays from the same vendor be joined. In addition, moving storage out of the isolated data center to access over an IP network puts it at risk of intrusions that before were not possible. Many industry watchers advocate the use of IP Security (IPSec), Fiber Channel Security (FCSec), and Secure Socket Layer (SSL) to secure transport of storage over the IP network. What are the key vulnerabilities and challenges in these technologies? What short and long-term advice do you offer to customers considering these technologies?

Safford: Network storage is certainly one of those areas in which we have a direct conflict between security requirements and convenience and performance. Particularly in the high performance area, like supercomputing centers, the need is for flexible availability of high performance storage. So we've seen in the market a lot of response in terms of products that are fiber-attached, very high speed, high performance, lots of spindles, but are not terribly secure. That is certainly one model of why you keep your supercomputer or high-performance center in a protected environment. But it's not good from a security perspective if you're going to spread this all over campus and try to maintain a centralized storage.

If you want to put some security on it, the best selection probably is the IPSec approach. Here you're going to pay a convenience penalty and a performance penalty, so it's very important to understand what your users are doing, where they are, and what their real requirements are. It's interesting because rather than see the industry converge on a middle-of-the-road type philosophy where you have middle level security and middle level performance, we're actually seeing a bifurcation here in which the industry is kind of separating into two camps: the ultra high-performance, low-security camp and the lesser perfor-

mance but more secure camp. I think we're going to continue to see that because there's just not a one-size-fits-all solution for everything the universities need to do. So in high performance cases try to contain it with physical security, and for the general-purpose distributors where security is more important, go with something like the IPSec type solutions. I definitely think we're going to continue to see this bifurcation in this particular sector.

Magnussen: Although outsourcing security is still a controversial subject, an increasing number of businesses are electing to turn over the round-the-clock monitoring of their intrusion-detection systems, firewalls, and VPNs to outside security service providers. What are the major pros and cons of this model for managing security? What advice do you offer to customers considering this model versus the in-house approach found in most colleges and universities?

Safford: Well, you're going to find questions on both sides of the fence on this one. At A & M we did roll our own. That was a very viable solution for that particular environment. Fortunately we had some good people working on this and were able to roll our own solutions that were specifically tailored to our environment.

On the other hand, that's very expensive in terms of personnel, and it demands that you have on hand people who have a high degree of expertise in these areas. The other side is the outsourcing or consulting like we do at IBM. We work very closely with IBM Local Services Group. We provide them a lot of the state-of-the-art tools. The advantage of going in that direction is that you don't have to grow your own expertise, and you don't have to commit your own manpower to it.

There is some economy of scale, and there's also some economy of performance in terms of getting the very best tools that you might not be able to afford otherwise. For example, IGS does security for something like ten thousand companies. Their intrusion detection systems deal with something like a million and a half

alerts per day. They developed, and we've helped them develop, some industrial strength software solutions to automate the vast majority of this. In a single site you might not have the economies of scale to develop this type of solution. You might not have the expertise. An outsourcing company has a pool of talented people that are spread out over all of their accounts. You don't generally get flareups or incidents at all sites simultaneously, so they can spread very good expertise and very good tools over a very large area, and therefore do it more economically.

So there are advantages and disadvantages both ways. I've done both of them and they both work. You can do both ways; it kind of depends upon the size of the university, what people you have, what level of expertise they have, what level of attack you're experiencing, and the various economics behind it.

Magnussen: I agree. A campus with a 200-person IT staff has the same needs as a campus with a 5-person IT staff.

Safford: Absolutely. And some of these tasks, in particular things like intrusion detection and security auditing, essentially take at least a full-time person each. It's very difficult for a part-timer, someone who has other work to do too, to keep up with all the vulnerabilities, the logs, and incidents. You have the minimum commitment of at least a couple of people and that's just not feasible in the small sites, while it is more feasible if you have 200 people.

Magnussen: Although these are hard times for many in the IT industry, the status of information security professionals is on the rise—at least based on how much they're getting paid. What advice do you offer to those considering careers in information security? How important is certification from associations or organizations such as the SANs Institute and the International Information Systems Security Certification Consortium? What are the implications for colleges and universities offering degree options in this area?

Safford: This is an excellent question, and I'll be talking about that more coming up. Two things are really important for security professionals in terms of preparing for a career in this area. One is absolutely critical: a strong, fundamental, theoretical background obtained at a university, preferably even graduate level. There are things you end up doing that require a very strong background in the languages, algorithms, and automata. We see people trying to work in this field that don't have that background, and they basically can't succeed without that kind of formal education. We get almost all of our people here from a PhD, university background. Even applied in the field, that level of formal training is absolutely critical.

On the other hand, it's also important to have practical, hands-on experience. We very much like people who have worked in the open source community and the Linux community who have demonstrated the ability to work in large programming tasks. That shows that they can take ideas based on formal training and apply them to do interesting things. Practical experience is very important both in the programming space and in the system administration space.

If someone hasn't been a system or network administrator, they don't really understand the nature of the threat. They don't really understand how important this is to people. They don't understand that down time can have really serious consequences. So I think it's very important to have workers with all those kinds of variables: formal training and experience and ability to do programming projects. The ideal person is a PhD who has written kernel modules and has been the administrator in a university setting or something like that.

Magnussen: With either the undergraduate or graduate degree programs, how much of the curriculum today is dedicated to security issues?

Safford: I think a reasonable amount is dedicated to security. I think that perhaps there's been an underappre-

ciation of the other basic courses, which is kind of the fundamental foundation on which you build the security. This gets back to the issue that the language, automata, and the algorithm courses are very important. I cannot overstress that. I think that universities could put a little more emphasis in two areas: basic cryptography and software engineering. Most universities have some sort of software engineering course. I think it's important for that course or a following course to deal specifically with the issues of security. There is an underappreciation of security throughout the entire development lifecycle—the requirements, design, implementation, testing, maintenance, and so forth. There's an underappreciation in the entire industry of security in these areas. We continue to see things like 802.11B come out with serious design errors. We see products come out without basic requirements for security where they say, "Well, we'll put that security in version 2." We continue to see code coming out with

buffer overflows and parsing errors. It's clear we're not doing a very good job of educating on those aspects of the development cycle. So we're actually here trying to write some course material in those areas.

Magnussen: Like the initial version of SNMP which was transported over non-secure communications. That doesn't give you a warm fuzzy feeling.

Safford: When you go back to the origin of the Internet, with the TCP and Telnet and FTP, there was no threat model. People did not even understand there was a requirement for these things. You can forgive them their ignorance back then. SNMP was kind of on the middle level at just about the time that people started realizing, "Hey, we need to do something with the requirements phase, we need to at least put security against our target threats in as a requirement." We continue to see that. When you see something with 802.11B, which is very recent, coming out with serious design

Stinger Ringers

The Loudest Ring for your buck!



The Stinger Ringers have established themselves as the choice for industrial/office applications requiring loud telephone ringing. Its rugged design is well suited for indoor as well as outdoor use.

There's a Stinger for all your applications:

The Model 196 Stinger operates from the ringing current on tip and ring, while the Model 198 Stinger operates from 24VDC and a contact closure. Both ringers give you a whopping 110dba output, with convenient protective connections.

Whether for noisy industrial areas, office, or for in-home use for the hearing impaired, Stinger Ringers are a sound you can depend on.

Dees

COMMUNICATIONS

1-800-654-5604 www.dees.com

Privacy Bills Before Congress Have Major Differences

by Amy Worlton
Wiley, Rein & Fielding

Privacy legislation has received significant attention on Capitol Hill, but vast differences between House and Senate bills diminish prospects for enactment. The two major privacy bills differ markedly on many elements, such as the scope of activities for which consumer consent is required, the degree of interference with existing federal privacy laws, and whether consumers will have access rights or a private right of action. The two bills have some commonalities, as they both preempt state privacy laws and require businesses to adopt information security policies. But the difficulty in reconciling these bills, along with broad-based opposition from business groups to both pieces of legislation, suggests that Congressional leaders will not reserve time in the busy legislative calendar this fall to address privacy issues.

In the Senate

In May, the Senate Commerce, Science and Transportation Committee marked-up the *Online Personal Privacy Protection Act* (S. 2201), introduced by the Committee's chairman, Sen. Ernest Hollings (D-SC). The bill is primarily directed at online entities such as Internet service providers and online retailers. But it would cover offline organizations if they collect personal data via online advertisements or their web sites. Moreover, the bill reported to the Senate floor would empower the FTC to propose comprehensive rules to govern personal data handling offline. Small businesses would be exempt.

The bill would also require covered service providers to obtain users' opt-in consent to the collection, use or disclosure of their "sensitive information" (e.g., financial and health information) and opt-out consent for other kinds of personal information. Users would have a reason-

able right to access their personal information stored by covered organizations, as well as a right to suggest corrections and deletions. Organizations would face affirmative obligations to protect the security of personal information.

Most commentators predict that the bill's chances for passage on the Senate floor are slim. Industry coalitions are expected to challenge the legislation due to its creation of a private right of action, broad FTC rulemaking powers and conflicts with existing federal privacy laws.

In the House

In the House, Representative Cliff Stearns (R-FL), Chairman of the House Subcommittee on Commerce, Trade and Consumer Protection, recently introduced the *Consumer Privacy Protection Act* (H.R. 4678), which would apply both to online and offline activities. The bill calls for notice and opt-out consent when a business plans to use personal information for purposes unrelated to a transaction with a customer (e.g., to sell personal information to third parties). It also requires businesses to adopt security policies and take reasonable steps in response to government security alerts. Non-profit entities and small businesses that meet certain eligibility criteria are exempt.

Self-regulatory programs, backed up by the FTC, provide enforcement under the Stearns bill. The bill blocks private actions and broadly preempts state action. With the support of Chairman Stearns and the co-sponsorship of the Chairman of the House Energy and Commerce Committee, Rep. Billy Tauzin (R-LA), the bill is anticipated to pass both the Subcommittee and the Committee. But the bill could be slowed by limited support in other House committees with jurisdiction over it and among the House leadership.

Contact Amy Worlton at aworlton@wrf.com.

errors, it shows that people doing development and software engineering discipline for this development are not aware of the security-specific aspects. Certainly that's something we need to teach.

Magnussen: Lack of security is the number one issue inhibiting enterprise adoption of Web services, according to a recent study by the Hurwitz Group. In addition, one out of every four of the top 1,000 companies in the US has a security flaw in its network infrastructure that could cut off all of its global and Web-based traffic, according to another recent study. What does the future hold for networking? What are some of the predictions of leading thinkers in the areas of carrier services, network security, application integration, Web servers, and business process automation? Over the next 3 years, what fundamental changes do you see occurring?

Safford: Let me throw out some other statistics that I think are even scarier to give you an appreciation of what the real underlying problem is.

One of the things that I think is really interesting to do is look at the trends. Look not only at what the hackers are doing today, but also at what they did before, and try to predict what's going to be there tomorrow and understand what we're facing. You've probably seen some of the CERT charts that show essentially exponential growth in the discovery of vulnerabilities in our system. What's the problem? Why are we discovering vulnerabilities in our software at the rate currently of 5,000 per year, which is 14 per day, just enormous numbers?

We've done some studies on this to try to figure out what our research strategy should be. Basically the conclusion we've come to is that we're dealing with systems of historically unbelievable complexity. Your average desktop PC represents something like a hundred million lines of source code. This is staggering. The Apollo moon rocket had roughly a million parts in it, 747s have a million and a half parts.

We're dealing with something like a hundred million lines of code. This is complexity we've just never dealt with before. What we're finding is that with this hundred million lines of code, the current software development life cycles I talked about are producing code with the quality of about one security bug for 1,000 lines of code. If you do the math, that means that on your desktop you've probably got something like 100,000 security bugs on your system. These are just phenomenal numbers. So we don't see any near-term trend of vulnerabilities going away, nor do we expect to see perfect systems any time soon.

Another trend that is very interesting is that the hackers now are starting to attack the clients. Universities and business enterprises are then up to a

sort of bastion mentality: "Let's put up walls around our data center. Let's keep the bad guys out with things like firewalls." And what's happening is that all the hackers are saying, "Okay fine, you're going to protect your data center; I'll go break into the client of one of your administrators who's authorized to come in, and I'll come in over his connection."

So it's not going to be adequate to think about just protecting your data center or just protecting your central machines. You have to protect the entire system—the clients and the network and the server. This is a definite trend that we've seen. We've seen it with things like the QAZ virus, which grabs user names and passwords of the clients. It's not just dealing with one thing that's horrendously



Telemanagement Solutions

- ▶▶ Call Accounting
- ▶▶ Inventory / Cable
- ▶▶ Service Order
- ▶▶ Directory
- ▶▶ Modular Architecture
- ▶▶ Low Cost of Entry

PLUS: InfoCall E-911
Addressing Internal and External
Public Safety Needs
Learn More: www.enhanced911.us

▶▶ www.infogrp.com ▶▶ 1.866.infogrp ▶▶ www.enhanced911.us

Partners: Siemens | Nortel | Avaya

So it's not going to be adequate to think about just protecting your data center or just protecting your central machines. You have to protect the entire system; you have to protect the clients and the network and the server.

complex, but also dealing with very complex systems and complex hosts and clients and servers and networks.

Looking at how we're approaching it in research, we have basically five main strategy areas:

1. The first one I mentioned was the band-aid type approach. We have intrusion detection, firewalls, and security vulnerability scanners. What we're seeing now is that these have slowly matured.

The next step that's coming in this area is the integration of all of these different sensors. In the past, for example, at A & M, we had one intrusion detection system, one host-auditing program, and one drawbridge program. And what we're seeing is that the trend in this area is to recognize that no one of these is going to be perfectly strong.

You want to have lots of intrusion detection sensors and auditing systems scattered around. You want to do real-time intrusion and real-time auditing. We're going to see these frameworks of security tools develop into things like Risk Manager, which started in this area, and other vendors have similar things. We'll see the integration and expansion of these sensors throughout the university or enterprise. That will definitely help make these tools a lot

better by reducing false alarms, false positives, and false negatives. You'll get more meaningful and useful output.

I mentioned that IBM's Managed Security Services deals with a million and a half alerts per day. One of our goals is to get this down to numbers that are much, much smaller; that are much more meaningful; that don't represent misconfigured machines or routine periodic scanning but actual serious intrusions.

2. Our second strategy is to say, "Okay, given our operating systems as they are right now and tools as they are right now, what can we do to make the overall system more robust?"

The approach is to go to distributive and autonomic type systems. Rather than having one central file server, for example, you might consider having file servers replicated and distributed around so that if any one of them breaks or is broken into, we have replication and availability. We can do things like cryptographic crosschecking and cryptographic protection of these files if they're scattered around distributed systems such that even if a minority of the machines are broken into the data is still confidential and secure and still has good integrity. The idea then is to say, "Well, if our individual components aren't secure, let's distribute the problem over a lot of them and challenge the hackers to have to break into a very large numbers of machines scattered all over the place." Take advantage of all these distributed wireless clients to make the system more secure.

Magnussen: So you're looking at distributive data set that's actually scattered across multiple machines so that anybody pulling information only gets a piece of the puzzle.

Safford: Right. In other words, it's kind of fun to turn the problem around and say, "Well, our problem is that we have hundreds of millions of machines connected on the Internet and that's not secure." Maybe part of the solution is to take advantage of those hundred million machines scattered around the Internet. You see things like grid computing. In our own particular

research project on wireless security auditors, we just announced a distributed wireless security auditor. The idea is that rather than have a human expert walk around with an auditing tool once a week, we've put a little software application on everybody's wireless client or notebook and we have them continually auditing the network for us invisibly and reporting in, and in an autonomic fashion recognizing misconfigured access points and actually fixing them.

So part of the thing is to take these unsecure components that are distributed and take advantage of that in terms of autonomic security.

3. The third area is to actually try to attack the problem on the end host. We've known for thirty years the theory behind how to make operating systems secure. This is the work that was done by Roger Shell and the department of defense in the original orange book.

The theory behind how to make these systems more secure is actually well understood, but there are a lot of reasons why it hasn't been done: expensive software, difficulty, poor user interfaces, niche market...a lot of different reasons that are just excuses for why the industry hasn't produced robust, secure operating systems. But it's something that can be done. The theory is well understood; it's just a matter of sitting down and doing it.

We're working with the open source Linux community to try to take Linux not one step farther but two or three steps forward in security. We talk about the Linux system maybe having a hundred million lines of code. One of the things to do is to do good engineering, good design, good architecture such that the application code—which is probably 99 of those million lines of code—is not security critical. Have the kernel be the only thing that is security critical. If an application has a bug, that's fine, the operating system can contain it. The operating system can keep it from getting to things that it is not supposed to get to, regardless of its bugs, regardless of hackers attacking it.

So we are working with the open source community, the LSM security modules, and the NSA is working with us with security enhanced Linux, SGI. IBM and a large number of players are working on this. Probably in the next couple of years you're going to see distributions coming out that are going to be much, much more secure than existing systems.

4. Another thing that we've been working on is a hardware assist. A couple of years ago we shipped the cryptographic co-processor called the 4758. Basically it's putting a secure computing environment into hardware—something you can use on the server. This is a PC I-card you can put in your server machine regardless of its operating system. It has a very secure, tamper-proof environment, so you can do very powerful functions on it. Sean Smith and I wrote a paper in the September issue of the *IBM Systems Journal* in which we showed, in fact, that if you have one of these, you can do something like a Web server in which you can give the hacker physical control of the machine or the server and the password for it, and he cannot read a single bit of data, he cannot alter a bit of data, and he cannot even tell which valid users are reading what bits of data. So these secure co-processors are a way of, on the server side, moving the sensitive part of the application into hardware, which is a very good approach.

On the client side, as I mentioned before, the hackers are starting to attack the client. We also can put some hardware in there to help protect the one thing that the hackers are really after, which is the authentication information of the valid users. Currently, pretty much everybody uses user name and password. If we can get this conversion over public-key based hardware tokens, then we can authenticate the hardware token on the client to the secure co-processor hardware on the server. Under this scenario, it doesn't matter if there are bugs in the software because the hackers can't get to this strong authentication information.

IBM's cofounder of the Trusted Computing Platform Alliance [TCPA] has announced the formal specification for what's called the TCPA chip, the security chip. It's actually shipping now on T30 notebooks, and we can see it's really a major step forward because it basically puts the authentication from the client to the server into a hardware chip. A person's private key is generated on this chip, it never leaves the chip, and it can be used to do secure authentication to the server in a way that we can say, "No hacker can ever get that private key." So it's a very important thing—hardware on the client, and hardware on the server.

The TCPA chip, by the way, is one of these major developments that I think is very important to look at because it's not just IBM, it's not just Intel; 180 companies, including Microsoft, IBM, and Intel, all major PC players, have signed on to the TCPA standard. We are going to start

seeing clients coming out with this hardware built in such that we can have the hardware foundation for good client-server type communication. This is a very important development and trend.

5. The final thing, which I mentioned before, is the education aspect of it. Industry and universities really need to work together to educate future leaders in the field to understand the secure development life cycles, what's important at the requirement stage, design stage, implementation stage, and what's a buffer overflow and so on. How are they exploited? How do you defend against those? Teaching all this so that as the next generation of software comes out, hopefully we'll reduce this 100,000 bugs to something considerably less. So we think that education is very important and it really needs to be a partnership.



MiCTA

***MiCTA is pleased to announce...
membership agreement for all
ACUTA members!***

Member benefits include cost savings, negotiated service agreements, consulting services, problem solving assistance, training opportunities, conferences, information clearinghouse and more!

Be sure to attend MiCTA's 2002 Fall conference October 14 - October 16 at the Hyatt Orlando.

For more information, visit www.micta.org or call (888) 870-8677.



Watching the Network

by Earl Carter
Cisco Security & Technologies
Assessment Team

[Y]ou must be able to monitor your network so that you can identify any unusual behavior and identify situations in which your security policy is being violated, either due to an incorrectly configured device or an attacker bypassing established security mechanisms.

Whenever people open up a new business, one of their first concerns is protecting their physical assets. Along with other security measures, they install new locks and some type of burglar alarm. Universities, businesses, and many homeowners routinely use burglar alarms to protect their valuable possessions. When an unauthorized person enters a protected area, the burglar alarm generates an alert. This alert can actually notify the police directly or may notify someone who is responsible for site security.

When it comes to computer networks, however, many people fail to take the same security precautions that they commonly use to protect their physical assets. Failing to adequately protect access to your computer resources can result in unnecessary network downtime, increased costs, the loss of intellectual property, and even legal liability if a compromised system is used to attack other computer networks.

Computer networks, especially academic networks, are exposed to a diverse group of users. Furthermore, these users need to access the network from a broad spectrum of locations. Ensuring that these various legitimate users access only authorized resources while also preventing unauthorized users from infiltrating the network can be a very challenging task.

Know Your Enemy

Attackers fit into two broad categories: *external* and *internal*. External attackers represent people who have no authorized access to your network, whereas internal attackers start with some type of authorized access to your network. External attackers must penetrate your network via a perimeter security device. Internal attackers, however, can launch attacks from internal systems to other internal systems or even systems on other networks. (Attacks from this group are also called the insider threat.)

Besides the type of attacker, another distinction for attacks against your network is whether the attack is structured or unstructured. *Unstructured* attacks are the least severe because the attacker is usually working alone and may not have any specific attack targets. *Structured* attacks usually involve more than one attacker, and the attack may be funded by an external entity. These attacks normally have well-defined goals and specific targets. Thwarting structured attacks from internal attackers is the most difficult task for a network security administrator.

When attacking your network, attackers will target your network devices (i.e., routers, switches, computers, IP phones, etc.) as well as the network protocols that the different devices on your network use to

communicate with each other. These attacks will usually model one of the following different attack methodologies:

- Ad Hoc – Random probing and attacking
- Methodical – Ordered comprehensive probing and attacking
- Surgical Strike – Attack on a single target
- Patient – An attack carried out very slowly over a long period of time
- Blitzkrieg – An all out massive assault against a network

Although all of these methodologies incorporate the same basic data collection and attack techniques, they vary with respect to speed and comprehensiveness. A patient attacker is trying to avoid detection and may perform reconnaissance over a period of several months, making his presence extremely difficult to detect. In a *blitzkrieg*, however, the attacker(s) are conducting an all-out massive assault on your network in an attempt to either totally disrupt network operation or mask the real attack underneath the noise created by all of the activity on the network.

Security Barriers

Numerous security mechanisms, such as firewalls, user authentication, VLANs, and VPNs establish security barriers to prevent unauthorized access to network resources. Using correctly configured barriers such as firewalls to protect the perimeter of your network does an excellent job of keeping external attackers from accessing your internal system resources. Nevertheless, they provide only limited protection for devices such as public Web servers that must be accessible from virtually any computer connected to the Internet.


With the numerous threats from assorted attackers, it is crucial that you protect your network beyond the basic perimeter security devices such as firewalls. Just as physical locks can be picked and keys stolen, the security devices implemented on your network can potentially be circumvented. Therefore, you must be able to monitor your network so that you can identify any unusual behavior and identify situations in which your security policy is being violated, either due to an incorrectly configured device or an attacker bypassing established security mechanisms.

Intrusion Detection Systems

Intrusion detection systems enable you to monitor your network looking for intrusive activity. An intrusion detection system is effectively a burglar alarm for your computer network. An intrusion detection system monitors certain characteristics of your computer network, such as network packets, host logs, or system calls. Before entering into the explanation of how an intrusion detection system works, it is helpful to explain a couple of terms that are commonly heard with respect to the operation of an intrusion detection system.

MySoft.net

Don't just surf the net – catch the wave!
100% browser based telemanagement software from Compc.




USE YOUR BROWSER TO MANAGE:

- ✔ Customer focused web apps
- ✔ Oracle or MS SQL database
- ✔ e-billing and e-resale
- ✔ Assets and cost allocation
- ✔ Work order process/work flow
- ✔ Circuits and invoice verification
- ✔ Voice/data resource tracking

Tom Tow, Senior Analyst at The Gartner Group, said in a USA Today article, "No one wants to buy client-server and desktop PC applications. They want Internet based products." Will your vendor be left behind? Will you get stuck with an outdated product? Why take that risk?

Experience MySoft.net for yourself.
See a live demo over the web.



COMPCO

5120 Virginia Way ~ Brentwood, TN 37027
615-373-3636, ext 148 ~ www.compc.com ~ sales@compc.com

Design and Operations Criteria: Trust No One

by Ron Walczak, RCDD

Walczak Technology Consultants

We live in a world where some people seem to have too much time on their hands, and many of these folks have creative talents that give them the ability to crack security codes, firewalls, and the like. What's worse, they can do it in the safety of their own home from halfway around the world (our communications server averaged nine unauthorized access attempts one day in June from points all around the globe). In addition to routers, firewalls, and virus protection discussed in this issue, another area of security that should be given its due is the physical security of your network. Focus with me on minimizing the threat closer to home: physical disruption and theft of service caused by the people who work for, and reside at, your institution.

Motivations to disrupt can include plain old vandalism, anger at the institution or another student (revenge), exuberance (we won the game!), and boredom, to name a few. The motivation to steal services needs no explanation. And the motivations are the key to protection. It takes more thought, time, and effort to steal than it does to break, making vandalism a more common problem. So how do you minimize the opportunities for these types of security breach? Consider the following list of design criteria starting at the wall plate:

- Metal faceplates do not crack.
- Angled jacks protect jacks and cables against over-exuberant furniture moving.
- Surface-mounted raceways screwed to the wall (not just adhesive) do not pull off.
- Cables in conduits do not get cut; cables laid across ceiling tiles are fair game.
- Dedicated wiring closets that can be locked without half the campus having keys to the room is preferred to log entries. (Make sure there is a manual key override.)

Card-key access is preferred. Installing alarming devices in the room (access and environmental monitoring) provides even better protection.

- Consider alarm devices that monitor connectivity status on ports. (Warning: These products sit between your switch and horizontal wiring. They insert power on the cable to monitor connections—effectively reducing your horizontal cable speeds to 100 mbps.)
- Limited, card-key access to locked server rooms is preferred to log entries. (Make sure there is a manual key override). Media storage should always be controlled (locked up). Disks, CDs, tapes, and zip cartridges are easy to steal and are also a potential source of virus attack.
- Speaking of media, how thorough is the disk erase process you use when pulling PCs from active service to discard or donate? You *DO* use an erase program, don't you?

Theft of service requires a bit more time and usually a pilfered key to the wiring closet. Most campus designs provide student connectivity flexibility via patch panels in the wiring closets. Who has time to actively monitor whether a connected port has a *paying* subscriber? Once in the closet, an ambitious soul with patch cords can become a business unto himself, selling connectivity to fellow students at a "discount." The institution is most vulnerable during semester startup when techs are running mad trying to connect subscribers—leaving closets unlocked or propped open.

Bottom line: You expose it, you risk it.

Ron Walczak is the principal consultant with Walczak Technology Consultants, Inc., in Prospect, Pennsylvania. Visit his Web site at www.walczakconsultants.com.

As with any alarm system, not all of the alarms generated by an intrusion detection system represent actual intrusions. Some alarms are triggered by normal user activity. These alarms are known as *false positives*. Controlling false positives is vital to successfully deploying intrusion detection on a network, since they erode confidence in the intrusion detection system. Home burglar alarms can fall prey to similar problems with respect to false alarms. After responding to numerous false alarms, the police response time is likely to increase due to the assumption that any alarms are just another false alarm.

Another term that is commonly used is a *false negative*. In this situation, an intrusion detection system fails to alarm on an intrusion that it is designed to detect. False negatives represent a failure of the intrusion detection system since they represent situations in which the intrusion detection system missed a monitored intrusive event.

To understand how intrusion detection systems operate, it is useful to examine the different triggering mechanisms an intrusion detection system can use to detect intrusive activity and the locations within your network that the intrusion detection system is monitoring.

Current intrusion detection technology uses two major triggering mechanisms:

- Anomaly detection
- Misuse detection

Anomaly detection involves defining profiles that represent normal user activity. When a user's activity deviates from the established profile, an alarm is generated. On the positive side, anomaly-based detection systems will alarm on anything that falls outside of the defined profile. This means that the anomaly-based system can detect intrusions based on attacks that it has never seen before. Furthermore, it is difficult for an attacker to know what traffic he is generating will be considered abnormal and thereby generate an alarm. Associating the alarms generated with a specific type of attack, however, can be very difficult. In addition, during the initial training period in which the profiles are created, the network is not being monitored for intrusive activity.

A misuse detection system (also called a signature-based detection system) has a specific signature for each intrusive event that it is watching for on the network. With this system, the



LocusDialog- Speech Telephony Solutions

The #1 solution for enhancing campus communications with the ease and effectiveness...

Use one phone number and natural spoken requests to reach students, faculty, departments and services, even a favorite off-campus pizza place!
Ideal for any size campus.

the convenience and flexibility...

Integrates to existing digital or analog PBXs and Centrex infrastructures.
Unique proactive support for minimum maintenance.
User-friendly 24/7 operation; like live operators, minus the overhead costs!

of speech-dialed connection!

With over 600 Liaison™ systems successfully installed, LocusDialog's speech-powered solution is all you need for always making the right campus connection!

Learn more

www.locusdialog.com/education/
1 888 GO-LOCUS,
just say "Sales Department"

Try our demo: **1 888 757-DEMO**



LocusDialog™
Speech Telephony Solutions

user knows exactly which types of attacks the intrusion detection system should detect. Whenever activity on the network matches one of these signatures, the intrusion detection system generates an alarm. Associating the alarm with a specific type of attack is rather easy, but a misuse detection system can only detect intrusive activity that matches one of its predefined signatures. Therefore, an efficient signature-update mechanism must be established to keep the misuse detection system current. Misuse detection systems must also maintain state (stored information) for signatures that involve data observed across multiple packets or data sources.

Network-based or Host-based Systems

Besides specific triggering mechanisms, your intrusion detection system must also look for triggering events at different locations within the network. Monitoring may be network based or host-based.

Network-based intrusion detection involves placing sensors at various locations within your network. These sensors capture network traffic and analyze it for malicious activity. Each one of these sensors is watching your network, looking for unusual or intrusive activity. When a sensor generates an alarm, this information is relayed to a centralized monitoring console where you can get a macroscopic view of your entire network. This approach is similar to placing cameras at various locations across a campus (entry doors, labs, computer rooms, etc.). A drawback to this approach, however, is that it can be difficult to determine if certain attacks actually succeeded (e.g., an attacker may have launched a Windows Internet information server exploit against an Apache Web server).

With host-based intrusion detection, a software agent resides on each of the machines in your network. This agent is looking for intrusive activity on a single computer. These agents can

either examine system logs or system calls to find intrusive activity. Like the network-based sensors, these host-based agents can report to a centralized monitoring console. Since host-based monitoring relies on specific operating system characteristics, you need to have an agent for every type of operating system that resides on your network. Furthermore, host-based agents are usually not available for infrastructure equipment, such as routers and switches. Correlating the information from the individual host-based agents into a network-wide perspective can also sometimes be difficult. Nevertheless, the host-based agents can usually provide positive confirmation as to the success or failure of a specific attack against the host that they are monitoring.

Besides generating alarms when intrusive activity is observed on your network, many intrusion detection systems can also react to attacks against your network by updating access control lists on your routers and firewalls to stop further attacks from specific hosts. Host-based intrusion detection systems that monitor system calls, as opposed to system logs, can also be configured to disallow malicious system calls, thereby preventing specific attacks from succeeding.

To be functional, an intrusion detection system must incorporate a monitoring location and a triggering mechanism. The different monitoring locations and triggering mechanisms each have their own pros and cons. Therefore, many intrusion detection system vendors are incorporating many if not all of these mechanisms into their systems in an attempt to maximize the functionality. These systems are referred to as hybrid systems. One of the more popular hybrid intrusion detection systems currently available incorporates both network-based and host-based monitoring in an attempt to get a complete picture of the activity on the network, from the macroscopic perspective down to the microscopic

perspective. You may also see a hybrid system that combines misuse detection with anomaly detection.

Meeting Today's Security Needs

Today's computer networks are continually increasing in complexity. Just a few years ago, a university network consisted mainly of a few computer labs and the network used by the faculty and administrative personnel. Today, however, almost every student on campus uses the university's network. Many universities allow students to register via their computers. Other institutions have wireless networks that enable students to access the network from literally anywhere on campus.

Besides the number of people allowed to access the network, the functionality provided by a university's network has undergone tremendous growth. It is not uncommon for a typical university network to support numerous functions such as student registration, IP telephony, e-mail, class assignments, specific class Web sites, and distant learning. Access to today's university networks is extremely diverse, making the problem of securing these networks very complicated. Deploying an intrusion detection system can help monitor this diverse network and verify that the defined security policy is being followed.

Earl Carter is a member of Cisco's Security Technologies Assessment Team (STAT) and author of the Cisco Press book titled *Cisco Secure Intrusion Detection System*. For additional networking technology and certification titles visit www.ciscopress.com. Carter can be reached at ecarter@cisco.com.





Reviewed by: Justin M. McNutt,
University of Missouri–Columbia

Information Security Best Practices *205 Basic Rules*

by George L. Stefanek

Published by: LLH Technology Publishing, 2002. 194 pages.

Information Security Best Practices, like many network security-related books, is an interesting amalgam of the seemingly obvious and the obscure. The *205 Basic Rules* mentioned in the subtitle provide a simple, straightforward format that leads logically from one topic to the next.

The book begins with a discussion of the threats to a network. What kinds of attacks exist? How do hackers break into networked systems? Where are the greatest risks to a system?

The next section discusses security policies, how to tailor those policies to a particular environment, and why management support is critical to successful policy implementation (and some tips on how to get that support). For reference, a sample security policy comes on the CD-ROM included with the book.

Chapters five through 19 enumerate the 202 remaining rules (three are listed in the policy section). Every subject from physical security to operating system guidelines to network

architecture suggestions is covered. Several reference sections and a bibliography provide additional useful information.

Overall, this book is a fast read that covers all of the essentials of network security without getting bogged down in esoteric discussions about strong encryption algorithms. It gives the reader a road map rather than an encyclopedia and serves as a guide toward greater overall network security. While the book does not go into minute detail on every subject, all of the major aspects of network security are covered. The CD-ROM version of the text (PDF format) is convenient for quick searches, and it provides some useful security utilities, such as one tool that can pull passwords from a Windows workstation—handy for presentations to management on why physical security is important.

I recommend this book to any network administrator of intermediate to advanced skill who is responsible for the security of a network. The nontechnical discussions help the administrator make compelling arguments to management, while the technical parts provide the basis for the overall plan.



Register Online at
www.league.org



0111001
00110100111
10010100



FOR INNOVATION
IN THE COMMUNITY COLLEGE

2002 CIT

CONFERENCE ON
INFORMATION
TECHNOLOGY

November 17-20
Long Beach Convention Center
Long Beach, CA

The League for Innovation's annual Conference on Information Technology (CIT) is the premier showcase of the use of information technology to improve teaching and learning, student services, and institutional management.

Hosted by Los Angeles Community College District
and Long Beach City College

Cybercrime: Are You Ready?

by Megan Statom

Cybercrime includes theft, fraud, malevolent activity, and espionage carried out through or upon the commercial and public information telecommunications systems.

At the sixth annual National Colloquium for Computer Security Education in Redmond, Washington, this past June, Richard Clarke, White House special advisor for cyberspace security, warned that an information

war is approaching, and when it arrives the \$15 billion lost every year to computer hackers will “seem like nothing.”

Clarke acknowledged that the government is not going to be able to forewarn businesses when a cyber attack will take place. “Law enforcement can’t save the private sector,” he stated.

What matters are the vulnerabilities within corporate networks. Clarke says the most vulnerable networks are the ones found in college and university systems, some of which have little—if any—protection. Clarke urged IT directors to push for better security at their own schools.

Communications technology professionals must improve their knowledge of cyber attacks and the steps that can be taken to prevent and recover from them. ACUTA will offer a

three-day study of disaster preparation and business continuity at the Winter Seminars in Tempe this coming January 12–15. A good overview and the usual first-class exchange of ideas among peers will provide a valuable introduction to this important topic. For those who need even more, a variety of certification and degree programs are now being offered at several institutions. Here are a few examples.

The Cybercrime Studies Institute

Anne Arundel Community College in Glen Burnie, Maryland, is home to the Cybercrime Studies Institute. The college partnered with The Windermere Group, LLC, to create the institute in order to offer training in a high-tech computer training facility, fashioned for cybercrime computer and legal training. The institute offers classes designed for employees and consultants of companies concerned about cybercrime and IT professionals involved in network support issues.

Classes that can be taken at the Cybercrime Studies Institute are Network Security Fundamentals and Network Defense and Countermeasures.

Network Security Fundamentals is a 48-hour course for Windows NT/2000 and UNIX network administrators. After completing the course, administrators should understand the fundamental aspects of network security, be familiar with common techniques used to attack networks, be able to create router security using the functions of access control lists, and be able to define the common Internet components and techniques used in Web hacking.

“The cyberbattlefield is real. It’s a place where computers are used instead of guns, data packets instead of bullets, and firewalls are used instead of barbed wire.”

—Richard Tracy,

Cybercrime...Cyberterrorism...Cyberwarfare...: Averting an Electronic Waterloo, November 1998, Center for Strategic and International Studies.

Network Defense and Countermeasures is also a 48-hour course intended for Windows NT/2000 and UNIX network administrators who have a firm knowledge of basic network security. The course is meant to provide administrators with superior knowledge of network defense. It teaches IT professionals how to take protective measures for networks, the different methods of intrusion detection, network monitoring, and countermeasures that can be taken.

"IT personnel are aware that the threat of having your network attacked is very real," says Elizabeth Harrison, manager of the Cybercrime Studies Institute. "The number of incidents is increasing exponentially every year. The problem is that too many network administrators don't truly understand how to protect the network. You should know how to set up defensive measures to mitigate risk, not just how to react to an attack if it happens."

When the series of courses has been completed, the student is recognized as a *cybercrime specialist*, defined by the Institute as one who "uses knowledge and skills of a legal, business, and technical nature to detect and collect evidence of fraud, theft, espionage, and malicious activity."

The Cybercrime Studies Institute was established in April 2002. The \$1,350 fee for each class includes instruction, lab fees, the continuing education certificate, and all course materials. Students—a maximum of 12 per class—are generally network administrators and technicians or people who are seeking a career change. The program is unique in that it is designed to be taken over a short four-week period and then immediately applied on the job, minimizing the chance for the skills learned to be outdated when the program is completed.

Computer Security at GWU

George Washington University (GWU) in Washington, D.C., has recently been certified by the National

Security Agency as a Center of Academic Excellence in Information Assurance Education. The university offers a new graduate certificate program in Computer Security and Information Assurance, a plan for those who need to zero in on the most current knowledge in the sphere of computer and network security.

"When you're talking about IT directors, you basically have two types: the person who is in charge of the management of the security of the enterprise and the technician who implements the technical solutions to increase security," states professor Dianne Martin, director of the Cyber Security Policy and Research Institute at GWU. "Our programs address both types, and each needs further training. The management and oversight of security measures, from security badges to the protection of floppy disks and CDs, requires a new level of training because security problems and capabilities are becoming more and more sophisticated. What IT professionals need to realize is that you do have both aspects which have to be addressed."

While GWU has been offering computer security courses for years, this certificate in Computer Security and Information Assurance has only been available for a year. The program consists of four courses related to computer security: Introduction to Computer Security; Viruses, Worms, and Network Security; Information Policy; and E-Commerce Security.

Introduction to Computer Security provides instruction on techniques for security in computer systems, including authentication, logging, authorization, and encryption. Viruses, Worms, and Network Security educates the student about Web security and intrusion detection, and about protection against statistical inference. Information Policy covers issues related to privacy, equity, and intellectual property, including criminal justice and law enforcement implica-

tions. In E-Commerce Security, IT professionals discuss advanced technical topics involving e-commerce security, including X.500 registration systems, X.509/PKIX certification systems, secure payment methods, smart cards, and authorization models in open distributed environments.

Students can take the classes in what the school calls *cohorts* in which they take all four classes at a somewhat accelerated pace. These groups are typically 10–15 students per cohort. If the student opts to take the classes through open enrollment, the class sizes are a little larger at 30–35 students per class. Most of the students in this program are IT professionals returning for more education and certification in the area of computer security. The program cost is \$9,950, which includes all books, lab fees, student fees, and a light supper each class evening.

The Canadian Centre for IT Security

The Canadian Centre for Information Technology Security in British Columbia provides education and research on computer security and high-tech criminal investigation. In 2000, the Centre, which is a joint venture between the University of British Columbia and the Justice Institute of British Columbia, began offering a certificate in Internet and Technology Security.

The program covers all areas of information security, encompassing 14 modules and 210 hours of instruction and class work over nine months. Participants spend three hours every week in online learning, consisting of online lectures, readings, research, discussions, and assignments. In addition, there is one face-to-face meeting per week, which features guest speakers, lab work, and other learning experiences.

The Data Transmission and Network Topologies part of the program studies how data is transmitted across private and public commu-

SECURITY AGENDA

Managing the Threat from Within

Tad Deriso, Director
CHR Solutions, Inc.

By far the greatest threat to network security is internal users of the network. From accidentally opening infected e-mail attachments to setting up a small departmental 802.11 wireless network without the help of the campus IT group, users on campus constantly test the limits of network security.

Ron Hutchins of the Office of Information Technology at Georgia Tech notices that the problems on their network come from users' indifference to network security. The campus network is "scanned" hundreds of thousands of times each day from the outside, and there are robust protection tools to mitigate outside security threats. But there must also be effective policies and enforcement procedures in place to help mitigate security problems that can arise from users' activities.

From a wireless perspective, 802.11 wi-fi networks are proliferating on college campuses. David Hoyt, chief information officer at Collin County Community College District in Texas, agrees that wireless networks can be a major cause of concern for potential network security breaches. Because the technology uses unlicensed spectrum, anyone with a wi-fi card installed on a laptop can pick up the signals and create potential problems on the network or use the campus network to launch offensive attacks on other networks. Much has been written recently regarding security for wi-fi networks, and network administrators should take those concerns to heart.

The communications professional can and should be proactive and take steps to prevent the institution from becoming a victim or an unwitting participant. Serious

measures should be taken to educate users in the campus community about network security and how each one can act as a guardian of the campus network. This would include providing examples of how users can inadvertently cause security breaches and identifying ways users can be aware of their actions. A policy statement, with enforceable penalties for noncompliance, could be a way for campus administrators to raise the visibility of network security.

From an audit perspective, administrators should make sure that all physical network devices are secured and unavailable to others. Secured communications closets, or secured cabinets in public storage rooms, can go a long way to preventing any accidental or malicious security breaches. Take a laptop equipped with a wi-fi card around campus, and see how many wi-fi networks are detected. This can tell you if there are unauthorized wireless networks that may allow others to infiltrate network security. For those that are detected, make sure there are security provisions in place, and make sure your internal telecom staff knows how to plug security gaps in wireless networks.

While no network can be truly 100 percent secure, communications professionals would be wise to take immediate steps to implement enforceable policies and procedures and increase awareness of the importance of network security within the university community.

Tad Deriso is director of CHR Solutions, Inc., an ACUTA corporate affiliate in Norcross, Georgia. He can be reached at Tad.Deriso@chrsolutions.com.

communications networks, looking in detail at the transmission methods, transport formats, and security measures used. Students also learn how routers and firewalls are designed and used to protect networks.

Another module, Network Security, covers in detail the different Web application attacks that are prevalent and the security defenses against them. It also studies the main security protocols used today to secure different applications and communications channels, such as e-commerce and virtual private networks.

Students are usually IT specialists, system administrators, auditors, law enforcement personnel, and corporate security managers. There is a maximum of 25 students per class. The cost of this program is \$7,200, which covers course materials and books.

Sources say cybercrime is escalating at a rate of 500 percent per year. While that statistic can be staggering to any communications technology professional, it should not discourage us from protecting our institutions from attack. It is absolutely essential for today's IT personnel to be armed with the most up-to-date information available. "The spotlight has been on cyber security in recent months because a few government officials have said that cyberspace is the next sector for terrorism," says GWU's Martin. "The whole notion of protecting our telecommunications infrastructure nationally in this area is critical. IT professionals have to step up to the plate."

Megan Statom is the ACUTA communications assistant. She can be reached at mstatom@acuta.org.



Bill D. Morris Award 2002



Bill D. Morris, University of Central Florida, was president of ACUTA in 1988–89. He passed away shortly after stepping down as president, and his memory is honored with the presentation of this award each year.

Previous Award Winners

1990	Del Combs, ACUTA Admin. Dir.
1991	Mike Grunder, Yale Univ.
1992	Sydney Paredes, US West
1993	James S. Cross, PhD, Longwood College
1994	Mal Reader, Univ. of Calgary
1995	Valerie Turner, No. Michigan Univ.
1996	Luther Robb, Penn State Univ.
1997	Patricia Searles Nelson, Cornell Univ.
1998	Whitney Johnson, No. Michigan Univ.
1999	Anthony Tanzi, RCDD, Brown Univ.
2000	Ruth A. Michalecki, Univ. of Nebraska
2001	Anthony Mordosky, Rowan Univ.

Corinne Hoch

“A professional in the finest sense of the word.” That’s what most of her colleagues say about this year’s winner of the Bill D. Morris Award, Corinne Hoch of Columbia University.

Corinne has earned a reputation as an organizer and a leader through her dedicated efforts on her campus as well as her commitment to the association; but since September 11, 2001, she will always be known to ACUTA members as the one who called us to action and lead the drive to donate supplies for the rescue efforts at the World Trade Center.

As President Maureen Trimm remarked at the presentation of the award at the annual conference, “This year’s recipient of the Bill D. Morris award was in her Manhattan office, on a typical early fall quarter day, only a few miles north of the World Trade Center. What the rest of her day was like, and the days to come, tell me much about the personal qualities of grace under pressure; of commitment to the students, staff, and faculty of her university; of communications technology skills and inventiveness; and mostly about connections to the larger community.

“That this larger community includes ACUTA is fortunate for us all, in that [Corinne’s] call on the listserve to inform us about ways in which we could individually help survivors and rescue workers helped each of us around the country to be a part of this community effort.

“In a panel discussion at the ACUTA fall seminar in Albuquerque, she shared with us the many things she wished she could have been better prepared to do in such a disaster, and of course, the many things she and her colleagues did do.

“As her boss told me, she is the person the president of her university counts on to help craft messages to students, including the broadcast messages sent out in September to inform, calm, and console the community. In fact, she is known as the ‘Rolm phone lady’ by the students who hear her as the voice of Columbia University.”

Since joining ACUTA in 1990, Corinne has contributed to the growth of ACUTA programs and services, especially the users groups. After being introduced through the Rolm Users Group, she was asked to take on the role of planning and coordinating the 10 users group meetings at ACUTA annual conferences. She rose to this challenge, developing a set of procedures and an annual timeline that have resulted in a polished process.

For the past year, as chair of the Vendor Liaison Committee, she has demonstrated once again her talents as a facilitator and her positive approach to collegial relationships.

As Maureen Trimm remarked, “ACUTA is fortunate to have her as a member, a volunteer leader, and a friend.”

Congratulations, Corinne Hoch. You exemplify the qualities that we honor in memory of Bill D. Morris: dedication, vision, professionalism, and leadership. And they are correct who call you “a professional in the finest sense of the word.”



Advertisers' Index

By advertising in the *ACUTA Journal*, these companies are not only promoting products and services relevant to telecommunications in higher education, they are also supporting our association. As you have opportunity, we encourage you to mention to these companies that you saw their ad in our journal.

- ★ **1 Nation** 25
 (813/855-8850)
 4027 Tampa Rd., #3000, Oldsmar, FL 34677
 info@1nationtech.com
 www.1nationtech.com
 - ★ **Amcom Software** Inside Back Cover
 Kathy Veldboom (952/946-7715)
 5555 West 78th St., Minneapolis, MN 55439
 kveldboom@amcomsoft.com
 www.amcomsoft.com
 - ★ **ATL** 23
 Sandra Escobar (203/399-0132)
 198 Lawn Ave., Stamford, CT 06902
 sescobar@buy-atl.com
 - ★ **CBi** 29
 Donald Goodearl (603/524-8400 x3301)
 42 Franklin St., Laconia, NH 03246
 dgoodearl@cbibilling.com
 www.CBibilling.com
 - ★ **Compco** 37
 Randy Burns, Vice President, Sales & Marketing (615/373-3636 x148)
 5120 Virginia Way, Brentwood, TN 37027
 rburns@compco.com
 www.compco.com
 - ★ **Daycom Systems** 13
 Barry Herzberg (858/200-3121)
 6759 Mesa Ridge Rd., #150, San Diego, CA 92121
 barryh@daycomsystems.com
 www.daycomsystems.com
 - Dees Communications** 31
 Louis Champan (425/869-1963)
 4130 148th Ave. NE., Redmond, WA 98052
 lchampan@dees.com
 www.dees.com
 - ★ **Info Group** 33
 Michael Grillo (508/628-4500)
 46 Park St., Framingham, MA 01702
 mgrillo@infogroup.com
 www.infogroup.com
 - Integrissys** 21
 Dennis Dinsmore, RCDD (603/431-8155)
 545 Lafayette Rd., Portsmouth, NH 03801
 ddinsmore@integrissysgroup.com
 www.integrissysgroup.com
 - Lascomm** 27
 Eli Spater (805/496-8053)
 2009 Dewberry Court, Westlake Village, CA 91361
 eds@lascomm.com
 www.lascomm.com
 - ★ **League for Innovation in the Community College** 41
 Cindy Miles, Vice President, Senior Program Officer (480/705-8200)
 4505 East Chandler Blvd., Ste. 250, Phoenix, AZ 85048-7690
 miles@league.org
 www.league.org
 - ★ **LocusDialog** 39
 Stephane Couture (514/954-3804)
 460 Sainte-Catherine West, Suite 730, Montreal, Quebec CAN H3B 1A7
 stephane.couture@locusdialog.com
 www.locusdialog.com
 - ★ **MICTA** 35
 Clancy DeLong, Asst. Treasurer (989/772-2623)
 1500 W. High St., Mt. Pleasant, MI 48858
 cdelong@micta.org
 - ★ **PaeTec/Pinnacle** 5
 Rick Cunningham, Vice President, Sales & Marketing (734/975-8020)
 1530 Eisenhower Place, Ann Arbor, MI 48108
 rick.cunningham@paetec.com
 - ★ **Scitec** 15
 (217/384-6041)
 1212 E. University Ave., Urbana, IL 61802
 - ★ **Startel** 11
 Maribeth Hogoboom, Director, Sales & Marketing (949/863-8700)
 17661 Cowan Ave., Irvine, CA 92614
 maribeth.hogoboom@startelcorp.com
 - ★ **Teledex** Inside Front cover
 Dean Compoginis (408/363-3100)
 6311 San Ignacio Ave., San Jose, CA 95119
 deancompoginis@teledex.com
 www.teledex.com
 - Vernier Networks, Inc.** 17
 Sales (866-VERNIER, 866/837-6437)
 465 National Ave., Mountain View, CA 94043
 info@verniernetworks.com
 www.verniernetworks.com
 - ★ **Vibes Technologies** 7
 Lon McCloskey (763/971-9050)
 7125 Northland Terrace N., Ste. 400, Brooklyn Park, MN 55428
 lgmccloskey@vibestech.com
 - ★ **Western Telecommunications Consulting, Inc.** 19
 Shelley Hasselbrink (213/689-5314)
 801 South Grand Ave., Ste. 700, Los Angeles, CA 90017
 shasselbrink@wtc-inc.net
 www.wtc-inc.net
- ★ Indicates ACUTA Corporate Affiliate

For information about advertising in the *ACUTA Journal* contact KCS Intl., LLC.
 717/397-7100 • www.kcsinternational.com

From the Executive Director

Continued from page 48

continuing to view technology as a strategic necessity for their campuses.

When it became apparent that September 11 and the economy would have a measurable effect on our institutional and corporate members, and on their participation in ACUTA, the staff worked quickly to develop recommendations for new programs that would make the benefits of ACUTA more accessible to members with limited travel budgets.

We initiated a new series of post-event audio seminars, making some of the best-rated sessions from our quarterly seminars available to members by audio conference. I am pleased to report that well over 400 people at nearly 150 different sites have participated in these post-event audio seminars so far, and the evaluations show that they have been well received. In addition, we continue to offer audio seminars on hot topics in the regulatory arena, which are well attended as always.

In addition, the staff developed a plan to reduce expenses by re-examining every major ACUTA activity and to develop new sources of revenue. The board of directors approved these recommendations, and most have been implemented. Our goal was to maximize the cost-effectiveness of our operations without having any negative effects on member service.

Several publications that were previously offered in print form have been transitioned to electronic format, thereby reducing costs and speeding delivery to our members. The most significant of these changes to electronic format was the *ACUTA News*. The publications committee and staff worked very hard on researching member preferences and redesigning the newsletter as a quality electronic publication. I hope that you will grow

to appreciate the new speed of delivery, reliable arrival on the first business day of each month, and the convenience of being able to forward electronic versions of the newsletter to other interested people on campus.

I am happy to report that the ACUTA institutional membership has remained very strong during the past year. We retained well over 95 percent of ACUTA's institutional members from the prior year, and many new institutions were added to the membership. This is evidence of our members' continuing satisfaction with the return on dues investment.

Last year at this time, I reported on enhancements to the ACUTA Web site that reflect our migration to a portal environment that will allow you to customize the ACUTA home page to provide the information that best meets your needs. Although we are continually developing the site, we have introduced several new features this month, which are designed to make the site more useful to you:

- By selecting your own username and password, you can create a "My ACUTA" home page that provides access to a wide range of members-only information.
- You can customize news feeds on a wide variety of technology and educational topics, so that every time you log on to the ACUTA site you will see the latest headlines on the subjects that you have selected.
- In addition, you may tell us about your job responsibilities, so that you will receive information about seminars, publications, and other ACUTA products that are designed to fit your needs.
- You can also update your membership records on the Web.
- Improved search capabilities will help you sort through the resources on our site to retrieve the information you need to solve problems on a daily basis, and there are a whole

host of other improvements that I don't have time to mention here.

In tandem with the development of new products and services, and re-examining our operations to maximize cost-effectiveness, we have continued to offer the programs that ACUTA members value. The Journal continues with four high-quality issues per year, with another series of outstanding articles, interviews, and excellent advertising support from the vendor community. In addition, we published the monthly electronic Legislative/Regulatory Update, and closely monitored federal regulatory activities. We kept our members informed of new developments and commented on proposed regulations both independently and in cooperation with other higher education associations. We continued to strive to produce the best quality and most focused educational programs anywhere, targeted to the needs of higher education communications and networking technology professionals.

As in any successful organization, the accomplishments really belong to a team. Every member of the ACUTA staff team has contributed to many of the projects that I have mentioned today. So, I would like to thank the entire ACUTA professional staff for their outstanding efforts in a very challenging year.

In summary, I am pleased to report that, in that very challenging year, ACUTA continued to move forward in pursuit of new goals and strategies and continued to develop new programs and services to meet the changing needs of our members.

Thank you.





Jeri A. Semer, CAE
ACUTA Executive Director

From the Executive Director

Executive Director's Report to the Annual Business Meeting

Each year, I have the opportunity to provide a report to the attendees at the annual business meeting of ACUTA, summarizing the activities of the association's professional staff during the prior year. We had good attendance at the business meeting this year in Reno, but not all members are able to attend. For that reason, I will use this column as an opportunity to share the annual report with those who were not able to participate in the business meeting.

The year since we met at the 2001 business meeting at Disney World has been an intense and active year for the ACUTA professional staff, as it has undoubtedly been for all of you.

As 2001-02 President Maureen Trimm reported, it has been a year in which we have worked alongside our elected leaders and other dedicated volunteers to reexamine ACUTA's mission and goals, and to develop a strategic plan that will effectively carry us forward as an organization. Staff members participated in strategic planning sessions with the board and committee chairs and as members of the teams that developed the objectives and action items that will make this plan a reality. The staff will also be very involved in implementing the action items.

I personally am very pleased with the outcome of this effort. I believe that our new strategic plan is a visionary document that embraces the many changes that are occurring in both higher education and technology, and it sets forth a realistic agenda for the future of ACUTA. The plan will guide the development of new

programs and services as we evolve to meet the changing professional needs of our current members and as we reach out to new segments of the higher education community.

I could not make this report without acknowledging some of the challenges that ACUTA has faced in the last year. The tragedies of September 11 and its aftermath have, of course, affected the United States and the entire world in ways that are only just beginning to be measured, and the nation's associations have not been immune to its effect. Like many organizations in higher education and other fields, ACUTA felt the effects of these events in reduced attendance at the programs that immediately followed the attacks. I am pleased to say that we bounced back in April with a very well attended Spring Seminar in Philadelphia, and we are also pleased with the response to the 2002 Annual Conference in Reno.

Prior to September 11, our corporate affiliates and other vendors in our industry were already feeling the negative effects of declining profits in the telecommunications and information technology industry. As a result, some companies curtailed their participation in the Fall 2001 and Winter 2002 Seminars. However, I am very pleased to report that corporate support of ACUTA has also rebounded very strongly, with combined exhibits and sponsorships at the Annual Conference in Reno exceeding last year's conference by more than 30 percent. The college and university market is strong, and our members are

continued on page 47



**Cut your costs.
Streamline your communications.
Bring it all together with one system.**

**Amcom
Comprehensive Call Processing Solutions**

- Speech recognition
- PC attendant console
- Web-enabled information and services via PC and wireless devices
- Enhanced 911 notification

Never has unified communications been more important to your faculty, administrators and students. Never has it offered greater productivity gains and cost reductions. And never has it been easier to implement and use.

Amcom CTI solutions. Designed with innovation in mind. Built to last using industry-standard hardware, software and protocols.

SERVICES

- Professional system planning and project management
- Turn-key installation and end user training
- 7 x 24 x 365 support

PLATFORMS

Oracle database
Nuance • Intel/Dialogic
Windows NT • Linux



1-800-852-8935
www.amcomsoft.com

acuta



Fall Seminars

October 20-23, 2002

Denver, CO

Marriott City Center

I. Student Services & Revenue Generation

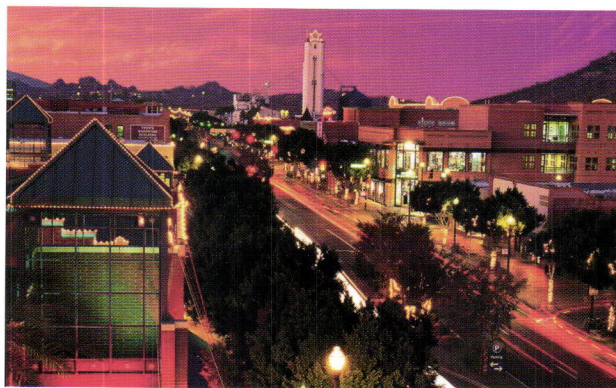
In this track, you will learn about the telecom and IT services students are demanding and cost-effective ways in which to deliver them. You'll explore new opportunities to generate revenues and to fund IT operations in the wake of declining commissions in traditional student long-distance resale.

II. Best Practices in Data Networking

Data professionals and managers responsible for campus network operations will share their experiences regarding the unique demands of university networks. Case studies will cover the limitations of various media used for transmission, network redundancies and quality of service, techniques for bandwidth management, network security issues, and the impact of putting voice traffic on the data network.

For more details or to register online, visit our Web site at

www.acuta.org



Winter Seminars

January 12-15, 2003

Tempe, AZ

Wyndham Buttes Resort

I. Developments in Communications Technologies & Applications

This seminar will provide updates on technologies that are evolving such as IP telephony, IP video, speech recognition, and unified messaging. Support applications such as customer relationship management systems, content management systems, and other innovations that impact campus networks will also be featured.

II. Disaster Preparation & Business Continuity

Attendees will learn risk assessment techniques as well as ways to develop practical disaster plans. Techniques to evaluate risks and the potential costs of recovery will be covered, and specific campus examples will be offered. Protection of telephony as well as network facilities will be discussed.