12-1-2009

Method for Securing Online Community Service: A Study of Selected Western Australian Councils

Sunsern Limwiriyakul

Edith Cowan University

Recommended Citation

Limwiriyakul, S. (2009). Method for Securing Online Community Service: A Study of Selected Western Australian Councils. DOI: https://doi.org/10.4225/75/57b417dc30df4

DOI: 10.4225/75/57b417dc30df4

7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2009

A Method for Securing Online Community Service: A Study of Selected Western Australian Councils

Sunsern Limwiriyakul
School of Computer and Security Science
Edith Cowan University

Abstract

Since the Internet was publicly made available, it has become popular and widely used in a range of services such as Email, News, IRC, World Wide Web around the globe. Progressively other services such as telephony, video conferencing, video on demand, interactive TV, Geospatial Information System (GIS), have emerged and become available on the Internet. Nowadays, Internet broadband communication infrastructure, both wired and wireless, make the concept of a Digital Community possible. The Digital Community has been growing and expanding rapidly around the world. This changes the way we live, work and play. Creating a Digital Community can empower local authorities to carry out more activities with limited resources, yet encourage business growth, provide better services, and enhance security (Intel, 2005b). This research will specifically examine the concept of a secure digital community in terms of Online Services Internet Technologies in selected local councils in Western Australia. However the research is significant to all digital communities.

Keywords

Internet, Internet Security, Digital Community, Online Security, Secure Email system, Secure Online Library system, Secure Online payments

INTRODUCTION

Since the Internet has become publicly available, it has developed into a popular and widely used community in many areas around the world. Along with the Internet broadband communications infrastructure, it brings the concept of a Digital community. A “Digital Community” is a connected community that uses Internet-based communication and computing infrastructure based on open industry standards to provide flexible and innovative services to meet people’s needs (Intel, 2005a).

Both the World Wide Web and email are popular Internet technologies that are being used in most councils in Western Australia. However, there are other Internet related or convergence technologies that are currently in use or potentially will be used in some Western Australian councils such as Voice over IP, Voice over Wireless (VoWLAN), Wireless LAN, Geospatial Information System (GIS), Global Positioning System (GPS). These technologies provide services such as online payment for council rates, online library services, security patrol, digital surveillance, telephony (VoIP), online GIS, and Internet café to local government employees, local residents and community groups. As the Digital Community concept starts to take shape, Internet related services will be more widely available to its people. For example, e-Voting, e-Polling, e-Health, and internet-radio.

Security is one of the most important factors in the Digital Community to ensure the confidentiality and privacy of users’ (residents’) information. Therefore, what can a modern Internet connected council do to meet this goal? Has the current system been implemented securely in order to meet the national and international security standards?

Significance of Research

This research will specifically examine the level of security of common Internet technologies that are currently deployed at selected local councils in Western Australia by using the OSSTMM 2.2 – Section C (Internet Technology Security) model as a main security testing methodology benchmark model. However, other information security standards will also be used to assist the OSSTMM methodology. Such relevant standards include the Information System Security Assessment Framework (ISSAF), AS/NZ ISO/IEC 17799:2001, ISO/IEC 27001:2005.

Moreover, other guidelines and recommendations from recognized organizations such as the National Institute of Standards and Technology (NIST), the Center for Internet Security (CIS), and several reference information security books, journals and articles are also referred to in the report.

The OSSTMM security model can be divided into six manageable sections for testing. Each section can in turn be viewed as a collection of test modules, with each module being divided into sets of tasks as shown below (Herzog, 2006).

However, due to time constraints, this research will focus on Section C (Internet Technology Security) of the OSSTMM 2.2. which may overlap and also contain elements of other sections directly or indirectly.

Section C – Internet Technology Security

- Logistics and Controls
- Posture Review
- Intrusion Detection Review
- Network Surveying
- System Services Identification
- Competitive Intelligence Scouting
- Privacy Review
- Document Grinding
- Internet Application Testing
- Exploit Research and Verification
- Routing
- Trusted Systems Testing
- Access Control Testing
- Password Cracking
- Containment Measures Testing
- Survivability Review
- Denial of Service Testing
- Security Policy Review
- Alert and Log Review

This research aims to analyse and test the security of common online Internet technologies which are currently used at the selected local councils in Western Australia. In particular the security of online services and electronic mail (Email) will be tested.

Demand and Use of Internet Technologies Related Services

Western Australia has 142 Local Government Authorities which equates to 23 percent of the total of Australia's local governments. Some Local Government authorities are voluntarily grouped in order to provide better services to their people through collaborative resource sharing (Stanton, 2004). Findings released by the Australian Bureau of Statistics (ABS), show that the number of Western Australian households with access to a home computer has increased from 44% in 1998 to 71% in 2006. The number of Western Australian households with Internet access also increased from 15% in 1998 to 62% in 2006. Moreover, at the end of 2006, the number of Western Australian households with broadband Internet access increased to 51%. According to another ABS study carried out in 2004-2005, 48% of businesses use electronic lodgements with government organisations via the Internet or web. Electronic payment was the most common activity with 30% of businesses using the Internet to make payments to government agencies (ABS, 2006).

Another technology that has increased usage is the Wireless Local Area Network or WLAN for employees and local residents to access library catalogue, the Internet or council services. Some local councils in Western Australia are providing WLAN 'hotspots' within public locations. For example, City of Melville provides the service in their Community Centre and Council Chambers whilst the Town of Cottesloe, the Town of Mosman Park, and the Shire of Peppermint Grove provide these services at their libraries. The City of Wanneroo is in the process of deploying WLAN in their new community centre. This type of WLAN technology provides flexibility and convenience to both local government staff and residents. These studies indicate that Internet usages are increasing and the demand for government agencies to provide electronic lodgements such as rate and licensing payment are growing as well.

Out of the 142 councils in WA, there are 132 councils that have their own websites (WALGA, 2007). The following figure 1.0 summarises the type of on-line services and Internet related technologies provided by each of the councils listed.

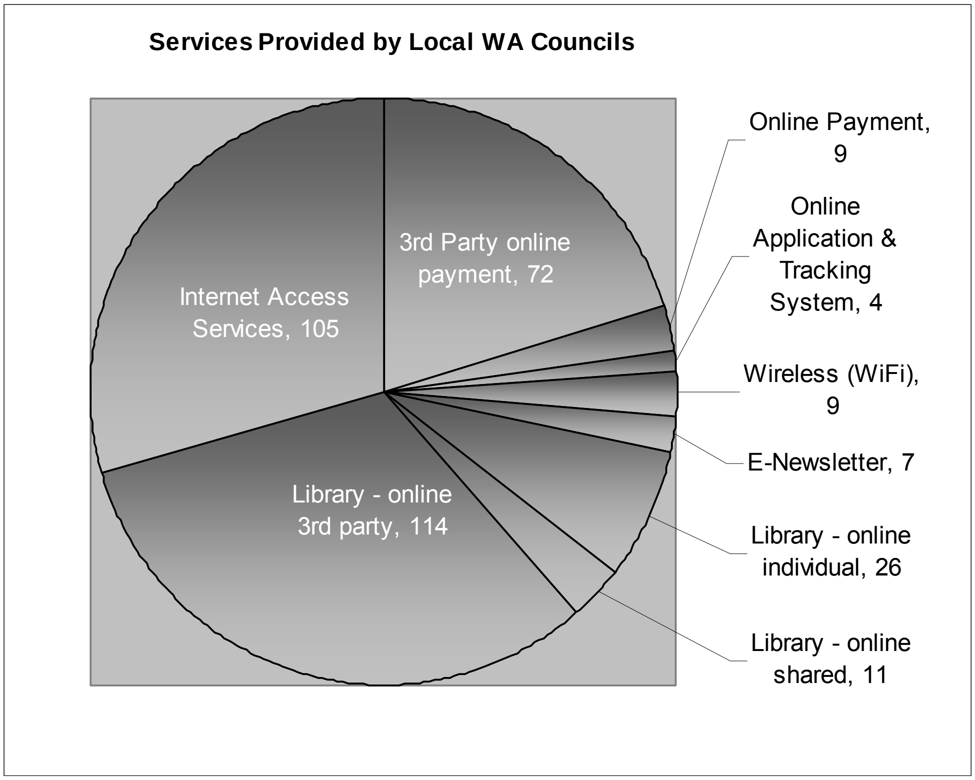

Figure 1 – Services Provided by Local WA Councils

Risks associated with providing online services

Many Western Australia Local Councils provide online payment service using 128 bit Secure Socket Layer (SSL) technology over the Secure HTTP (https). The payment services include rates, licencing, parking fines, dog infringements, and building applications. However, the key component that is missing from the SSL transaction is a method for the resident to be able to identify the council as being legitimate. Moreover, there is no method for the council to make sure that the resident is who they say they are. While SSL provides a secure communication pipe, it does not provide a way of verifying whom each participant is dealing with.

In Western Australia, a number of councils have been using wireless network technology to provide services such as Internet access, surveillance cameras, and mobile computing that allow for real-time online access to the Council's information systems. However, the nature of the wireless technology is less secure when compared with its conventional technology counterpart (wired). Thus wireless technology may introduce a new level of risks when accessing online services.

The table below provides some examples of associated risks specific to Local Councils:

Table 1 – Risks associated to WA Local Councils

Type of Risks	Descriptions
Data integrity	Data lost or damaged due to virus attacks or where an intruder modifies a database.
Denial of Service (DoS) and Distributed Denial of Service (DDoS)	Once a council's system is compromised, (e.g. the council's web site, firewall, database, library, online payment systems), it will cause interruption or delay to the council's services provided to both council staff and residents.
Data Security	Council's content of the database may be stolen, intercepted, or exploited without being detected. This is achieved by intruders using Spyware.
Misuse of resources	Council libraries and community centres which provide Internet online service to public may be at risk of misuse such as browsing pornography, racism, and strong violence, as well as criminal web sites.
Security risks	Files downloaded from the Internet, or run from a medium may contain harmful software which can compromise the Council's information system.

There are some general risks associated with the online services:

Table 2 – General Risks to WA Local Councils

Type of Services	Risks
Emails	email scams, phishing, spam, harassing email, email bombing (massive emails), password attacks and social engineering.
Domain Name System (DNS)	if an attacker manages to get control of the DNS server, the attacker can carry out several attacking techniques such as phishing and farming.
World Wide Web (using Web to provide online services)	there are many risks and threats associated with the World Wide Web such as viruses, hackers, DoS, DDoS, fake web sites, identity theft, and data integrity.

As a result, it is crucial for local government to implement strong ICT security to protect the system. The ICT security should be implemented through well-articulated policies and procedures which are supported by local government staff, and supported by procedural, and technical solutions including controls, training, monitoring, and enforcement (Allen, Westby, & Mellon, 2007).

Research Focus

The first focus considers to what extent the Internet and related technologies are used by councils to provide online services to its employees and residents in selected councils. Secondly, can the types of these technologies be categorised using a framework to produce a level of security strength for Information Communication Technologies in Western Australia councils? Finally, what is the perceived versus measured reality of ICT security techniques used in each council?

RESEARCH METHODS

This research will employ multiple interpretive case studies. This is because multiple experiments strengthen research findings (Williamson, 2002). Furthermore, it allows the researcher to do cross-case analysis and comparison, as well as to investigate a particular phenomenon in diverse settings.

In order to increase the richness and reliability of the case study, both appropriate quantitative and qualitative tools will be used in this research. System testing, surveys, firewall system logfiles analysis (router, Intrusion Detection System, World Wide Web proxy server.), and analysis of email logfiles are examples of these quantitative tools.

The qualitative tools which will be used include open interviews, surveys and texture analysis techniques. "Interpretive researchers start out with the assumption that access to reality is only through social constructions such as language, consciousness and shared meanings" (Myers, 1997). The reason this writer chooses interpretive case studies is because the interpretive research focuses on the full complexity of human sense making as the situation emerges.

The writer anticipates there will be 3 local councils studied in this research. Because of the extensive nature of the data collection and collation, and its subsequent analysis, the writer believes this method can achieve the objectives of the study. For each study object, a basic framework will be implemented for the initial testing. As each study object is an independent case, further testing will be developed according to their organisational constraints.

DATA COLLECTION METHODS

Selection of Local Councils in Western Australia

Study cases will be selected from a number of Western Australia Local Councils. These councils are connected to the Internet and provide services to employees and residents via the Internet and convergence technologies such as the World Wide Web, Email, Online Library, Online payment, GIS and GPS systems. In order to collect meaningful data, this research will only look at cases where the council provide at least three online services mentioned above.

Testing Analysis

There will be several testing processes across different sections of Internet Technology Security such as email systems, Denial of Service, firewall systems, web applications, intrusion detection systems, port scanning, password cracking, internet border router systems, system fingerprinting and vulnerability.

Email System testing

Identifies email system information details and its weaknesses which can cause a council's information to leak. This includes areas such as email system information which comprises email server types, footers, encryption techniques, SMTP server paths, and bounced mails. The tests will examine email headers, bounced mails, and read receipts for the server trails. The process will also test email spoofing for internal connect, egression, and internal and external relaying (Herzog, 2006).

Denial of Service (DoS) Testing

The DoS will also include Distributed Denial of Service (DDoS). Some of the testing tasks and expected results used in the DoS testing process are to "test the exposure restrictions of systems to non-trusted networks, test heavy server and network loads, details of weak points in the Internet presence including single points of failure, details of DoS vulnerable systems" (Herzog, 2006).

Firewall Testing

Firewalls are used to control the network traffic flow between the council network, the DMZ, and the Internet based on the organisation security policies. They typically uses Access Control Lists (ACLs) to allow or deny network packets. The firewall testing aims to assure that only allowed network traffic is permitted into the network, whilst all else should be denied. The testing tasks and expected results used in the firewall testing process includes: "information on the features implemented on the firewall, outline of the network security policy by the ACL, testing the ACL against the written security policy or against the "Deny All" rule, identify that the firewall is egress filtering local network traffic, identify that the firewall is performing address spoof detection, test the ability of the firewall to handle very small fragmented packets, test the firewall's ability to manage an ongoing series of SYN flooding packets coming into the network, test the firewall's response to packets with the RST flag set, test the firewall's management of standard UDP packets, verify TCP and UDP scanning to server logs" (Herzog, 2006).

Internet (Web) Application Testing

Aims to find "security bugs" in server/client applications of the system from the Internet. There are several tasks in the testing phase. For example, "if accessible decompose or deconstruct the binary codes, find possible brute force password guessing access points in the applications, if possible find a valid login credentials with password grinding, bypass authentication system with spoofed tokens, gather excessive information with direct URL, direct instruction, action sequence jumping and/or pages skipping, gather sensitive information with Man-In-the-Middle attacks, inject excess/bogus information with Session-Hijacking techniques" (Herzog, 2006).

Intrusion Detection System (IDS) testing

This test is emphasised on the IDS performance and sensitivity. The testing tasks and expected results used in the IDS testing process include: "IDS sensitivity, reaction time, and performance under heavy load, type of packets and protocols dropped or not scanned by the IDS, list of IDS false positives and missed alarms, IDS architecture and list of unmonitored paths into the network" (Herzog, 2006).

Password Cracking
Is a process to check password validation and its strength using automated password testing tools which includes: "run an automated dictionary attack on the password file, run automated password crackers on encrypted files that are encountered (such as PDFs or Word documents), run a brute force attack on the password file as time and processing cycles allow, obtain the password file from the system that stores usernames and passwords such as smbpasswd (Unix systems), and Sam._ (NT systems), list of systems, documents vulnerable to crack attacks" (Herzog, 2006).

Port Scanning
Invasive probing of system ports on the transport and network level. Several network port scanning tools are used in order to collect and test the network information. The expected results from the port scanning testing are ports details (open and closed), Internet Protocol (IP) addresses and network addressing on both live and internal systems, network map, details of tunnelled and encapsulated protocols, routing protocols, any active services. (Herzog, 2006).

Border Router testing
The border router often acts as a defence on a network that controls and restricts the network traffic which flow between the council network and the Internet based on the organisation's security policy. It uses Access Control Lists (ACLs) to permit or block network traffic packets. Examples of performance testing tasks and expected results are "identify the router type and its features implemented, identify that the router is performing address spoof detection, identify if the router is providing network address translation (NAT), test the ACL against the written security policy or against the "Deny All" rule, test the router outbound capabilities from the inside, measure the ability of the router to handle both very small packet fragments and over-sized packets, measure the ability of the router to handle overlapped fragments such as that used in the Teardrop attack" (Herzog, 2006).

System fingerprinting
Is a testing analysis technique that examines system response in order to determine operating system type, patch level, system type, system enumeration and internal system network addressing (Herzog, 2006).

Vulnerability testing
To determine possible denial of service vulnerabilities, loops, holes of the systems.

DOCUMENT REVIEW

A review of each type of existing information, (whether physical, internet, network, or communication) in terms of security policies and procedures documentation, will be undertaken with the agreement and acceptance by each selected council. Moreover, for the purpose of analysis and comparison, copies of any existing documentation will be compared with particular reference to suitable handling guidelines for each council respectively.

Several interviews will be conducted using one or more guiding questionnaires with two main stakeholders as follows below:

- ICT Management (ICT Manager, Chief Information Officer, Operation Manager)
- ICT Staff (IT Security, System and Network officers)

ICT Management has been chosen because it represents the central point of focus for those staff charged with the responsibility of making the final decisions of the Information System Management team. ICT Management then advise of, and provide directions for, the protection of the organization's ICT system. ICT Management is responsible for the following activities that are associated with security testing:

- "Coordinating the development and maintenance of the organisation's information security policies, standards, and procedures
- Ensuring the establishment of, and compliance with, consistent security evaluation processes for departments throughout the organisation
- Participating in developing processes for decision-making and prioritisation of system for security testing." (Wack, Tracey, & Souppaya, 2003)

ICT Staff have been chosen as the key stakeholders because of their day to day responsibilities in areas such as networks, system and voice communication operations, monitoring and maintenance. They should be responsible for the implementation of their own networks, system and voice communication securities and guidelines. An examination of their security practices will enable better understanding of any security issues faced by the Council. Other related staff such as security officers may also be interviewed in order to gather physical security information as necessary.

Depending on how well the data and voice systems are installed the monitoring, scanning, and vulnerability assessment penetration testing will provide better understanding of the information communication technology security issues faced by the council's management and ICT staff.

Interviews will be carried out at 2 stages at each selected local council with its management and ICT staff.
Stage1: Initial Baseline interview – to establish the level of security policies for information communication technologies and their enforcement by key stakeholders.

Stage2: Testing analysis interviews – these will be conducted with local council management and ICT staff after the analysis of their current ICT security implementation in order to determine reactions to the findings and possibility of any further improvements.

LIMITATIONS OF THE RESEARCH

There are several factors which the research will be limited by. A frequent criticism of case study methodology is that its dependence on a single case renders it incapable of providing a generalizing conclusion (Tellis, 1997). The local councils selected need to have reasonable Internet infrastructure and related technologies been installed. This situation may preclude the use of small regional councils/shires. However, it is expected that a good security framework recommended as a result of this study can be adopted by any other Council for their ICT security implementation.

Another limitation of this research is the time frame. The extensive nature of the data collection and collation, and its subsequent analysis, leads the writer to believe that three case studies can provide a good model of ICT security framework for local councils in Western Australia.

CONCEPTUAL FRAMEWORK

The following is the conceptual framework for each descriptive case study within the selected local councils:

- Document Review of Selected Local Council in Western Australia
- Interviews of Selected Local Council in Western Australia
- Analysis of Testing Results
- Reporting Details of Testing Analysis Back to Council
- Post Analysis Interviews

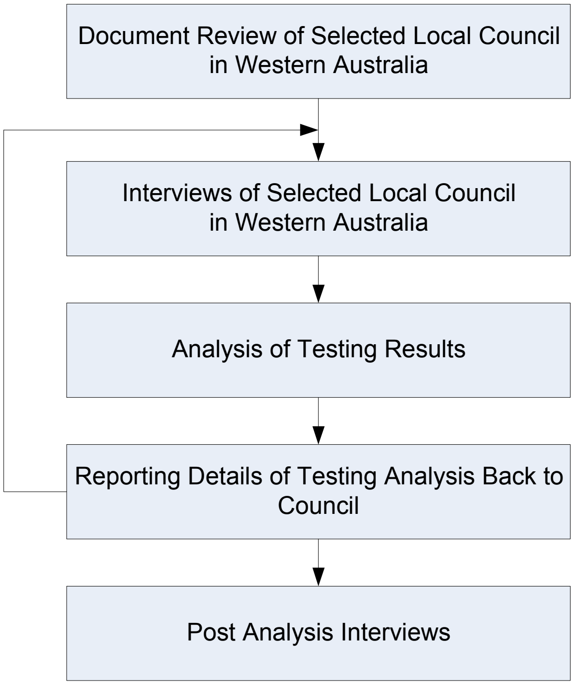
Document Review of Selected Local Council in Western Australia
Interviews of Selected Local Council in Western Australia
Analysis of Testing Results
Reporting Details of Testing Analysis Back to Council
Post Analysis Interviews

Figure 2 – Conceptual Framework

CONCLUSION

Using the section C – Internet Technology Security of OSSTM V.2.2 methodology as a main testing model to test the security of online services of the selected councils may cause some issues such as interruption of their online services. The model may need to be modified into smaller sub models to suits each council's online system environment. By end of this study it is expected that the author will develop a framework which can be easily deployed by any council in order to assist securing their online community services system.

REFERENCES

ABS. (2006). 8146.0 household use of information technology, Australia 2005-06. Retrieved January, 2008, from http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/B1A7C67456AE9A09CA25724400780071/$File/81460_2005-06.pdf

Allen, J., Westby, J., & Mellon, C. (2007). Governing for enterprise security (GES) implementation guide. Retrieved January, 2008, from http://www.cert.org/governance/ges.html

Herzog, P. (2006). OSSTMM 2.2 open-source security testing methodology manual Retrieved January, 2008, from http://isecom.securenetltd.com/osstmm.en.2.2.pdf

Intel. (2005a). Core technologies for developing a digital community framework: Solutions for transforming government Retrieved January, 2008, from http://download.intel.com/pressroom/kits/digitalcommunities/DCFramework_Whitepaper_5_081405.pdf

Intel. (2005b). Digital community best practices: Solutions for transforming government Retrieved January, 2008, from http://www.intel.com/business/bss/industry/government/digital-community-best-practices.pdf

Myers, M. D. (1997). Qualitative research in information systems. Retrieved January, 2008, from http://www.qual.auckland.ac.nz/

Stanton, D. (2004). Local e-government in Western Australia: How prepared are councils to deliver services and interact with communities in an electronic environment? . Retrieved January, 2008, from http://www.finance.gov.au/publications/future-challenges-for-egovernment/docs/AGIMO-FC-no1.pdf

Tellis, W. (1997). The case study as a research method uses and users of information -- LIS 391D.1. *The Qualitative Report, 3*(2).

Wack, J., Tracey, T., & Souppaya, M. (2003). Guideline on network security testing. Retrieved January, 2008, from http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf

WALGA. (2007). Local government: Council websites. Retrieved January, 2008, from http://www.walga.asn.au/careers/council_websites

Williamson, K. (2002). *Research methods for students, academics and professionals: Information management and systems* (2nd ed.). NSW, Australia: Quick print Wagga Wagga, Inc

COPYRIGHT