

Security Management in Intranet Systems

Kuo Lane Chen

School of Accountancy and Information Systems, University of Southern Mississippi, Hattiesburg, MS 39402
Phone: (601)266-5954, Kuo.Chen@usm.edu

Vance Etnyre

University of Houston – Clear Lake, 2700 Bay Area Boulevard, Houston, TX 77058
Phone: (281) 283-3168, etnyre@cl.uh.edu

Huei Lee

Department of Computer Information Systems, College of Business, Eastern Michigan University, Ypsilanti, Michigan 48197
Phone: (734) 487-4044, Fax: (734)487-1941, huei.lee@emich.edu

ABSTRACT

The introduction of the .NET platform by Microsoft and the growing popularity of Internet-based systems have caused major security concerns for system developers. Appropriate information security techniques must be used by system administrators to reduce the risk of information disasters. The purpose of this research paper is to examine possible information security problems and recommend possible ways to evaluate and reduce information system risks.

INTRODUCTION

The Internet and new information technologies have significantly changed the way business is conducted. Companies like E-Bay and Expedia.com have demonstrated that 'virtually' the entire operations of a business can be delivered at electronic speeds. All large businesses have developed websites to explain the basic products they deliver. Customer services such as product tracking and account balance verification are routinely offered on company websites. Many companies use the Internet as an inexpensive and uniform communication interface for every employee. This kind of computer system is referred to as the Intranet. The Intranet uses existing network infrastructure, Internet connectivity standards, and WWW software for internal communications (Laudon & Laudon, 2003). Many popular Enterprise Resource Planning (ERP) systems have moved to Intranet-based platforms.

The development of Intranet systems based on local area networks, isolated from the outside world by dedicated routers and firewalls, is being replaced by Virtual Private Networks (VPNs). A VPN uses HTTP and TCP/IP, the common communication technologies of the Internet, but it adds other features to provide necessary security.

Despite the growing popularity of VPN-based Intranet systems, security remains one of the major concerns regarding the use of the Internet. Organizations now have to contend with Internet “worms”, network intrusions, and compromised computers. For example, the publicized "Code Red" worm alone costs a university in the Midwest thousands of dollars in staff time and lost productivity. Thus, appropriate security control techniques must be used by the system administrators to prevent such information disasters.

LITERATURE REVIEW

Numerous studies have been written about Intranet and Internet security (Raisinghani & Savoie, 1999; Courigton, 2000; Panko, 2003). Because of the importance of and Intranet/Internet security, many colleges and universities offer information security curricula. These courses are supported by several textbooks on information security (Whitman & Mattord, 2003; Panko, 2002; Stallings, 2003). In 2002, Microsoft provided a system of advanced Internet development tools - the .Net Framework and XML Web services. The .NET platform is similar to Sun Microsystems's Java 2 Platform Enterprise Edition (J2EE). These systems aid application developers by providing useful tools to create web-based applications. They also provide security control structures for Intranet applications development (Stiefel & Oberg, 2002).

According to the 2003 annual Computer Crime and Security Survey conducted by Computer Security Institute in the U.S., 251 organizations report almost \$202 million in financial losses (Computer Security Institute, 2003). There are two security weaknesses inherent in the current infrastructure of Intranet-based systems. First, high-speed telecommunication lines (Internet backbone) are subject to line breakage, causing disruption of service. Second, messages and other information are susceptible to being intercepted, recorded or modified as they pass from the host to the recipient. There is virtually no law that prevents any Internet Service Provider (ISP) from observing, recording, selling, or giving away any information that passes through host computers. Major problems in Internet and Intranet security include virus attacks, denial-of-service, industrial espionage, and spam mail. There are many security management techniques discussed in the literature. Several of these security management techniques are discussed in the following sections.

SECURITY MANAGEMENT TECHNIQUES

Security control techniques exist to help organizations protect their information systems (Everett, 1998). These techniques can be divided into three major approaches: 1) general technological approaches, 2) behavioral approaches, and 3) systems programming approach.

General Technological Approaches

General technological approaches for security management methods include: 1) authentication, 2) authorization, 3) encryption, 4) digital certification, and 5) firewall systems. These approaches are described as follows:

1. Authentication

Authentication means that a person using the system is required to prove his or her identity (Panko, 2003). The forms of authentication include passwords, personal identification number, membership ID, or cryptographic key (Raisinghani & Savoie, 1999).

2. Authorization

Authorization means that only certain individuals or groups or users filling certain roles may have access to specific resources.

3. Encryption

Encryption converts the sender's message into ciphertext, which an interceptor will not be able to read. At the receiving end, the receiver decrypts the ciphertext back to the sender's original message. There are different encryption/decryption methods. For example, a simple N position shift encryption method subtracts an integer (certain number of positions in the alphabet) from each character in the message. This "N position" integer is also referred to as a "key". If the key is "1", the sender's original message "MONEY" will be encrypted into "LNMDX" in the transmission and converted back to "MONEY" when the receiver decrypts it (Panko, 2003). Despite the simplicity of this security method, half of all e-commerce sites do not use encryption to protect customers (Furger, 1998).

Various encryption protocols have been created to ensure Internet security. Secure Socket Layer (SSL), developed by Netscape Communications, is a popular encryption protocol that makes language passing through the Internet indecipherable. It has become a de facto standard for Internet e-commerce security (Panko, 2003).

4. Digital Certification

Digital certification is another way to assure security. Using digital certification, a sender adds to each message a digital certificate, which is created by a certificate authority (Panko, 2003). There are three levels of digital certificates: Class 1, 2 and 3. To obtain a Class 1 certificate, a person needs to provide his name, address, and an e-mail address to a certificate authority. Once the e-mail address is verified, the person will receive a Class 1 certificate. MasterCard, VISA, Microsoft, Netscape, and most other companies have agreed to the use of Secure Electronic Transaction (SET). When using the SET, a digital envelope of certificates specifies the payment details for each transaction, which is then encrypted for transmission.

5. Firewall Systems

Webopedia.com defines a firewall as "A system designed to (selectively) prevent unauthorized access to or from a private network." There are two kinds of firewall systems: Packet Filter Firewalls and Applications Firewalls. In Packet Filter Firewalls, the packet IP and TCP headers are examined any packet IP or TCP header containing a local resource address is terminated. A technique known as network address translation is also used in firewall systems. Applications firewalls, also known as proxy firewalls, examine the application layer messages to check for possible problems (Panko, 2003).

Behavioral Approaches

Behavioral approaches means that careful internal management can prevent security problems. Today there are various password-cracking programs available in the market (e.g. Jack the Ripper). Most password-cracking programs use a procedure similar to an automated dictionary trying word after word at a high rate of speed. If a person chooses a password that is easily remembered (i.e., first name or middle name), that password can be easily decoded by these software-cracking tools. These software programs present a threat to Internet security (Courington, 2000). This problem can be prevented by making the password more complex.

Research reveals that most serious financial losses occurred through unauthorized access by insiders (Rapalus, 1998). This means that control by limited access and personnel management is important duties for businesses conducting e-commerce. An experiment to evaluate different system access configurations is included later in this paper.

Systems Software Approaches

Since most PC-based systems in small and medium companies are Microsoft systems, it is important to discuss special approaches in Microsoft's new .NET platform. It has been widely reported that Microsoft's top executives believe so strongly in the importance of Web Services, that they have "bet the company" on the future success of this methodology. It creates a new programming paradigm for creating Intranet applications for small and medium companies.

The .Net environment gives programmers and service providers a single platform that can be used to compile programs written in several different programming languages. The Common Language Runtime feature of .NET allows providers with a mechanism that can combine components written in different languages into a coherent integrated package.

One of the most important features of the .NET platform is the ability to create Web Service applications. However, without Microsoft's Internet Information Service (IIS) package installed and activated, the user loses the ability to create Web Service applications. Also, in order to use the IIS package, the user must be granted administrative security clearance. As one can see, this creates major problems for the network security. Once the user is granted the permission to use the IIS package, this access to the critical network components with IIS makes the entire network vulnerable to severe accidents and malicious attacks because it allows users unnecessary access to other various resources of the server. In general, IIS provides only three types of security control techniques: authentication, authorization, and impersonation. Authentication includes forms, Passport authentication, and Windows authentication. In Passport authentication, the user is redirected to a login page on Microsoft's site. These security control techniques are sufficient for e-commerce, but more rigorous security control methods should be available to protect other more restricted configurations such as company Intranet systems. (Augustyniak, 2002).

One of the issues discussed in .Net Framework is the role-based security. Instead of examining each individual user name, an administrator can assign a user a specific role-

based security clearance. For instance, a general employee has the right to login into the systems, but he does not have right to revise the payroll file. Role-based security methods can be coded in various programming languages for .NET applications (Stiefel & Oberg, 2002).

The NET platform allows students to learn how to create and use Web Service applications - the hottest new topic in computing. This, however, opens a new security problem. Unlike most business settings, where each person has responsibility (and accountability) for a single computer, many universities use a "semi-open lab" environment. Although there are limitations to general use of all university computers, in a semi-open lab, any student can log in to any available computer. Although there is some temporary accountability in this scheme, additional security problems are inherent in this environment.

In any computing environment, a primary goal of system administrators is to allow convenient access to authorized users while denying access to unauthorized users and unauthorized uses of system resources. This requires a balance between the security concerns of system administrators and the access needs of system users.

RESEARCH METHOD

An experiment has been conducted to establish a method for balancing the needs of system administrators and system users. Graduate students within an MIS program at University of Houston – Clear Lake were divided into two groups. The participants were asked to identify themselves as primarily 'programmers' or primarily 'administrators'. Each group was asked to evaluate alternative modes of configuration in a university semi-open lab environment. The three alternatives for computer lab configuration are:

1. Alternative 1 – (Full Access to All)

One way to configure software in open labs is to have all authorized software available to all workstations. This would provide maximum access to software resources. The cost of doing this can be huge, however, and the exposure to risk of unauthorized uses and unauthorized users could be unacceptably large.

2. Alternative 2 (Segregating) – Restricting Access to a limited set of public resources

In this alternative, a small number of computers in the 'open lab' environment are configured to contain a full implementation of the .NET platform (including IIS), while the rest of the computers are configured with a limited configuration (excluding IIS). Only students from a special list are allowed access to the restricted computers.

3. Alternative 3 (Isolating) – Removing a limited set of resources from general availability.

Removing a limited set of resources from general availability and using them to create a local private network change the strategy in a significant way. Computers on the private network are subjected to risk as the server software executes, but that risk is isolated to

the private network. Computers in the “open labs” can be easily protected from these higher-risk machines.

In the experiment, seven students identified themselves as “primarily programmers”. Five students called themselves “primarily administrators”. Student participants were asked to evaluate each of the three configurations using four evaluation categories in a “10*10” weighted scoring scheme. The evaluation categories were: Accessibility, Cost Control, Performance Efficiency, and Risk Control. Each category was evaluated with a score from 0 (totally unacceptable) to 10 (ideal). Weights were assigned to each category with the total of all weights equal to 10.0. In such an evaluation system, the range of weighted scores is from 0.0 to 100.0.

The evaluation data is summarized in Tables 1 and 2.

Member	All Full Access					Segregated Subset					Isolated Subset				
	acc	cc	Eff	Rc	wt. score	acc	cc	eff	rc	wt. score	acc	cc	eff	rc	wt. score
1	10	2	4	3	45	5	6	4	7	55	5	6	7	9	70
2	10	3	5	2	47	4	5	6	7	57	4	5	5	8	57
3	9	3	4	2	42	4	7	5	7	58	4	4	5	9	58
4	10	2	4	1	39	5	6	6	6	58	5	4	4	10	60
5	10	3	3	2	41	5	7	6	6	60	4	5	5	9	60
Average	9.8	2.6	4.0	2.0	42.8	4.6	6.2	5.4	6.6	57.6	4.4	4.8	5.2	9.0	61.0

(acc: access; cc: cost control; eff: efficiency; rc: risk control)

Table 1: “Administrator” Evaluations (using weights of 2, 2, 3, 3)

Member	All Full Access					Segregated Subset					Isolated Subset				
	acc	Cc	Eff	Rc	wt. score	acc	cc	eff	rc	wt. score	acc	cc	eff	rc	wt. score
1	9	5	6	3	64	5	6	4	8	56	6	4	5	9	60
2	10	4	5	2	62	4	5	5	7	50	5	4	5	10	58
3	10	4	4	3	62	4	7	4	6	50	7	5	6	9	68
4	9	3	4	1	52	5	6	6	6	56	4	3	4	9	48

5	9	4	5	2	58	6	5	6	7	60	5	5	5	10	60
6	10	4	5	2	62	6	5	5	6	56	5	4	5	9	56
7	9	5	5	2	60	5	6	5	7	56	6	5	5	9	62
Average	9.4	4.1	4.9	2.1	60.0	5.0	5.7	5.0	6.7	54.9	5.4	4.3	5.0	9.3	58.8

(acc: access; cc: cost control; eff: efficiency; rc: risk control)

Table 2: “Programmer” Evaluations (using weights of 2, 2, 3, 3)

It can be seen from Tables 1 and 2, that the highest average evaluation score by “Administrator Evaluators” was 61.0, given to alternative 3 (“Isolated Subset”) and the highest average evaluation score by “Programmer Evaluators” was 60.0, given to alternative 1 (“Full Access”). In the Table 3, it can be seen that alternative 3 is favored by administrators because the category with the highest score (risk control at 9.0) has a relatively high weighting factor (3.0).

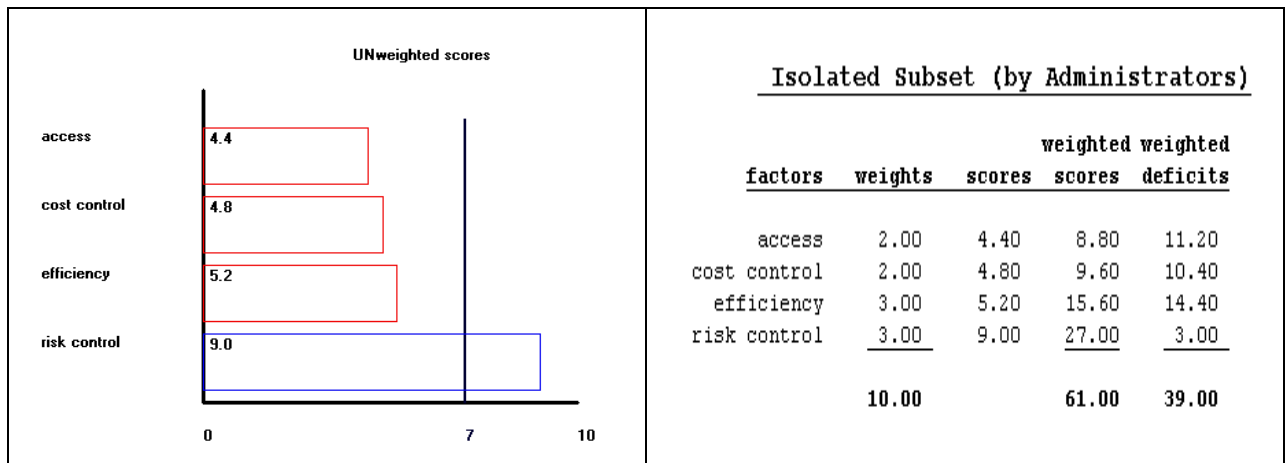


Table 3: “Administrator” Evaluations (Un-weighted scores)

For the same reason, alternative 1 (see Table 4) is favored by programmers because the category with the highest score (access at 9.4) has the highest weighting factor (4.0).

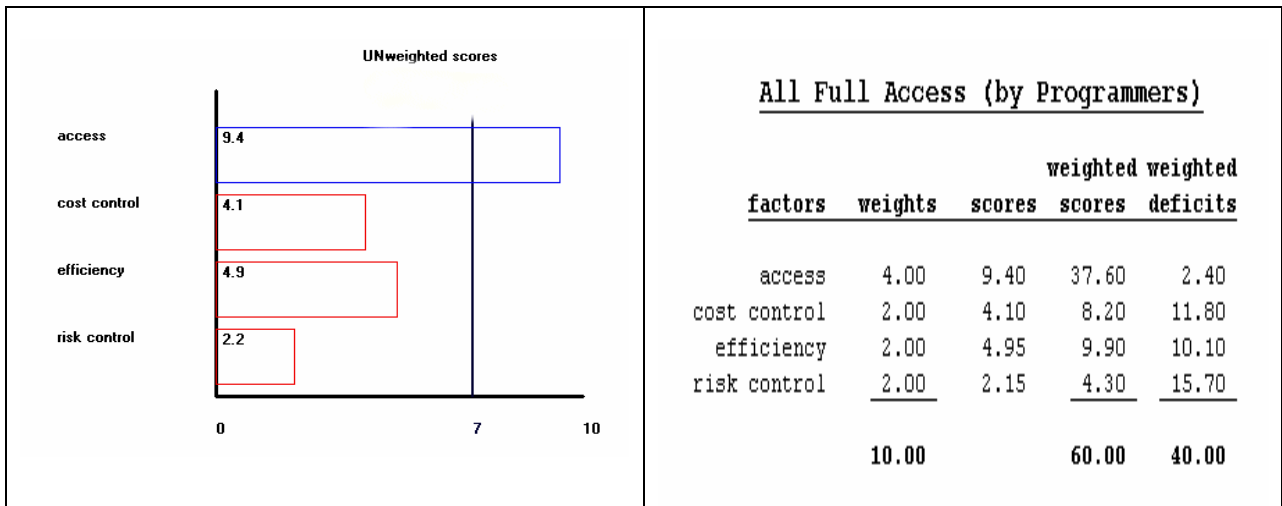


Table 4: “Programmer” Evaluations (Un-weighted scores)

ANALYSIS

The problem of resolving preferences is relatively easy in this situation. A balance should be found between the preferences of the programmers, who gave the highest rating to alternative 1 (“Full Access”), and the preferences of the administrators, who gave the highest rating to alternative 3 (“Isolated Subset”). Again, a weighted scoring scheme can be used to resolve this difference. The only difficulty would be assigning weights fairly to the preferences of programmers and administrators. If programmer preferences and administrator preferences are weighted equally, alternative 1 would have a combined weighted score of 51.4 (the average of 60.0 and 42.8) and alternative 3 would have a combined weighted score of 60 (the average of 59 and 61). This would indicate that alternative 3 (“Isolated Subset”) would be selected as the preferred configuration.

The difference in evaluations of alternative 1 by the two groups is very large, while difference in evaluations of alternative 3 by the two groups is very small. This means that almost any set of weights applied to each set of evaluations would give alternative 1 a combined score lower than the combined score for alternative 3.

CONCLUSIONS AND FUTURE RESEARCH ISSUES

In any computing environment, the primary goal of system administrators is to allow convenient access to authorized users while denying access to unauthorized users and unauthorized uses of system resources. This requires a balance between the security concerns of system administrators and the access needs of system users. One purpose of this paper is to review security management techniques for an intranet system. Another purpose is to propose a method for evaluating system configurations. The method proposed allowed for a balancing of concerns of system administrators and system users. The Research Methods section of this paper discussed a method and an experiment for evaluating various system configurations. The results of the experiment, which showed a preference for an “Isolated Subset” of system resources to implement high-risk applications, were limited to the type of configuration found at many universities.

Further studies can and should be conducted to see if the same evaluation method can be used in other computing environments.

REFERENCES

- Augustyniak, M. (2002). *.Net XML Web Services in 24 Hours*, Indianapolis, Indiana: SAMS.
- Computer Security Institute (May 29, 2003), Cyber attacks continue, but financial losses are down, <http://www.gocsi.com/press>.
- Courington, W. D. (2000). Internet Security: the Threat, *Proceedings of the Academy of Information and Management Sciences*, 4(1), Myrtle Beach, SC, 52-57.
- Furger, R. (1998). Buyer Beware: Is It Safe to Shop in Cyberspace? *PC World*, September 1998.
- Gupta, U. G. (2000), *Information Systems*, Prentice Hall, Inc, Upper Saddle River, New Jersey.
- Laudon, K.C. & Jane P. Laudon. (2003). *Essentials of Management Information Systems*, (5th ed.), Prentice-Hall, Inc., New York.
- Panko, R (2003). *Business Data Communications and Networking*. (4th ed.). Upper Saddle River, New Jersey: Prentice Hall, Inc.
- Panko, R (2002). *Corporate Computer and Network Security*, Upper Saddle River, New Jersey: Prentice Hall, Inc.
- Raisinghani, M. & Savoie, M. (1999). Designing Secure Systems for Electronic Commerce. *Proceedings of Decision Sciences Institute*, New Orleans, LA, 722-724.
- Stiefel, M. & Oberg, R. J. (2002). *Application Development Using C# and .Net*, Upper Saddle River, New Jersey: Prentice Hall.
- Stillings, W. (2003). *Network Security Essentials*. (2nd ed.) Upper Saddle River, New Jersey: Prentice Hall.
- Srinivasan, S, Evolving Security Standards and Loopholes, *Proceedings of the Academy of Information and Management Sciences*, 4(1), Myrtle Beach, SC, 2000, 52-57.
- Whitman, M., & Mattord, H. J., (2003). *Principles of Information Security*, College Technology, Thomson Learning Inc.