Security in a Web-Based Environment

William S. Hopwood, Professor of Accountancy, Florida Atlantic University, Boca Raton, FL 32307; *David Sinason*, Assistant Professor of Accounting, Northern Illinois University, 240 Wirtz Hall, DeKalb, IL 60115-2854; and *Robert Tucker,* Visiting Associate Professor of Accountancy, University of Illinois at Urbana-Champaign, Department of Accountancy, 1206 S. Sixth Street, Champaign, IL 61820

Introduction

In the last few years web-based electronic commerce has continued to grow at an exponential rate. Visa, for example, estimates that its internet-related revenues will grow at an annual rate of 81% over the next couple of years (Zbar, 1999). Overall, current statistics indicate that over 50% of all companies in the United States sell products over the internet (Salkin, 1999). The trend is expected to continue, and by 2001 internet sales are estimated to exceed $200 billion, up nearly ten-fold from 1997.

As is often the case, rapid growth brings with it a host of problems. According to one recent survey (Larson, 1998) 70% of corporate purchasing decision-makers indicated that because of security concerns they are not currently buying over the internet. This is no surprise given that 59% of companies with web sales report at least one security breach each year. Further, estimates show that about 30% of all credit card transactions over the internet involve fraud (Lucas, 1998). Other estimates show staggering losses totaling $250 billion dollars per year to electronic espionage (Radcliff, 1998).

Security has become the issue for web commerce. Despite annual expenditures for electronic security that exceed $6 billion, hacker attacks on web sites have continued seemingly unabated. Even the largest and most sophisticated organizations have not gone unscathed, and almost daily the financial press continues to report cases of hackers completely taking over corporate websites. For example, one cyber gang recently hijacked the New York Times website for three hours. Other hackers have co-opted the web sites for federal agencies such as the CIA, the FBI, NASA, and the White House. (See http://www.actionline.com/archives/news/ for some individual case reports).

Accountants, systems persons, and managers continue to struggle to maintain a grip on electronic security. And no company seems secure, despite enormous expenditures on security, and many are confused as how to approach the problem. The result is that those involved often find themselves putting out fires and playing catch up in a sea of raging technology.

This paper presents a systematic approach to developing and continuously improving a web security system within the context of the overall systems development effort and within the context of traditional accounting internal control processes and structures. Such a model allows for the enterprise-wide control of security risks over a prolonged period of time.

Although a website offers amazing new capabilities for communicating with a broader range of customers, it is still essentially an information system. Consequently, the well-established methods of information system analysis are applicable in assessing the system's risks and vulnerabilities regardless of the unique, new risks involved. We illustrate

tion, and group decision making process and has made scholarly presentations at the annual American Accounting Association Meeting among others.

Riahi-Belkaoui, Ahmed, College of Business, University of Illinois at Chicago, 601 S. Morgan, Chicago, Il, 60607. He is the CBA distinguished Professor of Accounting at the University of Illinois at Chicago. He obtained his Ph.D. degree from Syracuse University in 1973 and taught at the University of Ottawa and the University of Chicago before joining the University of Illinois at Chicago in 1981. He has published 64 books and in many journals including *The Accounting Review, Journal of Accounting Research, Contemporary Accounting Research, Journal of Accounting and Public Policy, Issues in Accounting Education, Accounting and Business Research, Accounting Organizations and Society, Journal of Business Finance andAccounting, Advances in Intern ationalAccounting, Advances in Public Interest Accounting, Research in Accounting Regulation, Journal of Business, Journal of Finance, Journal of International Financial Management* andAccounting, *and Financial* Management among others.

Picur, Ronald D., College of Business Administration, University of Illinois at Chicago, 601 5. Morgan St, Chicago, Il, 60607. He is a Professor of Accounting at the University of Illinois at Chicago. He obtained his Ph.D from Northwestern University in Accounting and Information Systems in 1973. Professor Picur served as the Comptroller and Chief Financial Officer of Chicago from 1985 to 1989. He previously taught at the Urbana-Champaign campus of the University of Illinois. Picur's primary research interest is in comparative analysis of governmental entities. His publications appeared in such journals as *Managerial Finance, Research in Governmental and Nonprofit Accounting, The Journal of Business Finance and Accounting, Research in Urban Policy, the Quarterly Review of Economics and Business* and *The Accounting Review.*

Hopwood, William S., School of Accounting, College of Business, Florida Atlantic University, 777 Glades Road, Boca Raton, Florida, 32307. Professor Hopwood is a professor of Accounting. He received his Ph.D. from the University of Florida in 1978. He served as professor at the University of Illinois at Champaign-Urbana, Florida State University, and the University of Houston before joining the Florida Atlantic University. He has published numerous articles in *The Accounting Review, Journal of Accounting Research, Contemporary Accounting Research, Auditing,* and other journals. He is also the author of a textbook on Accounting Information Systems.

Sinason, David H., College of Business, Northern Illinois University DeKalb, Il, 60115-2854. Professor Sinason is an assistant professor of accounting at Northern Illinois University. He received his Ph.D. in Accounting from Florida State University in 1996. Dr Sinason is a CPA and Certified Fraud Examiner. His research interests include auditing, fraud, auditor liability, and electronic commerce. He has published in *The Journal of Accountancy, Research in Accounting Regulation, Advances in International Accounting, Managerial Auditing, Bank Accounting and Finance,* and *American Business Law Journal*

Tucker, Robert R., College of Business, University of Illinois at Champaign, 1206 sincerely. Sixth Champaign, Il, 61820. He received his Ph.D. in Accounting from the Florida State University in 1987. His research interests include auditing, agent based modeling, experimental economics, game theory, and internet security. He has published in such journals as *The Accounting Review, The Journal of Accounting, Auditing and Finance,*

the approach to analyzing security by structuring the paper around each of the following phases of development: systems analysis, systems design, and systems implementation.

The Information Systems Development Literature

There are several different normative approaches to systems development besides the one we outline (see Weber 1999). For instance, the Sociotechnical Design Approach (Bostrom and Heinen, 1977) balances the objectives of maximizing task accomplishment with maximizing the quality of work life for systems users. The political approach (Markus, 1981) recognizes that changing systems can also change power structures, thus involving users may or may not be a good idea. The advantage of the soft systems approach (Checkland, 1981) is that it does not assume that decision makers have specific goals and a substantial understanding of the problem at the outset. The prototyping approach (Naumann and Jenkins, 1982) became popular with the advent of microcomputing. Users could prototype a system on their PC before going to full scale production. The Contingency approach (Gremillion and Pyburn, 1983), on the other hand, emphasizes the necessity of being flexible in the approach to development. The approach should vary depending on the social system, system size, and any uncertainty regarding requirements or technology.

Of course the worst alternative to the life-cycle approach is the piecemeal approach. Unfortunately, the piecemeal approach is too often taken when emerging technology, such as web commerce, is involved. The danger is that the technical people will be in charge, and the web site implementation will not be fully integrated into the larger systems development effort.

The move to Enterprise Resource Planning packages (ERP) systems such as SAP has been very much a move to avoid the piecemeal approach. Balanced against the potential advantages of a fully automated and integrated system, however, is the awareness that several recent conversions to SAP have resulted in paralyzing implementation failures. It appears a better considered approach to systems development could have averted disaster.

Security System Analysis

The purpose of the first phase, Systems Analysis, is to identify system threats, vulnerabilities and the associated losses. The basic formula is THREAT + VULNERABILITY = LOSS EXPOSURE. The ultimate goal of the security system is to control loss exposures.

Threats represent various sources of attack on the website. One threat, for example, might come from a malicious hacker who might attempt a denial-of-service attack by barraging the webserver with an unusually large volume of requests for information.

Vulnerabilities, on the other hand, represent security weaknesses in the website's security system. For example, a vulnerability would exist if password controls were lax for sensitive data on the web server.

Assessing Loss Exposures

Loss exposures are typically identified using either a quantitative or qualitative approach. In the quantitative assessment of risk, one computes each loss exposure as the product of the amount of the loss times the probability such a loss will occur. One immediate benefit of this approach is that it requires management not only to identify risks but also to develop ex-

act probability estimates for each potential loss. As beneficial as this exercise is, significant measurement error can occur. Consider the difficulty measuring the reputation damage from a system shut down or the cost of replacing computer software or hardware at some future date. In addition, system weaknesses present a problem only if a strategic opponent can exploit these weaknesses. Assessing a strategic opponent's knowledge and technical strengths, motives, risk preferences, and frequency of attack also makes estimation a formidable task.

Recognizing the difficulty inherent in measuring loss exposures for which the company has little experience, many companies opt for a qualitative approach. This entails a subjective ranking of risks in order of the significance of exposure they represent. Each exposure is assigned a score where exposures include loss of software, data, hardware, or facilities, as well as business interruption. Still other companies use a hybrid approach combining the best of the quantitative and qualitative assessment; that is, developing hard numbers of losses and probabilities where reasonably estimable.

Complementing and augmenting the life cycle approach are such quantitative risk assessment methods as network analysis (PERT), decision analysis, method of moments, stochastic dominance, and risk engineering.

Originally developed as part of the Polaris submarine project, the network method or Program Evaluation and Review Technique (PERT) (Hillier and Lieberman, 1974) models the process of development with nodes connected by lines. The nodes represent decision points and the lines represent activities to be performed. The graphical representation allows easy identification of the critical path which is the sequence of events having the longest duration or the highest cost.

A weakness of PERT in its early forms, since remedied by computer simulation, was that it lacked probability information on costs and schedule. In this respect, the decision analysis technique was an improvement (Raiffa, 1968). In this technique, a tree is constructed in which decision choices form branches. Different outcomes may stem from each of these branches and each of these outcomes has an associated probability and expected payoff. The decision is chosen which maximize the decision maker's utility.

Retaining the scheduling aspect of PERT, the Method of Moments (McNichols, 1976) weighs each cost by a probability density function (PDF) rather than a simple probability. Because disasters are often infrequent events, the distributions tend to be skewed and simple expected value analysis is inadequate. The key objective is to obtain an estimate a distribution of the total cost of the project. The stochastic dominance approach of Post and Diltz (1986) has a similar objective but recognizes the difficulty in exactly specifying the distribution function and proposes an alternative criterion of stochastic dominance.

In the risk engineering approach (Charette, 1990), one develops a damage index from the triplet $<s_i, l_i x_i>$ where s_i is the scenario risk and reflects what could go wrong; l_i is the likelihood risk, and x_i reflects the consequences of the ith scenario. Risk engineering is a practical approach designed specifically for software development.

To serve their consulting clients, many public accounting firms have also developed risk models such as business process measurement (BPM) (Bell, et al., 1997). However, most of these are proprietary and unpublished. To comply with professional standards in conducting certified audits, all public accounting firms must follow Statement on Auditing

Standards (SAS) No. 78, AU 319 and SAS No. 82, AU 316 (AICPA, 1996 and 1997) which detail how to assess internal control risk and fraud risk, respectively.

Again, these various risk models complement the systems development approach and can be used in conjunction with it.

Threats

In analyzing potential threats, it is useful to consider not only the sources (i.e. nature, and people) but also the means by which these threats are realized. The following two subsections study the problem from these two perspectives.

Sources of Threats to Security

Clearly, nature poses a serious threat to the system's operation and preventative steps should be taken to prepare for the possibility of calamities such as fire, power outages, earthquakes, and storms. Furthermore, procedures and plans for backup and recovery should be established to minimize the damage after a natural disaster has occurred. As serious as these threats are, they have been discussed elsewhere in the literature; consequently, we will focus on threats from strategic opponents.

Fraud is frequently analyzed as a pyramid with three components: fraudster's pressures, rationalizations, and opportunities (Albrecht, Wernz, and Williams, 1995). Though fraud represents only part of the security problem, the framework is apt in dealing with any strategic opponent in a variety of situations. Opportunities are akin to vulnerabilities which will be discussed in the Vulnerability section of the paper. The following subsection identifies potential strategic opponents and discusses their traits and motives.

Strategic Opponents and Their Motives.

The thought of a computer hacker, sitting alone in his room, spending hours attempting to identify passwords, breach firewalls, and decipher sophisticated encryptions consumes many managers responsible for electronic commerce. While this is a real threat, and stories of hackers breaching sophisticated systems make sensational headlines, many threats are from other sources. Potential intruders may be competitors, trading partners, employees, hackers, or customers.

Richard Powers of the Computer Security Institute singles out competitors as the single greatest threat in computer crime (Young, 1996). Competitors are a real hazard to companies engaging in electronic commerce, since the objective of electronic commerce is to allow customers and suppliers access to the company's computer and the information it contains (Wirszcyz, 1997). What makes competitors especially dangerous are their targets. Competitors and other outsiders are generally interested in obtaining cash, inventory, or customers' information. These thefts often leave evidence such as discrepancies in the cash or inventory balance or customers complaints about unauthorized use of personal information. Competitors may copy the customer list, look at the sales forecast, or view a competitive bid on a major project. Thefts of this nature may go completely undetected since nothing was removed or altered, but may result in a competitive disadvantage costing millions of dollars.

In addition to its competitors, companies must be cognizant of the risks associated with its trading partners. Companies are entering an era where electronic data interchange (EDI) allows trading partners, both customers and suppliers, access to the company's computer system. It is estimated that business-to-business commerce will be the largest segment of electronic commerce in the future. Hackers, competitors, customer's employees, and supplier's employees may use web sites linked through EDI to gain access to the company's system. Therefore, it is imperative that a business thoroughly investigates its EDI partners, including the security of that partner's computer system, before allowing that partner access to the company's computer system.

In addition to competitors, employee theft through e-commerce is an important issue. Disgruntled employees may wish to steal assets or sabotage the company as a means of revenge. Other employees may steal to satisfy a perceived need for cash. Regardless of their motives, employees are a real threat to electronic commerce systems. Many employees have access to information (passwords, codes, ID numbers, etc.) that allows them to circumvent existing internal controls. For these reasons, segregation of key computer duties must be maintained, passwords and IDs that allow access to the computer system beyond the firewalls must be kept to a minimum, and managers must be trained in identifying employee situations that might indicate that a fraud has been committed.

While it is important that managers broaden their perspective of potential electronic commerce criminals, the hacker is still a threat they must evaluate. Michael Vatis, Deputy Assistant Director and Chief of the National Infrastructure Protection Center for the Federal Bureau of Investigation indicates that a sophisticated understanding of computers and the internet is no longer required to successfully crack a company's computer (Lucas, 1998). ID numbers, passwords, credit card numbers, and fraud instruction guides are available in internet chat rooms. At the same time, hackers are getting more sophisticated and are finding better and faster hardware and software resources at their disposal. Ramiz Saffouri, a consultant with Advanced Software Applications Corp. claims that many electronic commerce sites do not adequately protect customer databases and are vulnerable to hackers seeking customer information (Morgan, 1999).

Even when the potential thief does not circumvent the firewalls and encryption designed to protect the computer, electronic commerce is still vulnerable. Cybersources, a developer of software systems that detect fraud, estimates that as much as 5 to 6% of the average internet retailers transactions involve consumer fraud (Corral, 1999). Others estimate that credit card fraud on the internet is as high as 30% (Lucas, 1998). Credit card fraud is more of a problem for electronic commerce for several reasons:

- Since credit card companies will not hold the defrauded customer liable, and, due to the high risk of credit card fraud on the internet, banks may not cover fraudulent expenses charged to electronic commerce vendors. Banks covering fraudulent "chargebacks" often charge significantly higher fees for the service (Corral, 1999).

- Unlike in-person transactions, when fraudulent credit card information is detected by an internet vendor, that credit card cannot be confiscated, and the fraudster and credit card are free to try alternative sites.

- Since actual cards and signatures are not required, fraud perpetrators are free to use stolen numbers, or even attempt to manufacture numbers for use.
- The remoteness of the buyer and seller make it extremely difficult to apprehend the fraud perpetrator. Indeed, the anonymity and remoteness of the transaction has been sited as attracting individuals to electronic commerce fraud who would otherwise not engage in fraudulent activity (Punch, 1999).

While electronic commerce threats may emanate from any of the above individuals, controls exist which can mitigate these risks. These controls will be discussed in the remainder of this article.

Some Common Approaches of Strategic Opponents.

In general, threats to webservers include denial-of-service, theft of proprietary information, and financial fraud. Denial-of-service attacks are the most common form of threat today and can be carried out in a variety of forms. Sometimes hackers shut down the entire web site, other times they modify the content of, say, the home page; and still other times they even redirect all incoming traffic to an alternate web site controlled by them. Regardless, the potential losses can be enormous, and large companies can lose millions of dollars in revenues in a matter of only hours.

Theft of proprietary information can take various forms, including theft of customer lists, credit card numbers, company-developed software, and so on. The loss exposure from such threats can be larger than might appear at first glance, because customers may quickly lose confidence in a website that cannot maintain privacy and confidentiality. In fact, concerns over privacy are at the very top of the list for today's potential web buyer.

The third category of threat is financial fraud, specifically the fraudulent obtaining of the company's goods or services. Such fraud can take various forms, including the fraudulent use of credit card information and the fraudulent manipulation of input data and/or files on the server. Hackers like to steal credit card numbers from one site and quickly use them on another site, before the theft is detected.

Vulnerabilities

Key vulnerabilities in an internet security system arise from weaknesses in various areas, including the following:

1. The operating system or its configuration
2. The webserver or its configuration
3. The private network and its configuration
4. Various server programs
5. General security procedures

Each of these areas is discussed individually.

Operating System Vulnerabilities

Since the webserver operates as an extension of the operating system, any failure in operating system security is likely to spill over into webserver security. Therefore, the administrator's primary task is to seek a secure operating system.

Unfortunately, however, no operating system is attack proof, for no sooner than one security hole is closed another is discovered. For this reason it is essential that the administrator diligently monitor ongoing advisory information published by the operating system vendor (e.g. at www.microsoft.com/security), and by other third-party advisory services such as CERT (www.cert.org).

A second problem with operating systems lies in their improper or suboptimal configuration. For example, by default Windows NT 4 comes preconfigured to include a "guest user" in its database of users authorized to access the system. The problem is, however, that this merely opens an unnecessary door through which an attacker might enter and begin attacking the system. Even Microsoft recommends that the guest user be disabled to enhance web security. In fact, Microsoft currently recommends 28 changes to the basic operating system configuration before running its IIS webserver (www.microsoft.com/security/products/iis/CheckList.asp). The administrator should therefore stay current on all literature published by the operating system vendor relating to configuration issues.

Webserver Vulnerabilities

Webserver vulnerabilities tend to be similar to those of operating systems and also require diligence in monitoring for security updates and information on configuration issues. These practices are especially important for webservers because they tend to have more security problems than the operating systems themselves. This is true because webservers and web-browsers tend to be more frequently updated than operating systems, and they serve more on the front line of security since they are the primary interface through which users pass.

Webservers are especially vulnerable to configuration problems, especially in relation to file permissions. A primary risk arises in the area of permissions for directories and files relating to executable scripts programs. Executable scripts and programs are a necessary component of any sophisticated web site. For example, a forms handler program must normally be executed anytime an anonymous user enters data into a form. Further, write access to somewhere on the website is required for the form data to be recorded. Therefore, the anonymous user must have both execute and write access, a potentially lethal combination when made available in the wrong way to a hacker: a hacker with execute and write access to the same directory can use the write access to upload a malicious program and then the execute access to run it. For this reason, write and execute access must never be granted to the same directory.

The problem, however, is that in many cases the web administrator, especially the inexperienced one, inadvertently grants both write and read access to the same directory. This might happen, for example, by the administrator placing script files in the wrong directory. With some web authoring tools the permissions might be created automatically, and so the damage can be done without the administrator being aware of it.

Private Network Vulnerabilities

When a webserver resides on a local network, many additional security risks are created. This is especially true when other machines in the local network have access to the machine running the webserver. For example, assume the webserver is running on machine A, and machine B has access to key files and directories on machine A. With this situation the hacker can break into machine B, and from there access the critical files on machine A. So in a local area network the webserver will only be as secure as any of the machines that have access privileges to the machine on which it is hosted. This poses a very serious problem, because it is next to impossible for the server administrator to enforce sufficiently strong security policies on user machines. In general, users may access the internet, run all kinds of strange and insecure programs, improperly configure their operating systems, and so on.

Hackers frequently seek to attack one computer through an alternate computer on the local network. One way to do this is to e-mail (in the form of an attachment) a Trojan-horse program on the alternate computer. The hacker might trick the recipient into opening the e-mail attachment by spoofing a return address from someone familiar. This is not a difficult task, since many organizations publish e-mail directories of their employees.

When the unsuspecting user opens the attachment he or she unwittingly installs the Trojan-horse program. One such program, Back Orifice, allows the hacker to remotely take control of the victim's computer, and from there access the host computer for the webserver. Everything is done in the background, so the victim might never realize what is happening.

Obviously, the situation is even worse if the webserver is run on a machine that is shared by more than one user. Any of the users might create vulnerabilities. The obvious solution is to as much as possible limit access to the webserver's host machine. This eliminates a plethora of possible problems.

Vulnerabilities from Various Server Programs

Many webserver host computers run other servers besides the webserver. Examples include FTP servers (for file transfers to and from other computers), e-mail servers, remote control servers (that permit legitimate remote computers to take control of the host computer). The problem is that all these additional server programs create potential problems. For example, under current standards the File Transfer Protocol (FTP) sends passwords in the clear with no encryption. Yet, many organizations rely on FTP for transferring sensitive data between the host computer and remote computers all over the internet. Thus, key passwords for sensitive directories are likely to be broadcast semi-publicly over the internet, where anyone with a little luck and a packet sniffer can discover them.

Further, the typical server program has the built-in capabilities to grant access privileges to remote users, and some server programs are relatively easy to break in to. Thus, the administrator needs to be careful not to run any server programs not absolutely necessary, and even careful consideration should be given to running them on separate machines that are logically, and perhaps physically, isolated from one another. Further, the additional server programs need to be given as much security-related attention as the webserver itself.

Improperly set permissions can also result in Domain Name System (DNS) spoofing. Some definitions are necessary. The DNS translates domain names such as www.micro-

soft.com into an IP address. Further, spoofing occurs when one IP address or domain name (i.e. Internet Protocol address) is substituted for another. In DNS spoofing, the hackers with write access changes the translation file rerouting websurfers to www.hacker.com. If the two webpages look identical, even prudent customers can be easily defrauded and the company's reputation damaged.

Other webservers are exposed to IP spoofing. Every packet of data that is transmitted over the internet contains an IP (Internet Protocol) address. If the source address is not secure, then the host computer can change the IP address to make it appear as though it is coming from another host (Ahuja, 1997). This could permit unwanted and unauthorized files to enter the company's networks (e.g. viruses, trapdoors, worms, Trojan horses). Configuring the system to filter packets with suspicious IP addresses or requiring a secure connection before transferring or receiving a packet will reduce this exposure.

Vulnerabilities in General Security Procedures

Tight operating system and webserver security mean little in the absence of good general security measures. The single most important consideration is that of promoting a general atmosphere of security consciousness. Too often sophisticated security measures are bypassed, for example, when a careless employee gives out a critical password over the telephone, or when an important security manual is discarded into the trash without shredding. The literature is full of cases in which very unsophisticated hackers broke into very secure systems.

Security techniques really boil down to one thing: access control. The main goal is to control access to the right individuals and for the right purposes. So it is no surprise that the most common type of attack involves the front lines of user access, namely user authentication, and specifically password cracking. There are many password-guessing programs publicly available with built-in dictionaries containing hundreds of thousands of words. The efficacy of these programs was demonstrated by a file left behind a hacker on one large system, a file containing nearly 50,000 correct passwords of a total possible of nearly 200,000, which was the number of user accounts on the system. With the aid of a password cracking program the hacker had managed to guess passwords for approximately 25% of the accounts on the system.

The best way to minimize the program of password cracking is to use strong passwords. This can be accomplished by requiring passwords to contain a minimum of 6-8 characters. Four-character passwords, used by many systems, are far too easy to guess. Security can be enhanced further by composing passwords of two unrelated words separated by a non-alphabetic character. Examples of strong passwords would include "dog%sky," "lamp&car," "plane$tree," and so on. Of course, passwords can be made even stronger if there is no need for them to be easy to remember, as in the case of "34tohh4s2$1." Further security can be added by configuring the operating system or server to lock out a user after three failed attempts to authenticate.

Security System Design

It is too often forgotten that good security design requires the company to adhere to the precepts of good general control, such a separation of duties, clearly delineated lines of authority, internal audit, good documentation, proper authorization and approval for both transactions and program changes, and so on. But once these things are achieved, and given

that the practices discussed above are followed, careful attention must be given to the prevention, detection, and correction of security breaches.

Prevention

The strongest approach to prevention is the layered approach to access controls. The main goal behind layering is to place multiple barriers between the would-be hacker and the company's sensitive data.

In general, security layers can be placed at the following levels: network, system, server, database, record, and field. At the network level firewalls can sometimes be used to restrict access to certain subsets of the internet population. Thus the webserver will appear visible to desired individuals and invisible to all others.

At the system level each user can be assigned specific privileges. For example, with Windows NT Server the administrator can create an individual user's profile in the User Manager and then assign the user specific access privileges, such as the user's ability to remotely shut down the system.

At the webserver level the administrator can further assign or restrict the user's privileges. For example, the user's server-level profile might be set so as to require encrypted authentication using the NT challenge-response method. This would be much more secure than the commonly-used basic authentication, which sends all passwords in as clear text.

It is possible to place additional authentication-related controls at the database, record, and field levels. These controls would restrict access to specific pieces of data authorized to the user. For example, a marketing manager might be granted access to a wide array of data for sales analysis, while a customer placing an order might only be permitted to fill in an order form and perhaps review open orders. Alternatively, strong security might be obtained by using the "sacrificial lamb" approach, by placing only the order data outside the firewall, on a dedicated server. All other resources would be hidden inside the firewall.

An alternative to encrypted authentication is to use the Secure Socket Layer (SSL) for communication between the server and the web browser. With this approach all communications, including transmissions of passwords, are secure. The only drawback is that SSL communication places a heavier load on the server, and many companies with large volumes of traffic prefer to use SSL only when absolutely necessary.

Of course, authentication controls are only as effective as the overall management of passwords, for any hacker who obtains the right passwords can do considerable damage. Thus, good password management must be maintained.

Authentication security can be enhanced through the use of digital certificates. Each user desiring authentication must present a valid digital certificate before an addition to a valid logon/password combination.

An additional layer of security can be obtained by encrypting all sensitive databases and files available through the web server. With this approach, encryption/decryption is performed on the fly to authenticated users. Thus any hacker that manages to somehow break in and steal a copy of sensitive data files will find them unreadable and useless.

The SET (Secure Electronic Transactions) protocol can be used to enhance security for credit card transactions. A big advantage of this protocol is that the merchant receives from the consumer only encrypted credit card number. The encrypted numbers are then forwarded to the bank for authorization, and the merchant never learns the credit card number, thus making credit-card-number theft impossible at the merchant level.

Detection

Security-breach detection is nearly as important as prevention. This is because no system is 100% secure and without good means for detection one may never know how much damage is being done until it is too late.

The main approaches to detection involve monitoring various logs and transaction auditing. By default many operating systems and web servers install with many critical logging functions turned off. So the administrator's task is to enable all the needed logging functions and then monitor the resulting logs. All accesses to the server should be logged to include the time, data, functions performed, and the user's IP address, the unique number that identifies every user and website on the internet. Finally, all security irregularities, such as failed logon attempts, should also be logged. The administrator must regularly monitor all logs and follow up on any problems.

Various audit programs can be put in place to monitor for unusual transaction activity. For example, the administrator might be alerted if there is an unusually high level of order activity from a particular customer.

Correction

When a security breach is identified, care must be taken to mitigate current or future damages. The first step is to make the appropriate modifications to block the intruder from making further attacks. In some cases, administrators, being unsure of exactly what to do, have shut down the entire web site.

Security System Implementation

Good implementation requires extensive testing, as well as training in operation. Simulations of various problems and security breaches should be included in the testing program, and all relevant employees should be taught to recognize and deal with security issues.

References

Ahuja, Vijay. *Secure Commerce on the Internet*. AP Professional, Boston. 1997.

Ahituv, N., S. Neumann, and M. Hadass. "A Flexible Approach to Information Systems Development." *MIS Quarterly*, June 1984.

Albrecht, W.S., G. Wernz, and T. Williams. *Fraud Bringing Light to the Dark Side of Business*. Irwin, Burr Ridge, Illinois. 1995.

American Institute of Certified Public Accountants. Consideration of Internal Control in a Financial Statement Audit. *Statement on Auditing Standards (SAS 78) Journal of Accountancy*, April 1997, AICPA.

____. Consideration of Fraud in a Financial Statement Audit. *Statement on Auditing Standards (SAS 82) Journal of Accountancy*, 1996, AICPA.

Bostrom, R.P., J.S. Heinen. "MIS Problems and Failures: A Socio-Technical Perspective - Part I: The Cause." *MIS Quarterly*, September 1997a.

____ and ____. "MIS Problems and Failures: A Socio-Technical Perspective - Part II: The Application of Socio-Technical Theory." *MIS Quarterly*, December 1977b.

Checkland, P.B. *Systems Thinking, Systems Practice*. New York: John Wiley & Sons.

Clarke, Raymond T. and Associates. *Systems Life Cycle Guide*. Englewood Cliffs, MJ: Prentice-Hall, 1987.

Corral, Cecile B. On-line Security, Payment Services Aid E-tailers Stung by Fraud. *Discount Store News*. April 19, 1999, pp.20-25.

DeMarco, Tom (1978). *Structured Analysis and System Specification*. Upper Saddle River, NJ: Prentice-Hall.

Gremillion, Lee L., and Philip Pyburn. "Breaking the Systems Development Bottleneck." *Harvard Business Review*, March-April, 1983.

Edwards, P. *Systems Analysis, Design, and Development with Structured Concepts*. New York: Holt, Rinehard and Winston, 1985.

Keen, Jeffrey. *Managing Systems Development*, 2nd ed. New York: Wiley, 1987.

Larson, Melissa. Search for the Secure Transaction: Barriers to E-Commerce Falling. *Quality*, August 1998, pp.61-63.

Lucas, Peter. A Security Blanket for the Internet. *Credit Card Management*, August 1998, pp.33-37.

Marcus, M.L. "Implementation Politics: Top Management Support and User Involvement." *Systems, Objectives, Solutions*, Vol. 1(4), 1981.

Morgan, Cynthia. Protecting Your Web Site Against Credit Card Fraud. *Computerworld*, March 8, 1999, p.71.

Naumann, J.D., and A.M. Jenkins. "Prototyping: The New Paradigm for Systems Development." *MIS Quarterly*. September 1984.

Punch, Linda. Card Fraud: Down But Not Out. *Credit Card Management*. June 1999, pp.30-42.

Radcliff, Deborah. Invisible Loot. *Industry Week*. November 2, 1998, pp.22-26.

Rittenberg, L.E. *Auditor Independence and Systems Design*. Altamonte Springs, FL: Institute of Internal Auditors, Inc. 1977.

Salkin, Steve. Fear of Buying. *Logistics Management & Distribution Report*. May 1999, p.101.

Shaw, J.C. and W. Atkins. *Managing Computer System Projects*. New York: McGraw-Hill Book Company, 1970.

Young, Jeffery. Spies Like Us. *Forbes*, June 3, 1996, pp.70-92.

Weber, R. *Information Systems Control and Audit*. Upper Saddle River, New York, 1999.

Wirszcyz, Rob. Ignore the Cynics: Accept the Challenge of Internet Business. *Management Today*. December 1997, pp.68-69.

Zbar, Jeffery D. No Longer a Novelty. *Credit Card Management (The Year 2000 Money Pit)*, March 1999, pp.8-12.