**IDEA GROUP PUBLISHING**

701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

**#ITP4358**

# MANAGING NETWORK SECURITY

Noushin Ashrafi and Jean-Pierre Kuilboer
University of Massachusetts, College of management, Department of MSIS, 100 Morrissey Blvd. Boston, Ma, 02125
Tel (617) 287-7868; E-Mail: Noushin.Ashrafi@umb.edu; Kuilboer@umbsky.cc.umb.edu

**ABSTRACT:**

*The networked world promises stunning opportunities including global e-commerce. At the same time, hazardous security threats pose a challenge difficult to predict and costly to prevent. The Computer Security Institute reports that 90 percent of companies surveyed had a security breach within the last 12 months (CSI, 2000). Technology theft cost corporations an average of $2 million and the collective losses in the U.S. alone are a reported $10 billion per year. Citizens are losing their privacy, are the targets of credit card fraud, and paying for higher cost of conducting business due to computer hackers. All these indicate that computer security deserves increased attention. There is a need for effective security management that offers active security policies and procedure, the right tools, and rapid responses to new threats. This paper elaborates on prevention policies, detection tools, and reaction methods and attempts to provide a deployment framework that could foster good practices in a commercial environment.*

## INTRODUCTION

The technological revolution has had a dramatic impact on how we do business. On-line transactions exceeds $1 trillion, E-commerce is becoming the mode of business activities, and E-mail, which enables business partners to share ideas globally has become the killer application of the Internet. With all the benefits, these changes have brought new risk to our lives. Computer crimes such as theft of intellectual property, software pirating, trade secret theft, fraud, embezzlement, industrial espionage, hacking, and other unauthorized access are frequent and costly. In the information age anybody is a potential computer crime victim.

In the 1980s, computer crime ranked only sixth among white-collar offenses. Today, with unauthorized computer intrusions increasing at more than 75 percent per year, computer crime ranks number one. Technology theft cost corporations an average of $2 million per year. According to FBI statistics, collective losses in the U.S. alone exceed $10 billion per year (CSI, 2000). Citizens are losing their privacy, are the targets of credit card fraud, or/and paying for higher cost of conducting business due to computer hackers.

Although, security awareness is on the rise, the security problems have not been resolved for a number of reasons. (1) As technology changes, new problems surface and old problems evolve making static solutions ineffective. (2) In an environment where competitive pressure is high and time to market is the primary concern, security does not always get its share of attention in terms of staffing and budget. (3) Pressure on profit margins have emphasized budget crunch and security is looked upon more of an overhead cost without a direct positive effect on corporate profits. To compound the problem, there is a clear contrast between the close control of past-centralized system and today's Internet-based environment, where the security policies are fragmented across protocol, platforms, vendors, and applications without a coherent framework.

Despite the obvious concern about information security, not much research has been published in this area. Only recently, articles comparing security measures for different network application systems or operation systems have started to appear in trade magazines (Avolio, 1998). In this paper we offer a pragmatic approach to computer security along the lines of security mechanisms. The paper elaborates on prevention policies, detection tools, and reaction methods and provides a deployment framework that could foster good practices in a commercial environment.

## PREVENTION

Organizations embracing e-commerce feel the pressure to expose the entire lines of business to a range of users: the internal employees, partners on the extranet, and the customers. Since the population of potential users will inevitably include some destructive individuals, organizations should take serious prevention measures to protect their information assets.

### Policies

Preventive measures can be categorized as policies and procedures applying to people and security infrastructure investments in both hardware and software. The human element is often the most vulnerable link of any security system. A false sense of security may be reached when a company invests in security architecture and forgets about the people involved (Chen, 2000). To avoid this problem, all employees from the CEO to the receptionist should be educated in security matters. On the other hand, a sense of paranoia and inflexibility in the system should not be instilled. Security measures should be the result of risk, cost, and benefit analysis.

Security policies and procedures should be developed along the user and system dimensions. User policies should be organized along a taxonomy based on needs-to-know basis. Guidelines should be established for all categories of users. Broad categories could include internal users (security administrator, business super-users, regular users, temporary users), contractors, partners, third party users such as customers, and third party of unknown identity. These policies and procedures should clearly state both the acceptable and prohibited behavior. Staff members with special access (defined as having passwords or privileges for special accounts such as root, administrators, super-users) should be particularly scrutinized and serve as examples of professionalism for the rest of the user community. Guidelines should outline courses of action when staff is called upon to view files belonging to another person. One such situation is when duty involves access to client source code, electronic mail viewing problem, file transfer, document format exchange, or mail returned to the postmaster, the policy should clearly state "do not inspect a client's file without consent or proper authorization." Further, Staff should refrain from divulging to third parties private information obtained while conducting their duties (for example divulging salaries or health information could expose the organization to lawsuits).

This paper appears in the book, *Managing Information Technology in a Global Economy*, the proceedings of the Inforrmation Resour es Management Association International Conference. Edited by Mehdi Khosrow-Pour. 

If staff members discover or suspect violation of fair use policy, they should inform the relevant security contact person. Similarly when investigating potential breach, any found evidence should be preserved and documented and a detailed record of why the investigation was instigated and what action was taken should be kept.

Other significant directives include "users should not attempt to access data or programs contained in systems for which they do not have authorization and explicit consent, nor should users run any program intended to scan or evaluate systems for security deficiencies [e.g. static analysis tools (COPS, tiger, tripwire), log tools (logsurf, swatch), network analysis tools (e.g. tcp_wrapper, SATAN, nfsbug), privilege (sudo, smrsh), authentication (npasswrd, S/Key), or C functions (msystem, trustfile)].

The acceptable statement of use within security policies should also address disruptive behavior. Users should refrain to purposely engage in activities that will harass other users within or outside the organization. Such conducts could include SPAM, use of resources outside the scope of authorized work, and fraudulent, harassing or obscene messages.

### Prevention Infrastructure

The first step in implementing a coherent security infrastructure is to know the business network. An analysis of risk, vulnerabilities, and threat will help the assessment of potential problems. Security solutions should be unified under a comprehensive framework covering preventive measures for network, operating systems, and applications. The most commonly used security measures are: Virus scanner, firewall, encryption technology, and Public Key Infrastructure (PKI).

The network is a complex building block of the computing architecture. Organizations make large investments in bandwidth, system management tools, and network security tools. With the wave of mergers and acquisitions many corporations are faced with a multitude of disparate systems that are difficult to protect. Most network management and security solutions were developed for small number of users on local networks and have scalability issue. Virus protection is the best known and the most commonly used security measure within the walls of the business. With a procedure to regularly update the signature files, virus scanners provide a range of benefits to the user and compensate for lenient policies (e.g. use of personal laptop, private e-mail, and floppy disks).

Firewall and encryption are the most common security features in the corporate world. Managers, reticent to the opening of their network to the external world, learned early that protection of the perimeter could keep unauthorized users from accessing precious resources. Implementation of a firewall requires the intense involvement of security staff. The hackers will force protection on 24-7 coverage, which could be a tremendous burden on the budget. Hence, many small to medium size businesses are seriously considering outsourcing. There are security firms that administer the firewall remotely through encrypted virtual private network. These firms also provide standard script and configuration that would take organizations a long time and a great deal of efforts to set-up in house. Often vendors' security portal provides security patches and updates, which could be used to harden your system.

Solutions such as Cryptology and public key infrastructure have received a lot of attention in the research community but have failed to bring the promised benefits in practice. Encryption is perceived as a hindrance by the end-user and will only work if it is completely transparent. To that end, both Microsoft and Netscape have added secure socket layer (SSL) as a common feature to their popular Web browsers (Treese, 2000).

Public Key Infrastructure (PKI) and digital certificate have followed a slower adoption curve. PKI is an encryption system with public and private key to code and decode the message between the sender and receiver. PKI is used mostly by business-to-business E-commerce and it provides an improvement in confidentiality, integrity, and non-repudiation. Although less efficient than symmetric encryption, PKI avoids the costly and dangerous practice of exchange of secret keys. As such, it will allow any third party to conduct business without the predefined agreement necessary with secret keys or traditional electronic data interchange. Digital certificates add the benefit of a strong authentication method vouched for by trusted third party.

The explosion of new systems has complicated the life of the business user. Numerous accounts and passwords tend to be confusing. To his effect organizations are investing heavily in directory service and implementing strong single login. A directory such as LDAP stores central information in a secure manner and keeps track of resources available to an individual. The user, upon login, will have access to all authorized computing resources. This implementation poses some difficulty, as it has to be integrated with legacy systems not designed with these features.

Enhanced security can also be achieved with the use of new technology such as Smartcards, which provide an almost unbreakable key at costs less than $3 per person and with readers readily available, the reasons not to use this security device are fading.

## DETECTION TOOLS

The number of users on the Internet is such that new and creative ways to attack networked systems emerge every day. Incidents of documented unlawful attacks appear at mind-boggling pace. Inexperienced hackers acquire canned toolkit from elite hackers to launch devastating attacks. The average cost of an attack has risen 26 percent to $970,000 in 2000.

Intrusion detection is a fairly new concept compared with encryption and authentication where the rules are better understood and security measure can easily scale up. Intrusion detection shares some principles with virus checking scanners. Detection tools are installed throughout the critical path on the network, scanning signature of known viruses.

The mechanism of intrusion detection is quite simple but the deployment is often proprietary and complex. It relies on scanning the network traffic both incoming and outgoing, detecting suspicious and abusive activities. Intrusion detection can be deployed at different level of granularity from single application to the network level.

Anomaly detection is easily implemented on an intranet where the network load is predictable but is much harder to implement on open e-commerce servers where the traffic could be random. Anomalies can be checked for the various layers of the Internet architecture.

Network intrusion detection can be placed directly on the segment to be monitored. If traffic is broadcasted to all devices then any location will do well for the Intrusion Detection System (IDS) sniffer. If served by switch then IDS should be placed on promiscuous port of the switch, on dedicated system loaded with minimum addressable service and not susceptible to easy Denial Of Service (DOS). If hackers can disable the IDS then they would have easy access to all resources on the system.

Attacks can be aimed at specific operating systems or applications using known weaknesses. Thus, multiple layers of detection have to be implemented. Host-based intrusion detection residing on the computer itself will help filter these attacks using system specific rules and application specific defenses. Operating

behind the firewall, these lines of safeguard will also prevent inside job perpetrated by employees. This host-based software will however not protect the network against network-layer attack such as SYN flood or ping of death.

The last line of defense will be application layer intrusion detection tied closely to specific applications such as a database server, e-mail, or Web server. They are highly specialized and have to follow any new weaknesses found in these environments. Given the large number of software and versions, each with their own security gaps, it is difficult to assess the effectiveness of these solutions.

Networked organizations are beginning to realize that security is a cooperative job and that if they support the community they will eventually collect the rewards (or avoid costly lawsuit). To this effect more and more companies are implementing Egress Sentinels. This class of intrusion detection mechanism will be located on routers at the edge of the network. They filter the outgoing packets and inspect their source address. Since organizations know the Internet address range of their computers, they are able to discern possible impostor, who is using their computers to flood an external target as part of a Distributed Denial Of Service (DDOS). Similarly Internet Service Providers (ISP) are starting to implement virus checking and SPAM control on their outgoing messages. They realize that this process can generate positive publicity and avoid large overhead boggling down the Internet backbone.

## REACTION

A generic security framework will include instructions about steps to be taken after a security incident has been detected. Again, the successful deployment of a sound measure will depend on the human element. Training should provide the essential building block of knowledge to be applied before the security professional could take appropriate action to remedy the disruption. Users or partner should be educated about irregular or adverse events that may occur as they conduct their business. Incident categories include, but is not limited to compromised system integrity, denial of system resources, illegal access or load on a system, malicious use of system resources for illegal use, tempering with electronic documents, or any physical damage to the computing systems.

Users should be informed to be on the look-out for peculiar processes running on their system, an abnormal slowdown of the system (not to be mistaken with heavy peak normal use), discovery of an intruder logged into multi-user system, alert from the virus checker installed on individual systems or the network, warning that an unauthorized remote site is attempting to access resources on the network.

In most cases the reaction to intruder attack will involve a team effort. Many people will eventually be involved in the response, whose responsibilities and actions should be clearly recorded in an incident log. Security personnel should always be informed of potential breach of security in order to improve preparedness for future defense.

It is important to note that security is an around the clock endeavor. Hackers will prefer off hours or weekend attacks, as they will rely on lax procedures when security personnel is unlikely to be around for quick response. Worm, Trojan, and virus attacks can strike at any time as innocent users triggered them.

When suspecting illegal activities, any user should have an idea whom to contact to report about potential breach. Some businesses are starting to create jobs with titles such as Installation Security Officer in charge of approving hardware and software to be installed on the network, and Computer Security Officer who should be well-trained and specialized in security measures.

With any criminal activity, it is important to preserve evidence of the crime. In the case of computer crime, the forensic should include a detailed log-book (written manually as hackers have ways to reach most computer files with a little persistence). The log should be started from the first warning, writing down the dates and times of the findings. For evaluation of cost and lost time, log should be kept and people contacting the security team or being contacted should be written down as potential witnesses if the case ever comes to trial. A list of devices and programs affected or potentially affected should be logged to avoid spreading of the incident and help in the cleaning effort.

In e-commerce, businesses are highly competitive and are working hard at building image and brand recognition. The work and years of effort can be wiped out by a single occurrence of network intrusion. Given that a company has lists of its customers either stolen or exposed to prying eyes, the trust will be gone forever (Camp, 2000). Specific procedures should be deployed for each class of security incidents. Viruses and Worms are the most common, hackers and cracker target organization with a high profile, and message integrity incidents are also often reported.

Viruses and worms will affect operations indiscriminately and will be introduced through multiple paths (e.g. infected disk, e-mail, programs). Viruses, Trojans and Worms are handled similarly. If not addressed, the viruses can be spread across the Intranet and it is critical to isolate the infected systems from the rest of the network. Isolation will stop the spread of the infection but could preempt rapid cleaning as patches and testing could be a labor-intensive process. Systems should be disconnected from the network but not powered down or rebooted unless the problem has a known solution (e.g. inoculation software knows the virus). In many cases a precise log has to be kept to avoid recurrence of the problem (variant of the Melissa virus are still around in most organization when the cleaning process misses a few hosts).

When suspicious behavior occurs on a host, the following guidelines must be followed:

- Report the problem to the appropriate security personnel.
- Identify the problem clearly such that they can identify and isolate the cause in a timely fashion.
- Let the security personnel run detection tools, including tools to verify the integrity of the system files.
- Copy and forward new viruses and worms to the Computer Emergency Response Team (CERT) in order to obtain timely remedy.
- Remove all infected code and programs from the host and keep the system isolated from the network until a protective measure is asserted.

When the network is deemed safe and the problem is under control regular operation can resume. In an on-line e-commerce environment the business can hardly afford to keep the system offline for extended period of time, hence, redundant systems could be built to take over in case the primary system is breached and needs to be fixed.

Security incidents involving hackers and crackers are of a different nature. While many are amateurs, some hackers and crackers can be highly skilled and understand the business security measures better than the employees. The Internet has been the breeding ground for a large underground hacking community with the combined ability to break almost any system. Incidents occur in three categories: illegal access to systems, illegal process running on the system, and traces left from past break-in (e.g. defaced banner or home page on a Web site). Methods employed to remedy the active session hack are of three types: killing the process and losing the trail of the attack, trying to trace back the hacker to

the initiating source, leaving the hacker access resource within a sand-box and try to understand and identify his/her method. Detection of hackers' activity often occur by accident but may be helped by automated procedures and rules such as tracing multiple failed login, a high load on the FTP port, uncommon Telnet and remote shell commands. If the prevention measures are appropriate (long password, not sharing passwords, no dial-in behind the firewall) many of these attempts should fail. In many cases time is of the essence as the hacker can be in and out of the site and cause damage in a matter of minutes.

Retaliation against the attacking site should be avoided because chances are that the hacker is using a link of unsuspecting sites to conduct the attack. The administrator of the identified site should be contacted in order to break the cycle and provide information about the nature of the attack. The globalization of the Internet makes this step more and more difficult as language barriers add to the difficulty of the technical complexity. Similarly to Virus, incident CERT should be informed of the attack and how it proceeded. Important information can be obtained from the audit trail if it is safely saved on independent storage. The hacker could delete the primary log files and still be caught after the fact when the integrity of system is restored. When the system was broken through a legitimate account all passwords should be changed on accounts visited by the hacker. Programs and data should be restored and a utility such as "cops" should be run in order to identify possible alteration of system files.

If past incidents are detected, they should similarly be investigated and reported to the security personnel. As with Virus, it is important to determine what path the hacker has taken to infiltrate the network. With mobile computers, non-approved software could be available within the intranet when employees or contractors plug their laptop to the network. A tight security policy should allow only approved hosts on the Intranet or should isolate the access though regular accounts from special accounts.

Post mortem analysis of security incident should provide the ammunition for prevention of future incident. Any hacker attack, if processed correctly, should result in a system less prone to intrusion. If the deployment of preventive, defensive, or corrective measures was less than optimal, a meeting of all parties involved should examine the validity of the process and what has been learned from the experience. The log of incident trail should be kept on file and improved security measures should be implemented. A cost/benefit analysis could also help reclassify some of the network segments or pinpoint necessary partitioning to isolate weak links.

## CONCLUSION

This paper provides a comprehensive approach for the security of information systems. This approach, however, could be expensive and a burden on company resources. For all but the largest organizations, managed security services could be a reasonable alternative for obtaining up-to-date security fixes and policy upgrades. Outsourced services based on automatic remote control could build a self-healing and elaborate immune system to businesses small or large. Security service providers will deliver easy to use and install security appliance and maintain them remotely, thereby alleviating the difficulties associated with tedious configurations and labor restraints. Commerce service and Internet service providers should take heed of this upcoming trend and accrue the benefits of a less wearisome wrapped solution. Together with the right set of security policies and the right deployment procedures this could be the strongest approach to-date to the rising security concerns.

## REFERENCES

Avolio, Frederick M, (1998) "A Multi-Dimensional Approach to Internet Security," Networker, April/May 1998, pp. 15-22.

Camp, Jean (2000) *Web security*, Addison-Wesley, Boston, 2000.

Chen, Ann (2000) " Mitnick to IT Managers: 'Everybody is suspect'," eWeek, September 28, 2000.

CIAC (2000) U.S. department of Energy's Computer Incident Advisory Capability. Security advisories at www.ciac.org

CSI (2000) *CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, 2000 at www.gocsi.com/fbi_survey.htm.

Hontanon, Ramon J. (2000) "Deploying an Effective Intrusion Detection System," Network Magazine, September 2000, pp. 60-67.

Treese, Win (2000) " Living on the Internet Security Plateau," Networker, September 2000, pp. 9-11.