Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

System Vulnerability Mitigation

This essay addresses various facets of IT security and offers insight into the different areas that should be considered when attempting to adequately protect a system. The paper begins by discussing the various Internet security problems facing networks today, such as software vulnerabilities, etc. Next, this document discusses factors that have contributed to successful attacks on various organizations within the IT community. It concludes with a discussion of pertinent security objectives and an outline featuring a ...

Copyright SANS Institute
Author Retains Full Rights

AD

System Vulnerability Mitigation

Student: Kevin Vasquez

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b, Option 1

Date Submitted: December 15, 2003

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Abstract

The world has become increasingly dependent on information technology (IT) and the remarkable services that it offers - particularly with regards to the Internet and modern computer systems. As a result, there is an ever-increasing need to secure these resources and the assets that are in contact with them from attack. It is imperative that users be aware of the potential security risks that face them so that they can allocate sufficient resources to minimize the dangers that these threats pose to their organization(s).

This essay addresses various facets of IT security and offers insight into the different areas that should be considered when attempting to adequately protect a system. The paper begins by discussing the various Internet security problems facing networks today, such as software vulnerabilities, etc. Next, this document discusses factors that have contributed to successful attacks on various organizations within the IT community. It concludes with a discussion of pertinent security objectives and an outline featuring a variety of topics that will help facilitate the development of a successful security model.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Introduction

Modern systems have benefited immensely from the advances in IT. The Internet is probably the most prolific of all of the recent innovations in IT in that it offers organizations and individuals unprecedented access to information though the simple click of a button – and, as a result, has gained considerable popularity. According to recent statistics, as of September of 2002, there were over 605 million people with access to the Internet.[1] In the year of 2000, the average growth rate was over 20 million users per month (or an average growth of 4.8% per month).[2] The number of countries connected to the Internet was a little over 200 by the year 2000.[3] There are currently an estimated 110 millions hosts visible to the Internet (note: due to firewalls, the number of hosts is difficult to predict) and over 110,000 networks in use.[4] From a financial perspective, the World Wide Web is on track to generate approximately 1.8 trillion dollars in 2003.[5]

Due to the increase in on-line use, there has been a huge expansion in the variety of uses for the Internet. Originally, the World Wide Web was used to trade research information between branches of the U.S. Military and Universities, but now there are hundreds of different applications available to an Internet user. These include: Electronic mail (email), Fax over the Internet, Multimedia applications, Games, Purchases/Financial transactions, and Internet Relay Chat (IRC). One can find a large number of organizations, topics, and subjects on the Internet. For example: Corporate, Government, as well as Library databases from around the world. One use that has greatly increased in the last few years is that of electronic commerce - both in the business-to-business and business-to-customers/consumer arenas. However, due to the ever-growing number of people and businesses utilizing the web, there is not only an increasing dependency on it, but also an increasing danger to assets that are tied to the web. Therefore, the issue of network and database security is becoming increasingly important.

Public, private, and government networks have seen a steady increase in the number of unauthorized users and rogue programs trying to either gain access or disrupt their systems. Individuals gaining unauthorized access to computer systems for the purpose of stealing or corrupting data, known as Hackers (also referred to as "Crackers"), have also increased in number and have gained international media attention as their crimes result in ever increasing amounts of lost revenue.[6] These technology troublemakers vary widely in their cultures, usually have little or no prior criminal record. They are usually technologically skilled and reclusive, and sometimes even employed by the very

---

[1] András Salamon, "Internet Statistics" The Internet Solution 5 February 1998. 30 August 2003 <http://www.dns.net/andras/stats.html>.

[2] [5] "How Many Online" Scope Communications Group and NUA December 2000. 1 September 2003 <http://www.nua.ie/surveys/how_many_online/world.html>.

[3] "Science and Technology" GEO – Global Environment Outlook March 2002 2 December 2003 <http://www.grid.unep.ch/geo/geo3/english/087.htm>.

[4] Russ Haynal "Network Wizards Internet Domain Survey" Information Navigators 1 January 2001. 1 September 2003 <http://navigators.com/>.

[6] "The List Web Hosts - Webopedia" INT Media Group 3 November 2003 <http://webopedia.internet.com/>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

firm they are attacking.[7] They tend to be an eclectic group that fear exposure, ridicule, and loss of status. The perpetrators' motivation may be one of many things ranging from espionage and/or the disruption public utilities, denial of service to those authorized entry into a given database/intranet, vandalism of the system or the system's data, the excitement/challenge of the actual act of breaking in to a network, or simply to learn and explore actual hacking and cracking techniques.

Internet Security Problems

There are a number of ways that an attacker can gain access into a system to which he/she does not have the proper authorization that one must be aware of in order to develop an effective security policy. One way is through the exploitation of software vulnerabilities. This method has been used in a great number of successful attacks because attackers are confident that the software area of a network will have holes in it.[8] Quality control is another common deficiency in network system design. This deficiency is mainly due to the fact that the legitimate technology sector has been unable to fix discovered deficiencies as quickly as Hackers have been able to utilize them. Additionally, most of these program/systems are based on code that was never intended to be "production" quality. They were "proof of concept" programs that became the basis of production systems and did not employ sufficient security measures.

With regards to security, there are many areas that are of particular concern; internal monitoring and capturing of network traffic is a good example. This aspect of security vulnerability deals with improperly configured nameservers that, if broken into, can give a Hacker all the names and IP addresses utilized by the internal systems. In some cases, this information can also include the OS and machine type. Hackers armed with this knowledge can then search the net for specific attack tools and target a specific machine inside a network.[9]

A common first step for Hackers looking to enter a system is through analyzing a targeted network through the use of specialized network-vulnerability scanners such as Nessus (the older SATAN and SAINT packages), Firewalk (which probes and identifies a network's firewall ruleset), or proprietary scanners such as Internet Security System's Internet Scanner and Axxent Technologies' NetRecon.[10] With the information provided by these network and proprietary scanners, Hackers can determine what the system's weaknesses are and develop an effective attack based on that analysis.

There are certain security measures that an attacker has to take into account when trying to gain access to a system, one of the most daunting being a Firewall. A Firewall is a system designed to prevent unauthorized access to and/or from a private network. Firewalls can be implemented in both hardware

---

[7] Dr. Edgar H. Sibley, "Policy & Other High Management Decisions" George Mason University 25 October 2003 <http://mason.gmu.edu/~esibley/>.

[8] [9] [10] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus" The SANS Institute 8 October 2003. 3 November 2003 <http://www.sans.org/top20/top10.php>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

and software, or a combination of both. They are frequently used to prevent unauthorized users from accessing private networks connected to the Internet, especially among intranets. All messages entering or leaving the intranet pass through the firewall that examines each message and blocks those that do not meet the specified security criteria.[11] Given the function of Firewalls, Hackers have had to devise different ways to by-pass them in order to gain access to the systems they want to access. Another common method used by Hackers is to take advantage of deficiencies related to IMAPs and POPs; two common email protocols that provide various features to email users. These email protocols allow users to access their email accounts from anywhere on the Internet. Firewalls usually allow email using these services to pass through; allowing the user access to their mail located on the network. Hackers have used IMAP's and POP's as a tool to bypass firewalls through the mail servers on the system, giving them access to the network's internal workings and data.[12]

Buffer Overflow (also known as a Flooding attack) is a security attack that does not try to steal information, but instead attempts to disable a computer or network. This type of attack is directed at a buffer holding data that has been entered, by the user, into a storage area within a program's memory for further processing. An overrun occurs when the length of the data stream sought to be stored exceeds the length of the available buffer. Hackers can exploit unchecked buffers to invoke overflows and to overwrite the original program code with new executables.[13] Since there is an ever-increasing number of companies who depend upon the Internet for services, such as taking orders for their product and/or services, every minute their system is down is a minute that they lose money. An example of a Buffer Overflow, known as a Smurf, deals specifically with a security breach in which a network connected to the Internet is swamped with replies to ICMP echo (ping) requests. A Smurf attacker sends PING requests to an Internet broadcast address. Internet broadcast addresses are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support as many as 255 hosts, so a single PING request may be multiplied 255 times. The return address of the request itself would be spoofed to be the address of the attacker's victim. Therefore all hosts receiving the PING request would reply to the victim's address rather than the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T1 or T3 line with ping replies, thereby bringing the entire Internet service to its knees.[14] An example of a piece of software that was vulnerable to Buffer Overflows was Microsoft's Outlook and Outlook Express; causing its e-mail clients to lose the use of the application in July of 2000. The buffer overrun vulnerability, which was initially discovered by an Argentinean security firm,

---

[11] "The List Web Hosts - Webopedia" INT Media Group 3 November 2003 <http://webopedia.internet.com/>

[12] [13] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus" The SANS Institute 8 October 2003. 3 November 2003 <http://www.sans.org/top20/top10.php>.

[14] "The List Web Hosts - Webopedia" INT Media Group 3 November 2003 <http://webopedia.internet.com/>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

allowed Hackers to launch an attack via the popular Internet e-mail software by sending email to a known user(s) of the Microsoft service. The attack was executed when the mail was being downloaded from the server. The recipients did not even need to open the mail, or even preview it, for the attack to infect their systems.[15]

Another attack that Hackers use to disrupt a network, known as *Disclosure, Modification, and Destruction of Resources*, takes WWW server code, which contains examples of exploitable CGI-BIN scripts in the cgi-bin subdirectory of a given network. The CGI-BIN scripts are for illustrative purposes and were not written with any particular system in mind - they can be found by checking the Websites on the target network. An attacker can modify/subvert these programs in a way that causes them to run other programs of the attacker's choosing – providing the attacker has the means to input the rogue program into the network.[16] In such an attack, a compromised system may then be used as a vehicle from which to launch a hostile attack. For example, nameservers are fairly static systems and are, therefore, not checked as frequently as a production or development system might be. As a result, a Hacker could break into the system and the malicious activity is not usually noticed until someone from the outside reports an attack originating from the nameserver system.[17] A malicious user can also use what are called Remote Procedure Calls (RPC). This allows a computer to run a program on another computer, so long as the two computers share files with one anther. The aforementioned buffer overflow attack is a way Hackers can force the RPC subsystem to run a program on the victim system. This program typically installs a backdoor into the system, which the attackers later uses to log into the system. IIS has a component called Remote Data Services (RDS) that may allow a Hacker to run remote commands with administrator privileges. IIS is the web server software found on most www sites deployed on Window NT and 2000 systems. These attacks can include: modifying the www page(s), disabling the server, or launching an attack on another site. But Hackers are not limited to the methods listed above. The Internet has countless software bugs and websites that teach Hackers how to break into and disrupt networks. Many of these sites actually attempt to out do each other by designing the best user-friendly site. Sites like www.rootshell.com, www.insecure.org, http://thc.pimmel.com, and www.securityfocus.com are excellent resources for Hackers, where one can download a wide variety of attacks tools.[18]

Contributing Factors

There are many contributing factors to the increase, over the years, of hacking and cracking of computer systems. One of these aspects is a disturbing

---

[15] Jaikumar Vijayan, "Microsoft scrambling to fix new Outlook security hole" CNN.com 21 July 2000. 8 October 2003 <http://www.cnn.com/2000/TECH/computing/07/21/ms. outlook.bugs.idg/>.

[16] [17] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus" The SANS Institute 8 October 2003. 3 November 2003 <http://www.sans.org/top20/top10.php>.

[18] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus" The SANS Institute 8 October 2003. 3 November 2003 <http://www.sans.org/top20/top10.php>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

lack of awareness of Internet threats and risks by the individuals who maintain today's modern networks. More and more computer systems are being connected to the Internet through cable-modems, DSL, or other direct connect methods. Security measures are often not considered until malicious users have penetrated the network. One of the simplest methods of gaining information about a victim's system is through the use of a file sharing mis-configuration. Unfortunately, users don't realize the extent of their neighborhood network and unwittingly share files with a computer outside of that intended neighborhood - creating a potentially serious security risk. Furthermore, many Internet sites also allow wide-open Internet access using tools like Network Neighborhood (Windows), AppleShare(Macintosh), or NFS(UNIX).[19] By default, the access is *read-write,* so anyone on the same network can access your files and change them if they are so inclined. In the past, most networks were small and only contained a small amount of an organization's relevant data (most information was on hardcopy only and many of them were not connected to the Internet). However, that situation has drastically changed over the years and networks, and the hardware contained within them houses a majority of most group's data and are usually connected to the Internet. So anyone, anywhere in the world, may be able to access your files, creating the potential for catastrophic results. Another problem is that the majority of Internet and Network traffic is unencrypted and can, therefore, be readily monitored and captured.

An additional security concern is the quality control (QC) of a system. This discipline affects a number of different areas such as the programming, TCP/IP, etc. Most companies simply don't have the time to check all possibilities to determining if a piece of code is "secure," due to constraints on personnel, money, and time. [20] Given this fact, only a small portion of coding can be checked to make sure that it is secure. There is also a real concern with the lack of security in the TCP/IP protocol suite on given systems. Most TCP/IP protocols are not built with security in mind. This means that an attacker could use software (e.g., protocol implementation) bugs to take advantage of the deficiencies of a system's TCP/IP protocol suite. This was the case with Unix Sendmail; one of the original Internet email programs. It was a graduate programming project that was never designed to work in a "production" environment. But, to the dismay of Internet security, it became the master email program for a majority of the mail servers on the Internet. The purpose of the program is to process and send a user his/her email (not the front end users see when they invoke their email program - like Eudora, Exchange, pine, elm, exmh). Sendmail's lack of security was exploited in 1988 by the Internet Worm; an experimental, self-replicating, self-propagating program, which caused many machines at locations around the country to either crash or become "catatonic." Computers were affected at many sites, including universities, military sites, and

[19] Brendan Kehoe, "Zen and the Art of the Internet" Widener University 3 November 2003 <http://sunland.gsfc.nasa.gov/info/guide/>.

[20] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus" The SANS Institute 8 October 2003. 3 November 2003 <http://www.sans.org/top20/top10.php>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

medical research facilities. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000. [21]

Security Objectives

There are three essential security objectives that are used to create a secure, viable network. These objectives are characterized by – Confidentiality, Integrity, and Availability. These core security objectives may either overlap or be mutually exclusive, depending on what design an organization wishes to have.

The first of the three, ***Confidentiality*** (Secrecy/Privacy), attempts to prevent, detect, and deter the improper disclosure of information. It ensures that the assets of a computing system are accessible only by authorized parties. The type of access provided to authorized parties is read-type access: reading, viewing, printing, or simply knowing the existence of an object. Confidentiality is the best understood of the three security points, because its definition is narrower than that of the other three and good examples exist for preserving confidentiality in the real world. Some underlying problems with confidentiality include: "Who determines who is authorized?" and "What constitutes seeing?" These aspects of confidentiality are often determined by the policies of the given organization - also discussed in this paper.

The second security objective is ***Integrity*****,** which incorporates the prevention, detection, and deterrence of the improper modification of information. This objective is achieved by ensuring that assets can be modified only by authorized parties or only in authorized ways. In this context, modification includes writing, changing, changing of status, deleting, and creating.

The final security objective is ***Availability*** (Denial of Service), which prevents, detects, and deters the improper denial of access to services provided by the network. An authorized party should not be prevented from accessing objects to which he or she has legitimate access. Furthermore, it also holds authorized users accountable for their actions and applies to both data and services (access to computing resources). Expectations for this objective include the presence of object or service in usable form, the capacity to meet service needs, progress (bounded waiting time), and the adequate time/timeliness of service. The main goals of availability are: timely response to authorized user requests and needs, fair allocation of resources, fault tolerance, utility or usability, and controlled concurrency (support for simultaneous access, deadlock management, and exclusive access). [22]

Another crucial security objective is ***Securing Computing Resources***, which is the prevention, detection, and deterrence of the improper use of computing resources, which include: Hardware, Software, Data, and Network resources.

Hardware Resources include computing equipment, such as the computers themselves, or other related items such as monitors, scanners, and

---

[21] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus" The SANS Institute 8 October 2003. 3 November 2003 <http://www.sans.org/top20/top10.php>.

[22] University of Miami Ethics Programs "Privacy/Data Protection Project" University of Miami 27 June 2003. 20 November 2003 <http://privacy.med.miami.edu/glossary/xd_confidentiality_integrity_availability.htm>.

[23] Charles P. Pfleeger, Security in Computing. Upper Saddle River, NJ: Prentice Hall, 1997.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

monitors. Security for items such as these is usually handled by a relatively small staff of computing center professionals.[23] Vulnerabilities in this area can result from the following attacks: interruption (denial of service) or interception (theft). Involuntary attacks, not intended to do serious damage to the hardware involved, can also result in accidental damage - such as: water, power surges, dust, etc. Voluntary attacks occur when someone actually wishes to do harm to the computer such as: theft or destruction of the system.[24] Below are the

Software resource security, which includes the operating system, utility programs, and application programs, usually poses a larger problem than hardware security and is handled by all programmers and analysts who create or modify programs for the system. Vulnerabilities can be exploited to launch the following attacks: interruption, interception, and modification. Interruption (deletion) is a common mistake made by users. Because of this software is usually carefully controlled through a process called configuration management, so that software is not accidentally deleted, destroyed, or replaced. Interception (theft) is the unauthorized copying of software. This is an important issue in computer security and has received a great deal of attention in the past few years. Software authors and distributors are entitled to fair compensation for the use of their products and the theft of their software cheats them of substantial revenue. Unfortunately, the problem of software privacy is growing, aided by the increase in Internet access speeds - making it easier to download large files from the web onto a distant computer. Lastly, there is the issue of modification (when a working program is modified, either to cause it to fail during execution or to cause it to do some unintended task). Modification is usually easy to achieve - simply changing a bit or two can convert a working program into one that fails. An example of modification is a Logic Bomb, which is a program that is altered in such a way that it usually works well, but fails in specialized circumstances. There are other types of modified programs that are changed to extend the functioning of a program so that an innocuous program has a hidden side effect. Some examples of this type of software are: Trojan horse, Viruses, Trapdoors, and Information leaks. A Trojan horse is a program that overtly does one thing, while covertly doing another. A Virus is a specific type of Trojan horse that can be used to spread infection from one computer to another. A Trapdoor is a program that provides a secret entry point. In this case, a Hacker typically sends a program with a Trapdoor to a network that he/she does not have legitimate access to. After the program is downloaded into the system, he/she can gain entry to the system through the Trapdoor. Finally, Information leaks occur when a program, after entered into a system, makes information accessible to unintended people or other programs. [25]

Data resources, in essence, consist of information of value to the public. Because their content is more likely to be stolen, damaged, or destroyed, they face a significant security risk. Unlike hardware or software, data has no intrinsic value. There is only a cost, perhaps measurable, to reconstruct or redevelop lost

---

[24] Dr. Edgar H. Sibley, "Policy & Other High Management Decisions" George Mason University 25 October 2003 <http://mason.gmu.edu/~esibley/>.

[25] "The List Web Hosts - Webopedia" INT Media Group 3 November 2003 <http://webopedia.internet.com/>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

data. For example, if an online retailer had its customers' credit card numbers stolen from them, the company does not, at first, know the actual monetary value of those numbers. But the lost revenue as a result of the theft and the subsequent loss of business due to the customers' mistrust in the company's security would be enormous; not to mention the credit card company's losses as a result of the fraudulent use of the cards. There are several qualities that Data Resource Security aspires to provide, they include: Confidentiality, Integrity, and Availability. Confidentiality is the prevention of unauthorized disclosure of information or data. Integrity is the prevention of an unauthorized modification of a given network or system. Availability is the prevention of denial of entry to authorized users.

Network resources are comprised of a combination of hardware, software, and data. What makes this resource potentially more vulnerable than the previous systems is the added complexities of a communications network. Unfortunately, communications within a system may occur through the use of an exposed medium providing distant access from potentially untrustworthy computing systems. Other network security problems include: lack of physical proximity, use of a non-secure, shared media, and the inability to positively identify remote users.

Accomplishing Security

The next issue we will discuss will be accomplishing security. This component is made up of three aspects: Policy, Mechanism, and Assurance. With regards to ***Policy***, an organization must decide exactly what it wants from its security and how it desires to implement it. A typical security policy needs to do the following: first, it should designate that some objects may only be disclosed to, or changed by, authorized users. Second, a policy should stipulate that sensitive data (or the existence of that data) is not disclosed to individuals not authorized to receive or view it. Third, these objects and information must be preserved over time. Fourth, no operations should make it possible to determine operational details through external observation.[26]

A typical security policy is layered into two types: the Organizational Policy and the Automated Information System Policy (which is contained within Organizational Policy). The Organizational Policy is the overall policy established for the group. Within the Organizational Policy structure exists the Automated Information System Policy. This policy consists of controls such as the frequency of changing passwords. These controls are frequently simple in nature, yet often have a tremendous effect on operations. There are several areas over which Automated Information System Policy has control including the computers, communications, and security areas of a network. The area where computers and security overlap is known as *Compsec*, and the area where communications and security overlap in nature is known as *Comsec*. The region where *Compsec* and *Comsec* overlap is known as *Infosec*.[27]

Next, there is the ***Mechanism*** component of achieving security. The mechanism component is, in effect, how to enforce the security policies of a

[26] Dr. Edgar H. Sibley, "Policy & Other High Management Decisions" George Mason University 25 October 2003 <http://mason.gmu.edu/~esibley/>.

[27] Charles P. Pfleeger, Security in Computing. Upper Saddle River, NJ: Prentice Hall, 1997.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

given organization. This is accomplished in three steps: prevention, detection, and tolerance. Prevention is the access control of an information system. Prevention is a more fundamental methodology in that it is used as a first-line of defense. Detection, on the other hand, seeks to prevent compromises in security by threatening discovery through auditing and intrusion detection. This method requires that the audit trail be protected from alteration so that those in involved with detection have an accurate record from which to conduct the analysis. Lastly, there is tolerance, which is a more practical approach. Tolerance suggest that the flaw is known, but either those involved do not know how to fix it or the problem is too expensive to justify fixing it. Sometimes detection is the only option, such as in those cases involving accountability in the proper use of authorized privileges or when dealing with the modification of messages in a network.

There is a final component in achieving security known as ***Assurance***. Assurance measures how well the security policy of a given system is working, and is, in effect, a measure of the mechanism component. There are several aspects of Security Assurance that must be considered. These are Access Control, Authentication, Data Integrity, Confidentiality, and Non-repudiation. Access Control involves determining whether a user or computer is authorized access to your system or network. Authentication makes sure that the user or computer at other end is who or what it claims to be. Next is Data Integrity, which is ensuring that the data that arrives is the same as that which was sent. Confidentiality protects sensitive information from being visible to an eavesdropper. Lastly, Non-repudiation (accountability) guarantees that the fact of a transaction can subsequently be proven to have taken place: sender and receiver agree that the exchange took place.[28]

There are other methods with which to attempt to achieve adequate security. One is called ***Security by Obscurity***, which states that if we hide the inner workings of a system it will be secure. There are several reasons why this method would prove difficult to execute. First, hiding the inner workings of a system is becoming less applicable as more systems become dependent and integrated with software that is compliant with vendor-independent open standards. Meaning, all that one would need is to determine what standard software your system uses to establish how your system works. Another reason it is difficult to obscure system operations is the rapid growth of computer technology expertise. It is far more difficult to keep a system concealed when there are an ever-increasing number of individuals who know how these types of systems work.

Yet another way of attempting to ensure adequate security is through the use of Legislation. ***Security by legislation*** says that if we instruct our users how to behave, we can secure our systems from attackers. This concept educates the Network-using populace as to what steps are needed to help ensure security. Legislation trusts that the "governed" will vigorously follow these steps. These security guidelines would include rules such as: users will not share passwords with other individuals, nor write down their passwords for recall purposes, nor type in their password while someone is looking over their shoulder.

[28] Dr. Edgar H. Sibley, "Policy & Other High Management Decisions" George Mason University 25 October 2003 <http://mason.gmu.edu/~esibley/>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Unfortunately, rules of these types are not very effective in ensuring security. For the most part, people, over time, become complacent with their security habits - even if specifically shown what they should and should not do. Though user awareness and cooperation is important, it cannot be the principal focus for achieving security.

Though security is important in any modern system, there are tradeoffs one must take into account when developing a system. There are three aspects of database design that are pertinent: Security, Functionality, and Ease of Use. However, often the degree to which each of these three components affects the ultimate design is determined by the cost. Given that Security, Functionality, and Ease of Use all have a certain "costs" associated with them, it is necessary to decide how these components are applied in the design of a system to meet the overall needs of its users. For example, if a system is being designed for the military, Security may take precedence over Functionality and Ease of Use. However, if the system is being designed for a group of users without much computer expertise, Ease of Use might be more important, therefore receiving more attention and investment than the other two components.

There are three challenges one must take into account when designing a system: Threats, Vulnerabilities, and Risks. Each of these design issues is important and an assessment of threats and vulnerabilities is necessary in order to determine what risks your system may manifest with regards to security. ***Threats*** are potential attacks on the system such as a threat from a hostile party with the capability to exploit a vulnerability. There are several classes of Security Threats, for instance (in order of importance): errors and omissions by insiders, natural/man-made/machine disasters, dishonest or disgruntled insiders, and outsiders. While this, of course, is only one possible ranking of Security Threats, it is a typical ordering used by many organizations.[29]

Vulnerabilities are weaknesses that may potentially be exploited to cause loss or harm. They are, in effect, the susceptibility of a system to threats such as the one mentioned earlier. A vulnerability is an aspect of a system that leaves it open to attack.[30] For instance, some systems may have security contingency plans that deal with natural disasters (such as tornados or hurricanes), man-made disasters (such as arson), or machine disasters (such as major software or design problem). Other systems may have taken account the risk disasters in the design of the system itself. Two examples of design concepts that take into account the risk of disasters are Electronic Vaults and Remote Journaling. The Electronic Vault concept incorporates two databases, the first database is used for day-to-day work, and the second is used to shadowing it. So if a disaster does take place, there exists a second database that can be used as a back up. This second database is usually on site or close to site for quick and easy access. Remote Journaling also incorporates the use of two databases, but instead of having both databases located at the same site, it has one located at the work place and the back-up database at a separate site. The database located at the work place sends the logs of operations of the OS by remote to the back-up database. This type of design allows for a major disaster such as

[29] [30] "The List Web Hosts - Webopedia" INT Media Group 3 November 2003 <http://webopedia.internet.com/>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

earthquake or fire, where the building that an organization is located in may be inaccessible or destroyed. In a case such as this, an organization can simply move to the second site and continue its work. Obviously, Remote Journaling is a more expensive design than Electronic Vaults, because you need to have access to two separate locations and the means to send large amounts of data over a greater distance.

Risk is the measure of the possibility of security breaches and the potential severity of the ensuing damage. With the threat of risks comes the need to manage those risks. There are three different areas of Risk Management: Risk analysis, Risk reduction, and Risk acceptance. ***Risk Analysis*** uses mathematical formulae and computer models. But the underlying parameters are often difficult to estimate. There is precious little historical data, and what does exist may be of little use. Risk Analysis employs Probability-based Quantitative, Qualitative, and Fuzzy mathematics. The Probability-based quantitative method uses quantifying predictability in a nonlinear forecast situation to run an ensemble of forecasts from slightly perturbed initial conditions.[31] The classic quantitative algorithm that laid the foundation for information security risk assessment is:

(Asset Value x Exposure Factor = Single Loss Expectancy) x Annualized Rate of Occurrence = Annualized Loss Expectancy [32]

With the Qualitative method, the metrics are all subjective in nature. Virtually every risk element can be characterized using two metrics, "Low, Medium, and High," or through "Ordinal Ranking." The terms "Vital, Critical, and Important," however, are descriptive only of an asset's value to an organization.[33] Fuzzy mathematics, deals with the truth or validity of a given statement, which is measured numerically (in most fuzzy systems literature) as ranging from zero (false) to one (true). Statements are true to various degrees; ranging from completely true, to half-true, to completely false. Using this method it is possible to reason in terms of words, such as small, medium, fast, slow and so on, rather than in terms of numbers. Therefore, ambiguities and contradictions can be easily handled; and uncertainties pose minimal problems. An example of this is FLOPS (Fuzzy LOgic Production System). FLOPS was originally developed in the early 1980's at the Kemp-Carraway Heart Institute by Douglas Tucker and William Siler for medical image analysis. It is based on fuzzy systems theory using fuzzy logic (which states a statement is true to various degrees, ranging from completely true through half-truth to completely false), fuzzy sets (a fuzzy set is one to which objects can belong to different degrees - called grades of membership), and fuzzy numbers (an ordinary number whose precise value is somewhat uncertain). FLOPS uses a different scale; confidences which range

---

[31] Eugenia Kalnay, Zoltan Toth, M. Steven Tracton, and Yuejian Zhu "Probabilistic Quantitative Precipitation Forecasts Based on the NCEP Global Ensemble" Environmental Modeling Center, NCEP, NWS/NOAA 11-16 January 1998. 5 September 2003 <http://wwwt.emc.ncep.noaa.gov/gmb/ens/precpap/precpap2.html>.

[32] [33] Micki Krause, Harold F. Tipton "Handbook of Information Security Management Volume 1: 4th Edition" The Disaster Center Bookstore 2000.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

from 0 (false) to 1000 (true) (since this scale economizes computer memory requirements).[34] There is an undeniable fact that threats put our assets at risk. Assets have value and potential threats challenge our ability to maintain that value. Threats have a distinct probability of occurrence and a variable severity of effect. Therefore, assets' susceptibility to various threats must be taken into account. Risk considers the expected loss from the possible action of a threat against an asset's vulnerabilities, as well the likelihood of an undesirable outcome within a given period of time. The *Assets–Threat Model* calculates the risk of an asset using the following formula R = V * P * S. In this formula R = Risk, V = Value of an asset, P = Probability of occurrence of threat, and V = Vulnerability of the asset to the threat (i.e., severity of the effect of the threat). With regards to probability, the Probability of occurrence is based on what has happened in the past.[35]

With the *System–Failure Model**,*** estimates of the probability of highly undesirable events such as: nuclear reactor meltdown or mid-air aircraft collision can be calculated. However, state space of complex systems is very large and makes this approach very difficult.

Risk Reduction, is the action taken to reduce the likelihood and impact of a risk. This methodology analyzes the probability-based estimates of potential hazards to a system that were determined in the risk analysis and allows those involved with the system's design to take necessary steps to avoid them.[36] Once the "cost versus acceptable-risk" parameters have been established, one moves into the realm of ***Risk Acceptance***. Risk Acceptance is embodied by two concepts: Certification and Accreditation. *Certification* is the technical evaluation of a system's security features with respect to how well they meet a set of specified security requirements. *Accreditation*, is the management action of approving an automated system, perhaps with prescribed administrative safeguards, for use in a particular environment; often for a given amount of time.

Conclusion

Despite the advantages of using information technology, system designers must also take into account the risks that go along with using such assets. Attackers and rogue programs are a real threat to systems' assets and, therefore, must be taken seriously when designing systems security. Of course there are costs associated with security implementation so it is important to understand a system's key vulnerabilities in order to fully appreciate which areas of security are of particular concern. Furthermore, it is very important to know what the potential losses/costs are if a system is attacked. Having this information will allow an organization to quantify the threat; thereby determining

---

[34] William Siler "Building Fuzzy Expert Systems" 8 September 2003 <http://members. aol.com/wsiler/>.

[35] Eugenia Kalnay, Zoltan Toth, M. Steven Tracton, and Yuejian Zhu "Probabilistic Quantitative Precipitation Forecasts Based on the NCEP Global Ensemble" Environmental Modeling Center, NCEP, NWS/NOAA 11-16 January 1998. 5 September 2003 <http://wwwt.emc.ncep.noaa.gov/gmb/ens/ precpap/precpap2.html>.

[36] "The List Web Hosts - Webopedia" INT Media Group 3 November 2003 <http://webopedia.internet.com/>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

how many resources should be put towards securing their system. It is becoming increasingly important to consider effective security measures during the system design phase. When secured properly, a good network can be an invaluable asset, but when system security is ineffective, a network can be a huge liability with enormous unexpected costs.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

List of References

"How Many Online" Scope Communications Group and NUA December 2000. 1 December 2003 <http://www.nua.ie/surveys/how_many_online/world.html>.

"Science and Technology" GEO – Global Environment Outlook March 2002 2 December 2003 <http://www.grid.unep.ch/geo/geo3/english/087.htm>.

"The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus" The SANS Institute 8 October 2003. 3 November 2003 <http://www.sans.org/top20/top10.php>.

"The List Web Hosts - Webopedia" INT Media Group 3 November 2003 <http://webopedia.internet.com/>.

Haynal, Russ. "Network Wizards Internet Domain Survey" Information Navigators 1 January 2001. 1 September 2003 <http://navigators.com/>.

Kalnay, Eugenia; Toth, Zoltan; Tracton, M. Steven; and Zhu, Yuejian. "Probabilistic Quantitative Precipitation Forecasts Based on the NCEP Global Ensemble" Environmental Modeling Center, NCEP, NWS/NOAA 11-16 January 1998. 5 September 2003 <http://wwwt.emc.ncep.noaa.gov/gmb/ens/precpap/precpap2.html>.

Kehoe, Brendan. "Zen and the Art of the Internet" Widener University 3 November 2003 <http://sunland.gsfc.nasa.gov/info/guide/>.

Krause, Micki; Tipton, Harold F. "Handbook of Information Security Management Volume 1: 4th Edition" The Disaster Center Bookstore, 2000.

Pfleeger, Charles P. Security in Computing. Upper Saddle River, NJ: Prentice Hall, 1997.

Salamon, András. "Internet Statistics" The Internet Solution 5 February 1998. 30 August 2003 <http://www.dns.net/andras/stats.html>.

Siler, William. "Building Fuzzy Expert Systems" 8 September 2003 <http://members.aol.com/wsiler/>.

Sibley, Dr. Edgar H. "Policy & Other High Management Decisions" George Mason University 25 October 2003 <http://mason.gmu.edu/~esibley/ >.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

List of References (continued)

University of Miami Ethics Programs "Privacy/Data Protection Project" University of Miami 27 June 2003. 20 November 2003 <http://privacy.med.miami.edu/glossary/xd_confidentiality_integrity_availability.htm>.

Vijayan, Jaikumar "Microsoft scrambling to fix new Outlook security hole" CNN.com 21 July 2000. 18 October 2003 <http://www.cnn.com/2000/TECH/computing/07/21/ms.outlook.bugs.idg/>.

The bibliographies and footnotes were done as shown in the MLA Handbook for Writers of Research Papers. (5th Edition) by Joseph Gibaldi. - found on pgs. 182, 183, 184, 186, 187, 269, and 281.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced