PROVIDING EFFICIENT INS FOR CORPORATE NETWORKS

***Kiran Kumar.V**
Lecturer, Dept. of ISE, SJBIT, Bangalore

****Fazal Mahemood**
Asst. Professor, Dept. of ISE, SJBIT, Bangalore. Email : fazalmahemood@gmail.com

*****Usha N**
Lecturer, Dept. of ISE, SJBIT, Bangalore. Email : Ushanagaraj.1986@gmail.com

ABSTRACT

Security continues to be an issue for organizations. Good information security is a mix of physical security, computer security, network security, backups, anti-virus software, firewalls, authentication methods, intrusion detection, confidentiality, integrity, availability, etc., Risk is the combination of threat and vulnerability. This paper deals with Information security in particular and concentrates on corporate networks. Threats without vulnerabilities pose no risk. Likewise, vulnerabilities without threats pose no risk. A secure system should still permit authorized users to carry out legitimate and useful tasks. It might be possible to secure a computer system against misuse using extreme measures. Most computer systems cannot be made secure even after the application of extensive "computer security" measures. Further more, if they are secure then functionality and ease of use often decreases. The assurance of security depends not only on the soundness of the design strategy, but also on the assurance of correctness of the implementation. There is no universal standard notion of what secure behavior is. "Security" is a concept that is unique to each situation. One technique enforces the principle of least privilege to great extent is even if an attacker gains access to one part of the system, fine-grained security ensures that it is just as difficult for them to access the rest. Further more, by breaking the system up into smaller components; the complexity of individual components is reduced. Most of the time people concentrate on coming out with efficient algorithms to analyze, process data. But not much importance is given to ensure data integrity, security, privacy, etc.

1. Introduction

Information is defined as knowledge obtained from investigation, study, intelligence, news, facts, data, a signal or character representing data. Security is defined as freedom from danger, safety, fear or anxiety. Information security means the measures adopted to prevent the unauthorized use, misuse, modification or denial of use of knowledge, facts, data or capabilities.

Securing network infrastructure is like securing possible entry points of attacks on a country by deploying appropriate defense. Computer attacks are now commonplace. By connecting your

computer to the Internet, you increase the risk of having someone break in, install malicious programs and tools on it, and possibly use it to attack other machines on the Internet by controlling it remotely.

Several major banks have been subject to attacks, in which attackers gained access into customer's accounts and viewed detailed

information about the activities on these accounts. In some instances the attackers stole credit card information to blackmail e-commerce companies by threatening to sell this information to unauthorized entities. Several online trading companies and ecommerce sites were shut down temporarily due to major packet flood attacks, also known as Denial-of-Service (DoS) attacks, causing these companies to lose revenue, customer satisfaction, and trust. A major software development company discovered that

Attackers had broken into its network and stolen the source code for future releases of its popular products. Just recently, the source code of the future flagship product belonging to a major software development company was stolen and made publicly available on the Internet.

Key Words: Security, access controls, hacker, authentication, firewalls, viruses.

2. history of security by design

The early Multics operating system was notable for its early emphasis on computer security by design, and Multics was possibly the very first operating system to be designed as a secure system from the ground up. In spite of this, Multics security was broken, not once, but repeatedly. The strategy was known as 'penetrate and test' and has become widely known as a non-terminating process that fails to produce computer security. This led to further work on computer security that prefigured modern security engineering techniques producing closed form processes that terminate.

3. Security trends

The requirements of information security within an organization have undergone two major changes in the last several decades. These are computer security and network security (or internet security).

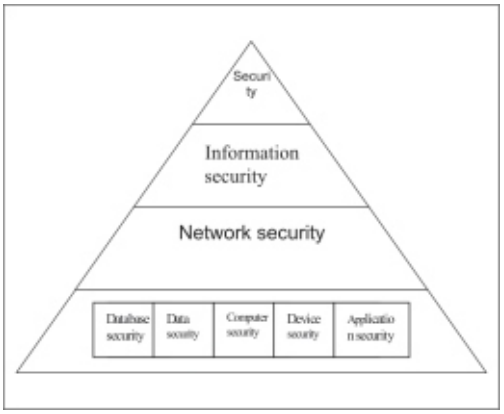


Figure 1 The hierarchy of security specializations

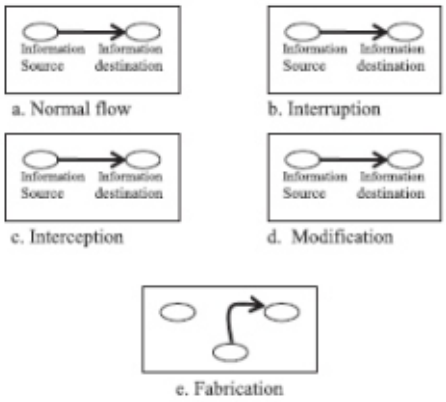
Computer security, with the introduction of the computer, the need for automated tools for protection files and other information stored on the computer became evident. This is especially the case for a shared system, such as time-sharing system, and the need is even more acute for systems that can be accessed over a public telephone network, data network, or the Internet. The generic name for the collection of tools designed to protect data is computer security. Network security, with the introduction of the distributed systems and the use of networks and communications facilities, the need for carrying data between terminal user and computer and between computer and computer has been evolved. Network security measures are needed to protect data during their transmission. The OSI (Open systems interconnection) security architecture provides a systematic framework for defining security attacks, services and mechanisms.

3.1. Security attacks

Security attacks are classified as either passive attacks, which include unauthorized reading of a

message of file and traffic analysis; and active attacks, such as modification of messages or files and denial of service.

Figure 2 Security threats



3.1.1. Interruption (denial of service). An asset of the system is destroyed or unusable. This is an attack of availability, shown in Figure 2 (b).

Example, destruction of a piece of hardware.

3.1.2. Interception (Access). An unauthorized party gains access to an asset. This is an attack of confidentiality, shown in Figure 2 (c).

Example, wiretapping to capture data.

3.1.3. Modification. To modify the data. This is an attack on integrity, shown in Figure 2 (d).

Example, changing values in data file.

3.1.4. Fabrication (repudiation). An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity,

shown in Figure 2 (e).

Example, addition of records to a file.

3.2. Security services

Security services include access control, authentication, data confidentiality, data integrity, non repudiation and availability.

3.2.1. Access controls. Each and every computer system within an organization should have the capability to restrict access to files based on the ID of the user attempting the access. If systems are properly configured and the file permissions set appropriately, file access controls can restrict legitimate users from accessing files they should not have access to.

3.2.2. Authentication methods. Authentication methods have been used to prove the identity of an individual to a computer system. Authenticating an individual can be accomplished by using any combination of something you know (like a password or PIN), something you have (like a smart card or a badge), or something you are (like fingerprints or a retina scan (using iris camera)).Passwords can be guessed or the person may write it down and the password becomes known to others. To alleviate this problem, security has moved to the other authentication methods- something you have or something you are. 80 Smart cards can be used for authentication (they are something you have) and thus can reduce the risk of someone guessing a password. However, if a smart card is stolen and if it is the sole form of authentication, the thief could act as a legitimate user of the network or computer system.

Biometrics is yet another authentication mechanism (something you are) and they too can reduce the risk of someone guessing a password. There are many types of biometric scanners for verification of any of the following: finger prints, retina/iris, palm prints, Hand geometry, Facial geometry and voice.

Each method usually requires some type of device (reader) to identify the human characteristics. There are several issues that arise with the use of biometric systems

including the cost of deploying the readers and the willingness of staff to use them. If an attacker can find a way to control the biometric system, there is no way for the biometric system to assist in the security of the system. But biometrics is the strong authentication method.

3.2.3. Confidentiality. Confidentiality service provides for the secrecy of information. Only the authorized person can view the information.

3.2.4. Integrity. Only authorized parties are able to modify the information. Unauthorized party can not have the rights to modify.

3.2.5. Nonrepudiation. Only neither the sender nor the receiver of a message is able to deny the transmission of information.

3.2.6. Availability. Information is available to authorized parties when needed.

Table 1 Information security services versus attacks

Attack	Security service		
	Confidentiality	Integrity	Availability
Access	X		
Modification		X	
Interruption			X
Repudiation		X	

3.3. Security mechanisms

There is no single mechanism that will provide all the services. Security mechanism is any process that is designed to detect, prevent, or recover from a security attack. Examples of mechanisms are encryption algorithms, digital signatures and authentication protocols.

Table2 Confidentiality mechanisms and requirements

Confidentiality mechanisms	Requirements
Physical security controls	Identification and authentication
Computer file access control	Proper computer configuration
File encryption	Proper key management

4. Intrusion detection system (IDS)

Intrusion is a set of actions that attempt to compromise the integrity, confidentiality, or availability of any resource on a computing platform. An IDS is a software tool that attempts to detect an intruder hacking into a system or a genuine user exploiting the resources of the system. IDSs may also be characterized by scope, as either network based or host-based. The key difference between network-based and host-based IDSs is that a network-based IDS, although run on a single host, is responsible for an entire network, or some network segment, while a host-based IDS is only responsible for the host on which it resides.

An IDS is a piece of software that runs on a host, which monitors the activities of users and programs on the host and monitors the network traffic on networks to which the host is attached. The objective of an IDS is to alarm the system's administrator of any suspicious and possibly intrusive event and possibly taking action to circumvent the intrusion. These actions can be as simple as writing the activities to a log file or as complex as controlling the system's and network's resources automatically by closing network ports or killing suspicious processes.

The objective of an IDS is to detect all intrusive actions for both successful and unsuccessful

attempts with 100% confidence on the network under consideration. Scanning computer systems for vulnerabilities is an important part of intrusion detection. Such scanning will help an organization to identify potential entry points for intruders. However, vulnerability scanning will not protect our computer system. Security measures must be implemented immediately after each vulnerability is identified. In fact, some of the IDSs were marked with the ability to stop attacks before they were successful.

5. Managing risk

Risk is the potential for loss that require protection. If there is no risk, there is no need for security. Risk factor is depends on vulnerability and threat. For example when we take the good diet (proteins, vitamins, carbohydrates, iron, calcium, etc.) then we can maintain good health. Here diet is the vulnerability and health problems are threats. If there is no vulnerability there is no threat and no risk. Likewise, if there is no threat, there is no risk.

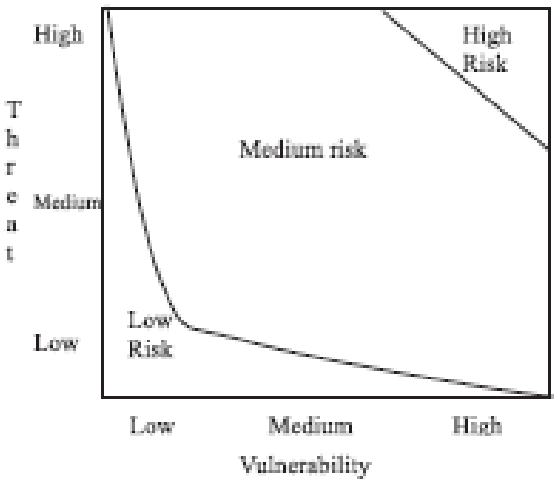


Figure 3 Relation between vulnerability and threat

Risk = Threat + Vulnerability

5.1. Vulnerability

Vulnerability is a potential avenue of attack. Vulnerabilities may exist in computer systems and networks (allowing the system to be open for a technical attack). Vulnerability is characterized by the difficulty and the level of technical skill that is required to enter (attack). For identifying vulnerabilities, find all the access points to information. These are:

- Internet Connections
- Connections to Other Organizations
- Remote access points
- User access points
- Physical access to facilities
- Wireless access points

Counter measures for vulnerabilities are:

- Firewalls
- Anti-virus Software
- Access Controls
- Two-factor Authentication systems
- Badges
- Biometrics
- Card readers for access to facilities
- Guards
- File access controls
- Encryption
- Intrusion detection systems
- Well trained employees

5.2. Threat

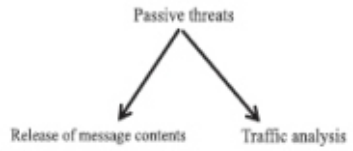


Figure 4(a) Passive network security threats

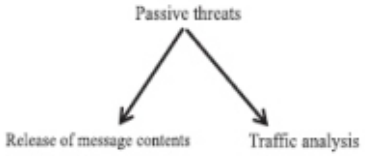


Figure 4(a) Passive network security threats

Threat is an action or event that might violate the security of an information systems environment. Components of threat are Targets, Agents and Events.

Threat is an action or event that might violate the security of an information systems environment. Components of threat are Targets, Agents and Events.

5.2.1. Targets. The targets of threat or attack are generally the security services like confidentiality, integrity and availability.

5.2.2. Agents. The agents of threat are the people who may wish to do harm to an organization. Agent must have three characteristics:

Access, Knowledge & Motivation.

Access, an agent must have access to the system network, facility or information that is desired. This access may be direct (the agent has an account on the system) or indirect. A component of access is opportunity.

Knowledge, an agent must have some knowledge of the target. The knowledge that is useful for an agent includes user IDs, passwords, location of files, physical access procedures, names of Employees, access phone numbers, network addresses, and security procedures.

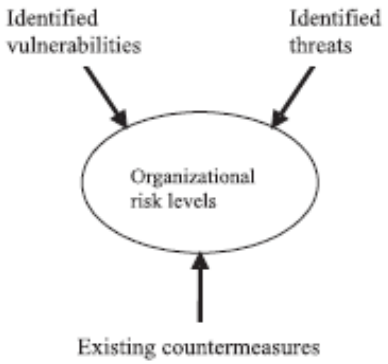
Motivation, An agent requires motivation to act against the target. Motivations to consider includes challenge, desire for money, goods, services or information and desire to do harm to an organization or individual.

Agents to be considered are Employees, ex-employees, hackers, Competitors (commercial rivals), Terrorists, Criminals, and general public, Customers of an organization, visitors, disaster and companies that supply services to an organization.

5.2.3. Events. Events are the ways in which an agent of threat may cause the harm to an organization. For example, a hacker may cause harm by maliciously altering an organizations web site. Another way of looking at the events is to consider what harm could possibly be done if the agent gained access. Harms include the following:

- Misuse of authorized access to information, systems, or sites
- Malicious alteration of information
- Accidental alteration of information
- Unauthorized access to information, systems, or sites
- Malicious destruction of information, systems, or sites
- Accidental destruction of information, systems, or sites
- Natural physical events that may interfere with systems or operations
- Introduction of malicious software to systems
- Disruption of internal or external communications
- Passive eavesdropping of internal or external communications

Theft of hardware or software Figure 5 Components of an organization risk assessment



6. Hackers Techniques

Hacker is an individual who breaks into computer. More appropriate term for hacker might be “cracker”, or “criminal”. Studies have

found hackers most often to be male, between 16 and 35 years old, loners, intelligent and technically proficient. The motivation of the hacker identifies the purpose of the intrusion, like challenge, fun, revenge desire for gain whether it be money, goods, services or information, vandalism (malicious intent). Even in the case of a successful conviction, the hacker may not receive much of a penalty. Consider the care of a datastream cowboy. In 1994, Datastream cowboy along with another hacker named kuji broke into the Rome Air Development Center at Griffis Air Force Base in Rome, New York and stole software valued at over $300,000. Datastream Cowboy, who was identified as a 16- year old living in the United Kingdom was arrested and convicted of the crime in 1997. His punishment was a fine of $1,915.

6.1. Weak Passwords

Weak password is the most common method used by hackers to get into systems. Many users do not understand how to choose strong passwords. Many passwords are short and these are easy to guess. It is much easier to guess a two-character password then an eight-character password. Few weak passwords are user's first name, user's last name, and the account name reversed. The best defense against weak passwords is good security awareness training for employees.

6.2. Open Sharing

When the internet was originally created, the intent was the open sharing of information and collaboration between research institutions. In the case of the UNIX systems, the Network File System (NFS) was used. NFS allows one computer to mount the drives of another computer across a network. This can be done across the internet just as it can be done across a local area network (LAN). If the default configuration on these systems were not changed, anyone could mount the system's root file system and change whatever they wanted to change. UNIX systems are not the only systems to have file-sharing vulnerabilities. Windows NT, 95 and 98 also have these issues. Any of these operating systems can be configured to allow the remote mounting of their file systems. The use of rlogin (remote login without a password) allows users to access multiple systems without re-entering their password.

6.3. Social engineering

The most powerful weapons for a hacker wishing to perform social engineering is a kind voice and the ability to lie. The hacker may use the telephone to call an employee of a company, act as a representative of technical support, and request a password to "fix a small problem on the employee's system".

The theft of a laptop or a set of tools can be useful to a hacker who wishes to learn more about a company. The best defense against social engineering is awareness training. Teach employees how the help desk might contact them and what information they might ask for. Teach the help desk staff how to verify employee Identities before giving out passwords.

7. Malicious Programs

Malicious code covers different types of programs like computer viruses, Trojan horse programs, worms, trap doors, and logic bomb.

7.1. Viruses

A computer virus is a program that can "infect" other programs by modifying them. In fact,

viruses are not structured to exist by themselves. When the program, which a virus is attached to, is executed, the virus code is also executed automatically and performs its actions. These actions normally include spreading itself to other programs or storage devices. Some viruses are malicious and delete files or cause systems to become unusable.

7.2. Trojan horse

Trojan horse is a complete and self-contained hidden program that is designed to perform some type of malicious action (unwanted or harmful function). Most Trojan horse programs also contain mechanisms to spread themselves to new victims. For example I LOVE YOU Trojan horse arrived as an e-mail with a Visual Basic program as the attachment.

7.3. Worms

Worms spread on its own and also replicates on its own. The first known example of a worm was the famous internet worm created by Robert Morris in 1989. The Morris worm was programmed to exploit a number of computer system vulnerabilities (including weak passwords).

7.4. Trap doors

A trap door is a secret entry point into a program that allows someone that is aware of the trap door to gain access without going through the usual security access procedures. Trap doors have been used legitimately for many years by programmers to debug and test programs.

7.5. Logic Bomb

One of the oldest types of program threat, predating viruses and worms, is the logic bomb. The logic bomb is code embedded in some legitimate program that is set to "explode" when certain conditions are met. Examples of condition that can be used as triggers for logic bomb are the presence or absence of certain files, a particular day of the week or date, or a particular user running the application.

8. Firewalls

Firewalls can either be hardware devices or software programs. They provide excellent protection from online intrusion. Firewalls are access control devices for the network and assist in protecting an organizations internal network from external attacks. By their nature, firewalls are border security products, measuring that they exist on the border between the internal network and the external network. Properly configured, firewalls have become a necessary security device. However, a firewall will not prevent an attacker from using an allowed connection to attack a system. Firewalls will not protect an organization from an internal user, since that internal user is already on the internal network. Firewalls are software packages that sit on top of general purpose operation systems (such as Windows NT or Unix) or on firewall appliances. The firewall will have multiple interfaces, one for each network to which it is connected. A set of policy rules defines how traffic from one network is transported to any other. If a rule does not specifically allow the traffic to flow, the fire wall will deny or drop the packets. A firewall is a network access control device that is designed to deny all traffic except that which is explicitly allowed, where as the router is a network device that is intended to route traffic as fast as possible. The key difference is a router is intended to route all traffic as fast as possible, a firewall is a security device that can allow appropriate traffic to flow.

9. Concluding Remarks

Computer attacks happen every day. The operating systems, software, and networking we are using have much vulnerability. Attackers scan our systems and networks for these vulnerabilities and break into the system. In order to combat this growing trend of computer attacks, both academic and industry groups have been developing systems to monitor networks and systems and raise alarms of suspicious activities, using intrusion detection systems (IDS).

There are several conferences, organizations, mailing lists, and web sites that discuss many aspects of computer Security and provide the user community with up-to-date news on the latest vulnerabilities and how to protect against them. Security should not be an all or nothing issue. Do not run an application with known security flaws. The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards and even then the security may be doubtful. The principal objective of this is to present the theoretic foundation of Information security.

References

[1] Eric Maiwald, "Fundamentals of Network Security", Dreamtech New Delhi 2004. Pp.4-29, 46-59, 178-189

[2] William Stallings, "Cryptography and Network Security principles and practices", second edition, Delhi, 2002 pp.4-11

[3] Roberta Bragg, Mark Rhodes-ousley, Keith Strassberg, "Network security",TataMc-GrawHill, New Delhi, 2004, pp.9-14

[4] William Stallings, "Network Security essentials applications and standards", Pearson Education, Delhi, pp.101-172

[5] S. Babu, L. Subramanian and j. Windom, "A data stream Management system for network traffic Management", proc. Workshop Network Related data management 2001.

[6] A. Feldman, A. Greenberg, C. Lund, N.Reingold, J. Rexford, and F. True, "Deriving traffic demands for operational IP Networks: Methodology and Experience", IEEE/ACM Trans. Networking, 2001, pp.265-279

[7] Douglas E. Comer, "Internetworking with TCP/IP Principles, protocols, and Architectures", Volume1, Pearson, New Delhi, 2006, pp.1-9

[8] Steven Alter, "Information systems The Foundation of EBusiness", Fourth edition, Pearson Education, New Delhi. Pp.543-559

[9] Modelling of E-Governance Framework for Mining Knowledge from Massive Grievance Redressal Data, G Sangeetha, LM Rao -International Journal of Electrical and Computer Engineering (IJECE), 2016

[10] 'Sustaining value maximization in entrepreneurship through ethics' published in AJMR-Refereed International Journal of management, September-2008