Volume 2, No. 3, March 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

INFORMATION AVAILABILITY: COMPONENTS, THREATS AND PROTECTION MECHANISMS

Suhail Qadir Mir[1], Mehraj-ud-din Dar[2], S M K Quadri[3],Bilal Maqbool Beig[4]

[1]Post Graduate Dept of Computer Science, University of Kashmir, Srinagar, J & K, India
suhailqadir@hotmail.com[1]
[2]Director IT&SS, University of Kashmir, Srinagar, J & K, India
[3]Director Post Graduate Department of Computer Science, University of Kashmir, Srinagar, J & K, India
[4] Post Graduate Dept of Computer Science, University of Kashmir, Srinagar, J & K, India

Abstract: This paper presents a review of the major components of the Information Availability and also in a dynamic scenario the major threats to Information Availability are identified and steps needed to counter them are also discussed. The threats to Information Availability exist everywhere with some doing it deliberately (deliberate-authorised and deliberate-unauthorised) and some are accidental. These are difficult to specifically protect against; the best that can be done is to establish a good baseline level for IT security. Availability can be compromised or challenged on a single user desktop system (PC) or a major Internet Communication pathway or at any single point or collection of points in between. With such a great risk to Information Availability and the dependence of organizations on Information, proper steps should be taken to ensure the Availability of Information and its critical resources. There is no one stop solution for Countering the attacks but systems and networks can be engineered to provide a level of security where we can say that the information is safe .

Keywords: Confidentiality; Integrity; Availability; Denial of Service (DoS); Protection Mechanisms.

INTRODUCTION

Internet provides us an easy access to Information. But along with ease of access, come risks. Among them are the risks that the valuable Information will be lost, Stolen, Changed or misused. If we can protect Information and Information System of an Organization from unauthorized access, use, disclosure, disruption, modification, recording, destruction, inspection then we can say that the Information is secure. Thus Information Security is the protection of Information and Information System and Hardware that use, store and transmit that Information. The main Goals of Information Security are confidentiality, integrity and availability. For over twenty years, they have been the core principles of information security. The three are also known as the CIA triad.

Confidentiality

The information can only be accessed by authorized people, example would be research data or customer credit card information, patient medical information in hospitals or personal information of employees in an organization. If that information is not secured, the company or the organization involved in that will eventually lose its reputation and business. When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality.

Integrity

Information can be corrupted when it is available on an insecure network. When Information is modified in unexpected ways, the result is known as loss of integrity. This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting.

Availability

Information Availability means that the Information requested or required by the authorized users should always be available. This means that the computing systems used to store and process the Information, the security controls used to protect it, and the communication channels used to transport it must be working correctly Availability is often the most important attribute in service-oriented businesses that depend on information (for example, airline schedules and online inventory systems). Availability has three components [1]:

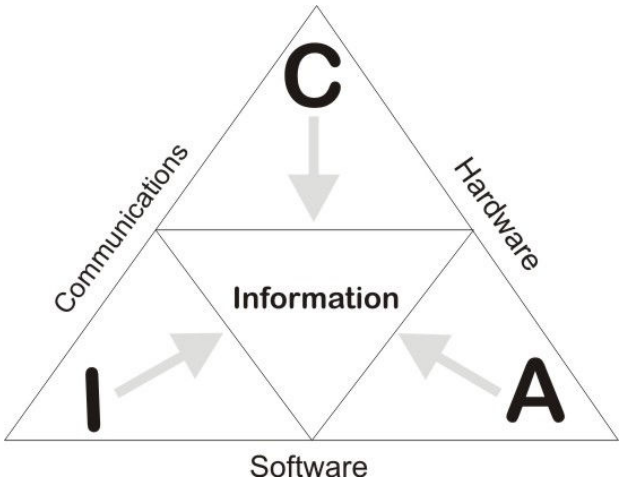

Fig 1: CIA triad

Reliability: Reliability is the probability of a system performing its purpose adequately for the period of time intended under the operating conditions encountered [17]. If the system is not reliable, there is no use in having the system. Users do not want to depend upon a system that cannot be trusted to consistently execute the user's requests.
Accessibility: Accessibility is "the degree to which a system is usable by as many people as possible without modification". There are several access control policies, such as Mandatory Access Control (MAC) and Discretionary Access Control (DAC) which are supported with access control services such as Role Based Access Control (RBAC) [18].

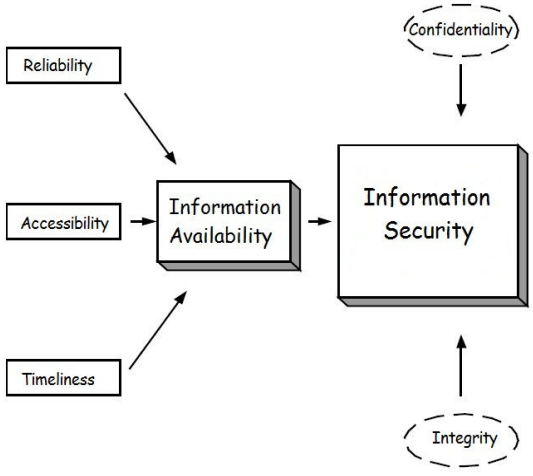

Fig 2: Components of Information Availability

Timeliness: Timeliness is the ability to access Information and Services in a timely manner. It is the responsiveness of a system or resource to a user request [22]. Information Availability is mostly measured by the amount of time an information resource is either processing or not (uptime and downtime). Users and organizations alike desire instant response to their requests; without good Information Availability, that desire may not be sufficiently met

INFORMATION AVAILABILITY A CONCERN

According to Brinkley & Schell [2], confidentiality and integrity can be achieved with a high level of enforcement, but the same assurance cannot be offered by availability. Lampson [8] states that access controls enable confidentiality and integrity. Hosmer [5] contradicts Lampson by asserting that access controls may serve to inhibit availability to users due to the mutually exclusive goals of confidentiality and availability. Availability, according to Parker [14], is considered "the least understood and most ignored purpose of security." Brinkley & Schell [2] wrote that there exists an "unboundedness of possible causes of a loss of availability." Brinkley & Schell are correct, there are a myriad of causes that could lead to information being unavailable. Tryfonas, Gritzalis, & Kokolakis [19] call availability be revisited at the macroscopic level because of our ever-growing dependence upon online information. Furthermore, Lipson & Fisher [10] wrote that "the problems of greatest concern today relate to the availability of information and continuity of services."

MAJOR SECURITY THREATS

The threats to Information Availability exist everywhere from Fire and Floods to producing an Electromagnetic pulse, to malevolent users and Random or Accidental System faults. These threats range from operating faults, which reduce a systems ability to process a users request to a Denial-of-Service (DoS) attack to completely deleting online information. Availability can be compromised or challenged on a single user desktop system (PC) or a major Internet Communication pathway or at any single point or collection of points in between. The main Categories of the threats for the Information Availability are as follows:

Denial of Service

Denial of Service attack (DoS attack) is an attempt to prevent legitimate users from accessing a computer resource or delaying of system operations and functions. The definition of 'resource' in the context of DoS is broad, and ranges from physical hardware and network equipment to application software. Preventing a user from accessing a computer resource is actually preventing the user from gaining access to Information. A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services. DoS attacks range from single packet attacks that crash servers to coordinated packet floods from multiple hosts. In single packet attacks, a carefully crafted packet that exploits a known operating system or application vulnerability is sent through the network to disable a server and/or any associated services it performs. The Slammer worm exploited one such vulnerability. In a flood attack, server or network resources are corrupted or exhausted by a flood of packets. Since a single site launching a flood can be identified and isolated fairly easily, a more sophisticated approach, called a Distributed DoS (DDoS) attack, is the tool of choice for many flood attacks. Attacks can be directed at any network device, including attacks on routing devices and web, electronic mail, or Domain Name System servers.

A DoS attack can be perpetrated in a number of ways[21]. The five basic types of attack are:

- Consumption of computational resources, such as bandwidth, disk space, or processor time
- Disruption of configuration information, such as routing information.
- Disruption of state information, such as unsolicited resetting of TCP sessions.
- Disruption of physical network components.
- Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Viruses and Worm attacks

Viruses and Worms are computer programs that make computer systems not to work properly, resulting in making valuable Information unavailable [7]. These work by disguising malicious code and dumping an unsuspecting user into executing it. Once running, viruses can take over a machine, spread, destroy or change information, attempt to propagate, or even lay dormant for a period.

There is a subtle difference between Virus and Worm; both can replicate themselves but when travelling on the network, Virus needs a carrier file. It can't travel on its own on the network; whereas Worms can travel on its own without anything. It doesn't actually need any infected file to stick in. Viruses and Worms are really annoying problem for all systems. The ultimate aim of these Viruses and Worms are making a good working system to malfunction and sometimes worms can sniff in and steal private information to send it to its creator. Earlier days, Viruses and Worms were spreading through floppy diskettes. Nowadays, they spread through Internet, which is a broad gateway for these malicious programs. It can spread quickly and affect all systems in an organization within a minute and make Information Unavailable to Users and thus can create millions of dollar loss for the organization.

Hacking or Intrusion attack

In this type of an attack an intruder gains access to a computer system without the knowledge of its owner. The people who do this kind of unlawful things are called as hackers. Once they get access to targeted systems, they can alter data available on those systems or steal private information such as SSN, personal information and sometimes some sensitive information related to bank and credit card accounts or even delete the Information and thus making it un-available for the intended users[7]. Most of the targeted systems for hackers are ecommerce websites, individual machines and sometimes bank websites that provide facility for online banking. The targeted systems for hacking are depending on the hackers and their personal types.

In order to do hacking, hackers have to crawl on the targeted systems and gather the information about its strength, weakness, operating systems used, unsecured folders, shared folders, configuration files etc. They will collect all these data and do analysis about how to compromise the targeted website or system. Once they find a way, they will enter through that, and try to exploit the systems. Some hackers will use Trojan horse programs to gain access to the targeted systems. Trojan horse programs are very dangerous threats for ecommerce websites and even for personal machines.

Eavesdropping or sniffing attack

It means seeing all packets passed through wires or sometimes through air for wireless networks. This attack is carried out by using Software called sniffer, which monitors data travelling over a network .Sniffers, can be used both for legitimate network management functions and stealing information from a network. Sniffers add risk to the network, since many systems and users send information on local networks in clear text. A sniffer program shows all the data going by, including user-id's, passwords, and the data inside the files, such as word-processing documents and screens full of sensitive data. TCPDUmp and Snoop are examples for sniffing tools and wire trapping is a classic example of Eavesdropping attack. Though Eavesdropping does not affect the Availability of Information directly but hackers to exploit a system and do all sorts of things then can use sniffers.

Spoofing attack

The exact meaning of spoofing is deceiving others. It is actually fooling other computer users to think that the source of their information is coming from a legitimate user. In such attacks a person or a machine impersonates another to gain access to a resource [7]. Now when a hacker gains access to a computer system, it can do a lot of things like, deleting information, modifying information, stealing information etc. Again like sniffing, spoofing does not affect Information availability directly, but paves a way for hackers to attack the system. There are several methods of spoofing. Some of them are as follows:

IP Spoofing: It changes the source-address of an IP packet to show that it is from a legitimate source, but really it might be coming from a hacker. Thus, the hacker attacks the system and at the same time hides his IP address from the eyes of firewalls. The targeted systems for IP Spoofing are UNIX systems. Basically, the services that require IP authentication are the main targets for IP Spoofing. This can be easily found and filtered by modern firewall systems with proper configuration.

DNS Spoofing: This will direct the users to incorrect location. In other words, directing the users to a different website and collecting personal information through web forms illegally. DNS Spoofing is actually very dangerous threat, because DNS is the one that manages domain names and creates equivalent IP addresses. Suppose, if the domain name is "http://www.sony.com/" and DNS calculates an IP address that is related to a hacker's site, the users will be directed to the Hackers website. If the hacker maintains his website similar to dell, then the users may think that the hacker's website is the real dell- website and may provide all bank or credit card information when trying to purchase something. Now, the hacker can get that Information easily without any difficulties.

ARP Spoofing: Another name of for ARP Spoofing is ARP Poisoning. ARP is actually maintaining a table of MAC addresses of all computers connected in a network. Any information that comes to ARP is delivered to respective computer based on the mappings available on the ARP's tables. Suppose, if ARP couldn't find MAC address for a message, it broadcasts a message to all systems to get a reply from the exact destination-machine with its MAC address;

when it gets the destination-machine's MAC address, it updates it on MAC table. This is the stage where ARP spoofing can happen. ARP Spoofing actually happens when a hacker (hacker's machine) sends a reply to the ARP's broadcasted message saying that the hacker's machine is the legitimate one. Then, ARP gets hacker's MAC address and adds it to its table. As a result, hacker will gain a legitimate connection to the network illegally. Once hacker is connected to the network, he can do all sorts of things.

Man-in-Middle Attack

It is an attack in which an attacker sniffs packets from the network, modifies them and inserts them back into the network. It uses IP spoofing to enable an attacker to impersonate another entity on the network. It allows an Attacker to eavesdrop as well as to change, delete, reroute, add, forge, or divert data. Man-in-Middle attack is actually an active form of Eavesdropping attack. Thus this kind of attack can make Information easily unavailable for the Intended users

Trap Doors

A trap door is a secret entry point in 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. Trap doors become threats when they are used by Malevolent Programmers to gain unauthorized access. When a hacker uses this kind of mechanism he can easily do whatever he wants to do, thus can attack Information too. It is very difficult to implement operating system controls for trap doors.

Logic Bomb

One of the oldest types of program threat, predating viruses and worms, is the logic bomb. The logic bomb is code embedded is some legitimate program that is set to "explode" when certain conditions are met. Examples of conditions that can be used as triggers for a logic bomb are presence or absence of certain files, a particular day or week, or time, or a particular user. Once triggered, a bomb may alter or delete data or entire files or cause a machine halt or do some other damage. One of the popular logic bombs was the CIH Virus it infected Windows 95 and 98 systems.

Trojan horse

Trojan horse programs are initially used for system administration purposes. System administrators used these programs to control their work-stations remotely. These programs are having two components; one runs as a server and another one runs as a client. The server part is installed on the work stations and the client is installed on the administrator's machines. Though it has a good purpose, its power can be used for bad purposes too. Hackers can use these programs to get control on their target machines and watch all the activities. A Trojan horse is a program containing hidden code that when invoked performs some unwanted or harmful function. Trojan horse programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly. For example , to gain access to the files of another user on a shared system, a user could create a Trojan horse program that, when executed, changed the invoking user's file permissions so that the files are readable by any user. This is very dangerous than Virus and DoS for the ecommerce businesses. The threatening issues with Trojan Horses are as follows:

- The main motive of a Trojan horse is data destruction.
- It allows gaining control over the target Machine and to steal or delete private Information available on the target system. This way it affects Information Availability.
- It can store key strokes and make it viewable for hackers. As a result, hackers can easily get the victim's login-ids and passwords and that way facilitate the way for Information misuse.
- It can be installed very easily on the target machines simply by sending it as an email attachment. Basically, Trojan horse programs affect the very basic principles of information security.

Bacteria

Bacteria are programs that do not explicitly damage any files but their sole purpose is to replicate themselves. A typical bacteria program may do nothing more than execute two copies of itself simultaneously on a multiprogramming system. Both of these programs may then copy themselves twice and so on. Bacteria reproduce exponentially, eventually taking up all the processor capacity, memory, or disc space, denying legitimate users' access to those resources.

Social Engineering

Within the context of Information Security Social Engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the hacker. This can be done in several ways, usually involving the perpetrator posing as a person higher in the organizational hierarchy than the victim. The false representation may have been preceded by preparatory social engineering against others in the organization to collect seemingly unrelated information. This information used in the context of a later attack, makes the false representation more credible. Thus social engineering can also lead to making Information unavailable.

PROTECTION MECHANISMS

No matter how big and devastating the threats are, there are always ways of countering them. In this section we will see, what we can do to counteract them:

Denial of Service

There is no one stop solution for Denial of Service attacks but systems and networks can be engineered to counter them in following ways:

Absorb the attack: This implies that additional capacity has already been planned for, installed, and tested before an attack begins. On the negative side, there is an additional resource cost for this excess capacity even when no attacks are currently under way.

Degrade services: Once the critical services have been identified, it may be possible to design the network,

systems, and applications in such a way that noncritical services can be degraded in favour of keeping critical services functional through an attack. If the attack is protracted or extremely heavy, it may become necessary to completely disable noncritical services to provide additional capacity to critical services.

Shut down services: It is plausible that an organization could decide to simply shut down all services until an attack has subsided. While certainly not an optimal choice, it may be a reasonable response for some.

Your reaction to a DoS attack depends a great deal on the preparations made before an attack. Once an attack is under way, it may be too late to configure and install additional capacity or monitoring. These need to be in place ahead of time.

Viruses and Trojan horse attacks

The most known way to avoid these attacks is installing anti-virus software's on all systems. Some new Viruses and Trojans may even try to bypass antivirus software so, it is very important to keep virus-signature-database up to date. In addition to anti-virus software, users should be very careful while downloading files from internet or mails, because that may contain some malicious virus.

Hacking or Intrusion attack

We can use Firewalls and Intrusion Detection, complemented by strong Authentication systems to decide who is allowed to access what and who is allowed to do what. When these are properly implemented, Hackers main tools become useless and thus making our system secure.

Eavesdropping or Sniffing attack

The better way to avoid sniffing attack is Encryption. If sensitive information is encrypted before sending to wires, hackers can't really understand what it is. They need the key to decrypt the information. This way, the information sent over network could always be safe with encryption.

Spoofing attack

Authorization based on strong Authentication will prevent people from spoofing a user with desired privileges.

Man in Middle attack

Such attacks are completely defeated if an authentication phase is used and cryptographically tied to the communication system.

Trap Door attack

It is very difficult to implement operating system controls against Trap Doors, so the Entry points should be handled carefully by the programmers and should only be known to programmers who are trustworthy.

Logic Bomb

To prevent such attacks, it is always better to conduct a vulnerability test before releasing systems for operation and also keep backups to correct any damage caused by the logic bomb.

Bacteria

There is as such no way of preventing them. As they do not harm a system but can eat up CPU utilization time, so therefore to prevent them from eating up the resources one should try and make sure not to execute any useless or an unknown file.

Social Engineering

One should not come under any Influence Socially or be fooled by any one which may result in revealing critical information to the Hacker.

CONCLUSION

In this paper we discussed the main goals of information security and developed an understanding of Information Availability and its components. We also identified some important threats to Information security which Affect Information Availability and presented some countermeasures to prevent them. These Threats represent complex challenges to protect the information, and Systems that process, transport, and store it. With such a great risk to Information and the dependence of organizations on Information, proper steps should be taken to ensure the Availability of Information and its critical resources.

REFERENCES

[1] Andrew P. Martin & Deepak Khazanchi, 2006, Information Availability and Security Policy.

[2] Brinkley,D. L. & Schell, R. R. (1995). Concepts and terminology for computer security.

[3] M. D. Abrams, S. Jajodia & H. J. Podell Information security: An integrated collection of essays, 11-39. Los Alamitos, CA: IEEE Computer Society Press.

[4] CERT. Denial of Service Attacks. "http://www.cert.org/techtips/denialofservice.html" 1997.

[5] Hosmer, H. (1993). Security is fuzzy! Applying the fuzzy logic paradigm to the multi-policy paradigm. Proceedings of the 1992-1993 ACM SIGSAC New Security Paradigms Workshop, USA, 175-184.

[6] Howard B. , O. Paridaens, , B Gamm, 2001, Information security: Threats and protection Mechanisms.

[7] John Peter Jesan, 2005, Threats to Information Security, Nova South-eastern University

[8] Lampson,B. W. (1971). Protection. Proceedings of the 5th Annual Princeton Conference on Information Sciences and Systems, USA.

[9] Linda Pesante , "Information Security Basics" 2008 Carnegie Mellon University.

[10] Lipson, H. F. & Fisher, D. A. (1999). Survivability-A new technical and business perspective on security [Electronic version]. Proceedings of the 1999 workshop on new security paradigm, Canada, 33-39.

[11] Marek Ostaszewski Denial of Service attacks: analysis and countermeasures

[12] Michael E. Whitman, 2003, Enemy at the gate: Threats to Information Security.

[13] Michael E.Whitman and Herbert J. Mattord, "Principles of Information Security", Vikas Publishing house.

[14] Parker, D. B. (1992). Restating the foundation of information security. Proceedings of the Eighth International Conference on Information Security, Netherlands, 139-151.

[15] Pier Luigi Rotondo, Denial of Service (DoS) attacks and countermeasures.

[16] Quey-Jen Yeh , Arthur Jung-Ting Chang, 2007, Threats and countermeasures for information system security: A cross-industry study.

[17] Reibman, A. L. & Veeraraghavan, M. (1991). Reliability modeling: An overview for system designers [Electronic version]. Computer, 24(4), 49-57.

[18] Sandu, R. (1996). Access control: The neglected frontier Electronic version. Proceedings of the first Australasian conference on information security and privacy, Australia, 219-227.

[19] Tryfonas, T., Gritzalis, D. & Kokolakis, S. (2000). A qualitative approach to information availability. Proceedings of Information Security for Global Information Infrastructures. IFIP TC11. Sixteenth Annual Working Conference on Information Security, USA, 37-47.

[20] Wikipedia, Information Security, 2010 "http://en.wikipedia.org/wiki/Information_security"

[21] Wikipedia, Denial of Service, 2010 "http://en.wikipedia.org/wiki/Denial _of _Service"

[22] William Stallings, "Network Security Essentials", Pearson Education.

[23] Wood, A. (1995) Predicting client/server availability [Electronic version]. Computer, 28(4), 41-48.

