ISSN: 2277-9655
Impact Factor: 4.116

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

COMPUTER SECUIRTY WITH COMPUTER PROTECTIONAND NETWORK MANAGEMENT

Smt Ambikatai V Mittapally*

* MTech (CSE), Mie Lect Information Technology, Government Polytechnic Solapur, Maharashtra, India

DOI: 10.5281/zenodo.56880

ABSTRACT

Computer security, also known as cybersecurity or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them,aswellasfrom disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection,] and due to malpractice by operators, whether intentional, accidental, or due to thembeing tricked into deviating from secure procedures.The field is of growing importance due to the increasing reliance on computer systems in most societies and the growth of "smart" devices, including smartphones, televisions and tiny devices as part of the Internet of Things – and of the Internet and wireless network such as Bluetooth and Wi-Fi.

KEYWORDS: Computer Security, Security Measures, Ids,Security Of Design,Tpms, Secure Operating Systems, Firewall, Click Jacking, Network Security Management.

INTRODUCTION

Network outages, data compromised by hackers, computer viruses and other incidents affect our lives in ways that range from inconvenient to life-threatening. As the number of mobile users, digital applications and data networks increase, so do the opportunities for exploitation.

Importance of cyber security: Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. During a Senate hearing in March 2013, the nation's top intelligence officials warned that cyber attacks and digital spying are the top threat to national security, eclipsing terrorism.

A vulnerability is a system susceptibility or flaw, and many vulnerabilities are documented in the Common Vulnerabilities and Exposures (CVE) database and vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities as they are discovered. An *exploitable*vulnerability is one for which at least one working attack or "exploit" exists.To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of the categories below:

Phishing : Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Clickjacking : Clickjacking, also known as "UI redress attack or User Interface redress attack", is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page. This is done using multiple transparent or opaque layers. The attacker is basically "hijacking" the clicks meant for the top level page and routing them to some other irrelevant page, most likely owned by someone else. A similar technique can be used to hijack keystrokes.

Computer protection : In computer security a countermeasure is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Security measures :A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following**:**

- User account access controls and cryptography can protect systems files and data, respectively.
- Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware- or software-based.

Today, computer security comprises mainly "preventive" measures, like firewalls or an exit procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and can be implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as Linux, built into the operating system kernel) to provide real time filtering and blocking. Another implementation is a so-called physical firewall which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet. Reducing vulnerabilities : While formal verification of the correctness of computer systems is possible, it is not yet common. Operating systems formally verified include but these make up a very small percentage of the market.Cryptography properly implemented is now virtually impossible to directly break. Breaking them requires some non-cryptographic input, such as a stolen key, stolen plaintext (at either end of the transmission), or some other extra cryptanalytic information.Two factor authentication is a method for mitigating unauthorized access to a system or sensitive information. It requires "something you know"; a password or PIN, and "something you have"; a card, dongle, cellphone, or other piece of hardware. This increases security as an unauthorized person needs both of these to gain access.Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Training is often involved to help mitigate this risk, but even in a highly disciplined environments (e.g. military organizations), social engineering attacks can still be difficult to foresee and prevent.It is possible to reduce an attacker's chances by keeping systems up to date with security patches and updates, using a security scanner or/and hiring competent people responsible for security. The effects of data loss/damage can be reduced by careful backing up and insurance.

Security by design : Security by design, or alternately secure by design, means that the software has been designed from the ground up to be secure. In this case, security is considered as a main feature**.**
Some of the techniques in this approach include:

- The principle of least privilege, where each part of the system has only the privileges that are needed for its function. That way even if an attacker gains access to that part, they have only limited access to the whole system.
- Automated theorem proving to prove the correctness of crucial software subsystems.
- Code reviews and unit testing, approaches to make modules more secure where formal correctness proofs are not possible.
- Defense in depth, where the design is such that more than one subsystem needs to be violated to compromise the integrity of the system and the information it holds.
- Default secure settings, and design to "fail secure" rather than "fail insecure" (see fail-safe for the equivalent in safety engineering). Ideally, a secure system should require a deliberate, conscious, knowledgeable and free decision on the part of legitimate authorities in order to make it insecure.

Security architecture : The Open Security Architecture organization defines IT security architecture as "the design artifacts that describe how the security controls (security countermeasures) are positioned, and how they relate to the overall information technology architecture. These controls serve the purpose to maintain the system's quality attributes: confidentiality, integrity, availability, accountability and assurance services".Techopedia defines security architecture as "a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible." The key attributes of security architecture are: the relationship of different components and how they depend on each other.

- the determination of controls based on risk assessment, good practice, finances, and legal matters.
- the standardization of controls.

Hardware protection mechanisms :

While hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process,[65][66] hardware-based or assisted computer security also offers an alternative to software-only computer security. Using devices and methods such as dongles, trusted platform modules, intrusion-aware cases, drive locks, disabling USB ports, and mobile-enabled access may be considered more secure due to the physical access (or sophisticatedbackdoor access) required in order to be compromised. USB dongles are typically used in software licensing schemes to unlock software capabilities,[67] but they can also be seen as a way to prevent unauthorized access to a computer or other device's software. The dongle, or key, essentially creates a secure encrypted tunnel between the software application and the key. The principle is that an encryption scheme on the dongle, such as Advanced Encryption Standard (AES) provides a stronger measure of security, since it is harder to hack and replicate the dongle than to simply copy the native software to another machine and use it. Another security application for dongles is to use them for accessing web-based content such as cloud software or Virtual Private Networks (VPNs).] In addition, a USB dongle can be configured to lock or unlock a computer.

- Trusted platform modules (TPMs) secure devices by integrating cryptographic capabilities onto access devices, through the use of microprocessors, or so-called computers-on-a-chip. TPMs used in conjunction with server-side software offer a way to detect and authenticate hardware devices, preventing unauthorized network and data access.[70]
- Computer case intrusion detection refers to a push-button switch which is triggered when a computer case is opened. The firmware or BIOS is programmed to show an alert to the operator when the computer is booted up the next time.
- Drive locks are essentially software tools to encrypt hard drives, making them inaccessible to thieves.[71] Tools exist specifically for encrypting external drives as well.
- Disabling USB ports is a security option for preventing unauthorized and malicious access to an otherwise secure computer. Infected USB dongles connected to a network from a computer inside the firewall are considered by the magazine Network World as the most common hardware threat facing computer networks.[73]
- Mobile-enabled access devices are growing in popularity due to the ubiquitous nature of cell phones. Built-in capabilities such as Bluetooth, the newer Bluetooth low energy (LE), Near field communication (NFC) on non-iOS devices and biometric validation such as thumb print readers, as well as QR code reader software designed for mobile devices, offer new, secure ways for mobile phones to connect to access control systems. These control systems provide computer security and can also be used for controlling access to secure buildings.[74]

Secure coding

In software engineering, secure coding aims to guard against the accidental introduction of security vulnerabilities. It is also possible to create software designed from the ground up to be secure. Such systems are "secure by design". Beyond this, formal verification aims to prove the correctness of the algorithms underlying a system; important for cryptographic protocols for example.

Capabilities and access control lists

Within computer systems, two of many security models capable of enforcing privilege separation are access control lists (ACLs) and capability-based security. Using ACLs to confine programs has been proven to be insecure in many situations, such as if the host computer can be tricked into indirectly allowing restricted file access, an issue known as the confused deputy problem. It has also been shown that the promise of ACLs of giving access to an object to only

one person can never be guaranteed in practice. Both of these problems are resolved by capabilities. This does not mean practical flaws exist in all ACL-based systems, but only that the designers of certain utilities must take responsibility to ensure that they do not introduce flaws.

Capabilities have been mostly restricted to research operating systems, while commercial OSs still use ACLs. Capabilities can, however, also be implemented at the language level, leading to a style of programming that is essentially a refinement of standard object-oriented design. An open source project in the area is the E language.

Response to breaches

Responding forcefully to attempted security breaches (in the manner that one would for attempted physical security breaches) is often very difficult for a variety of reasons:

- Identifying attackers is difficult, as they are often in a different jurisdiction to the systems they attempt to breach, and operate through proxies, temporary anonymous dial-up accounts, wireless connections, and other anonymising procedures which make backtracing difficult and are often located in yet another jurisdiction. If they successfully breach security, they are often able to delete logs to cover their tracks.
- The sheer number of attempted attacks is so large that organisations cannot spend time pursuing each attacker (a typical home user with a permanent (e.g.,cable modem) connection will be attacked at least several times per day, so more attractive targets could be presumed to see many more). Note however, that most of the sheer bulk of these attacks are made by automated vulnerability scanners and computer worms.

NETWORK SECURITY MANAGEMENT

- Network security management is a complex process for managing and controlling which requires knowledgeand experience. Ariyapperuma et al. (2005) state that the demand for trained network security professionals hasincreased regularly due to the wide range of attacks on computer network. Therefore, network securitytechnology plays an important role for protecting all types of sensitive information and network resources.
- Thereare two types of data encryption, which currently use to protect the information between computer networks:
- Cisco Encryption Technology (CET) and Internet Protocol Security (IPSec).

CISCO ENCRYPTION TECHNOLOGY (CET): ROUTER TO ROUTER

- Packet filtering devices such as routers, firewall systems and encryption are important components of networklayer access control (Guttman et al., 2003). This also includes a network data encryption mechanism, which isprovided at the network layer (layer 3), and it can be encrypted. An IP packet is encrypted and decrypted only if*Proceedings of The 5th Australian Information Security Management Conference*the packet meets criteria that have been established, and the configuration of a router for encryption is set. Theactual encryption and decryption of IP packets takes place only at routers that are used to configure CET (CiscoSystems, 2003). The routers themselves are considered to be peer-encrypting routers while intermediate hops donot participate in the encryption and decryption process

Actual text or clear text, not encrypted, traffic that enters a peer router from the secure network side, is encrypted, and then forwarded across the unsecured network. When the encrypted traffic reaches the remote peer router, the router decrypts the traffic before forwarding it into the remote secure network. IP Packets are encrypted between the original router's outbound interfaces and decrypted at the terminal peer router's inbound interface (Cisco Systems, 2003). Encryption provides the use of a hidden transformation that requires a secret key to encrypt and to reverse the process (decrypt). However, some encryption methods can use the same key to both encrypt and decrypt the data. In encryption, there are two keys: one key to encrypt and another different one to decrypt which are referred to as asymmetric encryption. In an asymmetric encryption, one of the two keys is publicly known and the other is kept secret (Pike, 2002).

For the duration of the setup of every encrypted session, both participating routers try to validate each other. If both authentications fail then the encrypted session will not be established, and no encrypted traffic will pass.

Both authentications guarantee that they know each other in terms of trusted routers exchanging encrypted traffic, and prevent routers from being tricked into sending sensitive encrypted traffic to illegitimate destination routers (Cisco Systems, 2003).

INTERNET PROTOCOL SECURITY (IPSEC): ROUTER TO ROUTER

In the context of the OSI reference model, there are several strategic methods whereby an encryption mechanism may be applied. An IPSec is a framework of protocols, and the Internet Engineering Task Force (IETF) developed it. The protocols provide security for IP packets and any upper-layer protocol that uses IP services (SANS Institute, 2001).

IPSec provides security for the transmission of sensitive information over unprotected networks which acts at the network layer (Layer 3) by protecting and authenticating IP packets between participating IPSec devices, for instance, Cisco routers (Cisco Systems, 2002a; Pike, 2002). Network security services with IPSec are provided as optional services. These services are:

Data Confidentiality: the IPSec sender will encrypt packets before transmitting them across a network

Data Integrity: the IPSec receiver will verify packets sent by the IPSec sender to ensure that the data has not been changed during communication

Data Origin Authentication: the IPSec receiver will authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service

Anti-Replay: The IPSec receiver can identify and reject replayed packets.

CONCLUSION

Now that you have completed this webquest on Computer Security you are now aware of the possible security treats to computer systems. Not only that, but you are now better able to protect your computers as well as recommend security measures to others.Have you ever heard the terms Computer Virus, worms, Trojans, Cybercrime, hackers?Putting your computer in a bank vault with security officers with shot guns and Rin-tin-tin will not protect your computer's data.. It is therefore relatively simple to verify and validate firewall and protocol operation –an essential aspect of network management and fault diagnosis.

REFERENCES

[1] *Gasser, Morrie (1988). Building a Secure Computer System (PDF). Van Nostrand Reinhold. p. 3. ISBN 0-442-23022-2. Retrieved 6 September 2015.*
[2] **Jump up^** *"Definition of computer security". Encyclopedia. Ziff Davis, PCMag. Retrieved6 September 2015.*
[3] **Jump up^** *Rouse, Margaret. "Social engineering definition". TechTarget. Retrieved6 September 2015.*
[4] Veal, D. (2003) An investigation into computer and network curricula, Ph.D. dissertation, Edith Cowan University, Perth, Western Australia.