INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Review Paper on Security Measures for a System

Ankita Dongre[1], Trupti Kamthankar[2], Suvarna Baviskar[3], Akash Sharma[4]

[1] Asst. Professor, [2,3,4]Student
[1] G. S. Mandal's, Marathwada Institute Of Technology,
[2,3,4] G. S. Mandal's, Marathwada Institute Of Technology
Beed Bypaas Road, Aurangabad, Pin no.431028
[1]ankita.dongre@gmail.com, [2]tgkamthankar@gmail.com,
[2]suvarna22kar30@gmail.com, [2]akash.sharma305@gmail.com

***Abstract**: Security systems are constantly being a threat to ethical hackers; In today's scenario, it is very crucial task to manage the security for various system components. This paper gives a deep insight towards every aspect of system consider system software, system hardware & system database. Apart from the core security techniques provided to the system, the security can also be a matter of organization policies and communications. With hardware implementation the issues regarding security techniques can also be addressed using real time systems with every system in network connected to each other directly or indirectly. The authentication and maintaining confidentiality to your raw data information is a high priority culture in every organization. Studying this paper with implemented solutions in various application areas could be a great summary for security technique provided to the system in today's era of technology.*

***Keywords:** Authentication, access control, login policies.*

1. INTRODUCTION

Computer System's are protected by the use of special hardware & software, policies and practices against data corruption, destruction, interception, loss, or unauthorized access. Five essential services provided by a secure system are Authentication, Authorization, Integrity, Privacy and Non-repudiation. So we can use security measures like use a strong password, Protect confidential information, Make sure our operating system and virus protection are up-to-date, Use secure and supported applications, Beware of suspicious e-mails, store confidential information only on HSU servers, backup our data and make sure we can restore it, protect information in all its forms, learn to be security aware [1]. The security is provided to any kind of system by using three measures as Software Security, Hardware Security and Database Security which conceptually shown as follows:

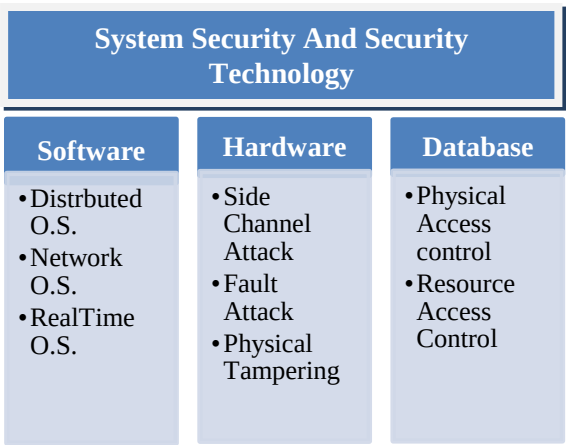

Figure 1: System Security Framework

2. SOFTWARE SECURITY

Software security is an idea implemented to protect software against malicious attack and other hacker risks so that the software continues to function correctly under such potential risks. Security is necessary to provide integrity, authentication and availability [2].

Basically there are two types of software's: System Software and Application Software. The security is provided by both kinds. The primary software security is provided by the operating system. So we performed analysis on various categories of operating systems for security issues and techniques.

2.1 Distributed System

The security components in distributed system are authentication, authorisation, access control and encryption by using protocols as Needham-Schroeder protocol, Kerberos protocol, and SSL protocol and for enterprise security policy: BS7799 framework. The security components of distributed systems are: security authentication, authorization, access control and encryption.

Authentication:- Generally, authentication is done by hardware which is pocket sized device or credit card which create password known as "SMART TOKEN" and transfer it to authentication server which is linked up to the network.

Authorization:- This is used to supply secure access point which enabling the users to linked up to the network once and also allow them access authorized resources. So, it can be done by software servers to prove client's identity to the authentication server by using another party rendering the services.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

Encryption:- This can be implemented by using RSA, PGP, DES like implicate algorithms which uses public and private key system.

Access Control:- This can be implemented by access matrices, access lists, capabilities lists which define access authorization to the computer resources for the user [3]. Most consumers do not have skills to evaluate a system for security. So, there is need of standard schemes for user's assurance. So the standards used are: US orange book Criteria, German Green Book, UK Criteria, European IT Security Evaluation Criteria (ITSEC) and many more. Also we are sending information across network by employing cryptography to secure the content and digital signature to verify the originator's identity [4].

2.2 Network Operating System

In general term "Network Security" means private communication in public world[5]. In network operating system based on different vendors of operating system working functionalities and vulnerabilities changes. According to their architecture: Login security, Trustees, High level security like physical access control, use of ACL Editor to set restrictions, restrict FTP access, and install password shadowing. As in the case of Netware, Novell directory services, vulnerabilities like Remote Console(R CONSOLE), Standard and default accounts, FAT Editing, Bindery reset on reboot and Delete files which contain security system. In Windows NT Local security authority, Security account manager and Reference monitor are used. Windows NT registry and security level settings i.e.1. Minimal-Antivirus software, Defrag and Disc scan 2.Standard-Establish and enforce policies, use of NTFS, protecting registry and general login services.3.High-Restricting FTP access and ACL, Registry keys, Event log and system auditing. In UNIX console security, installation media and configurations plays important role[6]. Major possibilities of attacks like Passive, Active, Distributed, Insider, Close-in, Fishing, Hijack, Spoof, Buffer overflow, Exploit, password attack are there[7].

2.3 Real-Time/Embedded Operating System

Real Time operating system is widely used for platforms ranging from embedded devices to sophisticated electronic devices (Aircraft). Classification can be done in four catogories: Monolithic, microkernel or nanokernel, hybrid and exokernel. The architecture of each category is different. Monolithic kernel is suitable for less complex platform such as embedded system where as Microkernel have multiple loosely coupled modules with high cohesion. Nanokernel or picokernel is a initial stage of microkernel where nano or pico represents control of computer clock, response time to a process. The exokernel accelerate the throughput of hardware. It also separates protection by dividing responsibilities. Using library operating system it provides mechanism to access low level resources. Hybrid kernel (Micro and Macro) it provides multiple interfaces to support other kernel running on the top of this hybrid kernel so it can be called as hypervisor. It provide resource sharing and hardware abstraction between kernels[8].

Secure partition guarantees to fully protect the operating system and user tasks from malicious code like denial-of-service attacks, worms, and Trojan-horses and each task of the resource needs to run correctly. The security level assessment techniques used in embedded real-time systems can control objects or computer program dialogue to work together for system hardware work more effectively. It can identify and prevent malicious code to explore system defect [9].

3. HARDWARE SECURITY

Neural network contains large number of interconnected processing elements and these elements work simultaneous to solve a specific problem.

Today, semiconductor chips are used to control systems and also to protect from security threats. Hardware devices like semiconductor chips often store private keys and other sensitive data used for the protection of the actual data is as important because direct theft. Even if totally secure algorithms and protocols are used, the intruder may be able to get secret data due to the implementation of hardware also they can be able to disrupt the hardware or service leading to failures in security system.

Attackers may aim at: learning the secrets, without studying private information taking advantage of victim hardware, harm to services and normal operation.

The hardware attacks are of basically three types:

- **Side-channel attacks**

It refers to information provided by the hardware. While performing normal computations, these can be carried out on unmodified hardware. e.g., time delays, power consumption and sound, electromagnetic and infrared radiations. In Timing attacks, attacker tries to find out the private key of any cryptographic algorithm which is time consuming process. In SPA attacks, the attacker observes current consumption and directly applies it to specific cryptographic processing. Electromagnetic analysis: In EM attacks, the attacker can attack the hardware from far or near.

- **Fault Attacks**

The attacker can easily attack on hardware fault and it may overlap with physical tampering. E.g. supplying noisy power or clock signals, incorrect voltage, excessive temperature, or high radiations of rays, laser etc.

- **Physical Tampering**

To carry out such attacks more expensive equipments are required. The system security can be reduced dramatically by revealing bits stored in EEPROM memory.

Cryptographic algorithms like RSA algorithm, Diffie-Hellman, CRT are may get affected through fault attacks. It involves access to chip internals memory, registers, etc. The

security to hardware can be provided by authentication using biometrics, fingerprint scanners, voiceprints, etc[10]

4. DATABASE SECURITY

Database may be extremely confidential or less but needs to protect from unauthorised access of users and other forms of security are needed. The organizations which provide the database systems like TERADATA, oracle, Access, Postgress itself provide some security. To maintain security the controls like Access restrictions on devices and software's, system auditing of security, its policies.

To secure database the authentication methodologies used are:

Hardware Security: Physical Access Control

In this we can control the access to physical components of the system. The primary consideration in this is establishing a security policy. Controls need to be applied in the areas where the devices/machines are kept, no access to unknown devices and by controlling access to operating systems either in person or remote.

Software Security: Resource Access Control

- Controlling access to RDBMS
  In this the login process is provided to the users by providing login ID/username and password. The general features include: User identifiers (user names), Channel or LAN identifiers (host, or client identifiers), Logon policies, Password control, User security interface, Client security.
- Controlling Data Access
  In this access rights statements like Grant and Revoke are given to a user by DBA.
  i. Automatic Rights: This means that the system automatically grants to the creator of a database, user, or object, and to a newly created user or database.
  ii. Implicit Rights: These are also called ownership rights that are implicitly granted to the immediate owner and to all indirect owners. The GRANT and REVOKE statements are used for explicit rights[11].

For any category, authentication (PAM) and access control by using UID (user identifier's) and GID (group identifier's) is focused whether Linux or Windows XP operating system (by default, it uses Kerberos for authentication & LSAAS for implementation of security policy) [12] and from the database vendors point of view, in addition to authentication, authorization, access restrictions, security policies and auditing and monitoring the database is done [13]. Third parties are in the market with software's which manages vulnerabilities for databases in the network of organization. Also, there is software which monitors database activities and helps auditors to implement secure policies and protect critical data even in cloud or virtual environments [14].

5. APPLICATIONS

There are various application areas where system security and security technologies are used. Now-a-days we can find the systems which can be maintain secure using security technologies. The use of secure RTOS software and related embedded computing security software tools are using mostly because of security threats and concerns. There is also need of information security, so they need support for open standards, safety certifications, security features, and virtualization. Some of them listed below:

1) Defence:- In it security is most important part, so that can be achieved in portable workstations, network needs, mobile networking, ground vehicles, manned and unmanned avionics[15].
2) Share Market:- In it data compression techniques for predicting stock markets behaviour which is accepted in market models in finance which are applicable to technical analysis, portfolio theory and non-linear market models[16].
3) NASA:-NASA's monitoring programme bundles security by providing IP address management (IPAM) for inventory management; Active Directory Group Policy Objects (AD-GPO) for configuration management; Vulnerability Management (VM) for which augments and supports inventory management. Patch Management (PM) is useful for software management, Operating System inventory and custom builds, Antivirus (AV) logs can also provide really good information on malware vectors into the environment [17].

6. CONCLUSIONS AND FUTURE WORK

This paper reviews the overall system security technologies and measures by briefly considering the aspects of hardware, software and databases. Also, today's application areas of these technologies implemented which precisely describing the security measures taken into consideration and support from the third parties.

7. ABBREVATIONS

ACL: Access Control List
SPA: Simple Power Analysis
CRT: Chinese Remainder Theorem
PAM: Pluggable Authentication Modules
LSAAS: Local Security Authority Subsystem Service

References

[1] www.businessdictionary.com
[2] Techopedia.com
[3] Adi Armoni (Tel-Aviv University ,Israel) Data Security management in Distributed computer system
[4] Prof. Steve Wilbur MSC in data communication

network and Distributed system, USL Distributed System Security, O.S. and Enterprise system.

[5] www.cs.columbia.edu

[6] csc.columbusstate.edu/summers/notes/cs459/ch6.html

[7] Computernetworkingnotes.com/network-security-Access-list-standards-and-extend/types-of-attack.html

[8] www.academia.edu/3100193/trusted_real_time_operating_system_identifying_its_characteristics

[9] Link.springer.com/chapter/ten.1007%2F978_3_642_23324_1_66#page_1

[10] www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.pdf

[11] Jem Berkes, University of Waterloo:Hardware Attacks on Cryptographic Devices Implementation Attacks on Embedded Systems and Other Portable Hardware

[12] Operating System Concepts 8th edition – By Silberschatz, Galvin, Gagne.

[13] http://docs.oracle.com/cd/B19306_01/server.102/b14220/security.htm

[14] http://www.mcafee.com/in/products/database-security/index.aspx

[15] http://www.militaryaerospace.com/articles/2012/03/embedded-real-time-operating-system-software-secures- military-mission-critical-data-from-growing-threats.html

[16] Ieeeexplore.ieee.org/xpl/freeabs.all.jsp?arnumber=305914&abstractaccess=no&uusertype=inst

[17] NASA-Continuous-Monitoring-Programme.pdf-Continuous risk management_070410_jld.pptx