International Journal of Computer Science
and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 6, Issue 1, Dec - Jan 2017; 35-42
© IASET

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

COMPUTER SECURITY IN THE HUMAN LIFE

MUDASSIR KHAN

College of Science & Arts Tanumah, King Khalid University, Saudi Arabia

ABSTRACT

After working many years on the computer security, I have seen most of the systems in service extremely vulnerable to attach. Actually installing security on the system is very expensive, that's why peoples are far away from this according to my experience. Since there's been small damage, people decide that they don't want much security. Security is playing crucial role in their life, but it is very difficult to have security on all the systems. Nowadays peoples are thinking towards security, because without security, very difficult to make daily transactions.

KEYWORDS: Security, Network Security Model, Network Security Life Cycle

INTRODUCTION

Peoples have been working on Computer Security for at least 30 years. During this time span, we have much success on the field of Computer Security. During these year's computer security reached at high level, but we have some issues and attacks besides on security. If we considered online transaction security has many issues. Nowadays security becomes important aspect in the human life without security it's very difficult to survive in this world.

What is Security?

Life would be great if we could all exchange information freely and never worry about any malicious intent, stealing of our information. However, we do not live in a perfect world, so we should focus about the safety and security of any data or information flowing across any network.

Day by day we are dependent on the Internet to manage our bank accounts, our medical records, and our credit card payments; we need to protect this valuable information. This means we must turn to network security.

What is the reality of security in human life?

The field of network security was form with the purpose of designing security methods to protect our most valuable assets from the cyber criminals.

If human in their real life entrust to network security, then we have three solutions; consisting of hardware, software and physical security methods used to combat any security threat. In all the devices such as routers, IDS's and firewalls are hardware devices used within a network to add security to its all users.

Anti-virus software and Virtual private network (VPN's) are some of the software tools used to add additional protection for any network.

The most secure networks in the real world will have combined with hardware, software and physical security methods together; finally these methods will provide any kind of protection protection to all users of any network.

Computer security, also known as cyber **security** or IT **security**, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them.

How people can live with such poor security in this real world system? The reason behind the real world security is not about to perfect gateways against determined attackers. Instead, it’s

- value,
- locks, and
- Punishment.

What is wrong with perfect securities? Because, security cost is too much. It’s very difficult to have secure systems in the human life. For security, there is a proper way to protect personal belongings against direct attackers, keep them in a safe deposit box. After many years of experience, banks have learned how to use time locks, alarms, and multiple keys to make these boxes quite secure. Finally as a result, people use them only for things that are seldom needed and either expensive or hard to replace.

Examples of Network Security

Firewalls

The basic and easily implemented method of network security is the firewall. A firewall can be software based, provided by windows, or hardware based, such as a router. The main idea behind a firewall is to allow authorized access to a computer while blocking unauthorized access. This is accomplished by configuring access conditions depends on user defined rules, IP addresses, and port accessibility.

VPN's: Virtual Private Networks

VPN's are used to establish an encrypted connection across a network while using the Internet as its transmission medium. A VPN uses the Internet, which is already in place. The benefit of VPN is that a secure data connection is established. VPN connection software encrypts the data being sent between one place and another. This is known as tunneling.

IDS: Intrusion Detection System

Intrusion Detection Systems consist of a combination of both hardware and software and work in conjunction with an existing firewall. IDS units are used to detect an intrusion threat to a computer system. IDS configurations use data analysis algorithms to compare data packet construction and frequency to established packet content definitions. If the packet construction observed does not match the packet construction expected, when compared to previously configured definitions, an alert is signified. Depending on the configuration of the IDS, the observed traffic is either blocked or let through to be marked for observation at a later date.

OVERVIEW OF COMPUTER SECURITY

Computer security based on confidentiality, integrity, and availability. The clarification of these three aspects varies, as they arise. The clarification of quality in a given environment is directed by the needs of the individuals, customs, and laws of the particular organization.

Confidentiality

Confidentiality is the secretion of information or resources. The need for having information secret arises from the use of computers in delicate fields such as government and industry. For example, military and public institutions in the government restrict access to information to those peoples are in need of that information. For example, all types of institutions keep personnel records secret.

Integrity

Integrity refers to the determination of data or resources. It is used in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called *authentication*).

Availability

Availability is the ability to use the information or resource needed. Availability is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all.

Security Threats and Attacks

- A threat is a *potential* violation of security.
- An attack is any *action* that violates security.
- An attack has an implicit concept of "intent"

Security Policy and Mechanism

- Policy: a statement of what is, and is not allowed.
- Mechanism: a procedure, tool, or method of enforcing a policy.
- Security mechanisms implement functions that help *prevent, detect, and respond to recovery from* security attacks.
- Security functions are typically made available to users as a set of security services through APIs or integrated interfaces.
- Cryptography underlies many security mechanisms.

Implementing Security

The implementation of security has two parts: the code and the setup/configuration. The code is the programson which security depends. The setup is whole data that controls the operations of these programs: folder structure, access control lists, group memberships, user passwords or encryption keys, etc.

The job of a security implementation is to defend against vulnerabilities. These take three main forms:

- Authenticating
- Authorizing

- Auditing

Every government entity or private enterprise business generally has a security plan in place which utilizes numerous types of controls to reduce or attempt to eliminate the adverse effects coming from security risks to their operations. For the most part there are three basic types of controls in use:

- **Technology** – software and hardware used to address internal and external threats to the security of the organization.
- **Process** – policies, processes, and practices to address vulnerabilities and to reduce security risks while establishing baseline standards of secure operations.
- **Ignore** the vulnerability and threat

NETWORK SECURITY MODEL

The network security model is based on Open system Interconnection model (OSI), developed in 1983 by the International Organization for Standardization (ISO). Same like OSI model, Network security model is a seven layer model that divides the daunting task of securing a network infrastructure into seven manageable sections. This model is generic and can be applied on all security implementation and devices. When an attack on a network has succeeded it is much easier to locate the specific issue and fix it with the use of Network Security Model. The Network Security Model is divided into seven layers are as follows.

- Physical
- VLAN (Virtual Local Area Network)
- ACL (Access Control Lists)
- Software
- User
- Administrative
- IT Department

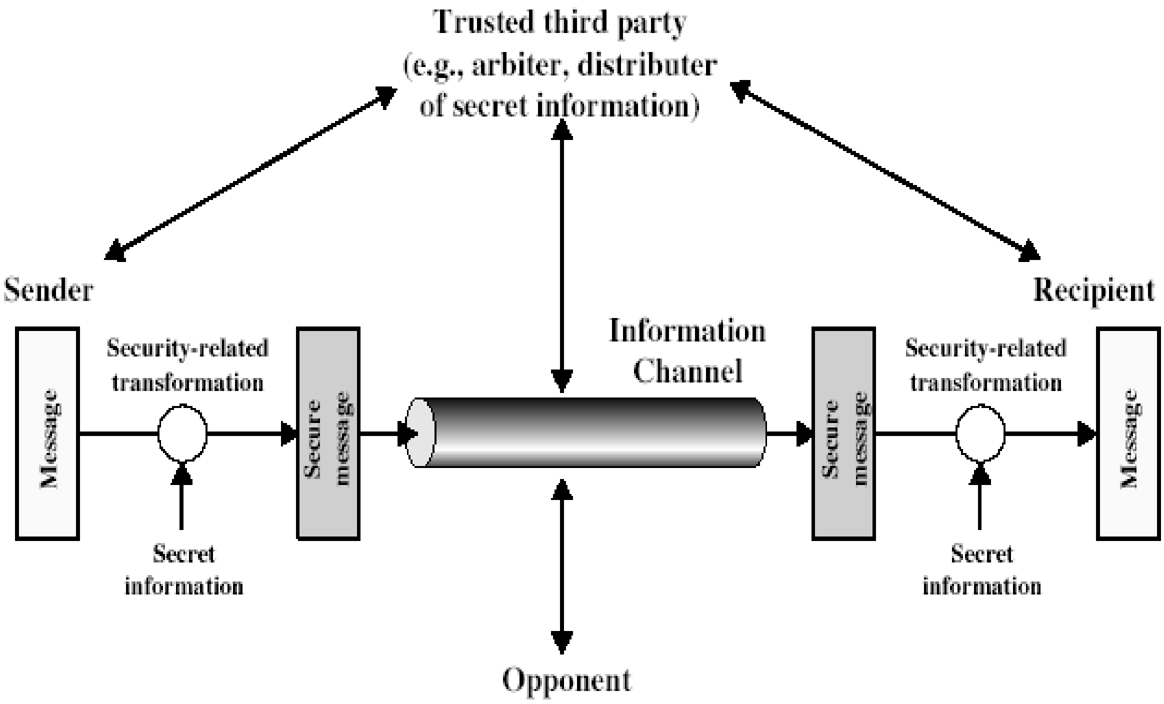

Figure 1: Model of Network Security

Why do we Need a Network Security Model?

The NSM will give the security community a way to study, implement, and maintain the network security that can be applied to any network. In addition we can say that, it can be use as a security tool. NSM provides the basic structure. It provides the new professionals with the knowledge to discover what has been implemented and what has not been implemented from a security stand point.

The Security Life Cycle

If the network security model has been implemented: a network security professional can begin a network security life cycle. The life cycle should contain checks and balances to make sure that all the layers are in secure state. The life cycle should begin with the technical standpoint. This means that the network security professional should focus at the current network security model to find any problem occurs or needful improvement to be done. The network security model should be tested periodically by a penetration test in order to find any exploits.

- Threats
- Policy
- Specification
- Design
- Implementation
- Operation and maintenance

CONCLUSIONS

After having the overview of security, I have concluded the basic ideas of computer security: secrecy, integrity, and availability, Implemented by access control based on the standard of authentication, authorization, and auditing. We discussed the reasons why it doesn't work very well in practice:

- Complexity in the code and especially in the setup of security, which overwhelms users and administrators.
- The Internet works only because we implicitly trust one another
- It is very easy to exploit this trust
- The same holds true for software

Security is also playing a very important role in the human life in this real world. As they are doing many day to day online transactions like e-commerce, banking, credit/debit card transactions, and many more transactions. We can say that the human life is surrounded by technology and they are totally dependent on this. For these daily life transactions we need a secure environment in the technologies used by human. The questions arises, are all the daily life transactions are 100 % secure. The answer is no, all the systems and technologies used by different companies and organizations are not 100 % secure. They are providing security but not at final level. That's why we have number of cyber crimes and attacks on day to day transactions. But another truth of human life in spite of less security their life is based on technologies or we can say smart world.

REFERENCES

1. Abadi and Needham, Prudent engineering practice for cryptographic protocols. *IEEE Trans. Software Engineering***22**, 1 (Jan 1996), 2-15, dlib.computer.org/ts/books/ts1996/pdf/ e0006.pdf or gatekeeper.dec.com/pub/DEC/SRC/research-reports/abstracts/src-rr-25.html
2. Anderson, Why cryptosystems fail. *Comm. ACM***37**, 11 (Nov. 1994), 32-40, www.acm.org/pubs/citations/ proceedings/commsec/168588/p215-anderson
3. Bell and LaPadula, Secure computer systems. ESD-TR-73-278 (Vol. I-III) (also Mitre TR-2547), Mitre Corporation, Bedford, MA, April 1974
4. CERT Coordination Center, CERT advisory CA-2000-04 Love Letter Worm, www.cert.org/advisories/CA-2000-04.html
5. Clark and Wilson, A comparison of commercial and military computer security policies. *IEEE Symp. Security and Privacy* (April 1987), 184-194
6. Denning, A lattice model of secure information flow. *Comm. ACM***19**, 5 (May 1976), 236-243
7. Eastlake and Kaufman, *Domain Name System Security Extensions*, Jan. 1997, Internet RFC 2065, www.faqs.org/ rfcs/rfc2065.html
8. Ellison et al., *SPKI Certificate Theory*, Oct. 1999, Internet RFC 2693, www.faqs.org/rfcs/rfc2693.html
9. Cisco Systems. (1998) IP security and encryption overview, URL

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scencove.htm, Accessed 20 April 2007

10. Cisco Systems. (2007b) Academy connection, URL http://www.cisco.com/web/learning/netacad/index.html, Accessed 25 March 2007
11. Barnett, M., MaKinster, J. G., & Hansen, J. A. (2001) Exploring elementary students' learning of astronomy through model building, URL http://inkido.indiana.edu/mikeb/portfolio/papers/VSS_barnett_hansen_McKinster.pdf, Accessed 9 March 2007
12. Maj, S. P., &Kohli, G. (2004) A new state models for internetwork technology, Journal of Issues in Informing Science and Information Technology, 1, 385 – 392, URL http://proceedings.informingscience.org/InSITE2004/062maj.pdf, Accessed 5 April 2007
13. Sisler, E. (1999) System administration: CLI or GUI, URL http://wallace.westminster.lib.co.us/linux/cli-vsgui.html, Accessed 26 May 2007
14. Wool, A. (2004) The use and usability of direction-based filtering in firewalls, Computer & Security, 23(6), 459-
15. Pike, J. (2002) Cisco network security. New Jersey: Prentice-Hall, Inc.

AUTHORS DETAIL

Mudassir Khan, Assistant Professor, College of Science & Arts Tanumah, King Khalid University, Saudi Arabia, Nationality: Indian