DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4641

ISSN No. 0976-5697

Volume 8, No.8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

NETWORK THREATS, ATTACKS AND SECURITY MEASURES: A REVIEW

Ruzaina Khan
M.Tech (CSE)
Department of Computer Science and Engineering
Jamia Hamdard
Delhi, India

Mohammad Hasan
Research Scholar
Department of Agricultural Economics and Business Management, AMU
Aligarh, India

Abstract: Network security has become vital for securing sensitive and confidential information of organizations which is being shared and transferred across global networks. Various studies have explored different aspects of network security and have listed common threats and attacks that have been damaging the networks globally. The methodology adopted in this paper is a review of papers with keywords network security, network attacks and threats and network security measures. The aim of this paper is to critically review the studies on networking security, categorizing various attacks and threats and measures that need to be implemented for protection. The paper also describes various concepts related to security including network security, cryptography and encryption.

***Keywords*:** Network security, Information security, Cryptography, Network threats and attacks, Network security measures

I. INTRODUCTION

Recent advancements in the field of information and technology and competitiveness on real time data have led to an increase in the transmission of data and information globally. As a result the organizations have become more vulnerable to network threats and attacks and are facing invasions in information security and computer networks [1] as the sources of bypassing and breaking through security have increased. The sensitive information being transmitted within the network can easily be accessed by an unauthorized user for malicious purposes [2]. The organizations have been facing interruption, interception, modification and fabrication [3] of their sensitive data from unauthorized sources which break into their security codes. As a result, the information security has become an extremely important aspect in ensuring safe and secured transmission of data through global networks [4].

II. SECURITY

Security has been described as a secure environment which is free from danger posed by adversaries who can afflict harm both intentionally or accidently. Data security has become of the major challenges for business organizations including securing communication channel, encryption techniques and maintaining the databases. With recent advances in technology the networks are no longer safe from attackers and any unprotected system can easily be breached from unauthorized sources with an intention to steal information for malicious purposes. A successful organization needs to implement six kinds of layers of securities namely physical, personal, operational, communication, network and information[2].

III. INFORMATION SYSTEMS

Information system is a combination of hardware and software components which enable personnel working within as well as outside an organization to share and transfer data for useful purposes. With increased cybercrime and hacking, the organizational networks have come under great security threat. Therefore, knowledge, awareness and training is essential for securing the information [3].

IV. NETWORK SECURITY

Network security is a vital component of information technology and can be categorized into four major areas including secrecy, authentication, nonrepudiation and integrity control [5]. It is a concept of securing and protecting network and data transmission from unauthorized users who can use the information for malicious purposes. It focuses on securing variety of networks including both public and private transactions and communications among businesses, government institutions and individuals [2]. Network security has become a major component in the organization structure because the information maintained passes through large number of systems and devices such as computers and routers and becomes very vulnerable to threats and attacks [6]

V. CRYPTOGRAPHY

Cryptography is the art of coding the information in such a way that it becomes difficult for an unauthorized person to capture, disclose or transfer it. It is a science of writing secret code by constructing and managing protocol in order to block the adversaries. It is a vital component of computer and communication network and an emerging technology which protects the information from eavesdropping. The process of securing the information is known as encryption and a secret or disguised way of writing a code is known as a cipher. The encrypted information can be transferred back to its original form by an authorized user who has the cryptographic key. Different kinds of ciphers have been used for encryption namely traditional and modern symmetric key ciphers. Traditional ciphers include substitution and transposition ciphers and DES (Data Encryption Standard) and AES (Advanced Encryption

© 2015-19, IJARCS All Rights Reserved

Standard) come under the category of modern symmetric key ciphers[3], [5], [7].

VI. ENCRYPTION

There are two types of encryptions: symmetric and asymmetric in nature. Symmetric encryptions use single key for encrypting as well as decrypting the code while Asymmetric encryptions work with two keys, public and private for encrypting and decrypting respectively [7].
Below are the top 10 threats which have affected Small and Medium Enterprises Data security. The following table summarizes the details of important threats.

VII. TYPES OF THREATS

Network security is highly threatened by the presence of various threats and attacks that can lead to disclosure of sensitive and confidential information. The basic difference between a threat and an attack is that while threat is a presence of a constant danger to the integrity of information, an attack is an actual act of breaching the security of the network.

Table 1: Network Threats

Threats	***Description***	***Security measures***
Insider attacks	The insider is a part of the organization that has full access and authorization of the network system. The insider can be of malicious or accidental nature and can be a threat to organization's confidentiality and integrity.	Implementing dual control principle helps more than one person to control login credentials for organization's servers.
Lack of contingency	Many organizations suffer due to lack of planning for situations involving bad data failure. As a result they do not have a backup system for restoring the lost data.	Developing sound information assurance methodologies helps develop personalized policies benchmarked from other organizations.
Poor configuration leading to compromise	Many organizations with lack of funds and experience often install networking gear without having skilled personnel to handle them.	Automated vulnerability audit scan is a method which performs check of the entire network and must be conducted at regular basis.
Reckless use of hotel networks and kiosks	Many attackers leave a key logger to access passwords and credential information from personal devices connected in an infected hotel network that are not much protected enough counter such attacks.	Forbidding turning off defenses through certain anti-virus solutions which are configured in such a way that they cannot be turned off without proper authorization.
Reckless use of Wi-Fi hotspots	Similar to key logger in hotel networks, the attackers put up an unsecured Wi-Fi network to capture secured information such as username and passwords of employees without making them aware of any threat to their computer.	Using encrypting connections which can be connected via Virtual Private Networks and encrypts the communication streams preventing eavesdroppers to listen to the data wirelessly.
Data lost on portable device	It is a common problem with most of the users who accidently leave their storage devices such as mobile phones, pen drives or USB stick in hotel rooms, taxis or trains making it easily available for attackers to retrieve sensitive information.	Centralized management of mobile devices through servers and software such as RIM's Blackberry Enterprise Server help the organization ensure encrypted transmissions and are capable of remotely wiping out data of lost devices.
Web server compromise	Poorly written customer application on websites have made easier for the attackers to penetrate thousands of servers with automated SQL injection attacks.	Auditing web app code is a measure which helps the users identify whether the developed code has been performing proper input validation or not.
Reckless web surfing by employees	Various spams, Trojans and viruses penetrate into the organization's network systems when the employees surf websites other than related to their business and end up getting victimized by pool of malware.	Web content filtering such as WatchGuard's WebBlocker which maintains updated URL of blocked websites
Malicious HTML email	This is a common email attack which links the user to a malicious website and triggers a drive-by download by a single click.	Implementation of outbound web proxy which includes setting up of LAN system redirecting all HTTP requests and responses to a web proxy server which monitors all the web traffic.
Automated exploit of a known vulnerability	Such kind of attacks affect the SMEs who are not able to install Windows patches within the same month their release and later on fall prey to attacks in the form of malicious patches.	1. Investing in patch management which maintains the network up to date by scanning the systems and identifying missing patches and software updates

© 2015-19, IJARCS All Rights Reserved

		2. Building an inexpensive test network which helps the organization to simulate a patch by installing it into a test system and studying its behavior.

Source: [8], [9]

VIII. TYPES OF ATTACKS

The networking attacks can be grouped into two major categories namely passive attacks and active attacks. Detailed description of both kinds of attacks is given below.

A. Passive attacks

In passive attacks the attacker eavesdrops or monitors the data transmitted to find the content of data transmitted or to analyse the nature of communication. Such attacks analyse traffics, monitors unprotected communications, decrypts weakly encrypted data and captures authentic information such as passwords. Such attacks can lead to disclosure of sensitive information without the knowledge or consent of the user [10]. These attacks are hard to detect as there is no loss and alteration of data. Therefore there are various encryption techniques to prevent these kinds of attacks rather than inventing techniques to detect them.

B. Active attacks

In active attacks, the attacker tries to circumvent or break into protected systems in the on-going communication networks. Such kind of attacks includes breaking into secured features, injecting a malicious code and stealing or modifying sensitive information[10]. In these kinds of attacks the data transmitted can be altered by the attacker or the whole data stream can be changed. Active attacks can be detected but these are difficult to prevent. Various error detection and correction techniques are used at various network layers to acquire a safe data transmission. Active attacks can take place in four ways: Masquerading, Replay, and Modificationof message and Denial of Service.

Networking attacks that have been damagingcompanies globally are listed below:

Table 2: Network Attacks

Network Attacks	***Percentage***	***Description***
Browser	36%	In these kinds of attacks the hackers add scripts without altering website's appearance which may lead the user to another website and may cause programs of malicious nature to be downloaded to the system. The attacker can then control the user's system remotely capturing personal information such as credit card and banking details to perform identity theft.
Brute Force	19%	It is a guessing technique of decoding password and pin number through trial and error basis. The attackers use automated software to guess thousands of combination of passwords. Locking account after failed multiple login attempts is one of the ways to prevent such attacks.
Denial of service	16%	These kinds of attacks block the user's access to a particular network to prevent them from retrieving information and services. The attacker creates an overloading traffic through malicious bot to a targeted IP address and floods network with more requests than the server can process.
SSL	11%	It is a kind of attack in which the attacker interrupts the data before its encryption and hence gets access to sensitive information of the system.
Scan	3%	It is a kind of application software which tries to retrieve information regarding open ports in server or host. They are combination of hostile searches which an attacker uses in order to gain access to a computer.
DNS	3%	It is an attack which redirects the network traffic to another system which is being controlled by the attacker. This attack corrupts the DNS server by introducing data into a domain name system cache to return an incorrect IP address.
Backdoor	3%	Such attacks bypass the intrusion detection systems and allow the hackers to access the information remotely. Many strategies may be adopted in backdoor attacks such as port-binding, connect back and connect availability.
Others	9%	The other attacks constitute to around 9% of the total attacks and may include all attacks which may be of small in nature but have significant impact on the security of network systems.

Source: [11]–[14]

© 2015-19, IJARCS All Rights Reserved

Various attacks have been listed by [1] in their paper which includes e-mail containing virus, network virus, web-based virus, attack on the server , service rejection attacks and network user attacks. They have mentioned that the major problem faced by the IT infrastructure is the vulnerability of computer networks and such problems arise mainly due to faulty implementation and design of information system including security procedures and controls. Another kind of security threat named insider attack which is being mentioned by [8], [9], is capable of causing irreparable damage to the activities and reputation of the organization.

There are other kinds of networks attacks which pose serious threat to the confidentiality of the organization. Some these attacks are listed below:

A. Phishing attacks

These kinds of attackers pretend to be as trustworthy persons with an intention to capture sensitive information through fraud email and messages [15]. They often create a fake website such as SBI bank or PayPal and try to trick the users by getting them click on a link and later on record their personal information including username and password [6], [10]. Such kind of attacks take as much as 9 to 10 days to resolve [16].

B. Close in attacks/Social Engineering

Known as bugs in the human hardware [12], these attacks involve physical interaction with the network, systems and components for getting unauthorized access to the information. The attackers establish social interaction with the victims through e-mail, messages or phone and tricking the latter to reveal personal information regarding the security of the system [6], [10]. The attackers try to exploit the emotional response of the victim who falls for their trust revealing to them their username, passwords and email address [15]. These kind of attacks also take around 9 to 10 days for getting resolved [16].

C. Viruses Worms and Trojans

Virus are programs that are written in order to alter the working of the victim's computer without its permission and authorization [15]. There are three ways in which a virus can enter an organization's system. Firstly, E-mail containing viruses which can infect system's email and spread throughout the organization. Secondly, Network viruses which breach the system through unprotected ports and can affect the entire network. Thirdly, Web based viruses that infect the system which visit their web page and also affects other internal network systems[1].

D. Hijack

This is a kind of an attack in which the hacker intercepts or takes over session between the user and another system and finally disconnects the later from the communication. The user remains under the impression that system is still connected and may send sensitive and confidential information to the hacker by accident [6], [10].

IX. SECURITY MEASURES

A. Firewalls

A firewall can be defined as a device which may be a computer or router acting between the internet and the organization network. Firewall lets only those packets to be transmitted through it into an organization's internal networkwhich fulfils its perimeters configured by the firewall administrator to be a safe data packet and filters the other packets. Firewall acts at network, transport and application layers. Packet –filter firewall acts at network and transport layer and proxy firewall acts on the application layer.Firewall checks the traffic according to the specific rules it has been configured for but there may be chances when the attacker can portray the harmful data to have perimeters which firewall finds safe to be transmitted through it.

B. Antivirus Systems

These systems are used to detect and eradicate malware from our systems. The antivirus system should be kept updated with the latest updates so that it would be easy for it to scan the latest virus signatures. Sometimes an antivirus system is not able to detect the infected file if it is encrypted or zipped.

C. Intrusion detection systems

It is a network monitoring device or software application which keeps track of any malicious actions and policy desecrations and if found it immediately reports about the intrusion to the administrator.They are a set of programs which help detect intrusions and save the system from getting affected. There are two kinds of intrusion detection systems, namely Anomaly Intrusion Detection and Misuse Detection or Signature Based IDS. The Anomaly Intrusion Detection system includes neutral networks and prediction pattern generation, while the Misuse Detection or Signature Based IDS includes state transition tables, pattern matching, genetic algorithms, fuzzy logic, immune systems, and Bayesian method and decision tree[17]. These systems may be Host –based IDS or Network –based IDS.The system matches the traffic with the attack pattern and if match is detected it gives the alarm to the administrator. However, the attacker may be clever enough to change the signature of the malicious traffic which the IDS fail to detect.

X. CONCLUSION

Globally expanding information networks have become vulnerable to emerging threats and attacks from malicious sources and pose a serious challenge for business and create research gaps for scholars. Researching and developing counter measures is a dire need for the organizations to protect their sensitive data from getting infected from unauthorized sources. Network security has now become an integral part of organization's confidentiality as it prevents unauthorized users from accessing the network systems, ensures safe transferring of sensitive data and provides a robust system of warning against alarm and fixing issues in

© 2015-19, IJARCS All Rights Reserved

case of security breach. This study provides a description of various kinds of threats and attacks on network systems and the common counter measures to mitigate the situation. Further studies can be conducted on organizations mapping the degree of damage they receive as a consequence of becoming victims of such attacks. Case studies on network organizations can also be conducted to understand the grey areas of networking security and aspects which needs to be addressed.

XI. REFERENCES

[1] F. S. Roozbahani and R. Azad, "Security Solutions against Computer Networks Threats," Int. J, pp. 2576–2581, 2015.

[2] S. Kaushik and A. Singhal, "Network Security Using Cryptographic Techniques," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 2, no. 12, pp. 2277–128, 2012.

[3] A. Singh, A. Vaish, and P. K. Keserwani, "Information Security: Components and Techniques," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 4, no. 1, pp. 2277–128, 2014.

[4] S. Tayal, N. Gupta, P. Gupta, D. Goyal, and M. Goyal, "A Review paper on Network Security and Cryptography," vol. 10, no. 5, pp. 763–770, 2017.

[5] M. R. Joshi and R. Avinash Karkade, "Network Security with Cryptography," Int. J. Comput. Sci. Mob. Comput., vol. 41, no. 1, pp. 201–204, 2015.

[6] P. Golchha, R. Deshmukh, and P. Lunia, "www.ijser.in A Review on Network Security Threats and Solutions," Int. J. Sci. Eng. Res., vol. 3, no. 4, pp. 3–5, 2014.

[7] S. Tayal, N. Gupta, P. Gupta, D. Goyal, and M. Goyal, "a Review Paper on Ad Hoc Network Security," Comput. Sci. Secur., vol. 1, no. 1, pp. 52–69, 2007.

[8] P. Scott, "Top 10 Threats to SME Data Security," 2008.

[9] J. R. C. Nurse et al., "Understanding insider threat: A framework for characterising attacks," Proc. - IEEE Symp. Secur. Priv., pp. 214–228, 2014.

[10] M. S. Gaigole, S. Kamaltai, and M. A. Kalyankar, "The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms," Int. J. Comput. Sci. Mob. Comput., vol. 45, no. 5, pp. 728–735, 2015.

[11] Calyptix, "Top 7 Network Attack Types In 2016," Calyptix Blog. 2016.

[12] C. Manimegalai and A. Sumithra, "An Overview of Attacks in the Network Security System," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 5, no. 10, pp. 816–819, 2015.

[13] D. O. of T. C. I. S. Officer, "Web Browser Attacks," Cyber Security Tips, vol. 3, no. 2, pp. 1–2, 2009.

[14] Diwakar Dinkar et al., "McAfee Labs Threats Report," 2016.

[15] A. Ahmad, "Type of Security Threats and It's Prevention," Int. J. Comput. Technol. Appl., vol. 3, no. 2, pp. 750–752, 2017.

[16] A. Yassir and S. Nayak, "Cybercrime: A threat to Network Security," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 12, no. 2, 2012.

[17] M. K. Asif, T. A. Khan, T. A. Taj, U. Naeem, and S. Yakoob, "Network Intrusion Detection and its strategic importance Network Intrusion Detection and its Strategic Importance," IEEE Bus. Eng. Ind. Appl. Colloq., pp. 140–144, 2013.

© 2015-19, IJARCS All Rights Reserved