IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 30-32
www.iosrjournals.org

Network Security and Authentication in Communication

M.T.Nehete[1]& V.G.Wagh[2]
[1,2](Department of Computer Science & Department of Physics K.V.N.Naik College, (MS), India)

Abstract:*Network Security has become very important in today's world, as a result of which various methods are adopted to bypass it. Network administrators need to keep up with the recent advancements in both the hardware and software fields to prevent their as well as the user's data. Authentication is one of the primary and most commonly ways of ascertaining and ensuring security in the network. This paper outlines the various attack methods which are used, various defense mechanism against attack and various authentication techniques.*

Key Words*: Attacks, Firewalls, Authentication, Router.*

I. Introduction

Network security refers to protecting the websites domains or servers from various forms of attack. Network security is important in every field of today's world such as military, government and even in our daily lives. Having the knowledge of how the attacks are executed we can better protect ourselves. Network security is mainly focused on the data and on the devices which are used to link to the internet. Email is a widely used service today and it is also contain many serious flaws, there is no system of authenticating the sender as well as the recipient, it is stored in multiple places during transmission and can be easily intercepted and changed. SPAM are serious security threat they only require very less manpower but affect millions to billions of Email users around the world, they can cruel link or even false advertisements.

Data Security is a challenging issue in the field of data communications. For securing information from hackers and crackers, authentication is the major phase in network security. It is a concept to protect network and data transmission over wired as well as wireless networks. Authentication is one of the primary techniques of ensuring that the person who is transmitting the information is whom he says he is. It is thus the process of determining the actual identity of users, systems or any other entity in network. To verify someone's identity, password is mostly used. To authenticate user or machines, different techniques can be used to perform authentication between user and machine or machine and another machine too. Different types of attacks are possible during authentication is shown below.

1.1 Different types of Security Attacks:

Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider.

1.1.1 Passive Attack

A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords.

1.1.2 Active Attack

In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to avoid or break protection features, to introduce malicious code, and to take or modify information.

1.1.3 Distributed Attack

A distributed attack requires that the adversary introduce code, such as a Trojan horse or back-door program, to a "trusted" component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution.

1.1.4 Insider Attack

An insider attack involves someone from the inside, such as a displeased employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task.

1.1.5 Close-in Attack

A close-in attack involves someone attempting to get physically close to network components, data, and systems in order to learn more about a network Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry into the network, open access, or both.

1.1.6 Phishing Attack

In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank. The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

1.1.7 Hijack attack

In a hijack attack, a hacker takes over a session between you and another individual and disconnects the other individual from the communication. You still believe that you are talking to the original party and may send private information to the hacker by accident.

1.1.8 Spoof attack

In a spoof attack, the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. This may be an attempt to bypass your firewall rules.

1.1.9 Buffer overflow

A buffer overflow attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell.

1.1.10 Exploit attack

In this type of attack, the attacker knows of a security problem within an operating system or a piece of software and leverages that knowledge by exploiting the vulnerability.

1.1.11 Password attack

An attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords. A brute-force attack is when the attacker tries every possible combination of characters.

Types of Authentication:

- Password authentication – This is "something a user knows." The most recognized type of one-factor authentication method is the password.
- Physical authentication – In addition to the first factor, the second factor is "something a user has." Examples of something a user has are a device that generates a pre-determined code, a signed digital certificate or even a bio-metric such as a fingerprint.
- Biometric authentication – In addition to the previous two factors, the third factor is "something a user is." Examples of a third factor are all bio-metric such as the user's voice, hand configuration, a fingerprint, a retina scan or similar.

II. Different Types Of Defense Techniques To Provide Security On Network

- Turn Off Ping Service

The primary purpose of a ping request is to identify hosts that are currently active. As such, it is often used as part of inspection activity preceding a larger, more coordinated attack. By removing a remote user's ability to receive a response from a ping request, you are more likely to be passed over by unattended scans or from "script kiddies," who generally will look for an easier target.

Password authentication	• Use of a password
Physical authentication	• Scannable card or key, as for building entry • Smart card containing information about its owner • Digital certificates
Biometric authentication	• Signatures and fingerprints • Visual identification based on photographs • Retinal eye scans and voice analysis

Fig. 1.1 Authentication Techniques

- Close unused ports

A closed port keeps your computer safe from unwanted outside communication. In security the term open port is used to mean a TCP or UDP port number that is configured to accept packets. There are various ports and maximum are by default open in our computer like FTP, TELNET, UDP, SMTP, FTP etc. In general we need only some port like FTP, HTTP etcHackers commonly use port scanning software to find which ports are "open" in a given computer, and whether or not an actual service is listening on that port.

- Use a firewall

  A firewall can help prevent hackers or hateful software from gaining access to your computer through a network or the Internet. A firewall can also help stop your computer from sending malicious software to other computers.

- Run antivirus software on each computer

  Firewalls help keep out worms and hackers, but they're not designed to protect against viruses, so you should install and use antivirus software. Viruses can come from attachments in e-mail messages, files on CDs or DVDs, or files downloaded from the Internet. Make sure that the antivirus software is up to date and set to scan your computer regularly.

- Use a router to share an Internet connection

  A network consists of routers from which information can be easily stolen by the use of malwares such as a "Trojan Horses". The synchronous network consists of switches and since they do not buffer any data and hence are not required to be protected.

- Don't stay logged on as an administrator

  When you're using programs that require Internet access, such as a web browser or an e-mail program, we recommend that you log on as a standard user account rather than an administrator account. That's because many viruses and worms can't be stored and run on your computer unless you're logged on as an administrator.

III. Conclusion

As internet has become a huge part of our daily life, the need of network security has also increased exponentially from the last decade. As more and more users connect to the internet it attracts a lot of criminals. Today, everything is connected to internet from simple shopping to defense secrets as a result there is huge need of network security. Billions of dollars of transactions happens every hour over the internet, this need to be protected at all costs. Network security can be maintained by making use of various authentication techniques. User has to use authentication technique depending on requirement. Password based technique is best if you have to remember a single password. But problems occur when we have to remember many passwords so we use those passwords that are easy to remember. Biometric technique cannot be easily stolen so it provides stronger protection. As signals, biometric can be easily copied by attackers so it should not be deployed in single factor mode. Furthermore we can choose a combination of above technique as discussed above. All the techniques have their pros and cons. We have to be smart to choose as per our requirement of safety of networks and information by considering cost factor also.

REFERENCES

[1] A R. F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University, 2010.
[2] B. Daya ,"Network Security: History, Importance, and Future ,"University of Florida Department of Electrical and Computer Engineering , 2013. http://web.mit.edu/~bdaya/www/Network%20Security.pdf
[3] Hafiz Zahid Ullah Khan, "Comparative Study of Authentication Techniques", IJVIPNS-IJENS Vol: 10 No: 04.
[4] J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library, 2000.
[5] Lawrence O"Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Vol. 91, No. 12, Dec. 2003, pp. 2019-2040 ã 2003 IEEE.
[6] M. M. B. W. Pikoulas J, "Software Agents and Computer Network Security," Napier University, Scotland, UK.
[7] [Online]Available: http://www.authenticationworld.com/Token-Authentication.
[8] [Online]Available: http://www.authenticationworld.com/Authentication-Biometrics.
[9] R. E. Mahan, "Introduction to Computer & Network Security," Washington State University, 2000.
[10] R. Morris, K. Thompson, "Password security: A case history," Comm. ACM, Vol.22, no. 11, Nov. 1979, pp. 594-597.
[11] Qinghua Li, Student Member, IEEE, and Guohong Cao, Fellow, IEEE "Multicast Authentication in the Smart Grid with One Time Signature", IEEE TRANSACTIONS ON SMART GRID, VOL. 2, NO. 4, DECEMBER 2011.