Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review of types of Security Attacks and Malicious Software in Network Security

Inam Mohammad
M.Tech(C.S)., Scholar, Graphic Era Hill University, Bhimtal, India

Rashi Pandey
M.Tech(C.S) Scholar, Graphic Era Hill University, Dehradun,, India

Aashiya Khatoon
M.Tech (C.S), Scholar, Bhagwant University, Ajmer, India

Abstract ***Cryptography is emerging technology which is important for Network Security. Network Security is the most important component in information security system and provide support and help to prevent from different types of security attacks. Network Security objective is to prevent the integrity, availability and confidentiality of information system.Network Security is for all hardware and software functions, characterstics,features,access control and administrative require to provide protection for hardware and software . Our focus of this paper is on defining the types of Security attacks and there harms on our information security system.***

Keywords: Network Security, Cryptography,access control, attacks.

1. Introduction

Hackers were highly skilled programmers who understood the details of computer communications and how to exploit vulnerabilities. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and generally open networks have generated an increased need for network security and dynamic security policies.[5]

Network Security & Cryptography is a concept to protect network and data transmission over wired/wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access.

Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password [1]. Network security starts with authenticating the user, commonly with a username and a password. Since this requires just one detail authenticating the user name —i.e. the password, which is something the user 'knows'— this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g. a security token or
'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g. a fingerprint or retinal scan). Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users [2]. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) helps detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network and traffic for unexpected (i.e. suspicious) content or behavior and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times. Individual events occurring on the network may be logged for audit purposes and for later high-level analysis [3]. Communication between two hosts using a network may be encrypted to maintain privacy.

2. Types of attack:

A usefull means of classifying security attack is in terms of Active attack and Passive attack. A passive attack attempt to monitor the information from the system but does not affect system resources. An active attack attempt harm system resources and their operations[4]. Classes of attack might include passive monitoring of communications, active network

attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states.[6]

A **passive attack** are in nature of eaves dropping on, or monitoring of transmission [4]. **Passive attacks** include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.[6]

Active attack involves some modification of the data Stream or creation of the false stream [4]. 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 circumvent or break protection features, to introduce malicious code, and to steal or modify information [6]. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks subdivided into four categories; masquerade, replay, modification of message, and denial of service.[4]

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. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.[6]

An **insider attack** are among most difficult to detect and prevent. It involves someone from the inside, such as a disloyal employee, attacking the network [4]. **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.[5]

In **Phishing attack** the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank or paypal. 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[5].

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.[5]

Spoof attack In a spoof attack, the hacker try to access the network IP address. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data. [6]

Buffer overflow A buffer overflow attack is when the attacker sends more data to system than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell.[5]

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.[5]

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.[6]

3. Types of malicious software

Virus malware that, when executed tries to replicate itself into other executable code when it succeeds the code is said to be infected code. When the infected code is executed, the virus also executes. **Worm** are computer programs that can run independently and can propagate a complete working version of itself onto other hosts on a network. **Logic bomb** are program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met. **Trojan horse** are computer program that appears to have a useful function, but also has a hidden and potentially malicious finction that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program. **Exploits** code specific to a single vulnerability or set of vulnerabilities. **Downloader** program that installs other items on machine that is under attack. Usually ,a downloader is sent in an e-mail. **Auto-rooter** malicious hacker tools used to break into new machines remotely. **Kit (virus generator)** set of tools for generating new viruses automatically. **Spammer** programs used to send large volumes of unwanted e-mail. **Flooder** used to attack networked computer systems with a large volume of traffic to carry out a denial-of-service(DoS) attack. **Keylogger** captures keystrokes on a compromised system. **Rootkit** set of hacker tools used after attacker has broken into a computer system and gained root-level access. **Zombie**, bot program activated on an infected machine that is activated to launch attacks on other machines. **Spyware** software that collects information from a computer and transmits it to another system. **Adware** advertising that is integrated into software. It can result in pop-up ads or redirection of browser to a commercial site[4]

4. Conclusion

Network Security is the most vital and important component of information security because it is responsible for securing all the information passed through a Network computer. Network Security consist of the provision made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network accessible resources from unauthorized access and continous monitoring of effectiveness combined together. We have

studied various cryptographic techniques to increase the security of network.

References

[1] Simmonds, A; Sandilands, P; van Ekert, L(2004) "Ontology for Network Security Attacks" Lecture Notes in Computer Science 3285 pp.317-323.
[2] A Role-Based Trusted Network Provides Pervasive Security and Compliance – interview with Jayshree Ullal, senior VP of Cisco.
[3] Daye Dittrich, Network monitoring/Intrusion Detection System(IDS), University of Washington.
[4] William Stallings, "Cryptography and Network Security", Vth edition.
[5] http://technet.microsoft.com
[6] www.computernetworknotes.com

