REVIEW ON VARIOUS TECHNOLOGIES TO COUNTER HACKING ATTACKS

VIKAS RAO VADI
Presently working as HOD Computer Science at Kalka Institute For Research And Advanced Studies.

ABSTRACT:

Computers permeate every aspect of modern life and business. They have found extensive use in both public and private sectors. Apart from their traditional use in terms of storage/retrieval, computers are used increasingly for decision making and trusted to control important operations without human supervision.

Introduction

Obviously, the potential for mischief is enormous if such systems are tempered with illicitly. Illicit tampering of computer systems (computer misuse) takes many forms and the most common are probably hacking and computer viruses. Hacking generally refers to activity of gaining unauthorized access to a computer system or network. Computer viruses generally refer to programs which replicate themselves, delete stored information or alter the stored information from the infected computer. Hacking is often the first step in a computer misuse instance. Once a hacker has managed to gain unauthorized entry to a computer system he or she can then try to reprogram the system, delete or modify the data contained therein.

Three types of attacks against computer system can be identified viz. Physical, Syntactic and Semantic. A physical attack uses conventional weapons, such as bombs or fire. A syntactic attack uses virus-type software to disrupt or damage a computer system or network. A semantic attack is a more subtle approach. Its goal is to attack users' confidence by causing a computer system to produce errors and unpredictable results. Syntactic attacks are sometimes grouped under the term "malicious software" or "malware". These attacks may include viruses, worms, and Trojan horses. One common vehicle of delivery for malware is email. Semantic attacks involve the modification of information or dissemination of incorrect information. Modification of information has been perpetrated even without the aid of computers, but computers and networks have provided new opportunities to achieve this. Also, the dissemination of incorrect information to large numbers of people quickly is facilitated by such mechanisms as email, message boards, and websites. Hacking tricks can be divided into different categories for example-Trojan programs that share files via instant messenger, Phishing, Fake Websites, Spoofing, Spyware, Electronic Bulletin Boards, Information Brokers, Internet Public Records, Trojan Horses etc.

The Role of Counter Hacking Attacks

Spyware is computer software that can be used to gather and remove confidential information from any computer without the knowledge of the owner. Everything the surfer does online, including his passwords, may be vulnerable to spyware.

Chat rooms and electronic bulletin boards have become breeding grounds for identity theft. When criminals have obtained personal identifying information such as credit card numbers or social security numbers, they visit hacker chat rooms and post messages that they have personal information for sale.

Information brokers have been around for decades, however, a new breed of information broker has emerged in recent years; the kind that sells personal information to anyone requesting it electronically via the Internet.

People search and genealogy websites have come under fire and some consumers are concerned that personal information online can be used to commit identity theft. Privacy advocates have become extremely concerned about the ease with which people can obtain personal information online.

The Impact of hacking activities on internet infrastructure can also be broadly classified into different categories viz. DNS Hacking Attacks, Routing Table Poisoning Attacks, Packet Mistreatment Attacks, Denial of Service (DoS)Attacks.

DNS attacks have illustrated the lack of authenticity and integrity of the data held within DNS as well as in the protocols that use host names as an access control mechanism. Routing tables are used to route packets over the Internet. They are generated by exchange of routing information or updates between routers. Poisoning attacks refer to the malicious modification or "poisoning" of routing tables. This can be achieved by maliciously modifying the routing information update packets sent by the routing protocols. This can result in wrong entries in the routing table and could lead to a breakdown of one or more domains of the Internet. In packet mistreatment attacks the malicious router mishandles packets, thus resulting in congestion, denial of service, and so on. The problem becomes intractable if the router selectively interrupts or misroutes packets resulting in triangle routing, i.e. loop formation. In Denial-of-Service-Attack, the packets are routed correctly but the destination becomes the target of the attackers. In a typical DoS attack, the attacker node spoofs its

IP address and uses multiple intermediate nodes to overwhelm other nodes with traffic. DoS attacks are typically used to take important servers out of action for a few hours, resulting in DoS for all users served by the server. It can also be used to disrupt the services of intermediate routers.

There are various state-of-the-art technologies for information security includes Biometric security solutions, Honey Pot Decoys and Padded Cells, Tokens, Cryptography and Digital signature technologies etc.

Biometric technologies are available today that can be used in security systems to help protect assets. Biometric technologies vary in complexity, capabilities, and performance and can be used to verify or establish a person's identity. Leading biometric technologies include Facial recognition, Fingerprint recognition, Hand geometry, Iris recognition, Retina recognition, Signature recognition, Vein recognition, Voice recognition, DNA Fingerprint, Deep tissue illumination & Keystroke pattern etc. Biometric technologies have been used in federal applications such as access control, criminal identification, and border security.

Facts of Counter Hacking Attacks

There are various ways through which a hacker can impersonate other users. The most commonly used method is eavesdropping on unsuspecting users to retrieve user accounts, passwords and other user related information.

The theft of user account number and related information is a very serious problem in any instant messenger. For instance, a hacker after stealing a user's information impersonate the user; the user's contacts not knowing that the user's account has been hacked believe that the person they're talking to is the user, and are persuaded to execute certain programs or reveal confidential information. Hence, theft of user identity not only endangers a user but also surrounding users. Guarding against Internet security problems is presently the focus of future research; because without good protection, a computer can be easily attacked, causing major losses. Hackers wishing to obtain user accounts may do so with the help of Trojans designed to steal passwords. If an instant messenger client stores his/her password on his/her computer, then a hacker can send a Trojan program to the unsuspecting user. When the user executes the program, the program shall search for the user's password and send it to the hacker. There are several ways through which a Trojan program can send messages back to the hacker. The methods include instant messenger, IRC, e-mails, etc. Current four most popular instant messengers are AIM, Yahoo! Messenger, ICQ, and MSN Messenger, none of which encrypts its flow. Therefore, a hacker can use a man-in-the-middle attack to hijack a connection, then impersonate the hijacked user and participate in a chat-session.

Denial of Service

There are many ways through which a hacker can launch a denial of service (DoS) attack on an instant messenger user. A Partial DoS attack will cause a user end to hang, or use up a large portion of CPU resources causing the system to become unstable.

There are many ways in which a hacker can cause a denial of service on an instant messenger client. One common type of attack is flooding a particular user with a large number of messages. The popular instant messaging clients contain protection against flood-attacks by allowing the victim to ignore certain users. However, there are many tools that allow the hacker to use many accounts simultaneously, or automatically create a large number of accounts to accomplish the flood-attack. Adding to this is the fact that once, the flood-attack has started and the victim realizes what has happened, the computer may become unresponsive. Therefore, adding the attacking user accounts to the ignore list of the instant messenger client may be very difficult DoS attacks are very easy to generate and very difficult to detect, and hence are attractive weapons for hackers. In a typical DoS attack, the attacker node spoofs its IP address and uses multiple intermediate nodes to overwhelm other nodes with traffic. DoS attacks are typically used to take important servers out of action for a few hours, resulting in DoS for all users served by the server. It can also be used to disrupt the services of intermediate routers.

Information Disclosure

Retrieving system information through instant messenger user is currently the most commonly used hacking tool. It can effortlessly collect user network information like, current IP, port, etc. IP address retriever is an example. IP address retrievers can be used to many purposes; for instance, a Trojan when integrated with an IP address retriever allows a hacker to receive all information related to the infected computer's IP address as soon as the infected computer connects to the internet. Therefore, even if the user uses a dynamic IP address, hackers can still retrieve the IP address.

Different Trojan programs were designed for different instant messaging clients. For example, with a user account and password stealing Trojans, a hacker can have full control of the account once the user logs out. The hacker can thus perform various tasks like changing the password and sending the Trojan program to all of the user's contacts.

A Case Study

Some instant messaging clients allow all communication to be saved in log-files. Even though this is a feature that is often requested and required by companies, it can sometimes be very dangerous to keep logs, as the logs may include sensitive company data. This was made evident in a case that occurred at the beginning of 2001, where a hacker stole logs from an instant messaging client belonging to the CEO for a company called e-Front. The hacker posted the logs to several places on the Web, thereby creating one of the worst possible corporate nightmares. The logs included sensitive company data regarding business partners, employees and affiliate websites. After the posting of the logs, several members of the senior staff for e-Front resigned. The e-Front case shows how dangerous it can be if a hacker is able to monitor instant messaging sessions. Even though the log-files were stolen in this case, sniffing the data-packets could have caused the same damage.

REFERENCES

[1] Janet J. Prichard and Laurie E. MacDonald Bryant University, Smithfield, RI, USA , "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks", Journal of Information Technology Education Volume 3, 2004

[2] Anirban Chakrabarti and G. Manimaran, Iowa State University, "Internet Infrastructure Security: A Taxonomy", IEEE Network • November/December 2002 0890-8044/02 © 2002 IEEE

[3] Tzer-Shyong Chen1, Fuh-Gwo Jeng, and Yu-Chia Liu "Hacking tricks toward security on network environments", Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCA T'06) 0-7695-2736-1/06 © 2006 IEEE