Network and Information Security Issues

Vandna Batra
A.P. M.R.I.U, Faridabad

Shrutika Suri
A.P. M.R.I.U, Faridabad

ABSTRACT
In today's information society, information has become a valuable asset and there is increasing dependence on access to information. This makes individuals, organizations, and nations highly vulnerable to information security attacks. Finding effective ways to protect information systems, networks and sensitive data within the critical information infrastructure is challenging even with the most advanced technology and trained professionals. This paper describes the various network and information security issues and the explained the technical aspects of how to improve network information security.

Keywords-
Malware, phishing, rootkits, spam, virus

I. INTRODUCTION
Network provides us with a wealth of quick information, through the network we will share our information and can be said that the network has become a part of our lives, It brings great convenience on our work, live and learning, but with the exception beyond this, has also given us a great deal of trouble. The increasing number of Information Security (IS) related incidents, organized crimes and phishing scams mean that IS deserves much closer attention.

Network security is generally taken as providing protection at the boundaries of an organization by keeping out intruders (hackers).Information security, however, explicitly focuses on protecting data resources from malware attack or simple mistakes by people within an organization by use of data loss prevention (DLP) techniques. Network security measures are needed to protect data during their transmission because virtually all business, Government and academic organizations are interconnected their systems with a collection of networks referred as Internet.

II. NETWORK SECURITY THREATS
A. Malware

Malware, short for malicious software, is software designed to harm or secretly access a computer system without the owner's informed consent. Malware includes compute viruses, worms, Trojan horses, spyware, dishonest adware, scareware, crimeware, most rootkits, and other malicious and unwanted software or program.

Viruses and Worms: The term virus has long been used generically to describe any computer threat, but in actuality it refers specifically to malware that inserts malicious code into existing documents or programs, and then spreads itself by various means. Today, viruses are still by far the most common type of network security threat, and over 90 percent of viruses are spread through attachments on emails. Both viruses and worms often work to open up new holes in your

network security in order to allow even more dangerous security threats to infect your network.

Trojan Horses: Trojan horse is any program that invites the user to run it, concealing a harmful or malicious payload. The payload may take effect immediately and can lead to many undesirable effects, such as deleting the user's files or further installing malicious or undesirable software.

Rootkits: Once a malicious program is installed on a system, it is essential that it stays concealed, to avoid detection and disinfection. The same is true when a human attacker breaks into a computer directly. Techniques known as rootkits allow this concealment, by modifying the host's operating system so that the malware is hidden from the user.

Backdoors: A backdoor is a method of bypassing normal authentication procedures.

B. Denial of Service Attack
This type of attack causes your computer to crash or to become so busy processing data that you are unable to use it. In most cases, the latest patches will prevent the attack. It is important to note that in addition to being the target of a DoS attack, it is possible for your computer to be used as a participant in a denial-of-service attack on another system.

C. Spam
Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. Depending on the source cited, spam makes up 70 to 84 percent of daily emails sent throughout the world. All that spam results in billions of dollars in lost productivity and creates an ever increasing need for IT resources to filter out this irritating and potentially malicious menace.

D. Phishing
Phishing refers to spam emails designed to trick recipients into clicking on a link to an insecure website. Typically, phishing attempts are executed to steal account information for e-commerce sites such as eBay, payments processors such as PayPal, or regular financial institutions' websites. A phishing email supplies you with a link to click on, which will take you to a page where you can re-enter all your account details, including credit card number(s) and/or passwords. Of course, these sites aren't the actual bank's site, even though they look like it.

Your company's mobile phones may not be safe either, as SMS messaging is now frequently used as a new type of phishing called smishing. Once the smishing is successful, other malware such as Trojans are sometimes released onto the mobile phone. These Trojans then make silent high cost text messages which go onto the sender's bill.

Some criminals are also using VoIP (Voice over internet protocol) to send vishing messages. These try to confuse people into calling the provided number usually an automated VoIP Call-In number - and revealing credit card details, which are recorded in audio form.

Phishing in all its varieties is a huge and growing problem for network security managers and business owners. As we all become more interconnected and access more and more personal information through networks, there become more and more opportunities for phishers to attack. To protect one's network, it is becoming increasingly vital that you educate your employees about the most common ways in which hackers try to phish your account information.

E. Packet Sniffers

Packet sniffers capture data streams over a network, thus allowing for the capture of sensitive data like usernames, passwords and credit card numbers. The result, unsurprisingly, is the loss of data, trade secrets, or online account balances. For network managers specifically, even bigger losses can come from lawsuits due to noncompliance of data protection regulations. Packet sniffers work by monitoring and recording all the information that comes from and goes to your computer over a compromised network. So in order to be effective, the packet sniffer must first have access to the network you are using. The most common way to do this is through using something called honeypots. Honeypots are simply unsecured wifi access points that hackers setup and trap people into using them. Typically, these honeypots are setup in public places such as airports, and the wifi network is titled something like "Free Public Wi-Fi". Unsuspecting individuals then sign onto the corrupted network and the packet sniffer then grabs their personal information when they enter things like their credit card info into a site.

F. Maliciously-Coded Web Sites

Maliciously-coded Web sites can take many different forms, from installing Trojan horses to redirecting you to an unrequested site. But one of the most threatening forms of maliciously-coded websites, those that are designed to steal passwords, are on the rise. A very common form of these Web sites takes advantage of human's charitable instincts by setting up traps in what appear to be sites that allow you to make donations to victims of natural disasters. Hackers set up a fake sign-in page, and then encourage unsuspecting victims to enter their credit card number and other personal information.

G. Password Attacks

A 'Password Attack' is a general term that describes a variety of techniques used to steal passwords to accounts.

- Brute-force: One of the most labor intensive and unsophisticated methods hackers use to steal passwords is to try to guess a password by repeatedly entering in new combinations of words and phrases compiled from a dictionary. This 'dictionary attack' can also be used to try to guess usernames as well, so developing difficult to guess usernames and passwords is increasingly vital to network security.
- Packet sniffers: Packet Sniffers glean data electronically from a compromised network.
- IP-spoofing: Similar to 'Honeypots', this attack involves the interception of data packets by a computer successfully pretending to be a trusted server/ resource.
- Trojans: Trojans are actually invasive, as discussed above, and of these methods, are the most likely to be successful, especially if they install keyloggers.

III. CONCLUSION

This paper examines network and information security issues. Network deployment still faces great challenges regarding malicious attacks and requires numerous countermeasures to migrate these attacks in existing implementation and future development. As the volume of financial and other data transactions increase over the Internet, the potential for harm from network threats also increases. As a consequence, complex security measures are increasingly a necessity even for the smallest of companies. As we continue to become an ever more networked society, the financial benefits attainable by hacking a network increase. As a result, it should come as no surprise that the number of attacks and the creativity spent in trying to breach a network continue to increase. Consequently, those that are tasked with defending networks must continue to educate themselves and their workforce on the newest types of attacks and make the necessary preparations to prevent against them.

IV. REFERENCES

[1] Network Security- http://en.wikipedia.org/wiki/Network_security

[2] Network & Information Security http://docs.google.com/viewer?a=v&q=cache:epBESAaaxOMJ:egovstandards.gov.in/standards_network_app+Networks+and+information+security

[3] http://docs.google.com/viewer?a=v&q=cache:J57DBziwuVoJ:www.softcomputing.net/jnca1.pdf+Networks+and+information+security

[4] Information Security- http://en.wikipedia.org/wiki/Information_security

[5] http://docs.google.com/viewer?a=v&q=cache:2bDBz8g3gJ8J:www.unapcict.org/ecohub/briefing-note-series/BN6.pdf+network+and+information+security

[6] Information Security Threats- http://www.enggpedia.com/computer-engineeringencyclopedia/dictionary/computer-networks/1708-network-security-information-security-threats-a-techniques-to-secure-networks

[7] Network Security Threats http://networksecuritythreats.org/network-security/network-security-threats-explained/

[8] http://www.cert.org/tech_tips/home_networks.html