International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 3| ISSN : 2456-3307

Cryptography Techniques

R.Sakthi Uma[1], Prof. R. Angelin Preethi[2]
[12]Department of Computer Science, Kamban College Of Arts and Science for Women, Tiruvannamalai, Tamil Nadu, India

ABSTRACT

Security is main issue of this generation of computing because many types of attacks are increasing day by day. Establishing a network is not a big issue for network administrators but protecting the entire network is a big issue. There are various methods and tools are available today for destroying the existing network. In this paper we mainly emphasize on the network security also we present some major issues that can affect our network.

Keywords: Security, Cryptography,

I. INTRODUCTION

For the first few decades of their existence computer networks were primarily used by university researchers for sending email, and by corporate employees for sharing printers. Under these conditions, security did not get a lot of attention. But now, as millions of ordinary citizens are using networks for banking, shopping, and filling their tax returns network security is looming on the horizon as a potentially massive problem.

Information systems have evolved in the last few decades from centralized and highly secure host-based systems to be decentralized. It is often said that in the enterprise model, "the network is the computer".Ultimately, the systems so large that they were hard to manage effectively.

To make things still worse, users of laptop and remote systems demanded connection into corporate offices from their homes, from hotel rooms, and from customer sites. Then the Internet becomes popular, and people inside the company wanted to connect out to it. To most administrators, the Internet is a nightmare that can potentially open the company's entire internal network to outsiders.

II. WHAT ARE THE THREATS?

Threats by floods and fires are easy to understand: the techniques for protecting against them area well known. But threats perpetrated by malicious users, disgruntled employees, and unknown hackers are a true nightmare. Every day some new technique for attacking systems is developed.

You may not know you are being attacked or have been attacked. No site is an exception. They break in using their computer and modem just for the fun or challenge. Professional hackers are quite busy as well.

A. Areas Of Security Weakness

The following list describes some of the weakest areas on company-wide networks:

- Well-known (and easily guessed) passwords, or leaked passwords, that compromise user logon and authentication

- Poorly implemented logon settings, user account rights, and file access permissions
- Disks and electronic mail that carry viruses
- Open doors into internal networks, created by users that access the Internet or by poorly implemented Internet firewalls
- Dial-up mobile and remote computers that have been stolen along with logon information

B. WHO ARE THE HACKERS?

You may not know any hackers personally; On the other hand, a hacker might be your next-door neighbor's son--someone with a computer and modem who is familiar with what you do, and who might guess your logon password because you use some derivative of your kids' names. Dangerous hackers are very knowledgeable about computers and security techniques, and they use sophisticated techniques to break into computer systems. Your competitor may hire such a hacker. If hackers cover their tracks, you might never know that they have stolen your customer mailing list or trade secrets.

Hackers often intend to make a profit or want to obtain free services. A phone hacker (or preacher) is intent on obtaining logon information to online services or on making long-distance phone calls through your phone system so that you pick up the charges. A hacker often uses information obtained during one break-in to access and break into another computer system.

C. The Internal Threat

A recent online survey by Network World magazine revealed that most security experts and readers felt that internal employees were the biggest threat to their information systems. Employees are familiar with the network, know which systems hold valuable information, and may have easy access to those systems through their own account or the account of another use. The American Society for Industrial Security estimates that 77 percent of information theft is perpetrated by insiders.

III. METHODS OF ATTACK

A. Phone Attacks

A preacher is a person who takes advantage of the telecommunications system to make free lone-distance telephone calls, listen to private conversations, access internal systems, or hack into other systems via the system broken into. Preachers are familiar with telephone switches, networks, and other equipment, and often have manuals from the manufacturers of telecom equipment that describe exactly how to operate and repair that equipment. Experienced preachers can manipulate telephone billing, access codes, and call routing.
Preachers can make free long-distance phone calls by gaining "dial-in / dial out" capabilities.

B. Hackers User Accounts and Passwords Attack

An attacker's first priority is to obtain user account names and passwords since this provides easy access to a system. Once inside, the hacker will find away to elevate his privileges. The attacker can obtain a list of user account names from a number of likely sources. Once a user account list is obtained, the hacker will try to determine which account will give the most access if broken into the pc support staff may inadvertently provide this information in the form of list of uses to contact in case of problems. Once a hacker obtains alginate user account name, cracking the password is the next step. Hackers take advantage of common passwords: if they know the user of an account, they may try various combinations of the user's kids and pets' names. Many people use the same password to log on to other systems, such as ATM machines. If a hacker obtains a user account name, but not a password, he can try brute force methods of breaking into the account. A program is set up to try thousands or millions of different passwords until the account opens. This method is ineffectively if logon restrictions that limit the number of attempted.

C. Electronic Eavesdropping and Cable Sniffing

A packet snifter is a device or software that can read transmitted packets. Packet sniffing is a passive eves dropping technique that is hard to detect. The packet-sniffing devices may be installed on internal or external networks. Although packet sniffing an internet transition line is not necessarily informative, sniffing a cable that runs into your facilities who are armed with packet snifters, or from hackers who have penetrated your building and planted listening devices.

D.Viruses and Trojan Horeses

Viruses are small programs that mimic the activities of real-life viruses. They get into computer systems by being copied from contained disks or downloaded from online services by unsuspecting users. Once a system is contaminated, the virus executes some immediate action, or waits until a specified time or for a specific command executed by the user. Viruses may display harmless messages or destroy the information stored on entire hard disks. A Trojan horse is similar to a virus, but contaminates a system by posing as some other type of program.

Viruses are created by authors who are fascinated by how quickly their virus may spread through computer systems. Terrorists and industrial spies create viruses that cause damage in order to seek revenge on an opponent or to viruses that cause damage in order to seek revenge on opponent or tom damage the operations of a competitor. Some viruses are intended targets.

E.Natural Threats

Obviously, not all threats to the integrity of your network come from people. Power surges, failing components, and other problems may bring down systems and cost your organization thousands or millions of dollars in down time. In some cases, continuous access to information is critical to the operation of the entire business.

IV. COUNTER MEASURES

A. Defining Security

Information security is the practice of protecting resources and data on computer systems and networks, including information on storage devices and in transmission. Make it your business to control and monitor the security of your systems and to implement security policies and procedures that people can follow.

- Identification and authentication
- Access control
- Accountability and auditing
- Accuracy
- Reliability
- Data exchange

B.Security Costs

Consider how much your organization can afford to spend on security. At the physical level, power surges, failing components and other problems may bring down systems and cost your organization thousands or millions of dollars in downtime. In some cases, continuous access to information is critical to the operation of the entire business.There are also direct costs, such as equipment costs, as well as administrative expenses. Beyond the dollar costs, there are expenses related to the inconvenience of the security system. It may simply take more time to get things done when complex procedures are in place to provide security

C. Protective Measures

There are a number of protective measures that help you "harden" your defenses. A few obvious steps are:

- Create security policies, plans, and job positions as appropriate.
- Set up a security-response team, experts who handle security problems.
- Perform background checks on personnel and keep tabs on employees who are disgruntled, who are working closely with other companies, and who are in the process of leaving the company.

- Classify your employees much the way the military classifies its personnel, giving some people higher clearance for access to sensitive information than others.

D. Backups

Backups are essential. If your systems are stolen, destroyed by fire, or corrupted by hackers, you'll need to go back to the last uncorrupted backup. The National Computer Security Association provides some interesting figures.The procedures you use to restore backups are critical in the case of virus attacks. Your backups may be corrupted, in which case you'll need to go back in the archive until you find a non-corrupted backup set. Back up as frequently as possible and place back up media into permanent archives as often as possible.

E.Encryption

You can use cryptographic techniques to protect files stored on disks and backups from prying eyes, or to conceal data transmissions and electronic mail. Encryption utilities scramble files and lock them with a password key. Using encryption may cause a drop in performance.

Encryption may give you the feeling that your files are private, when in fact someone might have cracked your encryption key and begun reading all your files. The stronger the encryption system, the better, but sure to implement additional security measures as appropriate. Also be aware that someone who gains access to your system might replace your encryption program with a Trojan horse version of the program that steals your password. Make sure the encryption software is protected and secure. Then take actions to monitor for possible virus infections.

F. Virus Protection

Viruses are a real threat to your network. They are easily contracted form unknown disks or by downloading files form online services, bulletin boards, and the Internet. Any of your network users can contract a virus at any time and spread it to the network. A virus is often hard to detect. It may wait on your system before it executes. Vigilant users or network administrators may detect unusual activity or notice an increase in the size of files (indicating potential infection).

Even after detecting and cleaning up a virus infection, there is still a good chance that the virus is lurking somewhere in your organization, ready to re-infect systems. It may even have infected the backup sets. You may need to implement a plan to detect and remove the virus throughout your organization. Check all workstations, disks, and other data sources for infections.

G. Advantages

These advantages can be lined up simply as

1. Protects personal data of clients on the network.
2. Protects information been shared between computers on the network.
3. Protects the physical computers from harm based from possible attacks on the network from the outside
4. Provides levels of access if the network has many computers attached so some computers may have more access to information than others. (Account system)
5. Private networks can be closed off from the internet making them protected from most outside attacks. Which makes them secure from Virus attacks.

V. 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. Most of the attacks can be easily prevented, by following many simply methods as outlined in this paper. As

new and more sophisticated attacks occur, researchers across the world find new methods to prevent them.

VI. REFERENCES

[1] 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

[2] Li CHEN,Web Security : Theory And Applications,School of Software,SunYat-sen University, China.

[3] J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library, 2000.

[4] A. R. F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University, 2010.

[5] S. A. Khayam, Recent Advances in Intrusion Detection, Proceedings of the 26th Annual Computer Security Applications Conference, Saint-Malo, France, pp. 224-243, 42, 2009