J. Comp. & Math. Sci. Vol.2 (1), 25-30 (2011)

Network Security Challenges and Cryptography in Network Security

DAYANAND SHARMA*, ABHIJIT KULSHRESHTHA[1] and SHRAWAN RAM[2]

*Research Scholar, Jodhpur National University, Jodhpur
[1]Associate Professor, Jodhpur National University, Jodhpur
[2]Assistant Prof., MBM Engg. College, Jodhpur.

ABSTRACT

The importance of network security has been significantly increasing in the past few years. As the number of autonomous systems or hosts are increasing every day due the wide spread use of the internet. We know that the internet has become the largest hub of every kind of the information. We have so many challenges to protect all valuable information from a variety of attacks. To design the efficient security policies and the implementation of these policies is a big challenge itself. In this paper we are particularly focusing on possible solutions and to provide the maximum level of the security. As we know that there are lot of antivirus software and intrusion detection systems has been designed but still we are not fully protected from all kinds of attacks. Cryptography is also a one of the best method for the protection from inside and outside attacks. As we know that each and every enterprise has their own local network of thousand of hosts and all the nodes are connected to the internet. Therefore the complexity of the network is increasing dramatically. Cryptography is the strongest tool to implement the security services. But at the same time its performance is not sufficient enough against some certain types of attacks.

Due to the lack of security polices Security issues, and basic situation in cryptography causing serious network security vulnerabilities. Addressing these issues is a key requirement for obtaining provable security and seamless policy configuration. In addition, with growth in network speed and size, the need to optimize the security policy to cope with the traffic rate and attacks is significantly increasing.

As the reach of today's networks has become global, they have become the focus of arguments over the values that should take care of their security.

Note: *the main idea of this paper is taken from Importance of cryptography in network security By Susan Storm et al ,26th May 2003.*

This paper consist of Network security issues, the role of cryptography, the status of network security and finally what steps must be taken while implementing the efficient security policy.

Keywords: network security, security policies, intrusion detection, Cryptography

INTRODUCTION

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography, which is the focus of this paper.

Normally the communication made over the internet is in plain text, which is unsafe. The data can be interrupted and intercepted anytime and anywhere. Therefore to communicate securely, it is important to adopt the cryptographic techniques and other security applications.

Cryptography prevents the companies to avoid forgeries, fraud, industrial espionage and other crimes. Cryptography techniques like encryption reduces the risks of un authorized access.

There is an enormous activity within the field of network security is to be done. As the internet is decentralized network of networks. Anybody can get connected to the internet with just one click and send out just about anything. Each organization that has internet connectivity to be responsible and take the necessary steps to ensure the security throughout the organization.

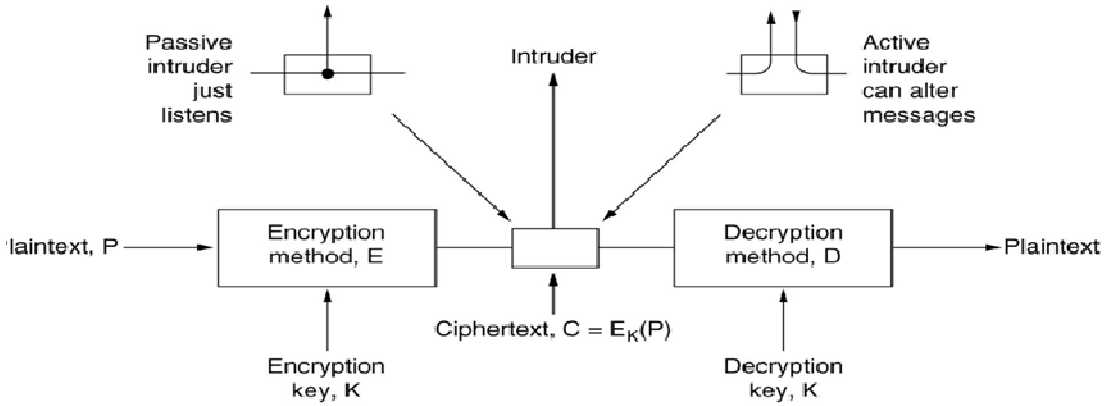
Application developers and IT specialist and company management must be taking the responsibility to maintain a correct security.

It is important to understand the role of Cryptography to understand the inherent vulnerabilities in network communication system.

We will begin this paper by defining five compulsory services to achieve network security. Cryptographically preventable attacks which will be followed by the vulnerabilities. Finally cryptographically based protocols will be discussed in the light of five services mentioned in the beginning part of this paper.

Security policy will be discussed precisely to come up with possible steps to avoid the security breaches.

BASIC SCENARIO IN CRYPTOGRAPHY [1]:



As per the above diagram , the scenario will be like:

- A(lice) sends a message (or file) to B(ob) through an open channel (say, Internet), where E(vil, nemy) tries to read or change the message
- A will **encrypt**the **plaintext** using a **key**transforming it into a "unreadable" **cryptotext**
- This operation must be computationally easy
- B also has a key (say, the same key) and **decrypts**the cryptotext to get the plaintext
- This operation must be computationally easy
- E tries to **cryptanalyze**: deduce the plaintext (and the key) knowing only the cryptotext
- This operation should be computationally difficult
- We will use **cryptography**to cover both the design of secure systems and their **cryptanalysis**–**cryptology**is also used sometimes[1].

SERVICES

Security services are intended to counter certain types of security attacks. They can be classified as follow:[6]

1-Authentication: This service involves the authentic communication .It also ensures the genuineness of user. This service not only monitors the initial stage but also take care of throughout the session.

2-Access Control: This service starts once authentication process is over. This service mainly takes care of controlling /limiting in network.

3-Data Confidentiality: this service protects the data from passive attacks. This service monitors contents of data and the packets where they are going to and coming from.

4-Data Integrity: The main purpose of this service is to detect when data has been altered in transit.

5-Non-repudiation: This service prevents the sender and receiver form denying sending a message.

VULNERABILITIES

The vulnerabilities include:

- Wiretapping
- Impersonation(IP-Spoofing)
- Message confidentiality violations
- Message integrity violations
- Code integrity violations
- Denial of service (DOS)

Though above mentioned vulnerabilities are good to keep an eye on but unfortunately they are discovered only after they have been exploited.[2]:

ATTACKS

Vulnerabilities are also called threats because the risk of their being exploited exists. A threat becomes an attack once the dreaded has occurred.[1] There is countless number of attacks. Some of them are:

Masquerade: Pretending to be someone, they are not. It is an attack on authentication and data integrity.

Bypassing: Controls circumventing access control.

Authorization violation: Circumventing both authorizing and access control.

Trojan horse: A program that has covert activity beyond what it appears to be doing. This attack makes all security services get compromised.

Trapdoor: A program that has a secret entry point.

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography, which is the focus of this chapter. But it is important to note that while cryptography is *necessary* for secure communications, it is not by itself *sufficient*. The reader is advised, then, that the topics covered in this chapter only describe the first of many steps necessary for better security in any number of situations.

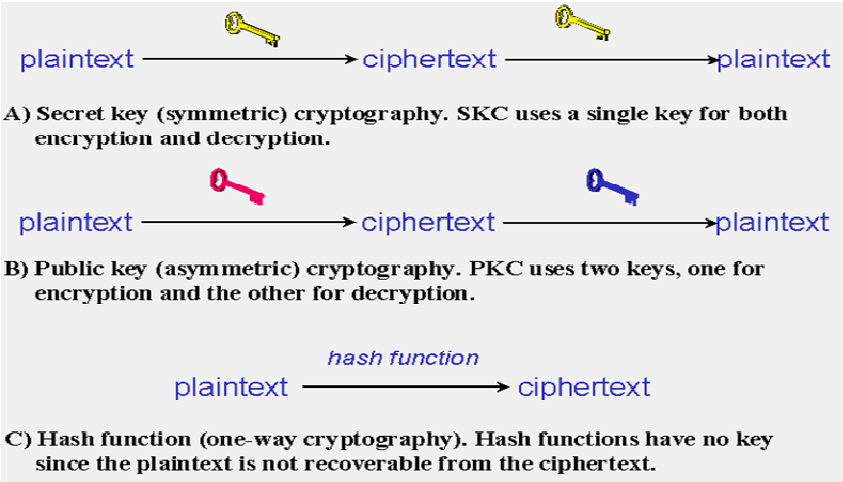


FIGURE 2: Three types of cryptography: secret-key, public key, and hash function.[7]

APPLIED CRYPTOGRAPHY

Cryptography can be applied anywhere in TCP/IP stack. It is widely used for data confidentiality.

All the security services would not be possible to offer anything without cryptography, no doubt.

Cryptography is also used in complicated protocols that help to achieve different security services.[6]

Cryptographically – based mechanism:

Some of the mechanisms are:

Encryption: used heavily to accomplish all security services

Access control mechanism: commonly access control list (ACL) or used capability list (UCL)

Data integrity mechanism: this mechanism aims at detecting the passive attacks in transit.

Authentication exchanges: this mechanism to realize authentic communication. In client server model, this includes various handshaking protocols and also includes the digital signature.

Traffic padding: a technique that aids in data confidentiality

Cryptographically –based protocols:

In short they can be defined as:

SSL

It creates secure tunnel to create a secure channel for exchange of arbitrary data

SSH

Similar to SSL, It uses an encrypted tunnel for exchange of data that can be used as a transport layer for other non-secure protocols

Kerberos

Complex protocol used in open distributed system to provide mutual authentication for both the client and server.

SET

Designed to protect credit card transaction over internet

PGP

Used for encrypting the content of an email inside a regular SMTP email with the use of asymmetric for convenient key exchange.[6]

Conclude:

CONCLUSION

It has been identified by various secret services that cryptographic implem-enttation satisfy some of the recommended It services.

An Attacker probably use the easiest point of entry for an attack; if some insecure software is not up-to-date, the vulnerability could lead to the attacker gaining complete access over the target host.

Attacks on insecure software can be done in some cases with tools downloaded from the internet.

It is found that the current status of network security is insufficient .while cryptography plays an important role, solving many of the foreseen problems.

This overall security depends on users, IT professionals and Administrators. The importance of cryptography will increase to a large extent in the coming year in pace with the growing traffic on networks.

RESEARCH ISSUES

Cryptography is an exciting area of research, and all aspects of it are being studied. New secret key ciphers incorporate techniques for defeating differential and linear cryptanalysis. New public key ciphers use simple instances of *NP*-hard problems as their bases, and they cast those instances into

the more general framework of the *NP*-hard problem. Other public key ciphers revisit well-studied, difficult classical problems (such as factoring) and use them so that mathematically breaking the cipher is equivalent to solving the hard problem. Still others are built on the notion of randomness (in the sense of unpredictability).

Cryptanalytic techniques are also improving. From the development of differential cryptanalysis came linear cryptanalysis. The use of *NP*-hard problems leads to an analysis of the problem underlying the cipher to reduce it to the simpler, solvable case. The use of classical mathematical problems leads to the application of advanced technology to make the specific problem computable; for example, advances in technology have increased the sizes of numbers that can be factored, which in turn lead to the use of larger primes as the basis for ciphers such as RSA.

Advances in both cryptography and cryptanalysis lead to a notion of "provable security." The issue is to prove under what conditions a cipher is unbreakable. Then, if the conditions are met, perfect secrecy is obtained. Similar issues arise with cryptographic protocols (some of which the next chapters will explore). This leads to the area of assurance and serves as an excellent test base for many assurance techniques.[8]

REFERENCES

1. Stallings, Williams. Network Security Essentials: Applications and Standards, New Jersey.C. (2000).
2. Pfleeger, Charles P..Security in computing. Prentice Hall PRT, New Jersy, C. (1997).
3. Joel Weise, Charles R. Martrin, Developing a Security Policy, Dec (2001) http://www.sun.com/blueprints/1201/secpolicy.pdf).
4. Jasu Mistry, Developing Security Policies for protecting Corporate Assets, Security Essentials, Version 1.2d, http://www.sans.org/reading_room/whitepapers/policyissues/developing_security_policies_for_protecting_corporate_assets_490.
5. net.educause.edu/ir/library/powerpoint/SEC0303.pps.
6. Importance of cryptography in network security By Susan Strom, Oskar Wiksten, (2003).
   Link: http://www.nada.kth.se/kurser/kth/2D1441/semteo03/lecturenotes/rapport_SS-OW_semteo.pdf.
7. Gary C. Kessler," An Overview of Cryptography", 16 March 2010 (Original version: May 1998), Link: http://www.garykessler.net/library/crypto.html.
8. Computer Security, Art and Science http://computer-security-art-and-science.org.ua/