Network Security Issues and Cryptography

Hemant Kumar
Research Scholar, Singhania Univesity, Pacheri Beri, Rajshthan

ABSTRACT:

With the advent of the World Wide Web and the emergence of ecommerce applications and social networks, organizations across the world generate a large amount of data daily. Information security is the most extreme basic issue in guaranteeing safe transmission of data through the web. Also network security issues are now becoming important. Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. In this paper we describe some of the recent research going on in the field of cryptography and network security. Discussion of these research papers emphasizes the security vulnerabilities of existent as well as new technologies in the field of Computer Networks.
Keywords: Network, Security, Cryptography, Cipher Text

INTRODUCTION:

We are living in the information age where information needs to be kept about every aspect of our lives. Today more than 80 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. This information can be thought of as an asset, and like every other asset, this information needs to be secured from attacks. To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entry when it is needed (availability). Thus, confidentiality, integrity and availability can be termed as the three most important security goals. There are currently two fundamentally different networks, data networks and synchronous network comprised of switches. The internet is considered a data network. Since the current data network consists of computer based routers, information can be obtained by special programs, such as "Trojan horses," planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet.
Cryptography means "Hidden Secrets" is concerned with encryption. cryptography, the investigation of systems for secure correspondence. It is helpful for examining those conventions, that are identified with different viewpoints in data security, for example, verification, classification of information, non-denial and information uprightness. Cryptography is the science of writing in secret code. More generally, it is about constructing and analyzing protocols that block adversaries; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Fig. 1 shows Cryptography in which plain text is converted in cipher text by using some encryption technique and again it is converted into plain text by using decryption.

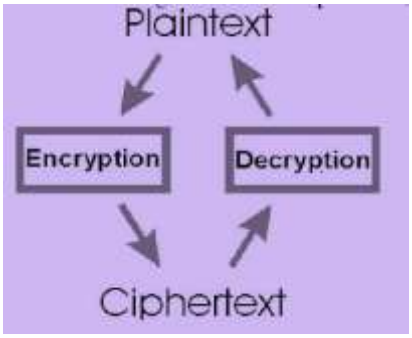

Fig 1: Cryptography

NETWORK SECURITY AND ISSUES :

For a wide variety of applications network security is key technology. Security is critical to networks and applications. In growing networks, network security is important requirement, but there is lack of security methods that can implemented easily. Although, network security is a critical requirement in emerging networks, there is a significant Network provides us with a wealth of quick information. Through the network we can share our data and can be said that the now networks are the essential part of our daily life. It brings great ease on our work, live and learning, but it also given us many problems. The increasing number of Information Security (IS) related incidents, organized crimes and phishing scams mean that IS deserves much closer attention. The three primary goals of network security which are confidentiality, integrity and availability can be achieved by using firewalls. Firewalls provide security by applying a security policy to arriving packets. A policy is a list of rules which define an action to perform on matching packets, such as accept or deny. When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. Network security provides protection by keeping away the hackers form the organization. Some network security threats are:

Spam:
Spam is digital junk mail. Spam is the use of email systems to send a vast amount of messages arbitrarily. There are various kind of spam like email spam, SEO spam, contact spam, link spam etc.

Virus:
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. They have the ability to duplicate themselves by hooking them to the program on the host and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET.

Trojan Horse:

"Trojan horse" refers to any program that bribe the user to execute it. In computing, it holds a very similar meaning — a Trojan horse, or "Trojan," is a malicious bit of attacking code that tricks users into running it willingly, by hiding behind a legitimate program. It can lead to many unwanted effects, like user's files can be deleted or another harmful software can be installed.

Denial of Services (DoS):
A DoS attack is performed by one machine and its internet connection, by flooding a website with packets and making it impossible for legitimate users to access the content of flooded website. This type of attack causes your computer to crash or to become so busy processing data that you are unable to use it.

Phishing
Phishing is a method with the goal of obtaining crucial data such as passwords, usernames, credit card numbers. Phishing endeavors are executed to consider data for web based business locales such as Amazon, eBay, payments processors such as PayPal, or any other financial website.

Rootkits:
These are designed to gain root access or we can say administrative rights in the user system. Once gained the root access, the hacker can do anything from stealing important and private files to personal data.

CRYPTOGRAPHY MECHANISM:

Cryptography is a technique to achieve confidentiality of messages. The term has a specific meaning in Greek: "secret writing". Cryptography is where security engineering meets mathematics. Billions of people around the globe use cryptography on a daily basis to protect data and information, although most do not know that they are using it.Cryptography is a method of protecting data and communications through the use of codes, so that only those for whom the information is intended can read and process it. The term cryptography is associated with changing plain text in another form called cipher text with the use of encryption and again cipher text to plain text with the use of decryption. Basic objectives of Cryptography are:

- Confidentiality: Information can't be perceived by an individual for whom it isn't intended to be.
- Integrity: The information cannot change in database or during transmission.
- Non-repudiation: At later stage sender can't deny their intention of creating information.
- Authentication: The sender and receiver can confirm each other's identity and the source/destination of the information.

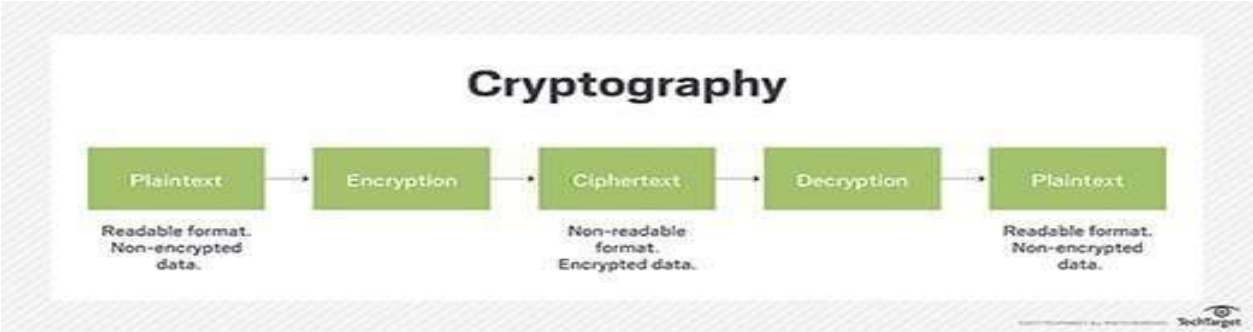

Fig 2: Process of Cryptography

Key: A key is a group of numeric or alpha numeric characters. Encryption algorithm uses key to change the data so that an intruder can't read the message or information.

Plain Text: The message generated by source which it is wants to send to destination is the plain text message. Basically it is original message and it has some meaning. For example if a person named as John wants to say "Hello Dear" to another person named as Rita, so this message is plain text.

Cipher Text: The message that is meaningless to everyone and can't read by intruder is called Cipher text. For example "LXFOPVEFRNHR" is cipher text of ATTACKATDAWN. Cipher text is also called Encoded data because plain text is converted to cipher text using Encoding mechanism. In process of Decoding, Cipher text is again converted to plain text.

Encryption: It is the process of changing plain text to converted form i.e cipher text. Two things are required in this first is Key and second is an encryption algorithm. Encryption is happen at source side.

Decryption: Opposite procedure of encryption is called decryption. In this cipher text is converted back into plain text with the help of a Key and unscrambling calculation.

CONCLUSION:

As the relevance and significance of privacy of data is increasing day by day, the importance of network security and cryptography is increasing parallely. Network Security is an important concept that is gaining attention as more and more internet usage is increasing. Installation of networks is still facing various problems regarding dangerous attacks. Cryptography plays a vital and critical role in achieving the primary aims of security goals, such as authentication, integrity, confidentiality, and no-repudiation. Cryptographic algorithms are developed in order to achieve these goals.

REFRENCES:

[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] Zhijie Liu Xiaoyao Xie, Member , IEEE ,School of Mathematics and Computer Science and Zhen Wang, Key Laboratory of Information Computing Science of Guizhou Province , Guizhou Normal University Guiyang , China, The Research of Network Security Technologies.

[7] The Research of Firewall Technology in Computer Network Security, 2009 Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications by Xin Vue, Wei Chen, Yantao Wang, College of Computer and Information Engineering Heilongjiang Institute of Science and Technology Harbin, China.

[8] Daemen, J., and Rijmen, V. "Rijndael: AES-The Advanced Encryption Standard, Springer, Heidelberg, March 2001.

[9] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. London: Academic Press,2011: Pp. 5-19.

[10] Shouhuai Xu, Xiaohu Li, Timothy Paul Parker, Xueping Wang, "Exploiting Trust based Social Networks for Distributed Storage of Sensitive Data", IEEE Transactions on Information Forensics andSecurity, Volume 6, Issue 1, 2011, pp 39-52, DOI: 10.1109/TIFS.2010. 2093521

[11] Lo-Yao Yeh, Yu-Lun Huang, Anthony D. Joseph, Shiuhpyng Winston Shieh, Woei-Jiunn Tsaur, "A Batch-Authenticated and Key Agreement Framework for P2P-Based Online Social Networks", IEEE Transactions on Vehicular Technology, Volume 61, Issue 4, pp 1907-1924, 2012, DOI: 10.1109/TVT.2012.2188821.