Review on Cryptography in Network Security

Mitesh Sharma
M.E. Scholar, Department of Computer Science and Engineering
M.B.M. Engineering College
Jai Narain Vyas University, Jodhpur

Abstract—With the explosive growth in the Internet, network security has become an inevitable concern for any organization whose internal private network is connected to the Internet. Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one who has the decipher key, and data cannot be changed means the original information would not be changed or modified; this is done when the sender includes a cryptographic operation called a hash function in the original message. A hash function is a mathematical representation of the information, when any information arrives at its receiver; the receiver calculates the value of this hash function. If the receiver’s hash function value is equivalent to the sender’s, the integrity of the message is assured. Network security is setup to guard against unauthorized access, alteration, or modification of information, and unauthorized denial of service. When a network is connected to the network that is vulnerable to potential intrusions and attacks. Security of data can be done by a technique called cryptography. So one can say that cryptography is an emerging technology, which is important for network security. This paper covers the various cipher generation algorithms of cryptography which are helpful in network security. Cryptography in the past was used in keeping military information, diplomatic correspondence secure and in protecting the national security. However, the use was limited. Nowadays, the range of cryptography applications have been expanded a lot in the modern area after the development of communication means; cryptography is essentially required to ensure that data are protected against penetrations and to prevent espionage. Also, cryptography is a powerful mean in securing e-commerce.

Key Words: Plain Text, Cipher Text, Attacks, Cryptography, Symmetric Encryption, Hash Algorithm.

I. INTRODUCTION

Nowadays, cryptography plays a major role in protecting the information of technology applications. Information security is an important issue, for some applications. Have the top priority such as ecommerce, e-banking, e-mail, medical databases, and so many more, all of them require the exchange of private information. Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. Cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing.

For example, let us consider a person named Alice a sender who wants to send a data message which has a length of characters to a receiver called Bob. Alice uses an unsecure communication channel. Which could be a telephone line, computer network, or any other channel. If the message contains secret data, they could be intercepted and read by hackers. Also they may change or modify the message during its transmission in such a way that Bob would not be able to discover the change. In this survey a various ways of encryption is viewed and have been compared. A lot of examples have been provided.

Network security is a new and fast moving technology and as such, is still being defined. When considering the desired learning outcomes of such a course, one could argue that a network security analyst must be capable of analyzing security from the business perspective in order to adhere to recent security legislation, and from the technical perspective in order to understand and select the most appropriate security solution. Network security originally focused on algorithmic aspects such as encryption and hashing techniques. While these concepts rarely change, these skills alone are insufficient to protect computer networks. As crackers hacked away at networks and systems,
courses arose that emphasized the latest attacks. Currently, many educators believe that to train people to secure networks, they must also learn to think like a cracker. The following background information in security helps in making correct decisions: Attack Recognition, Encryption techniques, Network Security Architecture, Protocol analysis, Access control list and vulnerability. For Network security cryptography is present. In cryptography data that can be read and understood without any special measures is called plaintext or clear text.

II. Cryptography Goals

By using cryptography many goals can be achieved. These goals can be either all achieved at the same time in one application, or only one of them. These goals are:

a) **Confidentiality:** It is the most important goal, that ensures that nobody can understand the received message except the one who has the decipher key.

b) **Authentication:** It is the process of proving the identity, that assures the communicating entity is the one that it claimed to be. This means that the user or the system can prove their own identities to other parties who don’t have personal knowledge of their identities. (The primary form of host to host authentication on the Internet today is name-based or address-based; and both of them are notoriously weak).

c) **Data Integrity:** It ensures that the received message has not been altered in any way from its original form. This can be achieved by using hashing at both sides the sender and the recipient in order to create a unique message digest and compare it with the one that received.

d) **Non-Repudiation:** It is mechanism used to prove that the sender really sent this message, and the message was received by the specified party, so the recipient cannot claim that the message was not sent.

e) **Access Control:** It is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources. If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access.

III. IMPORTANCE AND APPROACHES

The information that we need to hide, is called plaintext. It’s the original text. It could be in a form of characters, numerical data, executable programs, pictures, or any other kind of information. The plaintext for example is the first draft of a message in the sender before encryption, or it is the text at the receiver after decryption. The data that will be transmitted is called cipher text. It's a term refers to the string of “meaningless” data, or unclear text that nobody must understand, except the recipients. It is the data that will be transmitted exactly through network. Many algorithms are used to transform plaintext into cipher text.

Cipher is the algorithm that is used to transform plaintext to cipher text. This method is called encryption or encipher (encode), in other words, it’s a mechanism of converting readable and understandable data into “meaningless” data, and it is represented as follows:

\[ C = E_{k}(P) \]  

(1)

Where is the encryption algorithm using key .

The opposite of cipher mechanism is called decipher (decode) that is the algorithm which recovers the cipher text, this method is called decryption, in other words it’s the mechanism of converting “meaningless” data into readable data.

\[ F = D_{k^{-1}}(C) \]  

(2)
The Key is an input to the encryption algorithm, and this value must be independent of the plaintext. This input is used to transform the plaintext into cipher text, so different keys will yield different cipher text. In the decipher side, the inverse of the key will be used inside the algorithm instead of the key.

Computer security it’s a generic term for a collection of tools designed to protect any data from hackers, theft, corruption, or natural disaster while allowing these data to be available to the users at the same time. One example of these tools is the A-vast antivirus program.

Network security refers to any activity designed to protect the usability, integrity, reliability, and safety of data during their transmission on a network. Network security deals with hardware and software. The activity can be one of the following anti-virus and anti-spyware, firewall, Intrusion prevention systems, and Virtual Private Networks.

Internet Security is measures and procedures used to protect data during their transmission over a collection of interconnected networks. While information security is about how to prevent attacks, and to detect attacks on information-based systems. Cryptanalysis (code breaking) is the study of principles and methods of deciphering cipher text without knowing the key. Typically this includes finding and guessing the secret key. It’s a complex process involving statistical analysis, analytical reasoning, mathematical tools, and pattern-finding. The field of both cryptography and cryptanalysis is called cryptology.

Symmetric encryption refers to the process of converting plaintext into cipher text at the sender with the same key that will be used to retrieve plaintext from cipher text at the recipient. While asymmetric encryption refers to the process of converting plaintext into cipher text at the sender with different keys that will be used to retrieve plaintext from cipher text at the recipient.

Passive attacks mean that the attackers or the unauthorized parties just monitoring on the traffic or online communication between the sender and the recipient, but not attempting to breach or shut down a service. This kind of attacks is very hard to discover, since the unauthorized party doesn’t leave any traces. On the other hand active attacks mean that the attackers are actively attempting to cause harm to the network or the data. The attackers are not just monitoring on the traffic, but they also attempt to breach or shut down the service.

Authentication is the process of determining whether someone is the same person who really is, such as login and password in login pages while authorization is the process of ensuring that this person has the ability to do something. Brute force is the attacker who is trying all of the possible keys that may be used in either decrypt or encrypt information.

IV. TYPES OF CRYPTOGRAPHY

There are many types of cryptography, including codes, Steganography (hidden or secret writing), and ciphers. Codes rely on codebooks. Steganography relies on different ways to hide or disguise writing. Ciphers include both computer-generated ciphers and those created by encryption methods. The different types of ciphers depend on alphabetical, numerical, computer-based, or other scrambling methods.

a) Codes and Codebooks

A well-constructed code can represent phrases and entire sentences with symbols such as five-letter groups, and is often used more for economy than for secrecy. A properly constructed code can give a high degree of security, but the difficulty of printing and distributing codebooks—books of known codes—under conditions of absolute secrecy limits their use to places in which the books can be effectively guarded. In addition, the more a codebook is used, the less secure it becomes.

Imagine a codebook with two columns. In the first column is a list of all the words that a military commander could possibly need to use to communicate. For example, it contains all the possible geographic areas in a region, all possible times, and all military terms. In the other column is a list of plain words. To create a coded message, the encoder writes down the actual message. He then substitutes words in the codebook by finding matches in the second column for the words in the message and using the new words instead. For example, suppose the message is Attack the hill at dawn and the codebook contains the following word pairs: attack = bear, the = juice, hill = orange, at = calendar, and dawn = open. The encoded message would read Bear juice orange calendar open.

If the coded message fell into enemy hands, the enemy would know it was in code, but without the codebook the enemy would have no way to decrypt the message. Codebooks lose some of their value over time, however. For example, if the coded message fell into enemy
handsand the next day the hill was attacked at dawn, the enemy could link the event to the coddmessage. If another message containing the word orange were captured, and the following day, something else happened on the hill, the enemy could assume that orange = hill is in the codebook. Over time, the enemy could put together more and more code word pairs, and eventually crack the code. For this reason, it is common to change codes often.

b) Steganography:
Steganography is a method of hiding the existence of a message using tools such as invisible ink, microscopic writing, or hiding code words within sentences of a message (such as making every fifth word in a text part of the message). Cryptographers may apply steganography to electronic communications. This application is called transmission security. Steganography, or secret writing, seems to have originated almost as early as writing itself did. Even in ancient Egypt, where writing itself was a mystery to the average person, two distinct forms of writing were used. Hieratic or sacred writing was used for sacred communication by the priests, and demotic writing was used by other literate people. The ancient Greeks and Romans, as well as other civilizations that flourished at about the same time, used forms of steganography. The invention of the first shorthand system was presumably intended as a form of secret writing. Shorthand first came into wide use in ancient Rome, with notae Tironianae ('Tironian notes'), a system invented by Marcus Tullius Tiro in 63 BC.

c) Ciphers
Ease of use makes ciphers popular. There are two general types of ciphers. Substitution ciphers require a cipher alphabet to replace plaintext with other letters or symbols. Transposition ciphers use the shuffling of letters in a word to make the word incomprehensible. Ciphers are the secret codes used to encrypt plaintext messages. Ciphers of various types have been devised, but all of them are either substitution or transposition ciphers. Computer ciphers are ciphers that are used for digital messages. Computer ciphers differ from ordinary substitution and transposition ciphers in that a computer application performs the encryption of data. The term cryptography is sometimes restricted to the use of ciphers or methods involving the substitution of other letters or symbols for the original letters of a message.

d) Computer Ciphers & Encryption
Government agencies, banks, and many corporations now routinely send a great deal of confidential information from one computer to another. Such data are usually transmitted via telephone lines or other nonprivate channels, such as the Internet. Continuing development of secure computer systems and networks will ensure that confidential information can be securely transferred across computer networks.

e) Cryptanalysis
Cryptanalysis is the art of analyzing ciphertext to extract the plaintext or the key. In other words, cryptanalysis is the opposite of cryptography. It is the breaking of ciphers. Understanding the process of code breaking is very important when designing any encryption system. The science of cryptography has kept up with the technological explosion of the last half of the 20th century. Current systems require very powerful computer systems to encrypt and decrypt data. While cryptanalysis has improved as well, some systems may exist that are unbreakable by today's standards.

Today's cryptanalysis is measured by the number and speed of computers available to the code breaker. Some cryptographers believe that the National Security Agency (NSA) of the United States has enormous, extremely powerful computers that are entirely devoted to cryptanalysis. The substitution ciphers described above are easy to break. Before computers were available, expert cryptanalysts would look at ciphertext and make guesses as to which letters were substituted for which other letters. Early cryptanalysis techniques included computing the frequency with which letters occur in the language that is being intercepted. For example, in the English language, the letters e, s, t, a, m, and n occur much more frequently than do q, z, x, y, and w. So, cryptanalysts look at the ciphertext for the most frequently occurring letters and assign them as candidates to be e, s, t, a, m, and n. Cryptanalysts also know that certain combinations of letters are more common in the English language than others are. For example, q and u occur together, and so do t and h. The more ciphertext that is available, the better the chances of breaking the code.

Security services
**Security Requirements:**

**Confidentiality:** Protection from disclosure to unauthorised persons.

**Integrity:** Maintaining data consistency.

**Authentication:** Assurance of identity of person or originator of data.

**Non-repudiation:** Originator of communications can’t deny it later.

**Availability:** Legitimate users have access when they need it.

**Access control:** Unauthorised users are kept out. These are often combined: User authentication used for access control purposes, Non-repudiation combined with authentication.

**Security Threats**

Information disclosure/information leakage, Integrity violation, Masquerading, Denial of service illegitimate use, Generic threat: Backdoors, trojan horses, insider attacks. Most Internet security problems are access control or authentication ones. Denial of service is also popular, but mostly an annoyance.

**V. SYMMETRIC AND ASYMMETRIC ENCRYPTION**

Encryption is the strongest and the safest way in securing data. Certainly, it is the most common one. Encryption systems are divided into two major types or forms, symmetric and asymmetric.

**Symmetric encryption** is known as secret key or single key, The receiver uses the same key which the sender uses to encrypt the data to decrypt the message. This system was the only system used before discovering and developing the public key. A safe way of data transfer must be used to moving the secret key between the sender and the receiver in symmetric encryption. Figure 4 shows how the system works. Symmetric encryption occurs either by substitution transposition technique, or by a mixture of both. Substitution maps each plaintext element into cipher text element, but transposition transposes the positions of plaintext elements.

**Asymmetric encryption** is slower and very complicated in calculations than symmetric encryption. Therefore, asymmetric encryption deals with plaintext as a group of numbers which are manipulated in mathematics, while the plaintext in symmetric encryption deal as group of symbols and characters, the encryption process may permute these symbols, or may substitute one symbol by another. So the nature of the data determines the system of encryption type. And every system has its own uses. For example, asymmetric encryption may be used in authentication or in sending secret key for decryption.

**V. Model for Network Security**

Using this model requires us to:

- design a suitable algorithm for the security transformation
- generate the secret information (keys) used by the algorithm
- develop methods to distribute and share the secret information
- specify a protocol enabling the principals to use the transformation and secret information for a security service
VI. CRYPTOGRAPHY TECHNIQUES OF SECURED MANETS/WSNS DESIGN

Security is the combination of processes, procedures and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non-repudiation.

- **Confidentiality:** The goal of confidentiality is to keep sent information from being read by unauthorized users or nodes. MANETs/WSNs use an open medium, so usually all nodes within the direct transmission range can obtain the data. One way to keep information confidential is to encrypt the data. In WSNs, confidentiality is achieved to protect information from disclosure when communication is between one sensor node and another sensor node or between the sensors and the base station. Compromised nodes may be a threat to confidentiality if the cryptographic keys are not encrypted and stored in the node.

- **Authentication:** The goal of authentication is to be able to identify a node or a user and to prevent impersonation. In wired networks and infrastructure-based wireless networks, it is possible to implement a central authority at a router, base station, or access point. However, there is no central authority in MANETs/WSNs, and it is much more difficult to authenticate an entity. Confidentiality can be achieved via encryption. Authentication can be achieved by using an authentication code (MAC) (Menezes, Oorschot & Vanstone, 1996).

- **Integrity:** The goal of integrity is to keep a sent message from being illegally altered or destroyed during transmission. When the data is sent through the wireless medium, the data can be modified or deleted by malicious attackers. The malicious attackers can also resend it, an action known as a replay attack. Integrity can be achieved through hash functions.

- **Non-repudiation:** The goal of non-repudiation is related to the fact that if an entity sends a message, the entity cannot deny that it sent the message. By producing a signature for the message, the entity cannot later deny having sent that message. In public key cryptography, anode, A, signs the message using its private key. All other nodes can verify the signed message using A’s public key, and A cannot deny that its signature is attached to the message.

- **Availability:** The goal of availability is to keep the network service or resources available to legitimate users. It ensures the survivability of the network despite malicious incidents. In a WSN, the examples of risk of loss of availability can be sensor node capturing and denial of service attacks. One solution could be to provide alternative routes in the protocols employed by the WSN to mitigate the effect of outages.

- **Access control:** The goal of access control is to prevent unauthorized use of network services and system resources. Obviously, access control is tied to authentication attributes. In general, access control is the most commonly needed service in both network communications and individual computer systems.
Cryptography is very strongly tied to mathematics and number theory. It is, therefore, difficult to create a new design using composite cryptographic techniques without the sound security analysis behind it, usually based on cryptographic reasoning. One way to reach this goal is to learn from others by reviewing the current MANET/WSN security schemes, and also to understand the network to further understand how cryptographic techniques combine with MANETs/WSNs to provide a security service with reasonable network performance, scalability, storage, and synchronization. Certainly the security design can be evaluated using different techniques. Our goal is to provide perspective using cryptographic techniques and study basic cryptographic techniques (as seen in Figure 1) when applied to authentication, trust, and key management in MANETs/WSNs. Furthermore, we can study several of the most commonly used cryptographic techniques and see how they are employed to deal with different tasks and balance security and performance.

It is a common approach today to use software engineering design patterns to illustrate the design of object-oriented programming. Likewise, in security and performance of MANETs/WSNs, cryptographic techniques can successfully be used in different stages of network bootstrap, packet communication, and factors to be evaluated. These techniques can certainly be reused after the analysis as known techniques from the cryptography perspective. One of the approaches we take here is to break down the design using cryptographic techniques and do some reverse engineering, then see how the new design is formed using different cryptographic techniques.

CONCLUSION

Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one that has the decipher key, and "data cannot be changed" means the original information would not be changed or modified; this is done when the sender includes a cryptographic operation called a hash function in the original message. A hash function is a mathematical representation of the information, when information arrives at its receiver; the receiver calculates the value of this hash function. If the receiver’s hash function value is equivalent to the sender’s, the integrity of the message is assured. In this survey paper we describe and compare between symmetric and asymmetric encryption technique. Cryptology presents a difficulty not found in normal academic disciplines: the need for the proper interaction of cryptography and cryptanalysis. This arises out of the fact that in the absence of real communications requirements, it is easy to propose a system that appears unbreakable. Many academic designs are so complex that the would-be cryptanalyst doesn’t know where to start; exposing flaws in these designs is far harder than designing them in the first place. The result is that the competitive process, which is one strong motivation in academic research, cannot take hold.

Many applications are useful in real-time and daily life that are implemented by cryptography through implicit or explicit. For example banking systems, ATMs, Smart cards, Magnetic strip technology, National Security Agency (NSA) to trace information through RADAR and with well equipped material, E-commerce, E-economics, business information, operating systems, databases and finally in system protection. In this way Cryptography has many roles and many applications provide many example to show the differences.

REFERENCES:
