Network Security Issues and Cryptography

PriyaTrivedi[1], Sanya Harneja[2]

[1]Information Technology, Maharishi Dayanand University
Farrukhnagar, Gurgaon, Haryana, India

[2]Information Technology, Maharishi Dayanand University
Farrukhnagar, Gurgaon, Haryana, India

[1]priyatrivedi77@gmail.com , [2]sanyaharneja@gmail.com

Abstract:
In the recent years there have been a radical evolution in the aspects and requirements of network security. Networks are subject to attacks from malicious sources. There are different factors contributing to these changes. There is a shift from threats like Denial of Service (DoS) to dynamic content-based attacks like rootkits, key loggers, and Virus, Worms, Trojans and Phishing. Network security is responsible for securing all information passed through the network. Network security starts with authenticating, commonly with a username and a password. One of the techniques used in network security is Cryptographic .Cryptographic is a looming technology, which is important for security. As applied to computer network security, cryptography protects data from theft or alteration and can also be used for user authentication. This paper describes the vulnerability and various threats in network, analysis of current network security and issues with current security solutions and also the Cryptographic techniques used in network security. [1][2]

Keywords- Network, Threats, Cryptography, issues, security solutions.

Introduction:

For the first few decades, computer networks were primarily used by university researchers for sending e-mail and by corporate employees for sharing some devices like printers. Under these conditions, security is not that much necessary. But nowadays, as millions of ordinary citizens are using networks for banking, shopping and many other purposes, network security is a potentially massive problem.

The network needs security against attackers and hackers. Network Security includes two basic securities. The first is the security of data information i.e. to protect the information from unauthorized access and loss. And the second is computer security i.e. to protect data and to thwart hackers. Here network security not only means security in a single network rather in any network or network of networks.

Another part of network security includes the computer security. Computer security means to protect your computer system from unwanted damages caused due to network. One of the major reason for such damages are the viruses and spywares that can wipe off all the information from your hard disk or sometimes they may be enough destructive and may cause hardware problems too. Certainly the network must be protected from such type of damaging software. The people who intentionally put such software on the network are called Hackers. As the network computers are part of it, so the computer security from Hackers is also a part of network security [2]

.

Network Security:

In the field of networking, the area of network security consists of provision and policies adopted by the network administrator to monitor and prevent unauthorized access, misuse, denial of computer network and network –accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.

Network Security is concerned with people trying to access remote services that they are not authorized to use. Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone. Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, nonrepudiation, and integrity control. [3]

Secrecy:

Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized users.

Only the sender and intended receiver should be able to understand the contents of the transmitted message. Because eavesdroppers may intercept the message, this necessarily requires that the message be somehow encrypted (disguise data) so that an intercepted message cannot be decrypted (understood) by an interceptor. This aspect of secrecy is probably the most commonly perceived meaning of the term "secure communication.”.

Authentication:

Authentication is a process that ensures and confirms a user’s identity. Authentication is one of the five pillars of information assurance (IA). The other four are integrity, availability, confidentiality and nonrepudiation. Both the sender and receiver need to confirm the identity of other party involved in the communication - to confirm that the other party is indeed who or what they claim to be. Face-to-face human communication solves this problem easily by visual recognition. When communicating entities exchange messages over a medium where they cannot "see" the other party, authentication is not so simple.

Nonrepudiation:

Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Integrity Control:

Integrity, in terms of data and network security, is the assurance that information can only be accessed or modified by those authorized to do so. Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either maliciously or by accident, in transmission. [3][6]

Cryptography:

The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext.

Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and
Space complexity [5]. Figure 1 is representing conventional encryption.

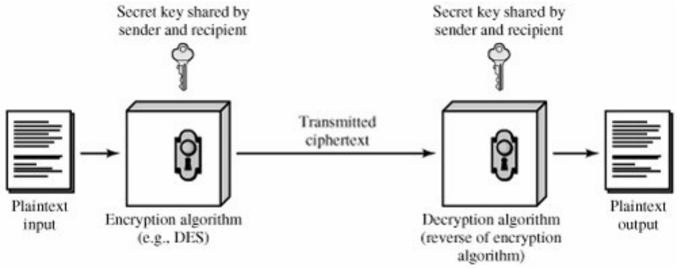
Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 1: A Simplified Model of Conventional Encryption

Types of Cryptographic Algorithms:

There are several ways of classifying cryptographic algorithms. Here it will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are (Figure 1):

Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.
Public Key Cryptography (PKC): Uses one key for encryption and another for decryption. [4]
Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

Secret Key Cryptography (SKC):

With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 2, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

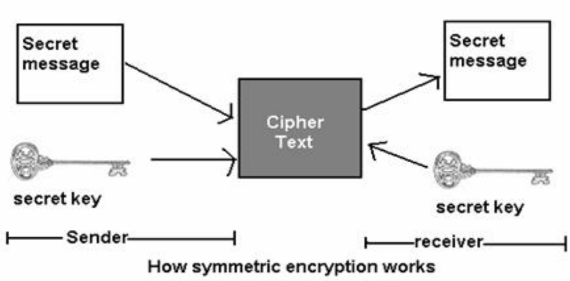

Figure 2: Secret Key Encryption

Public Key Cryptography:

Public-key cryptography, also known as asymmetric cryptography, is a class of cryptographic algorithms which requires two separate keys, one of which is secret (or private) and one of which is public. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt cipher text or to create a digital signature. The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other – as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both. Public key algorithms, unlike symmetric key algorithms, do not require a secure initial exchange of one (or more) secret keys between the parties.

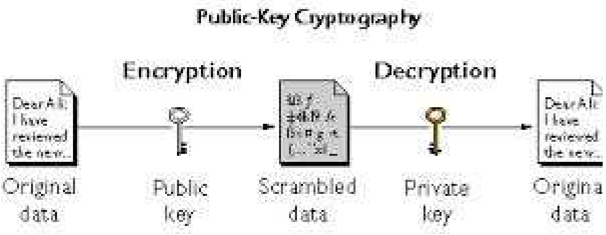

Figure 3: Public Key Cryptography

Public-key cryptography algorithms that are in use today for key exchange or digital signatures include:

RSA: The first, and still most common, PKC implementation, named for the three MIT mathematicians who developed it — Ronald Rivets, Aid Shamir, and Leonard Adelman. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. The public key information includes n and a derivative of one of the factors of n; an attacker cannot determine the prime factors of n (and, therefore, the private key) from this information alone and that is what makes the RSA algorithm so secure. [4][6]

Diffie-Hellman: After the RSA algorithm was published, Diffie and Hellman came up with their own algorithm. D-H is used for secret-key key exchange only, and not for authentication or digital signatures [5].

Hash Function:

Hash functions, also called message digests and one-way encryption, and are algorithms that, in some sense, use no key (Figure 1C). Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file. [6]

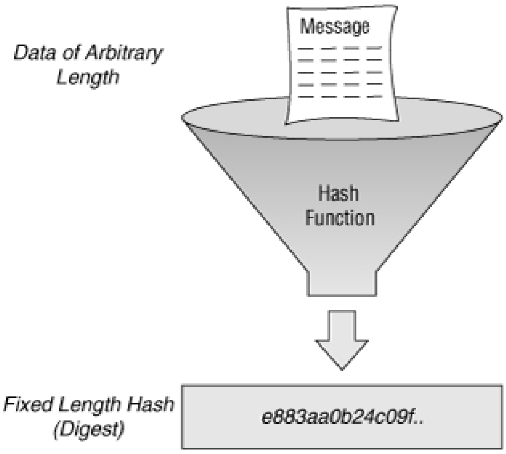

Figure 4: Hash Function

Application of three cryptographic technique:

Hash functions, for example, are well-suited for ensuring data integrity because any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender.

Secret key cryptography, on the other hand, is ideally suited to encrypting messages, thus providing privacy and confidentiality. The sender can generate a session key on a per-message basis to encrypt the message; the receiver, of course, needs the same session key to decrypt the message.

Asymmetric schemes can be used for non-repudiation and user authentication; if the receiver can obtain the session key encrypted with the sender's private key, then only this sender could have sent the message.

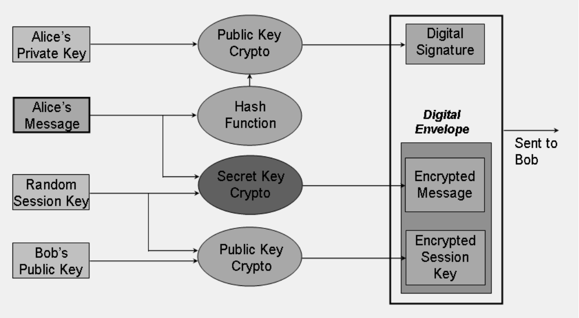

Figure 5: Sample application of the three cryptographic techniques for secure communication.

This diagram purposely suggests a cryptosystem where the session key is used for just a single session. Even if this session key is somehow broken, only this session will be compromised; the session key for the next session is in no way based upon the key for this session, just as this session's key is not dependent on the key from the previous session. [5]

Conclusion:

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together. We have studied various cryptographic techniques to increase the security of network.

References:

[1] Simmonds, A; Sandilands, P; van Ekert, L (2004) Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp.317–323.

[2]”Advance cryptography algorithm for improving data security” published in International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 1, January 2012.

[3]”Network Security Using Cryptographic Techniques” published in International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 12, December 2012

[4] Aameer Nadeem, Dr. M.Younus Javed, ―A performance comparison of data Encryption Algorithm‖, Global Telecommunication Workshops, 2004 GlobeCom Workshops 2004, IEEE.

[5] “Gary C. Kessler,” An Overview of Cryptography”.

[6] The "No Network is 100% Secure" series - Cryptography -A White Paper.