ANALYSIS OF NETWORK SECURITY USING CRYPTOGRAPHY

Mazhar H. Malik[1], Muhammad Adnan Rafi[2]
[1]Department of Computing, Global College of Engineering and Technology, Muscat, Oman.
Email: mazhar@gcet.edu.om
[2]Department of Engineering and Applied Science, Aston University, Birmingham, UK.
Email: rafim@aston.ac.uk

ABSTRACT*—As the users of computers increase similarly usage of the internet also increases. The usage of the internet is common and important to personal computers, computers in organizations, and most secure military computers. Internet, as well as network applications, are increasing rapidly, the internet structures are not secure themselves and therefore allow many security threats and attacks to occur. There are a lot of techniques and methods for network security. Cryptography is a strong encryption technique that is remarkably hard to break. It converts the information from its original form to an un-understandable and scribbled form. There are many cryptographic techniques and in this paper, we will discuss the cryptographic techniques in terms of secure, fast, quality, and block size.*

Keywords-Network Security, Cryptography, Symmetric Encryption, Asymmetric Encryption

1. INTRODUCTION

With the passage of time and new trends of technology, the world is now becoming more interconnected. Computers are all around the world and information/data travels from these connected computers using different communication/connection techniques to send and receive that data and hence security of all data and information has great importance.

Cryptography is generally referred to as "the study of secret". Cryptography consists of two parts Encryption and the Decryption. In Encryption, data are changed from its original form to some un-predictable/ciphertext form as shown in figure 1.

Similarly, Decryption converts that unreadable form of data to its original form.

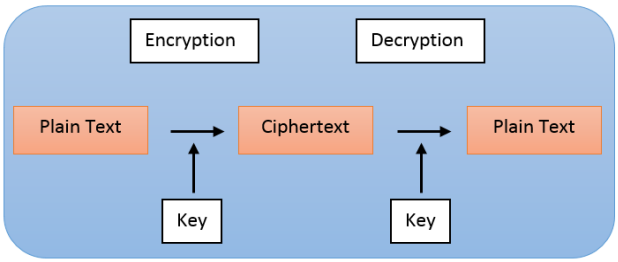

Figure 1: Architecture Diagram

In data security, a sender's data are altered into unreadable data for transferring it to the data network. Even if this unreadable data are interrupted during transmission, a process or method is required to decode that message. With the passage of time security techniques developed and enhanced such that fully strong cryptography in the previous years now easily decoded/traced today. Cryptographic techniques and methods have to be advanced because hacker's advancements are also non-stopped. While transmitting cipher-text over a data network, the important thing is to make the network security for credential data. This protects the cipher-text from unauthorized access and attacks so that it will diminish the risk of many attacks to penetrate the information. A secure network also stops unauthorized access from intercepting unauthorized code into the network. Therefore, strong ciphers are required as well as secured networks. There are two basic kinds of different networks, data networks like the internet and switched synchronous networks like ATM, etc. Since the data network which is the internet of today comprise of computerbased routers, special kind of programs are used to access information over routers, such as "Trojan- horses" lodged into routers.

The synchronous networks also known as switched Networks do not buffer/store messages and that's why they are not rendered by attackers easily. This is the reason security is stressed mostly in networks that connect to the internet and data networks which is the internet of today.

The vast topics of network security are considered by exploring the following:

1. History and background of security and attacks in networks
2. Types of internet attacks, threats, and security techniques and methods
3. Internet architecture and susceptible security facets of the Internet
4. Network Security for networks linked to the internet
5. Existing development and enhancement in network security in software and hardware

On the ground of this research, the fate of the secure network and network security is anticipated. New developments that promise will also be focused to be aware of where the security for networks is lying.

2. Common Internet anti-threat and Attack Methods

Common Internet anti-threat and Attack Methods are divided into categories. Some attacks access personal information or system knowledge, such as phishing and eavesdropping. Attacks can also affect the system's functionality, such as trojans, viruses, and worms. There is another kind of attack that is a denial of service (DoS)-attack in which the system's resources are consumed uselessly and make the machine or resources unavailable. There are many different forms of network interruptions, such as smurf attacks, land attacks, SYN Flooding, and teardrop attacks. DoS attacks are much famous than these attacks, but these attacks work in some way even if they aren't declared commonly by any name.

A. Viruses:

Viruses are auto-running programs which replicate themselves that mostly use files for infecting and spreading on victims system. Once a virus attached file is opened, the virus automatically activated itself and starts infecting the system.

B. Worms:

Similar to viruses a worm also replicates itself and spread over the target system, but they do not use any file to extend over the target machine. Two known basic types of worms are network-aware and mass-mailing. Network-

aware worms chose a target and if the worm succeeds in accessing the target host, it can use Trojan or other to infect it. Mass mailing worms are concerned with emails to infect other systems. For the Internet, Network-aware worms are a major issue.

C. Eavesdropping:

Interference of data being sent and received over the network by unauthorized access is called eavesdropping. It has two types

a. Passive eavesdropping

b. Active eavesdropping

In passive eavesdropping someone only furtively listens to the sent messages. While in the Active eavesdropping the attacker listens and injects its malicious data into the communicated messages. This can distort the messages being sent. So this way the sensitive information can be stolen.

D. Phishing:

Phishing is an attack to get confidential data from a group, an individual, or an organization. Phishers trap users into unveiling personal data or sensitive information like credit card numbers, credentials of online banking, etc.

E. Trojans:

Trojans for a user look like benign programs, but in reality, they actually have malicious purposes. Trojans typically hold some other infecting programs such as a virus.

F. IP Spoofing Attacks:

IP address spoofing attack method which is most frequently used is an attack in which an intruder sends IP packets from a fake (or "spoofed") source address so as to cover up itself. Denial-of-service attacks frequently use IP spoofing to overload devices and networks with packets that appear to be from valid source IP addresses. The identity of the attacker is concealed in different ways making hard to be detected and prevented. IP protocol technology that is the current technology of IP protocols, IP spoofed packets cannot be removed.

G. Denial of Service:

Denial of Service attack is an attempt when the system cannot respond with the requestors due to receiving too many requests. This attack is a try and aimed to make a network resource or machine unavailable to its hosts, such as to momentarily or permanently infect or suspend services of the host linked to the Internet.

H. Technology for Internet Security:

Internet threats are the major problems in the computer world as long as internet communication is occurring to make information accessible and transmitted across the Internet. There are different security and detection mechanisms and methods to deal with such kinds of attacks.

I. Cryptographic Systems:

Nowadays, cryptography is the most powerful and widely used tool in securing data over the transmission. It involves different codes and ciphers to convert information into an unreadable data form.

J. Firewall:

A firewall is a predefined security rules-based control method and boundary defense. It is used to block incoming and outgoing traffic. A firewall is the frontier defense system against attackers. This system is designed to avoid unauthorized access to a private network. Firewalls are usually implemented in both the hardware and the software.

K. Intrusion Detection Systems:

An IDS (Intrusion Detection System) is a system that is used as an extra protection measure and helps protect against computer intrusions. IDS systems can be software or hardware devices that are used to discover attacks. These systems are used to monitor connections for attacks. These IDS systems can also be used to monitor and alert of attacks and can also be used to block the attacks.

L. Anti-Malware Software and Scanners:

Malware is short for malicious software such as viruses, worms, Trojan, and horses. Special software called anti-Malware tools is used to determine malware and cure the infected system.

M. Secure Socket Layer (SSL):

To achieve a fine level of security b/w a web-browser and a website Secure Socket Layer (SSL) is used which is a set of protocols that is a standard way for browsing security. SSL is intended to create a secure channel between a web server and the web browser to make exchanged information protected. SSL uses certificates to provide authentication of clients to the server. Hosts send a certificate to the server to show their identity.

3. Encryption Methods

There are three basic encryption methods which vary with each other on their techniques

A. Hashing:

Hashing is a technique that is used to create a unique and fixed-length key for a message or data. Hashing is hard to break because a little change in the message would be easily tracked due to the uniqueness of hashing to aspecific message. Hashing, not an encryption technique as such it is very useful and has a valuable mark in proving that data is changed or not from the original message.

B. Symmetric Methods:

Symmetric methods also called private key cryptography because it uses only one private key for which is not publically available to all so it's security also increases because no one can access it to decrypt. In this method sender first, encrypt data using a single key, and send this data to the receiver after receiving the data receiver use a single key to decrypt the data so the message must remain secure.

C. Asymmetric Methods:

The asymmetric method is different from symmetric the reason is it uses both public and private keys. It is also called the public-key method. A freely available key is used to encrypt the message and send it to the receiver and a private key also use to decrypt this message.

4. Difference between Symmetric and Asymmetric Methods

Symmetric and asymmetric encryption both algorithms are different in the following key points of view.

Symmetric is more secure and fast because they use a single key which is also called a private key. Access to that private key not easy as compared to the public key which is used in Asymmetric encryption algorithms. In Asymmetric data is encrypted with one key called the public key and decrypted with other key called the private key. Almost 3,000-bit required to achieve the same security level of symmetric algorithms that use 128-bit. Symmetric is practical and fast as compared to the

Asymmetric algorithms are slow and impractical to encrypt a piece of huge information. Symmetric algorithms are often used in computers due to speed. Often both

symmetric and Asymmetric used together, such that randomly generation of the key is encrypted by a public key, and message encryption done by a private key. This type of encryption is called Hybrid encryption.

Symmetric encryption algorithms use the same single key for both processes of encryption and decryption and it is easy to derive the decryption key from the encryption key, whereas in asymmetric encryption the decryption key cannot be derived from the encryption key and therefore in asymmetric encryption both keys of encryption and decryption are different. Symmetric encryption algorithms stream ciphers and block ciphers are used in symmetric encryption algorithms. We use stream ciphers to encrypt for a single bit of a message whereas a block of bits is encrypted using block ciphers. Some examples of popular symmetric encryption algorithms:

Asymmetric Encryption Algorithms Asymmetric encryption algorithms normally employ different keys both for encryption and decryption, typically encryption and decryption keys vary from each other and cannot be derived from each other.

Asymmetric-encryption-algorithms:

- RSA Algorithm
- Diffie-Hellman
- Digital-Signature Algorithm

A. RSA Algorithm:

Rivest-Shamir-Adleman (RSA), named on the three MIT mathematicians who designed and developed it[9]: Ronald Rivest, Adi Shamir, and Leonard Adleman is one of the first and most popular algorithms that use public-key asymmetric encryption algorithm. It is also used in digital signatures, encryption of data blocks, and key exchange. The factoring of this algorithm is the security of RSA, which is based on the three major processes: Key Generation, Encryption, and Decryption.

In this algorithm a user when sending a message then RSA takes two large prime numbers and produces a product of that number also gets auxiliary value. These prime numbers must be kept confidential only someone with a well-known grip on prime numbers can easily decode that message if it is accessed by someone. RSA now a day widely used due to its integrity, authenticity, and non-reputability.

A. Diffie-Hellman:

D-H is 1stpublic key encryption, developed by Diffie-Hellman in 1976 [11]. In this algorithm, we use a discrete form of logarithms. In this algorithm sender and receiver exchange a confidential key to each other.

Diffie-Helman is a process of sharing a secret between the sender and receiver in such a way that the key can't be seen. That's an important distinction “This Algorithm not sharing key it just use to create a key together”.

B. Digital Signature Algorithm:

In 1991 NIST proposed an algorithm for digital signatures which is called Digital signature Algorithm. This algorithm adopted by FIPS (Federal Information Processing Standard) in 1993. It is an electronic signature of handwritten signatures. It consists of both public and private keys. The signature generation uses a private key for the generation process and the public key for the verification of electronic signature Symmetric Encryption Algorithms

- AES-Rijndael
- Blowfish
- CAST-5
- DES
- IDEA
- RC-2
- RC-4
- RC-6
- SEED
- Serpent
- JEA
- T-DES(Triple DES)

A. AES-Rijndael:

AES (Advanced Encryption Standard) encryption algorithm AES symmetric encryption strategy will displace the conventional method Data Encryption Standard (DES). US Government's NIST issued entries of encryption calculations which in turn consequence to AES. NIST stands for the Institute of Standards and Technology and that is finished in 2000. Advanced Encryption Standard was a 21stcentury successor that was a reaction of the rising practical attempts against DES. AES was a result of dispatch of a call for proposition from NIST. In the second round top five algorithms selected, the latest standard from five of that algorithm was Rijndael selected. NIST's answer behind selecting Rijndael that this algorithm is compatible and performance in both software and hardware development environment was exceptional in every single conceivable mode. Its low memory essentials and amazing key setup time make it exceptional. Force and timing attempts are issues but this algorithm is gentler to protect against them. Comparing all five algorithms NIST show that every one of them had enough security. Vincent Rijmen and Joan Daemen[10] were cryptologists who were Belgian. In November 2001 NIST as a Federal Information Processing Standard selected AES as secure encryption (FIPS-197). Ciphers used in Rijndael are conventional square. Rijndael's algorithm uses keys sizes 256,192,128 key for encryption. Every different length of the key makes the algorithm to act as an unexpected way due to key size variations. Rijndael adopts the convention of square ciphers. AES algorithm utilizes 3 key sizes: a 27-, 192-, or 28-piece encryption key. All the encryption key sizes cause the algorithm to act somewhat in an unexpected way, so the expanding key lengths not only offer a big sized bit which can easily mix up the information data, additionally enhance the unpredictability of the algorithm.

B. Blowfish:

Blowfish is a technique that encrypts in symmetrically that is developed in 1993 by Bruce Schneier as an alternative to existing encryption strategies. Blowfish is license-free, tested, and is accessible free for use and implementation. Blowfish uses block size26- bits and a variable key length from 25 bits to a maximum of 448 total bits. It is a 24-round Feistel cipher and uses extensive key-subordinate S-boxes. When deciding the Key, it generates an extensive pseudo-arbitrary search for tables by making a few encryptions.

The tables rely upon the key provided by the client in a very tough manner. This tactic has been turned out to be exceedingly safe against numerous attacks, for example, straight cryptanalysis and differential. Unfortunately, this also implies that it is not the optional algorithm that can be chosen for conditions where a vast space of memory is not accessible. Blowfish is comparative in structure to CAST-27, which utilizes altered S-boxes. The main known attack against Blowfish depends on its frail key classes.

C. CAST-5:

The innovators of CAST are Carlisle Adams and Stafford Tavares. CAST also stands for Carlisle Adams and Stafford Tavares. CAST is a conventional 64-bit block cipher that has a place with the standard of encryption algorithms called Feistel ciphers. CAST-128has the Feistel structure which is a DES-like (SPN) Substitution-Permutation Network cryptosystem.CAST-128uses eight altered S- boxes. CAST 128 backings variable lengths of key somewhere around 40 to 128 bits. CAST- 128 is immune to both direct and differential cryptanalysis. Right now, breaking CAST short of brute force has no known method. PGP uses currently the default cipher as CAST.

D. DES:

DES is a symmetric (Private-key) algorithm using a square cipher of size 64 bits. But it uses only 56 bits of key length. In 1977United States acquired the DES (Data Encryption Standard), the asymmetric algorithm as a Govt. Standard.DES encode-decode information in 64- bits block, utilizing a 56bits key. It carries a plaintext of 64bit block of as input and resultant is a cipher-text of 64-bits block. Since it commonly works on a block of the corresponding length and it utilizes both modifications and substitutions as a part of the algorithm. DES has 24 iterations that mean the principle algorithm is rehashed 24 times to create the cipher-text. The brute force attack takes an exponential measurement of time corresponding to its key length for iterations. So as the number of iterations increases with key length, the security of the algorithm grows up exponentially.

For a long time, DES-enciphered information was sheltered in light of the fact that a couple of associations had the computing power to break it in any case. In 1998-July a group of cryptographers broke a DES-enciphered data just in 3 days. In 1999 a system of 10,000 desktop personal computers split a DES enciphered message within a day. DES was unmistakably no safer and from that point forward T-DES (3-DES) has risen as a more grounded technique.

Triple DES encodes information thrice and uses an alternate key for no less than one of the 3 passes giving it a total key size of 112-168 bits. This should create a normal quality of about 112 bits, which is sufficient to defend against brute force attacks. T-DES is much more potent than DES that is single; nonetheless, there are some new block ciphers where slightly fast than T-DES. Notwithstanding, cryptographers have established that T-DES is not allowed as a permanent solution, and in 1997, the NIST which is short for the National Institute of Standards and Technology requested recommendations for a cipher to supplant DES completely, the Advanced Encryption Standard (AES).

E. IDEA:

Dr. X. Lai and Prof. J. Massey develop International Data Encryption Algorithm. This is the symmetric encryption algorithm used to replace the DES standard. It uses a 128 size bit key to encrypt and decrypt a message, unlike DES. Its large length of key makes it not easy to break down to trying every possible key. This is known as the best algorithm of encryptions for some years. There is no practical attack found on this algorithm. This algorithm is hard to linear and differential analysis.

F. RC2:

Due to security issues, the details of the algorithm were kept secret from the public. RC2 consists of a changeable key length cipher. That was developed by Ron Rivest for RSA (Data Security). The NSA suggested a couple of changes.

G. RC4:

In 1987 RC4 invented by Ron Rivest. This algorithm consists of a variable key length stream cipher. This cipher size is up to 2048 bits (256 bytes). As compared to others this algorithm is very fast. In this algorithm, security is not so much important but the message not easy to break. This algorithm is useful in many applications due to its fast speed. Its random number-generator and output of this generator is the same as the data stream.

H. RC6:

RC6 is a symmetric algorithm that uses key-block-cipher. This is invented from RC5. It was developed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin to overcome the flaws of the Advanced Encryption Standard (AES). Federal Advanced Encryption Standard (AES) chose the RC6 encryption algorithm from one of the five finalists.

I. SEED:

In 1998 Korea Information Security Agency design an algorithm SEED which is a block cipher. SEED consists of 128 blocks and 128 key sizes. Its structure is a Feistel Network structure rotated 24 times. This algorithm has been developed to reduce key attacks related to differential and linear cryptanalysis. SEED uses two 8x8 S-boxes.

J. Serpent:

The serpent is developed by Ross Anderson, Eli Biham, and Lars Knudsen. Which is a more secure block cipher and very fast. Different combinations of key use to operate this algorithm. Federal Advanced Encryption Standard (AES) also selected among Serpent other five finalists.

K. JEA:

Roger Needham and David Wheeler of Cambridge Laboratory of Computer invented the Tiny Encryption Algorithm which is very fast and a little bit secure. The key scheduler is the weakness of this algorithm, and therefore it is not suggested if security is more concerned. TEA is provided in 24 and 25 iteration different versions. The more iteration makes data more secure, but this makes slower the speed.

L. TripleDES (T-DES):

Triple DES is a newer version of the Data Encryption Standard (DES). In this algorithm, a key is used of size 64-bit and effective key of 56-bits and parity keys of 8bits. Triple-DES's block size is 8 bytes. T-DES encrypts the chunks of data which is 8 byte. Triple DES uses DES in original encryption three different keys improve three times security of DES. It is very slow but its security point of view makes it valuable especially in banks.

5. Future Research Directions

There is some work has done and proposed a solution for future network development is called Software-Defined Networking (SDN)[1]. SDN focused and highlighted the typical security issues which are defined in [1][7]: Application layer, Control layer, Data layer, Northbound, and Southbound Interface. A deep analysis and review has done of the latest progress and research, on the obtainable results of each layer and finally present the idealized global security architecture shown in figure 2.

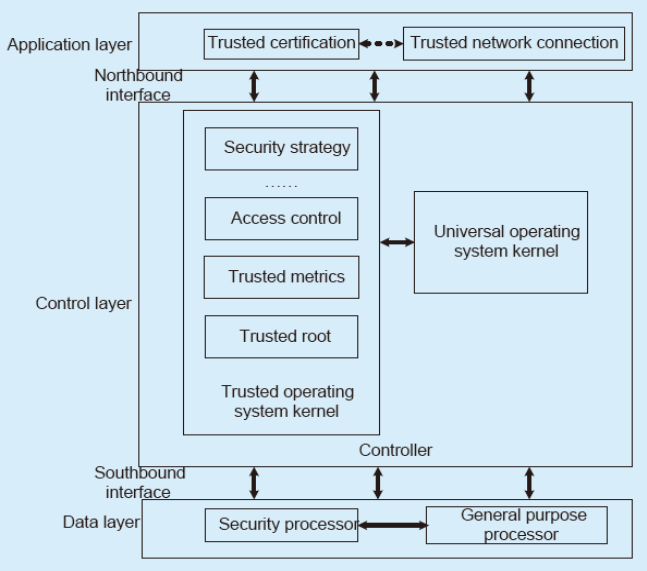

Figure 2. Idealized global security architecture [1].

SDN will feasibly switch traditional network security architecture, as it brings favourable prospects for network management in terms of programmability, simplicity, and elasticity. Although currently a lot of research has done on SDN for making it standardize this emerging paradigm, careful consideration requires to be also paid to security at this initial design phase[3][4].

SDN also widely used in largescale complex networks, traffic engineering, load balancing, and link failure recovery instead of just protecting networks [5]. SDN allows the separation of the data traffic and control with OpenFlow switch which provides the opportunities for further research and testing the new idea without changing the current network[8].

6. CONCLUSION

Network Security is the most important part of securing information due to its accountability and responsibility for securing all data transmitted over the network. We have deliberated different cryptographic methods to make the strong security of the network. Different Encryption algorithms have their own pros and cons, this paper gives a general description of different cryptographic algorithms along with parameters. Most important thing is to make encryption algorithms as strong as possible so that they can't be easily breakable or readable.

7. REFERENCES

[1]. Y. Liu, B. Zhao, P. Zhao, P. Fan and H. Liu, "A survey: Typical security issues of software-defined networking," in China Communications, vol. 16, no. 7, pp. 13-31, July 2019.

[2]. S. Sezer *et al.*, "Are we ready for SDN? Implementation challenges for software-defined networks," in *IEEE Communications Magazine*, vol. 51, no. 7, pp. 36-43, July 2013.

[3]. S. Shin, L. Xu, S. Hong and G. Gu, "Enhancing Network Security through Software Defined Networking (SDN)," 2016 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa, HI, 2016, pp. 1-9.

[4].Shu, Z., Wan, J., Li, D. et al. Security in Software-Defined Networking: Threats and Countermeasures. Mobile Netw Appl 21, 764–776 (2016). https://doi.org/10.1007/s11036-016-0676-x.

[5].Wu, Kun-Ru & Liang, Jia-Ming & Lee, Sheng-Chieh & Tseng, Yu-Chee. (2018). Efficient and Consistent Flow Update for Software Defined Networks. IEEE Journal on Selected Areas in Communications. PP. 1-1. 10.1109/JSAC.2018.2815458.

[6]. F. Hu, Q. Hao and K. Bao, "A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2181-2206, Fourthquarter 2014.

[7].Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," in Proceedings of the IEEE, vol. 104, no. 9, pp. 1727-1765, Sept. 2016.

[8] F. d. O. Silva, J. H. d. S. Pereira, P. F. Rosa and S. T. Kofuji, "Enabling Future Internet Architecture Research and Experimentation by Using Software Defined Networking," 2012 European Workshop on Software Defined Networking, Darmstadt, 2012, pp. 73-78.

[9] R.L.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communication of the ACM, Volume 21 No. 2, Feb. 1978.

[10] Daor, Joa & Daemen, Joan & Rijmen, Vincent. (1999). AES proposal: rijndael.

[11] W. Diffie and M. Hellman, "New directions in cryptography," in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976.