Study on Network Security Algorithm

1st Ms.Vinaya Kulkarni
School of Computer Science
MIT-World Peace University
Pune, India

2nd Ms. Shivali Kirdat
School of Computer Science
MIT-World Peace University
Pune, India

3rd Ms. Sneha Patil
School of Computer Science
MIT-World Peace University
Pune, India

4th Dr. C.H.Patil
Head, School of Computer Science
MIT-World Peace University
Pune, India

Abstract- **Network security is a concept of securing data through wireless transmission with the help of cryptography. The Network administrator performs the task of securing data while transmission, avoid unauthorized access of data, avert data misuse and modification of network resources. Network security is used in various computer network sectors such as private and public. Networks used in the organizations, enterprises, institutions etc. are in the form of private or public. Cryptography is concept of securing data with the help of secret keys. Cryptography is the encryption and decryption of data with secret keys using various algorithms. In this paper network security are described on the basis of the services of security. The security services are as confidentiality, authentication and integrity, digital signature, web security, email security, IP security and authentication applications. This paper gives detail study of network security algorithms and their applications. The algorithms are as follows: 1.DES 2.AES 3.RSA 4.MD5 5.SHA-512 6.HMAC 7.DIGITAL SIGNATURE 8.SSL 9.SET 10.PGP 11.ESP 12.AH**

I. INTRODUCTION

Network security is required for all hardware and software function. Administrative and management is necessary to provide protection for hardware and software. Secrecy is also necessary.
Cryptography is very important for network security. Unauthorized access should be prevented. Network security is material part of information security. It is important to secure information passing through network, computers.
We have to take care of network security.

II. NETWORK SECURITY ALGORITHMS

A. Cryptography Key

1. Symmetric key algorithm

a. DES

For the encryption of electronic data, Data Encryption Standard (DES) is used. It is a symmetric key algorithm. Although its very not secure because to its key length which is short of 56 bits which is criticized from the applications. Methods to crack block ciphers DES was introduced considering to have been a catalyst for the study of cryptography.

It can be said that it has ”jump started” the non-military development and study of encryption algorithms. Except of the cryptographers in military and intelligence, there were very few cryptographers in 1970s also very little study of cryptography. Nowadays there are many cryptologists and mathematics department which have strong programs in cryptography. A whole generation of cryptanalyst has tried to crack the DES algorithm.

b. AES

AES is an algorithm for electronic data which was established by the U. S. National Institute of Standard and Technology AES Advanced Encryption Standard in 2001. The algorithm is asymmetric key algorithm, means that not different but same key is used for encrypting as well as decrypting the data. Taken from a design principle called as a substitution permutation network AES is generated. It is useful in hardware and software. As DES used Feistel network, AES does not. AES algorithm has 128 bits block size, key of 128,192 or 256 bits which is fixed.

2. Asymmetric key algorithm

a. RSA

Rivest-Shamir-Adleman is one of the first public-cryptography systems. Its used for secure data transmission. The encrypting key in this system is not kept private. It is based on difficulty of product factorization of two prime numbers which are large in size. This algorithm has 4 steps. They are key generation, key distribution, encryption and decryption.

B. Hash Function Algorithm

1. MD5

This MD5 Message digest algorithm produces 128-bits Hash values. This was suffering from extensive vulnerabilities. At the beginning it was used as cryptographic hash function. MD5 is new one, Used to replace MD4 hash function. Later on it is specified as RFCI -321. From 2019 it is used widely.
Application-v
MD5 is used in software. It gives assurance to intact transferred file. By this user compares checksum of downloaded file. In distribution packages MD5 sum is used. "Get-File-Flash" installs Microsoft utilities. MD5

provides error checking. Corrupt and incomplete download is checked by using MD5. In electronic discovery it is used.

Algorithm

Variable length message is fixed in length output of 128 bits in MD5.Then blocks of 512 bits are prepared of input message. Message is padded first a single bit one is appended to the end of message. MD5 algorithm is divided into four 32 bits word. Main algorithm uses each 512 bits message block to modify the state. Process of message block is of 4 stages.

2. SHA-512

SHA - 512 performs on data given to it. It plays important role in digital security and cryptography. It is simple math with diagrams. SHA -2 including SHA -256, it is group of hashing algorithms.

Hashing Function

Input data is produced as output of fixed length. Hash function should be that which divides output value equally.

Input formatting:

SHA512 has an input size limit. Original message, padding bits, padding size are three parts of message.

Hash buffer initialization:

Default value is used to start off the process for the first block it is stored some where for next use final hash digest has used for processing phase of SHA-512 for intermediate result.

Message processing:

It is done upon formatted input. 1024 bit block and result of previous processing is taken in this method. Message block is expanded in words by utilizing message sequencer.

Output:

Intermediate result are taken for processing next block. SHA-512 algorithm is used for processing original message. It is one part of hashing algorithm.

3. HMAC

HMAC is special type of message authentication code. Secret key is used to derive two key inner and outer.

This provides better immunity against length extension attacks.

Cryptographic strength of HMAC is as per size of secret key. Brute force is some times used to uncover the secret key this is defect in this method. From 2011 abstract theory and source code is used.

C. Digital Signature Algorithm

This algorithm has two keys, public and private. To generate the digital signature, private key is used which can be checked by the given public key. This signature helps authenticate messages, integrity and non-repudiation. This algorithm has mainly four operations: key generation, distribution,, signing and verification of signature.

D. Web Security Algorithm

1. SSL algorithm :

Secure Socket Layer Algorithm (SSL) is an encryption algorithm which is designed to communicate between the network layer and application layer of networks. It provides security to communicate interaction models such as client side and server side. The SSL algorithm provides security services such as confidentiality, digital signature, web security. SSL uses cryptographic system to secure data with the usage of private and public keys.

The working of SSL algorithm is done with the help of SSL handshake. It uses both symmetric and asymmetric cryptography. Before the sending data from browser to server firstly the verification is done using SSL certificate. Firstly client sends required information to the server. The server also responds to the information received from the client. The client verifies the SSL certificate which is authenticated from Certificate Authority. If the authentication flops, then client declines the connexion. If the authentication succeeds, then it proceeds. The client induce secret key and encrypts the data with servers public key and dispatch to server. If server wants to verify the authentication of client server request it to client and client sends certificates to server. The decryption of session key through server is done by its private key and then dispatch to the client with the encrypted of session key.

Applications:

It is serviced in credit cards, login, for browsing social media.

2. SET ALGORITHM

Secure Electronic Transaction is a type of electronic transactions which itself explains that it is used for the online financial transaction communication. The transactions using the credit cards over the web using network. SET algorithm is used for the purpose of security protocols and formats as SSL, STT, S-HTTP. It is not a type of online payment system. The key features of SET are that it provides i)confidentiality to information requested and stored ii)integrity of data provided iii)cardholders bank account approval iv)service provider merchant authentication. The SET algorithm protocol works as follows: When customer opens an account with a bank it obtains bank card known as debit card, credit card named as master card, rupay, visa etc. for the purpose of online transactions. After the verification of customers identity it receives digital certificate which is verified by the asymmetric public key of RSA and the expiration date of the bank cards. Merchants too have their certificates. Merchant has possession of two certificates for two public keys one for signing messages and one for key exchange. The customer order process involves the browsing of merchant's website to buy the products. Customer sends the list of purchasing items to merchant who returns a product lists form. Along with product list merchant sends the duplicate copy of certificate to customer so that they can

verify authorized valid store. Customer sends order lists and billing details of credit cards along with customers certificate. The details of payment are send to merchant in encrypted way so that merchant also can't read and the customer is also verified by merchant. Finally merchant sends request to customer for payment confirmation so that customer is able to do sufficient purchase. After the confirmation of payment authorization order confirmation is send to customer and the purchased products or services are delivered to the customer.

E. Email Security Algorithm

1. PGP

Pretty Good Privacy (PGP) is hybrid cryptosystem extremely used for security of emails which provides the services of i)confidentiality through encryption ii)authentication with use of digital signature iii)compression iv)compatibility and v) segmentation of mails. PGP works on four types of keys for the encryption and decryption of emails. The main function provided by this algorithm is to send safe and secured data through mails.

The PGP encryption works on the important concept of symmetric-key, public-key cryptography and digital signatures. Firstly the encrypted plain text is compressed using PGP. PGP uses secret key which is used only one time. The random numbers are generated using this key which is used for encrypting plain text into cipher text. After the mails are received by receiver then session key is used as public key to encrypt the data on receiver's side. Decryption is done in the reverse manner of encryption.

F. IP SECURITY Algorithm

1. ESP

Encapsulating security payload (ESP) protocol is used in internet protocol security. The services provided by the protocols are confidentiality through encryption, authentication through use of public key, antireplay services through sequence number mechanism and limited traffic low confidentiality through security gateways. ESP uses both tunnel and transport mode to process the encrypted data. The components of ESP header are i)security parameter index(SPI) ii)sequence number iii)payload data iv)authentication data v)next header vi)padding vii)padding length. ESP does not protect the data header to protect it in tunnel mode the overall packet is enclosed in different new packet so the header data can be also get protected by any misuse.

2. AH

Authentication header protocol is used in internet security protocol. AH provides the security services as integrity for IP datagrams, authentication for IP datagrams, nonrepudiation and replay attacks. The components of AH protocol are i)next header ii)payload length iii)authentication data iv)reserved v)security parameter index vi)sequence number. In tunnel mode the IP packet which contains header data is also encrypted. AH can be used in the combination of ESP or in a nested fashion. AH provides anti-replay mechanism at discretion of receiver to protect data from service attacks.

CONCLUSION

Today in society there is data resources in large amount which increases the need for its security. Networks for banking, shopping, service delivery will needs efficient mechanism when it comes to security. Cryptography techniques are already insecure like DES for some applications. There are flaws in the algorithms which are already in existence. To secure our network and data we need to come up with new algorithm mechanisms to make sure our privacy is secured.

IV. REFERENCES

[1] Data_Communication_and_Networking_by_Behrouz.A.Foro uzan_4 th.edition
[2] William Stallings,"Cryptography and Network Security Principle and Practice",Fifth Edition,2011.
[3] A. O. Freier P. Karlton and P. C. Kocher. The SSL Protocol, Version 3.0. Netscape Communications, 1996
[4] Eric Maiwald,"Fundamental of Network Security",2004
[5] Jie Wang,"Computer Network Security: Theory and Practice",Second Edition,2006.
[6] Bellare, Mihir; Canetti, Ran; Krawczyk, Hugo, "Hash Functions for Message Authentication",1996.
[7] Kumar, S. N. Review on network security and cryptography. International Transaction of Electrical and Computer Engineers System, 2015.
[8] Kaur, S., Kaur, R., & Raina, C.K, Review on Network Security and Cryptography,2017.
[9] Shyam Nandan Kumar, Review on Network Security and Cryptography, ITECES,2015,3(1).