Web Security Techniques: Review and Evaluation

Song Feng Lu
Associate Prof
Huazhong University of Science and Technology

Haider Ali Mohammed
Master in Computer Applied
Huazhong University of Science and Technology

Omer Farooq
Master in Computer Applied
Huazhong University of Science and Technology

ABSTRACT

Any web security system should achieve three conceptual goals are; confidentiality, integrity and Non-repudiation, and authentication. Also any system of communication when it is designed with these security services are taken into account and these security services must be defined and can be shortened format as (CIA).In this paper, we are going to discuss the theoretical background on the objectives of web security, and it will be touched upon the other subjects such as symmetric cryptography, asymmetric cryptography, the hash function, confidentiality, integrity, non-repudiation, Authentication, Communication and Network Security and its types ,and we will focus on the digital signature concepts.

Keywords

Symmetric cryptography, Asymmetric cryptography, Hash Function, Digital signature, Integrity.

1. INTRODUCTION

We ask that authors follow some simple guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace the content with your own material.

A fundamental goal of cryptography is to process address these three areas in both theory and practice. Cryptography is the prevention and detection of cheating and other malicious activities. We can say that the sensitive information that is sent via computer network be vulnerable to attacks by hackers. So must protect this information for potential by some hacker threats; they can read and change the contents of the message and information and exploit this information for the personal benefit.

To confirm that the information sent is safe and has not been penetrated and the information never changed during the transmitter. Cryptography is an art of transferring data from one point to other in a form than the third party can't understand it. The data can be in any form [1].

Cryptography is done by following two basic steps encryption and decryption:

- Encryption is converting the original information into unreadable cipher information by using a key (or in other words set of rules), this happens in the senders end.

- Decryption is converting back the cipher information into the original information by using a key (or in other words set of rules), this happens in the receivers end.

By these two steps the cryptography protects the information from sharing it with other than the desire person while transferring it. Cryptography can be classified in several ways. On the base of number of keys used to encrypt and decrypt, cryptography can be classified into type Symmetric and Asymmetric [2].

2. SYMMETRIC OR SECRET KEY CRYPTOGRAPHY (SKC)

Symmetric Cryptography (also known as Secret key cryptography, single-key encryption, one-key encryption and private key encryption) uses a single key for both encryption and decryption process during the communication .Can be divided into Stream algorithms (Stream ciphers) and Block algorithms (Block ciphers) [3] .Fig1 shows Symmetric cryptography.

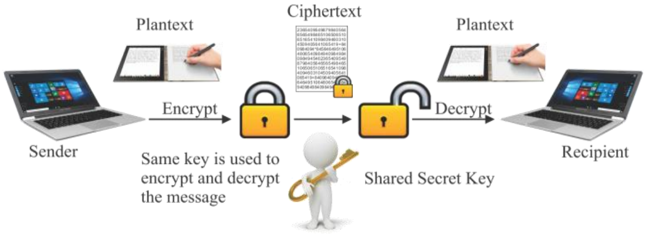

Fig1. Symmetric Cryptography

2.1 Stream Ciphers

Work on encrypt a bits of data one at a time - run on 1 bit (or sometimes 1 byte) of data at a time (encrypt data bit-by-bit). Stream ciphers are smaller and faster to proceed than block ciphers, however, they have an significant security hole. If the same key stream is applied, proven types of attacks may cause the information to be revealed [4].

2.2 Block Ciphers

Block cipher (mode for encrypting data in blocks) is a symmetric cipher which encrypts data by shattering it down into blocks and encrypting data in each block. A block cipher encrypts data in steady sized blocks (commonly of 64 bits). The most used block ciphers are Triple DES , Blowfish, CAST5, AES, and RC6 [5]. Table 1 shows the different between stream cipher and block cipher.

Table 1. Different between (stream cipher & block cipher)

Stream Cipher	Block Cipher
Encrypt data (bit by bit)**.**	Encrypts data in fixed sized blocks.
Typically faster from block cipher.	Typically slower than Stream cipher.
Not need to more memory, because its work on only a few bits at a time they have relatively low memory requirements.	Typically require more memory, since they work on large chunks of data and often have "carry over " from previous block.
Cannot provide integrity protection or authentication.	Can to provide integrity protection, in addition to confidentiality**.**

3. ASYMMETRIC OR PUBLIC KEY CRYPTOGRAPHY (PKC)

Asymmetric cryptography, also known as Public Key Cryptography, uses two different keys, namely private key and public key, for encryption and decryption process. Public key is mostly used to encrypt the data and the public key can be distributed openly to anyone to encryption who needs to communicate with the recipient. And the private key is used decrypt the encrypted data in the receiving end.

There are many algorithms used asymmetric Cryptography same as the RSA algorithm, El Gamal algorithm, and Elliptic Curve Algorithm.., et. Fig2. Shows Asymmetric cryptography. Asymmetric cryptography is more efficient than the symmetric cryptography. PKC is used in digital signatures, key management purposes and facilitating no repudiation [6].

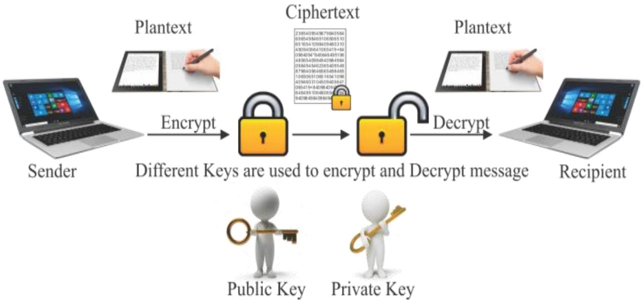

Fig 2. Asymmetric Cryptography.

4. HASH FUNCTION

Hash functions, also known as a message digest or one-way encryption, use no key method. It uses a computed fixed-length hash value based on the original text makes it impossible to retrieve the original data. Hashed functions change values from a large (possibly very large) domain into a smaller range. It uses a mathematical transformation to irreversibly encrypt information. Hash algorithms are used to encrypt passwords, the creation of digital signature and random number generation etc. Hash Functions are an substantial tool in data security meanwhile the internet. They are prepared to supply message integrity, i.e. if the message has been varied after transmission from a sender and before it may be received by the identical receiver, can be traced by the receiver, and thus, such a modified message can be discarded. This property is also useful in many other applications such as Collision resistance can be attained if it is hard to find two different messages, having same message digest as output. Apart from these requirements, the hash function should be accepting a message of any size as input and computation of the message digest must be fast and efficient. Examples of hash functions are MD2, MD4, MD5, Secured Hashing Algorithms are (SHA-1, SHA-2and SHA-3) and etc. hash function is irreversible and supports the one way property which means that there is no way to extract the input data again from the output after hashing [7]. Fig 3. Shows Hash Function.

All Hash Functions are intended to have following three properties:

1) Collision Resistance- It is computationally infeasible to find x, y, $x \neq y$ such that H(x) =H(y).

2) Pre-image Resistance- Given an output value y, it is computationally infeasible to find x such that h(x) = y.

3) Second Pre-image Resistance- Given an input x', it is computationally infeasible to find x such that H(x) =H (x').

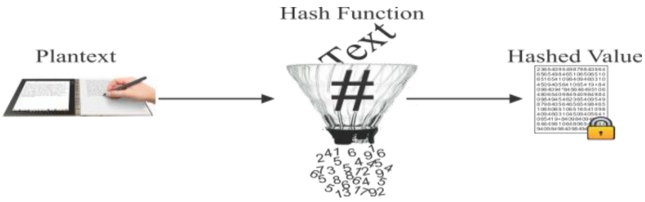

Fig 3. Hash Function

5. DIGITAL SIGNATURE

Digital signature is an electronic signature used to authenticate digitally transferred data and to ensure that the content of the message or the document sent has no changes. Digital signature cannot be imitated and can be time stamped automatically, avoiding the chances of the sender to repudiate it later. Digital signature of the digital certificate- issuing authority is also included in the digital certificate, so it is possible to check the originality of the certificate by anyone. Digital signature has same value as the physical signature on paper. It uses asymmetric cryptography to encrypt the data, providing reason to believe that the data was send by the claimed sender.

Same time the digital signature is one of the concepts in public Key Infrastructure, the information or the identity of the user is tied to the public key.

The Digital certificate is signed by the Certification Authority that provided it, to ensure trust in the signed data. Digital signature software became a powerful business tool in recent years. It provides ability to sign online. Documents, contracts, different kinds of form, tax filing can be executed online. This technology is secure, legally robust, and efficient, and saves all parties time, money, and hassle [8]. Fig 4 shows Digital Signature.

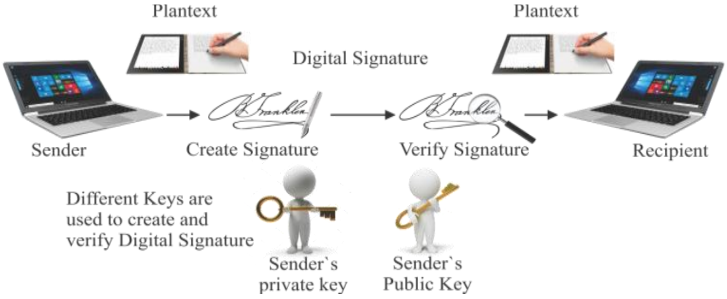

Fig 4. Digital Signature

The digital signature provides four main characters for the data sent. They are:

1) **Confidentiality and Privacy:** guarantee that any person can read the message except only the sender and meant receiver should be able to sense the contents of the transmitted message. Because eavesdroppers may oppose the message, this need demand that the message be somehow encrypted (gilding data) so that an intercepted message cannot be decrypted (grasp) by an interceptor. This aspect of secrecy is possibly the most as a rule perceived meaning of the term "secure communication." Note, however, that this is not only a restricted definition of secure communication, but a rather restricted definition of secrecy as well [9].

2) **Authentication :** Though letter may often have information about the structure sending a message, that information may not be exact. Digital signatures can be used to authenticate the exporter of messages. When ownership of a digital signature secret key is limited to a specific user, a righteous signature shows that the message was sent by that user. The value of high dependability in sender authenticity is mostly obvious in a cash status. For example, suppose a bank's Sub-office sends instructions to the central office requesting a change in the balance of an account. If the central office is not contented that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake [10].

3) **Integrity:** In many screenplays, the receiver and sender of a letter could have a want for confidence that the message has not been modify midst transmission. Though encryption hides the contents of a message, it may be potential to change an encrypted message without grasp it. However, if a message is digitally signed, any alteration in the letter after signature will revoke the signature. Furthermore, there is no active way to adjust a letter and its signature to output a new message with a righteous signature, because this is still considered to be computationally infeasible by most cryptographic hash functions [9] [10].

4) **Non-repudiation:** Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some data cannot at a later time dismiss having signed it. Similarly access to the public key only does not enable deceitful party to fake a valid signature [10].

6. COMUNICATION AND NETWORK SECURITY

Previously, we have introduced many basic cryptographic tools, from symmetric algorithms to hash functions. However, only with these tools, we are far from making our communication secure enough. Cryptographic algorithms should be applied based on a certain security protocol or mechanism. A faulty designed security protocol or mechanism with serious flaws, even with the most secure cryptographic algorithm, can be easily broken by an adversary without any cryptanalytic attack. For instance, for a poor design secure protocol, an adversary may simply parse a data packet and apply a reply attack to obtain the important information without knowing the secret key [11].

6.1 Kerberos

Originally, Kerberos in the Greek and Roman mythology is a many-headed dog guarding the entrance of Hades. Now Kerberos is referred to a trusted third party used for authentication and authorization originally as a part of Project Athena at MIT in early 80s last century.

One of the significant features and design objectives of Kerberos is Single Sign On (SSO), which means that a user only needs to sign in once for credentials and then obtain a Kerberos ticket-granting ticket (TGT) and with TGT the user gains access to all systems. design objectives of Kerberos are secure, Modular and distributed architecture and support a large number of clients and servers for scalable [43].Kerberos is very is suited for large environments, two reasons are No individual computers have to do authentication and Application servers only have to share a secret with the Kerberos server [12].

6.2 SSL/TLS

SSL is designed to make use of TCP to provide a secure and reliable end-to-end service. Therefore, SSL can be used to secure all TCP connections. SSL is two layers of protocols, rather than a single security protocol.

SSL consists of two main components. The first component is SSL Record Protocol, which is responsible for compressing and encrypting data and serves for various higher-layer protocols. It provides both confidentiality and message integrity. Is the second component of SSL. This component is responsible for setting up and maintaining the parameters used by SSL record protocol. Among these protocols, SSL Handshake Protocol is the most complex one. It is not only used for authentication between a server and client, but also for negotiation of encryption and MAC algorithms and secret keys to be used to protect data sent in an SSL record [13].

6.3 IPSec

Different from SSL/TLS, IPSec can encrypt and/or authenticate all traffic at IP level, not TCP level. Therefore, all distributed applications, including distant logon, server/client, e-mail, file convey, web access, and so on, can be secured. The IPSec specification is quite complicated, consisting of a number of documents. Two protocols with different headers in IPSec can be used to provide security. One is an authentication protocol with Authentication Header (AH), the other is a combined encryption/authentication protocol with Encapsulating Security Payload (ESP). For ESP, there are two cases: with and without the authentication option. These two protocols can provide different services. IPsec also has two modes are Transport Mode and Tunnel Mode [14].

7. WEB SECURITY EVALUATION

Building an optimum web security system from our point of view should use the following methods:

7.1 RC6 (Rivest Cipher 6)

Is a symmetric key block cipher derived from RC5. Same time RC6 is an evolutionary refinement of RC5 that is intended to meet the requirements of the AES. Similar RC5, RC6 fabricate essential use of data-dependent rotations. New structures of RC6 have the utilize of four working registers instead of two, and the implying of integer multiplication as an additional primitive procedure. Apply of multiplication greatly increases the spread done per round, permit for greater security, fewer rounds, and increased throughput.

RC6 is a parameterised family of encryption ciphers that basically use the Fiestel framework; 20 rounds were fixed for the AES surrender. The round task of RC6 uses variable relay that are orderly by a quadratic function of the data.. Each round too comprise 32 bit modular multiplication, addition, XOR, and key addition. Key addition is also used for pre- and post-whitening. RC6 was present to the AES expansion effort by RSA Laboratories [15].

7.2 Elliptic Curve Digital Signature Algorithm (ECDSA)

ECDSA is a simple transposition of the DSA (Digital Signature Algorithm) to the elliptic curve. It was proposed in 1992 by Scott Vanstone. It has the feature to offer keys with more smaller sizes for a same level of security. This incontestable advantage explains why it has become the most widely used numerical signature in different domains. ECDSA is work with a signer to beget a digital signature for data, with verifier to verify the authenticity of the signature. Every signatory has a private key and a public key. In reality, only the signer's public key permit anybody to verify the validity of the signature of the message. A third, who doesn't know the signer's private key, cannot beget the right signature. The private key is used in signature beget while the public key is used in signature verification. Before the signature generation and the signature verification, the message (M) is hashed using a hash [16]. Table 2 shows function public and private parameters of ECDSA.

Table 2 .Public and Private Parameters of ECDSA

Private Parameters	Public Parameters
Private Key 'd'	Public Key 'Q'
Random integer 'k'	Generate point 'G'
Elliptic Curve parameter 'a,b'	Order of field 'n'
Field characteristic 'q'	Signature (r,s)
	Message hash 'z'

7.3 SHA-2

In cryptography, SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512) which was designed by the National Security Agency (NSA) and was published in 2001 by the NIST as a U.S. Federal Information Processing Standard. SHA-2 comprise an outstanding number of changes from its predecessor, SHA-1. SHA-2 depend of a set of four hash functions with digests that are 224, 256, 384 or 512 bits [12]. 2005, security flaw were specified in SHA-1 a mathematical feebleness might exist which indicated that a sturdy hash function would be more acceptable. Although SHA-2 is similar to the SHA-1 algorithm, these offensive have not been successfully prolonged to SHA-2. A new hash function, SHA-3, was choice by The NIST hash function competition in 2012. The SHA-3 algorithm is not derived from SHA-2. The SHA-2 hash function is used in many scope of security system such as digital signature, tamper disclosure, password protection and so on. SHA-2 is very important algorithm for integrity and authentication.

Basic operations performed inside hashing algorithms are AND, OR, XOR (Boolean operations), modulo addition, rotation, shifting and bitwise complement operation, and each of these operations working on SHA-2 words. The SHA-2 hash algorithm is sub-divided into three sections such as padding unit, message scheduler and compression function [7]. Table 3 depicts a comparison between different SHA-2 hash functions.

Table 3. Comparison of SHA-2 hash functions

Algorithm	**Algorithm Internal state Size (bits)**	**Block Size (bits)**	**Message Length (bits)**	**Word Size (bits)**	**Round (N)**
SHA-224	256	512	264 -1	32	64
SHA-256	256	512	264-1	32	64
SHA-384	512	1024	2128-1	64	80
SHA-512	512	1024	2128-1	64	80

The reasons for using hash function or message digest in Digital signature are as follows:

-For efficiency: The signature will be much shorter and hence will be faster.

-For compatibility: A hash function can be used to convert an arbitrary input into the proper format.

-For integrity: Without the hash function, the original message has to be separated into small blocks to use the signature scheme. Hence there would be a lot of signed blocks. This can be prevented using the hash function.

8. CONCLUSION

For building good and solid security system to face all future challenges and implements the objectives of web security should have the following criteria: authentication, integrity, non-repudiation and confidentiality. In this paper we give an overview of cryptography and explain the most important parts. Then we evaluate some web security algorithms web security from our point of view and explain all arts in details. We can merge more than one security algorithms to encrypt data to create a longer key such as RC6, AES and Blowfish.

9. REFERENCES

[1] Shava FB, Van Greunen D. Factors affecting user experience with security features: A case study of an academic institution in Namibia. InInformation Security for South Africa, 2013 2013 Aug 14 (pp. 1-8). IEEE.

[2] Mathur R, Agarwal S, Sharma V. Solving security issues in mobile computing using cryptography techniques—A Survey. InComputing, Communication & Automation (ICCCA), 2015 International Conference on 2015 May 15 (pp. 492-497). IEEE.

[3] Mandal BK, Bhattacharyya D, Bandyopadhyay SK. Designing and performance analysis of a proposed symmetric cryptography algorithm. InCommunication Systems and Network Technologies (CSNT), 2013 International Conference on 2013 Apr 6 (pp. 453-461). IEEE.

[4] Al Shehhi MA, Baek J, Yeun CY. The use of Boolean functions in stream ciphers. InInternet Technology and Secured Transactions (ICITST), 2011 International Conference for 2011 Dec 11 (pp. 29-33). IEEE.

[5] Dewu X, Wei C. A survey on cryptanalysis of block ciphers. InComputer Application and System Modeling (ICCASM), 2010 International Conference on 2010 Oct 22 (Vol. 8, pp. V8-218). IEEE.

[6] Azaim MH, Sudiharto DW, Jadied EM. Design and implementation of encrypted SMS on Android smartphone combining ECDSA-ECDH and AES. InMultimedia and Broadcasting (APMediaCast), 2016 Asia Pacific Conference on 2016 Nov 17 (pp. 18-23). IEEE.

[7] Nugroho KA, Hangga A, Sudana IM. SHA-2 and SHA-3 based sequence randomization algorithm. InScience and Technology-Computer (ICST), International Conference on 2016 Oct 27 (pp. 150-154). IEEE.

[8] Agarwal N, Rana A, Pandey JP. Proxy signatures for secured data sharing. InCloud System and Big Data Engineering (Confluence), 2016 6th International Conference 2016 Jan 14 (pp. 255-258). IEEE.

[9] Devi TR. Importance of Cryptography in Network Security. InCommunication Systems and Network Technologies (CSNT), 2013 International Conference on 2013 Apr 6 (pp. 462-467). IEEE.

[10] Idalino TB, Coelho M, Martina JE. Automated issuance of digital certificates through the use of federations. InAvailability, Reliability and Security (ARES), 2016 11th International Conference on 2016 Aug 31 (pp. 725-732). IEEE.

[11] Bruce N, Kang YJ, Sain M, Lee HJ. An approach to designing a network security-based application for communications safety. InAdvances in Social Networks Analysis and Mining (ASONAM), 2015 IEEE/ACM International Conference on 2015 Aug 25 (pp. 1002-1009). IEEE.

[12] Zheng K, Jiang W. A token authentication solution for hadoop based on kerberos pre-authentication. InData Science and Advanced Analytics (DSAA), 2014 International Conference on 2014 Oct 30 (pp. 354-360). IEEE.

[13] Mensah P, Blanc G, Okada K, Miyamoto D, Kadobayashi Y. AJNA: Anti-phishing JS- based Visual Analysis, to Mitigate Users' Excessive Trust in SSL/TLS. InBuilding Analysis Datasets and Gathering Experience Returns for Security (BADGERS), 2015 4th International Workshop on 2015 Nov 5 (pp. 74-84). IEEE.

[14] Heinemann C, Chaduvu SS, Byerly A, Uskov A. OpenCL and CUDA software implementations of encryption/decryption algorithms for IPsec VPNs. InElectro Information Technology (EIT), 2016 IEEE International Conference on 2016 May 19 (pp. 0765-0770). IEEE.