HASH FUNCTIONS for MESSAGE AUTHENTICATION

Richa Arora
Punjab College of Technical Education, Ludhiana
Punjab Technical University, Jalandhar
richaarora2310@gmail.com

Abstract: **This paper talks about hash message authentication code which is used for message authentication using hash functions. It also discusses about keyed-hash functions and digital signatures.**

Keywords: *Hash Functions, HMAC, Digital Signatures*

1. INTRODUCTION:

Message authentication deals with processes which are used to ensure integrity of a message and identity of the sender. When a message is sent over some network, authenticator details, Signature and Message authentication Code (MAC) are also sent along. MAC is an authentication process in which secret key is used to generate cryptographic checksum which is sent along with the message. This cryptographic check sum is known as Message Authentication Code (MAC). In this process a common secret key is shared by both sender and receiver. If a message M is to be sent from Sender Cathy to receiver George using Key K, then MAC will be calculated as MAC=E(K,M).

E is the MAC function.

Message and MAC will be sent to the receiver.

MAC can be of any size, sometimes hash function is used in place of authentication scheme to fix the size. In order to identify the problem with MAC, timestamp and message sequence number are required. Various methods are used to authenticate the message

1.1 Session-Key – Session key is used to authenticate the message. Cathy and George create their session key.The session key is known to both sender and receiver. Session keys are transmitted in encrypted format to prevent the compromise of these keys.

1.2 Block Cipher- This is another method which is used for message authentication. Block ciphers treats the complete block of message as individual unit and creates an encrypted message of length equal to that of the block. This method uses the combination of substitution and transposition techniques. Encryption of the data is repeated multiple times in case of the block ciphers. CFB and CBC modes can be used to send the final block of data and this final block will depend on the previous blocks which are given as input to each Advancing stage.

1.3 Email Message Encryption

Every Email message that a sender sends travels a large distance before reaching the receiver. It travels

through many networks which may be monitored, insecure or making other kinds of passive or interception attacks onto the message. In such a scenario if a message is being sent in plaintext – anyone could read that message, provide he has access to any of these servers.

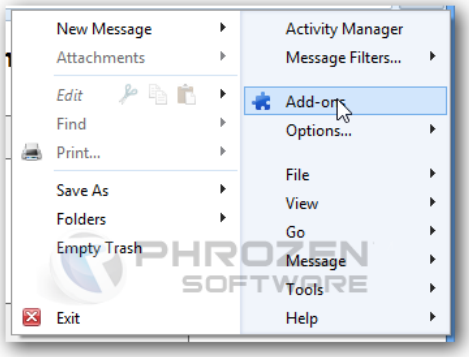
Pretty Good Privacy- a phenomenon developed by Phill Zimmermann. PGP is used for email and File storage apps to provide confidentiality and authentication services.

PGP is comprised of five different services – authentication, confidentiality, compression, e-mail compatibility and segmentation. PGP makes email encryption easy offers strong protection against spying eyes.

2. CONFIGURE PGP in THUNDER BIRD

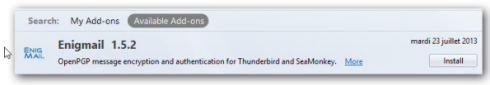
Mozilla's email program, Thunderbird with the Enigmail extension is the easiest tool to use.

1. Install the add-on which will integrate into Thunderbird the ability to use PGP encryption in your mails.



2. Search for **enigmail:** In the Add-ons window

3. Out of many add ons available-install Enigma.



4. Click **Install** button, then restart Thunderbird to apply Add-on configuration.
5. PGP Libraries for Windows must be installed.

3 . INSTALLING GNUPGP

1. Run the GPGP Installer, GNUPGP will appear under Program Files directory.

2. Once you've downloaded Enigmail, in Thunderbird open Tools -> Options -> Extensions -> Install New Extension, and then choose the Enigmail extension file.

3. When you've restarted Thunderbird with Enigmail installed, you will see an OpenPGP menu item. Open it and go to Preferences. There you'll find a dialog to point to your Gnu PGP binary. Click Browse. It will be installed under Program Files\GNU\GnuPG\gpg.exe.

4. Now you'll need to generate your public/private key pair. From the OpenPGP menu item, choose Key Management. From the Generate menu choose New Key Pair.

5. Choose the email address you want to create a key for, and set a passphrase. Hit the "Generate Key" button, and relax - it can take a few minutes.

Message Authentication codes HMAC and CBC-MAC:

Hash-based message authentication code is created to calculate a message involving a cryptographic

hash function with private key. HMAC-MD% or HMAC-SHA1 have been used for calculating HMAC. Cryptographic strength of the hash function used determines the strength of HMAC.

CBC-MAC: Technique to build message authentication code from block cipher. Cipher block chaining mode creates a chain of blocks in which each block is dependent on the previous block's encryption.

2. CRYPTOGRAPHIC HASH FUNCTIONS:

A user transmitting a message would never want the message to be tampered or analysed in any way. In such scenarios message authentication is a great tool to validate the messages. Hash function can be used for message authentication. MD-5 and SHA-1 are such hash functions. Generally hash functions are sent along with digital signatures. The Major point of consideration here is that hash functions don't use any key.

Cryptographic hash function is a deterministic procedure – that takes arbitrary blocks of data and returns fixed size data. The data encoded using Hash functions is called the message digest.

3. KEYED HASH FUNCTIONS

A secret key is used along with cryptographic hash function in case of Keyed Hash function. The cryptographic key is known only to sender and receiver, which introduces more security features.

4. DIGITAL SIGNATURES

Digital Signatures are used to ensure authentication. It is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of a message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message.[7] They are used to ensure that the original content of the message remains unchanged. User is given two different keys-private key and public key. Public key can be known to anyone who needs it but private key lies only with the desired users. Anyone with the public key can encrypt the message but it cannot be decrypted without the private key. Thus data is pretty useless without the private key , as it cannot be decrypted without the private key. With private key an authentic user can put digital signatures over a document. Digital signature is a tamp which is very difficult to forge. During the process of signing, the data is crunched down into few lines via a process called hashing. The crunched down data is called message digest, which cannot be changed v\back to original data.

References

[1]en.wikipedia.org/wiki/Message_authentication_code
[2]www.webopedia.com/TERM/E/encryption.html
[3]www.cs.princeton.edu/courses/archive/fall07/cos433/lec8.pdf
[4]x5.net/faqs/crypto/q94.html
[5] www.digitalsignature.in/
[6] en.wikipedia.org/wiki/Digital_signature
[7] www.phrozenblog.com/?p=512
[8] Cryptography and Network Security Principles and Practices, Fourth Edition By William Stallings

