Table of Contents

Message authentication is concerned with:
Fundamental levels of message authentication:
Lower level
Higher level
Some types of functions that may be used to produce an authenticator:
Message encryption:
Message authentication code (MAC):
Hash function:
Related posts:

Message authentication is concerned with:

- Protecting the integrity of a message
- Validating identity of originator
- Non-repudiation of origin

Fundamental levels of message authentication:

Lower level

There may be some sort of function that produces an authenticator: a value to be used to authenticate a message.

Higher level

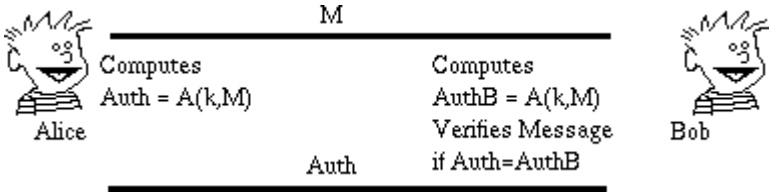
The lower layer function is then used as primitive in a higher-layer authentication protocol that enables a receiver to verify the authenticity of a message.

Some types of functions that may be used to produce an authenticator:

Message encryption:

The cipher text of the entire message serves as its authenticator. The analysis differs from symmetric and public key encryption schemes.

Suppose the message can be any arbitrary bit pattern. In that case, there is no way to determine automatically, at the destination whether an incoming message is the ciphertext of a legitimate message. One solution to this problem is to force the plaintext to have some structure that is easily recognized but that cannot be replicated without recourse to the encryption function. We could, for example, append an error detecting code, also known as Frame Check Sequence (FCS) or checksum to each message before encryption 'A' prepares a plaintext message M and then provides this as input to a function F that produces an FCS. The FCS is appended to M and the entire block is then encrypted. At the destination, B decrypts the incoming block and treats the result as a message with an appended FCS. B applies the same function F to attempt to reproduce the FCS. If the calculated FCS is equal to the incoming FCS, then the message is considered authentic. In the internal error control, the function F is applied to the plaintext, whereas in external error control, F is applied to the ciphertext (encrypted message).



Authentication using Private-key Cipher

Message authentication code (MAC):

A public function of the message and a secret key that produces a fixed length value serves as the authenticator.

This authentication technique involves the use of secret key to generate a small fixed size block of data, known as cryptographic checksum or MAC that is appended to the message. This technique assumes that two communication parties say A and B, share a common secret key ‘k’. When A has to send a message to B, it calculates the MAC as a function of the message and the key. MAC = CK(M) Where M – input message C – MAC function K – Shared secret key.The message plus MAC are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the shared secret key, to generate a new MAC. The received MAC is compared to the calculated MAC. If it is equal, then the message is considered authentic. A MAC function is similar to encryption. One difference is that MAC algorithm need not be reversible, as it must for decryption. In general, the MAC function is a many- to-one function.

Hash function:

A public function that maps a message of any length into a fixed length hash value, which serves as the authenticator.

A variation on the message authentication code is the one way hash function. As with MAC, a hash function accepts a variable size message M as input and produces a fixed-size output, referred to as hash code H(M). Unlike a MAC, a hash code does not use a key but is a function only of the input message. The hash code is also referred to as a message digest or hash value.

Related Posts:

1. Types of Attack
2. Security threats
3. Computer and cyber security
4. Introduction to network security
5. Intrusion detection tool
6. Categories of security assessments
7. Security terminologies and principals
8. Intoduction to intrusion
9. Intrusion detection tool
10. Categories of security assessments
11. Intrusion terminology
12. Cryptography attacks
13. Cryptography
14. SSH
15. MD5
16. Message digest functions
17. Digital signature
18. One way hash function
19. Hash function in network web security
20. Digital signature standard
21. SSL Secure socket layer