ECT-434
SECURE COMMUNICATION

Module 5: Message Authentication and Hash Function

Authentication requirements, Authentication functions- Message Encryption, Public Key Encryption, Message Authentication Code, Hash function

Message authentication is a mechanism or service used to verify the integrity of a message.

Message authentication assures that data received are exactly as sent by (i.e., contain no modification, insertion, deletion, or replay) and that the purported identity of the sender is valid.

Bushara A R
AP, ECE
KMEA ENGG.COLLEGE

Bushara A R, KMEA

1. Authentication requirements

Authentication Requirements In the context of communications across a network, the following attacks can be identified:

1. Disclosure: Release of message contents to any person or process not possessing the appropriate cryptographic key.
2. Traffic analysis: Discovery of the pattern of traffic between parties.
3. Masquerade: Insertion of messages into the network from a fraudulent source.
4. Content modification: Changes to the contents of a message, including insertion, deletion, transposition, and modification.
5. Sequence modification: Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.

Bushara A R KMEA

6. Timing modification: Delay or replay of messages.
7. Source repudiation: Denial of transmission of message by source.
8. Destination repudiation: Denial of receipt of message by destination

2. Message Authentication Functions

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

message authentication is concerned with:

- protecting the integrity of a message
- validating identity of originator
- non-repudiation of origin

- three functions used:

1. **message encryption** : The ciphertext of the entire message serves as its authenticator
2. **message authentication code (MAC):** A function of the message and a secret key that produces a fixed-length value that serves as the authenticator
3. **hash function:** A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator

Bushara A R KMEA

1. Message Encryption

➔message encryption by itself also provides a measure of authentication

a) symmetric encryption

➔if symmetric encryption is used then:

- receiver know sender must have created it
- since only sender and receiver now key used
- So, content cannot of been altered
- Provides both: sender authentication and message authenticity

b) public-key encryption

➔if public-key encryption is used:

- encryption provides no confidence of sender
- since anyone potentially knows public-key

➔however if

- ♦ sender signs message using his private-key
- ♦ then encrypts with recipients public key
- ♦ have both secrecy and authentication

Bushara A R, KMEA

Fig11: Basic Uses of Message Encryption

- Consider the straightforward use of symmetric encryption (Figure 11.1a). A message M transmitted from source A to destination B is encrypted using a secret key K shared by A and B. If no other party

knows the key, then confidentiality is provided: No other party can recover the plaintext of the message.

- Figure 11.1b) provides confidentiality but not authentication. The source (A) uses the public key PUb of the destination (B) to encrypt M. Because only B has the corresponding private key PRb, only B can decrypt the message. This scheme provides no authentication because any opponent could also use B's public key to encrypt a message, claiming to be A.
- To provide authentication, A uses its private key to encrypt the message, and B uses A's public key to decrypt (Figure 11.1c). This provides authentication using the same type of reasoning as in the symmetric encryption case: The message must have come from A because A is the only party that possesses PRa and therefore the only party with the information necessary to construct ciphertext that can be decrypted with PUa.
- To provide both confidentiality and authentication, A can encrypt M first using its private key, which provides the digital signature, and then using B's public key, which provides confidentiality (Figure 11.1d).

Bushara A R, KMEA

Message Authentication Code (MAC)

- a small fixed-sized block of data:
  - depends on both message and a secret key
  - like encryption though need not be reversible
  - appended to message as a signature

• receiver performs same computation on message and checks it matches the MAC
• provides assurance that message is unaltered and comes from sender

Message Authentication Code

This technique assumes that two communicating parties, say A and B, share a common secret key K. When A has a message to send to B, it calculates the MAC as a function of the message and the key:

MAC = C(K,M), where

M= input message
C=MAC function
K= shared secret key

Bushara A R, KMEA

- MAC provides authentication
- Message can be encrypted for secrecy

generally use separate keys for each can compute MAC either before or after encryption

Why use a MAC?

- sometimes only authentication is needed

sometimes need authentication to persist longer than the encryption

Mac Encryption

- The receiver is assured that the message is from the alleged sender. Because no one else knows the secret key, no one else could prepare a message with a proper MAC.

MAC Properties

- a MAC is a cryptographic checksum MAC = C (k, M)

- C is a function

    - condenses a variable-length message M
    - using a secret key K

Bushara A R, KMEA

- to a fixed-sized authenticator
- many-to-one function potentially many messages have same MAC
- but finding these needs to be very difficult

Requirements for MACS

MAC needs to satisfy the following:

1. knowing a message and MAC, is infeasible to find another message with same MAC
2. MACS should be uniformly distributed
3. MAC should depend equally on all bits of the message

Bushara A R, KMEA

Figure 11.4. Basic Uses of Message Authentication Code (MAC)

- The message plus MAC are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new MAC. The received MAC is compared to the calculated MAC (Figure 11.4a).
- The process depicted in Figure 11.4a provides authentication but not confidentiality, because the message as a whole is transmitted in the clear. Confidentiality can be provided by performing message encryption either after (Figure 11.4b) or before (Figure 11.4c) the MAC algorithm.

Hash Functions

★ A hash function is like a MAC

★ hash value h is generated by a function H of the form

- h = H (M)
- M is a variable-length message and H(M) is the fixed-length hash value.

➔usually assume that the hash function is public and not keyed

➔note that a MAC is keyed

- hash used to detect changes to message
- can use in various ways with message
- most often to create a digital signature

Hash Functions & Digital Signatures

☐Only the hash code is encrypted, using public-key encryption and using the sender's private key. As with (b), this provides authentication. It also provides a digital signature.

Bushara A R, KMEA

Figure 11.5. Basic Uses of Hash Function

a. The message plus concatenated hash code is encrypted using symmetric encryption. Because only A and B share the secret key, the message must have come from A and has not been altered. The hash code provides the structure or redundancy required to achieve authentication. Because encryption is applied to the entire message plus hash code, confidentiality is also provided.

b. Only the hash code is encrypted, using symmetric encryption. This reduces the processing burden for those applications that do not require confidentiality. E(K, H(M)) is a function of a variable-length message M and a secret key K, and it produces a fixed-size output that is secure against an opponent who does not know the secret key.

c. Only the hash code is encrypted, using public-key encryption and using the sender's private key. As with (b), this provides authentication. It also provides a digital signature, because only the sender could have produced the encrypted hash code. In fact, this is the essence of the digital signature technique.

d. If confidentiality as well as a digital signature is desired, then the message plus the private-key- encrypted hash code can be encrypted using a symmetric secret key. This is a common technique.

e. It is possible to use a hash function but no encryption for message authentication.

f. Confidentiality can be added to the approach of (e) by encrypting the entire message plus the hash code.

Bushra A.R., KMEA

Requirements for Hash Functions

1. can be applied to any size message M
2. produces a fixed-length output h
3. easy to compute h=H (M) for any message M
4. given h is infeasible to find x s.t. H (x)=h
5. given x is infeasible to find y s.t. H(y)=H(x)
6. is infeasible to find any x, y s.t. H(y)=H (x)

Bushara A R, KMEA