Message Authentication

Objectives

- Understand how message authentication works and its use for integrity
- Discuss what a hash function is
- Understand how different hash functions can be weaker or stronger than others

Integrity

- In the CIA triad, integrity means that data is accurate, complete and unaltered
- Integrity is important in case something is altered
- Think about an email that has been sent from your bank. How can you verify it? Can you call and check? Is there a way to verify who the sender was without calling?

CIA Triad

- Encryption
  - Protects against passive attacks
  - Maintains confidentiality
  - Example: someone actively listening in a network connection(eavesdropping)
- Message Authentication
  - Protects against active attacks
  - Maintains integrity
  - Example: someone pretending to be something they are not(spoofing)

Message Authentication

- Verifies received is authentic
  - Contents have not been altered
  - Validated identity of the sender
  - Verifies time and correct sequence
- Can use traditional encryption
  - Sender and receiver must know the key
  - However, only authentication can be used

Message Authentication steps

1. Sender generates message authentication code(MAC) via a MAC algorithm and appends it onto the message
2. Receiver verifies MAC by calculating the MAC with the same algorithm
3. Both sender and receiver must have generated their public and private key pairs and exchanged public keys

Hash functions

- A hash function produces the identity of the file or block of data
- In order to be able to be a considered a hash function, the function must:
  - Be used with any size of block
  - Produce a fixed-length output string of data that represents that block
  - Easy to compute
  - Cannot be reversed to find original block of data
  - Collision resistant – Collisions have occurred and hash functions are then depricated

Real World examples

- User wants to send a user a signed message
- Password checking
- Intrusion detection

Common algorithms and techniques

- MD5 – simple algorithm, produces 128bit hash, can have collisions
- SHA – Original algorithm 1993, produces 160bit hash, can have collisions
- SHA-1 Revised in 1995, produces 160bit hash, can have collisions
- SHA-256 Revised in 2001, produces 256bit hash, Block size is 1024
- SHA-512 Revised in 2001, produces 512bit hash, Block size is 1024
- HMAC – Hash is send with the message
- X.509 – Certificates