


4. Authentication Protocol

Thursday, February 18, 2021 12:55 PM

 Adding a level of security to authentication with symmetric key cryptography.

Authentic protocol 1.0:

Using a code

- May be replayed

Authentic protocol 2.0:

Using IP address

- IP spoofing attack: using somebody else's IP address

Source IP	Destination IP	Message	Source MAC	Destination MAC	CRC bytes
Can be replaced with another IP address					

Authentication protocol 3.0:


Using an unencrypted password and receiver may check database for username and password

- Intruder may save password

Authentication protocol 3.1:

Encrypting password with symmetric key cryptography

- Replay encrypted password

 Even if we use the same password between two users (encrypted or not) do not serve a perfect authentication protocol

Authentication protocol 4.0:

Rather than using the same password (encrypted or not) for every communication

1. Bob sends a **nonce** (unique, non-repeatable string)
2. Alice encrypts nonce with symmetric key
3. Bob receives the encrypted nonce; if he can decrypt with the same symmetric, he can verify Alice's identity
 - **This will not work with public key cryptography**; public key of receiver is available to everyone hence, nonce verification will not work
 - Playback attack is fully resolved here
 - Widely used scheme for authentication
 - No failure scenario

Authentication Protocol 5.0:

Authentication protocol 4.0 with asymmetric key cryptography

Encrypt the nonce with private key of sender. Receiver decrypts using public key of sender to verify nonce.

Vulnerability:

- Bob sends Alice nonce.
- Alice encrypts using private key
- Bob shares resource after verification of nonce
- Trudy has this information. Suppose Bob has no copy of Alice's public key (corruption/formatting of disk)
- Trudy may send Bob her public key and get verified

This vulnerability may be overcome with the intervention of a certificate authority.

- Digital signature is to ensure integrity of the transmitted message (and also to confirm origin of message)
- Authentication is to verify identity in order to provide a resource

