S.0

Outline

of

Network Security

CS:356

Mohamed Gouda

S.1 Secure Communication

- Entity S sends msg M to entity R

- This communication is <u>secure</u> iff it satisfies the following 3 conditions

1. Confidentiality:
   No entity other than S and R can understand M.

2. Integrity:
   S and R are sure that M is not altered after it is sent by S and before it is rcvd by R

3. Authentication:
   When R rcvs M, R can confirm that S is the entity that sent M.
   When S sends M, S can confirm that R will be the entity that rcvs M.

S.2 Tools to Achieve Secure Communcation

1. Symmetric Keys
2. Public and Private Keys
3. Secure Hash Functions
4. Msg Authentication
5. Digital Signature

S.3 Symmetric Keys

- Assign a unique symmetric key K to every pair of entities S and R. Only S and R know K.
- $K^+(M)$ denotes "encryption" of M using K
- $K^-(K^+(M))$ denotes "decryption" of $(K^+(M))$ using K
- Theorem: $K^-(K^+(M)) = M$

5.4 Confidential Communication Using Symmetrical Keys

- To provide cofidential communication from S to R using K:

  i. S computes $K^{+}(M)$ and sends it to R

  ii. R computes M as $K^{-}(K^{+}(M))$ from above theorem

  iii. Only S and R know and understand M

S.5 Public and Private Keys

- Assign two keys, K_S^+ and K_S^-, to every entity S. Key K_S^+ is named <u>public key</u> of S, and key K_S^- is named <u>private key</u> of S.

- Every entity knows K_S^+ but only entity S knows K_S^-.

- $K_R^+(M)$ denotes the "encryption" of M using the public key of R

- $K_R^-(K_R^+(M))$ denotes the "decryption" of $K_R^+(M)$ using the private key of R

- <u>Theorem:</u> $K_R^-(K_R^+(M)) = M$

$$K_R^+(K_R^-(M)) = M$$

S.6 Confidential Communication Using Public Keys

- To provide confidential communication from S to R using K_R^+ and K_R^- :

    i. S computes $K_R^+(M)$ and sends it to R

    ii. R computes M as $K_R^-(K_R^+(M))$ from above theorem

    iii. Only S and R know and understand M

S.7 Secure Hash Functions

- H is function that takes as input any msg M and computes as output a msg H(M) of fixed length such that following condition holds:

- It is computationally infeasible to find two distinct msgs M1 and M2 such that

$$H(M1) = H(M2)$$

S.8 Examples of Secure Hash

- Msg Digest 4 (MD4)
  Msg length = 128 bits

- Secure Hash Algorithm (SHA-1)
  Msg length = 160 bits

- MD4 is more efficient
  SHA-1 is more secure

S.9 Msg Authentication

- Each authenticated msg from S to R is of form:

$$(M, C)$$

M is a msg

C, called msg authentication code MAC of M from S to R, is computed as follows:

$$C = H(M|K)$$

| is concatenation

H is a secure hash that S and R know

K is a symmetric authentication key that only S and R know

- If R rcvs (M, C) and checks that $C = H(M|K)$, then R concludes that M was not updated after it is sent by S and before it is rcvd by R

S.10 Digital Signatures

- Before S sends M to R, S can "sign" M and attach the signature to M:

  (M, signature of M by S)

- Signature of M by S is computed as follows:

  $$K_S^-(H(M))$$

  H is a secure hash known to S and R

S.11

Source Authentication

- R can use the signature of M by S to prove that S is the entity that signed and sent M as follows:

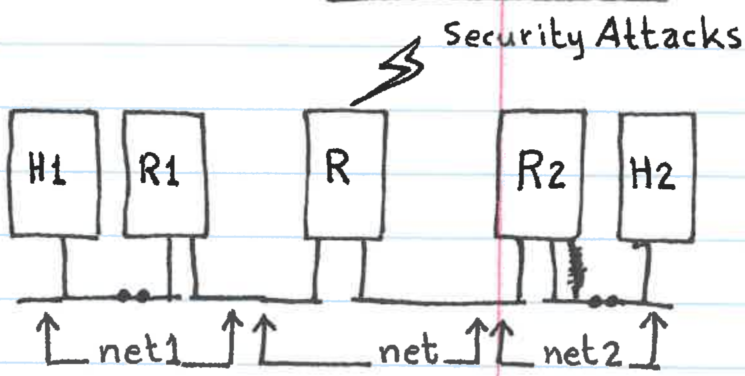
  1. R gets the signature $K_S^-(H(M))$ and the public key K_S^+ of S

  2. R shows that
     $$K_S^+(K_S^-(H(M))) = M$$
     as required by the above theorem

  3. This proves that S and only S could have signed and sent M

S.12

IP is Insecure



- Net1 is secure, belongs to secure network of some interprise
- Net2 is secure, belongs to secure network of some interprise
- Net is insecure, belongs to vulnerable public network

S.13 Attacks in IP

- **Lack of Confidentiality:**

  Payload of any packet that goes through net can be read and understood by any attacker in net

- **Lack of Source Authentication:**

  The original src of any pkt that goes through net can be corrupted

- **Lack of msg Authentication:**

  The payload of any pkt that goes through net can be corrupted.