ROYAL INSTITUTE
OF TECHNOLOGY

Networked Systems Security

Hash Chain

Module TA:
Mohammad Khodaei (khodaei@kth.se)

Panos Papadimitratos
http://www.ee.kth.se/nss

ROYAL INSTITUTE OF TECHNOLOGY

Hash Function

- Arbitrary length message → Fixed length message (Hash Value)
  - H(m)→ x
- Hash value, Message Digest or Fingerprint
- Properties
  - Collision resistance H(m1)→x, H(m2)→ x, m1 ≠ m1
  - Pre-Image resistance (one-way(-ness)) x → H(m1)
  - Low computational cost (efficiency)

Hash Chain

- Pick a random number r
- Generate k elements by hashing r successively k times

$$h^k(r) \leftarrow h^{k-1}(r) \leftarrow \cdots \leftarrow h^3(r) \leftarrow h^2(r) = h(h(r)) \leftarrow h(r)$$

$$\| \qquad \| \qquad \| \qquad \| \qquad \|$$

$$H_0 \leftarrow H_1 \leftarrow \cdots \leftarrow H_{k-3} \leftarrow H_{k-2} \leftarrow H_{k-1}$$

- H_0 is the hash chain anchor
- The remaining k-1 elements can be used for authentication
- Example:
  - A → B: $H(H^{k-1}(r), Data), Data$
  - Data can be verified later using $H^{k-1}(r)$

Hash Chain Example: S/KEY (one-time password)

- One Time Password Scheme
  - Untrusted public computers to counter password sniffing
- Generate Hash Chain of n elements from a secret ‘W’ (password)
  - $H(W), H(H(W)), \ldots, H^n(W)$
- $H^n(W)$ becomes public password
- Client uses $H^{n-1}(W)$ for one-time authentication
- Server checks if $H(H^{n-1}(W)) = H^n(W)$

Hash Chain Limitations for Authentication

- Cannot be used as a standalone solution
  - The hash chain anchor (H_0) should be either signed, or sent out using out-of-band mechanism
- The verification is delayed
  - Late key exposure (E.g., A. Perrig *"The TESLA Broadcast Authentication Protocol", 2005*)
- Challenging when missing some of the hash values
  - One has to know the number of missed values
- Integration with Public Key Infrastructure (PKI)

NOVOMODO: Scalable Certificate Validation And Simplified PKI Management

- $C = SIG_{CA}(SN, PK, U, D_1, D_2, \ldots)$
- Traditional Certificate Validation
  - CRL and OCSP
  - ***Challenges:*** Bandwidth, computation, communication (if centralized), security (if distributed)
- The system works as below:
  - CA Randomly selects two 20-byte values: Y_0, X_0
  - $Y_1=H(Y_0)$, the revocation target
  - $X_1=H(X_0)$, $X_2=H(X_1)$, …, $X_{365}=H(X_{364})$, the validity target
  - $C = SIG_{CA}(SN, PK, U, D_1, D_2, \ldots, Y_1, X_{365})$

S. Macali, **"Scalable Certificate Validation And Simplified PKI Management"**, 2002.

Revocation and Validation of a Certificate

- One day granularity for all certificates
- On the i-th day, the CA releases 20-byte proof of status
- If C is revoked, the CA releases Y_0, H-inverse of the revocation target Y_1
- Otherwise, CA releases X_{365-i}, i.e., the i-th H-inverse of the validity target X_{365}
  - E.g., the proof of certificate C on day 100 after issuance is X_{265}

S. Macali, **"Scalable Certificate Validation And Simplified PKI Management"**, 2002.

ROYAL INSTITUTE OF TECHNOLOGY

Hash Chain

Questions?