Network Security
Elements of Network Security Protocols

Identification

- **Passwords**
- **One-time Passwords**
- **Challenge response (strong authentication)**

Data integrity and data origin authentication

- **Data integrity** is the property whereby data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source.
- **Data origin authentication** is a type of authentication whereby a party is corroborated as the (original) source of specified data created at some (typically unspecified) time in the past.
- **By definition, data origin authentication includes data integrity**.

Cryptographic techniques for data integrity

- Message authentication codes (MACs)
- Digital signatures
- Appending (prior to encryption) a secret authenticator value to encrypted text
- Comments
  - MAC and method based on secret authenticator do not guarantee non-repudiation
  - All these methods do not provide timeliness by themselves

Identification

- **Identification** allows one party (the *verifier*) to gain assurances that the identity of another (the *claimant*) is as declared, thereby preventing impersonation.
- **The most common technique** is by the verifier checking the correctness of a message (possibly in response to an earlier message) which demonstrates that the claimant is in **possession of a secret associated by design with the genuine party**.
- Techniques which provide both entity authentication and key establishment are often integrated
- Other names: **entity authentication**, **identity verification**

Entity authentication vs message authentication

- Timeliness
  - Message authentication itself provides no timeliness guarantees with respect to when a message was created, whereas
  - Entity authentication involves corroboration of a claimant's identity through actual communications with an associated verifier during execution of the protocol itself (i.e., in real-time, while the verifying entity awaits).
- Information exchange
  - Entity authentication typically involves no meaningful message other than the claim of being a particular entity, whereas
  - Message authentication does

Passwords

Tecnica di Unix

- P is the user password
- P is not trivial

- For every user, the password server stores the pair $\langle S, Q \rangle$
- S is a pseudo-random sequence (seed)
- $Q = h(P||S)$
- h is a OWHF

- P is transmitted in clear over the secure channel
- The password server receives P and checks whether $Q = h(P||S)$, where P is the received password and $\langle S, Q \rangle$ are retrieved from the password file

Passwords

PROS

- An unauthorized access to the password file does not reveal any information
- S prevents an adversary to determine whether two users have chosen the same password by simply analysing their images
- S prevents a simultaneous attack to the passwords

CONS

- If the channel is not secure, password P cannot be transmitted in clear

One-time passwords (Lamport's scheme)

- **Secret *w***
- **OWHF *H***
- **Password sequence**: ***w***, ***H*(*w*)**, ***H*(*H*(*w*))**,…, ***H*^{t}(*w*)**
- The password for the *i*-th identification, **1≤ *i* ≤ *t***, is defined to be $w_i = H^{t-i}(w)$

One-time passwords (Lamport's scheme)

- **Goal**

  Claimant A identifies itself to verifier B using OTP from a sequence
- **One-time setup**
  a) A begins with secret ***w***
  b) A fixes a constant ***t*** defining the number of identifications to be allowed
  c) A transfers (the initial shared secret) $w_0 = H^t(w)$, in a manner guaranteeing its authenticity, to B.
  d) B initializes its counter for A to $i_A = 1$

One-time passwords (Lamport's scheme)

- **Protocol.** To identify itself for session ***i***, A does the following

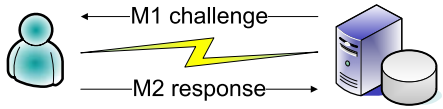
1. A computes $w_i = H^{t-i}(w)$ and transmits it to B

   A→B: A, *i*, w_i
2. B checks that $i = i_A$ and that $H(w_i) = w_{i-1}$. If both checks succeed B accepts the password, sets $i_A \leftarrow i_A + 1$, and saves w_i for the next verification

One-time passwords (Lamport's scheme)

- **Pre-play attack**.
  - An active adversary intercepts and traps (or impersonate B in order to extract) an as yet unused OTP for the purpose of subsequent impersonation
  - To prevent this attack, a password should be revealed only to a party which itself is known to be authentic
  - Challenge-response techniques address this threat

Challenge-response



$k[priv] = \langle n, d \rangle$ is the user private key

The server stores the user public key $k[pub] = \langle n, e \rangle$

The server challenges the user to answer a question

1. The server randomly chooses $r < n$ (the challenge) and sends it to the user
2. The user computes $f = r^d \bmod n$ (the response) and sends it to the server
3. The server identifies the user iff $r = f^e \bmod n$