Politecnico di Milano
Dip. Elettronica e Informazione
Milano, Italy

Authentication

Identification vs. authentication

- Identification is declaratory
  - "I am Stefano"
- Authentication is the verification of an identity
  - "This is my identity card which proves I'm Stefano"
- It is the foundation for an authorization phase
  - I am allowed to enter the parking lot
- It can be *unidirectional* or *bidirectional (mutual)*
- It can happen between humans, computers, or human to computer

The three factors of authentication

- There are several ways to authenticate an entity
  - Based on something it knows
    - A password, a pin, a secret handshake
  - Based on something it has
    - A key, a card, a token
  - Based on something it is
    - Based on his face, on his voice, or on his fingerprints
- Humans usually use the third, sometimes the second, seldom the first
- Machines, on the other hand, usually use the first or the second, and rarely the third
- *Multifactor* authentication is possible
  - Combining two, or three different factors

Something it knows

- Usual example: a *password* (pin, passphrase...)
  - But also a saved *cryptographic key*
- How do you prove you know it?
  - By *sharing* it
    - Unless authentication is mutual, you may be disclosing the secret to an attacker
    - Vulnerable to Man In The Middle and interception
  - By a challenge-response scheme of some kind
    - Computing a non-reversible function of the secret and a challenge, e.g. an hash
- In any case, this is a *weak* authentication scheme
  - Secrets can be shared, and if stolen the owner does not realize it; they can be snooped (e.g. *shoulder surfing*)
  - Guessing and/or cracking
- Used everywhere because it's deceivingly simple

Creating strong password schemes

- Correctly design password checking
  - By using a suitable challenge-response scheme
- Defend against secret loss and sharing
  - Appropriate policies and user education
  - Regular change of passwords
- Defend against secret brute forcing and guessing
  - Limit number of authentication attempts
  - Educate users to choose strong passwords (adequate length, not easy to guess such as dictionary words...)
- Defend the process
  - No storage of secrets in clear should be allowed
  - If a “recovery” scheme is used, its strength must be evaluated
  - User provisioning (i.e. setup) is often the weak link

Something it has

- Evaluates possession of a *token*
  - Examples: a key, an ID card, a passport...
- In computer security, often the token is:
  - A smart card (or a USB key)
    - The device contains a CPU and a non-volatile RAM with space for key storage
    - The device authenticates itself (and the user) to the host through a challenge/response protocol
    - The key does not leave the device
  - A one time password generator
    - It contains a counter and a private key
    - It encrypts the counter with the private key and displays a function of the result
    - The server knows the public key associated with the token, and is able to confirm the correctness of the function
    - Each password works for a limited time, e.g. 30-60-90 sec

Challenges in token authentication

- Interfacing with the host computer
  - Not any host has a smart card reader
- Tokens can be stolen or lost
  - Usually this calls for combination with a PIN or password
  - Two-factor authentication
- One-way vs. two-way authentication
  - As described until now, this scheme is one way, in some applications (e.g. credit card authorization) this scheme should be two-way, to avoid fraud
- Time-based tokens
  - Challenges in resynchronization

Something it is

- This is usually associated with biometric systems
  - Fingerprints
  - Hand geometry
  - Face geometry
  - Retina
  - Iris
  - Voice
  - DNA
  - Typing dynamics
- Requires the physical enrollment of user
  - "measurement" of the feature and creation of a template

Issues with biometric systems

- Interfacing with the host computer
  - If a card reader is a problem, go figure a retinal scanner
- Matching is not deterministic
  - False rejection, false acceptance trade-off
  - Voice recognition and typing dynamics are not usable
- Possibility of observation and duplication
  - E.g. fake fingerprints
  - … how do you change your password if duplicated?
- Evolution and loss of characteristics
- Users with disabilities
- Acceptability of measurement
  - Retina scan is invasive
  - DNA lengthy
- Privacy sensitivity

Authentication on a network

- Authenticating a user on a network entails the problem of *remoteness*
  - Transferring a password is almost straightforward
  - Transferring a fingerprint is more complex :)
- Actually, this is tightly coupled with the concepts of cryptography and secure protocols
  - So we will recall this later on during the course