

→ Authentication

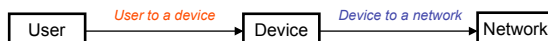
- Verification of a claim about the identity of an entity

→ Biometrics

- Physiological and behavioral traits for identifying individuals
- Biometrics used for authentication is problematic because
 - It has a low level of secrecy
 - It can be counterfeited
 - It is not easily changeable

→ Approach

- Authentication split in two parts



→ Local authentication: user to a device

- Biometric information is kept only in the device, not in a server on the network
- No need to change the infrastructure

→ Authentication of the device to a network

- Solved by other methods, e.g., by physical layer authentication

→ Challenges

- The local authentication takes place in unsupervised environments, e.g., at home
- The device is portable and can be easily stolen

→ Attacks

- The biometric information is not secret
 - An attacker may obtain the biometric information of the legitimate user and provide it to the biometric sensor
 - An attacker may create counterfeited (fake) biometrics
- The device may be a subject of a physical attack

→ Solution

- Fingerprint authentication with a Trusted Platform Module

→ Fingerprints

- Highly distinct, develop early in life, relatively permanent
- Mature technology, used to identify individuals for over a century
- Low-cost, small-sized implementations available

→ Trusted Platform Module (TPM)

- Protects the integrity and confidentiality of data with hardware support
- Identifies the device
- Performs integrity measurements and reports them

→ Functionality

- Biometric information is protected in the TPM and never leaves the device
- TPM can attest for the software running in the device and securely communicate this to a remote server

→ Target devices

- Cell/smart phones, PDAs, laptops
- Hardware tokens

→ Applications

- Bank applications
- Mobile commerce
- Access to health care anywhere and at any time
- Access to medical records