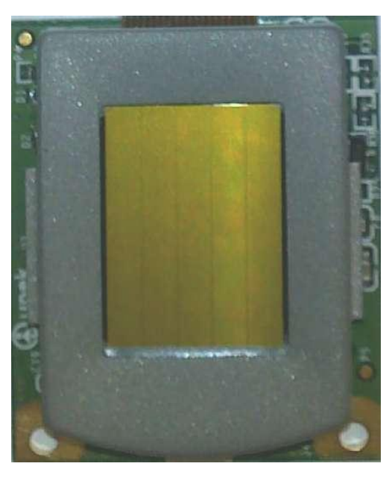
Authentication of Fingerprint Sensors

Vladimir Ivanov and John Baras

Fingerprints

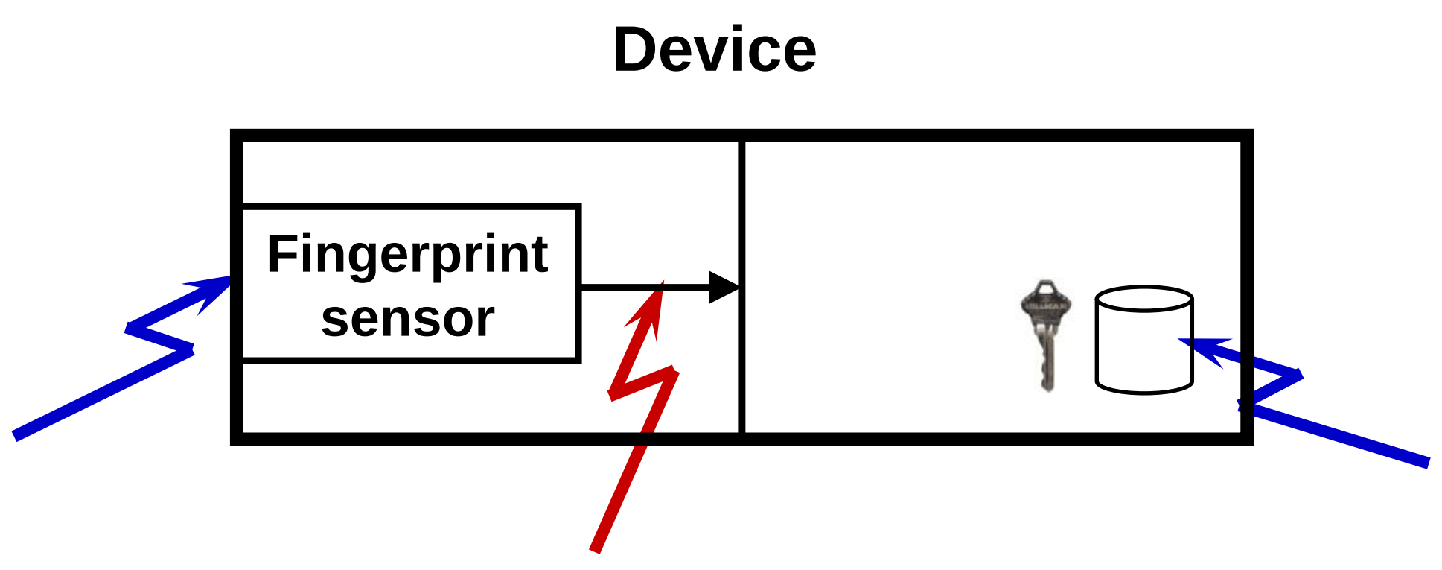
- Fingerprints
  - highly distinct
  - develop early in life
  - relatively permanent over time
  - used to identify individuals for over a century
  - low-cost and small-sized implementations readily available



- Problems of fingerprints (and of most biometrics)
  - have a low degree of secrecy
  - are set to become publicly available
  - are difficult to be changed
  - cannot be revoked

Challenges

- Portable devices
  - authentication in unsupervised environments
  - portable devices are easily stolen and physical attacks on them are possible



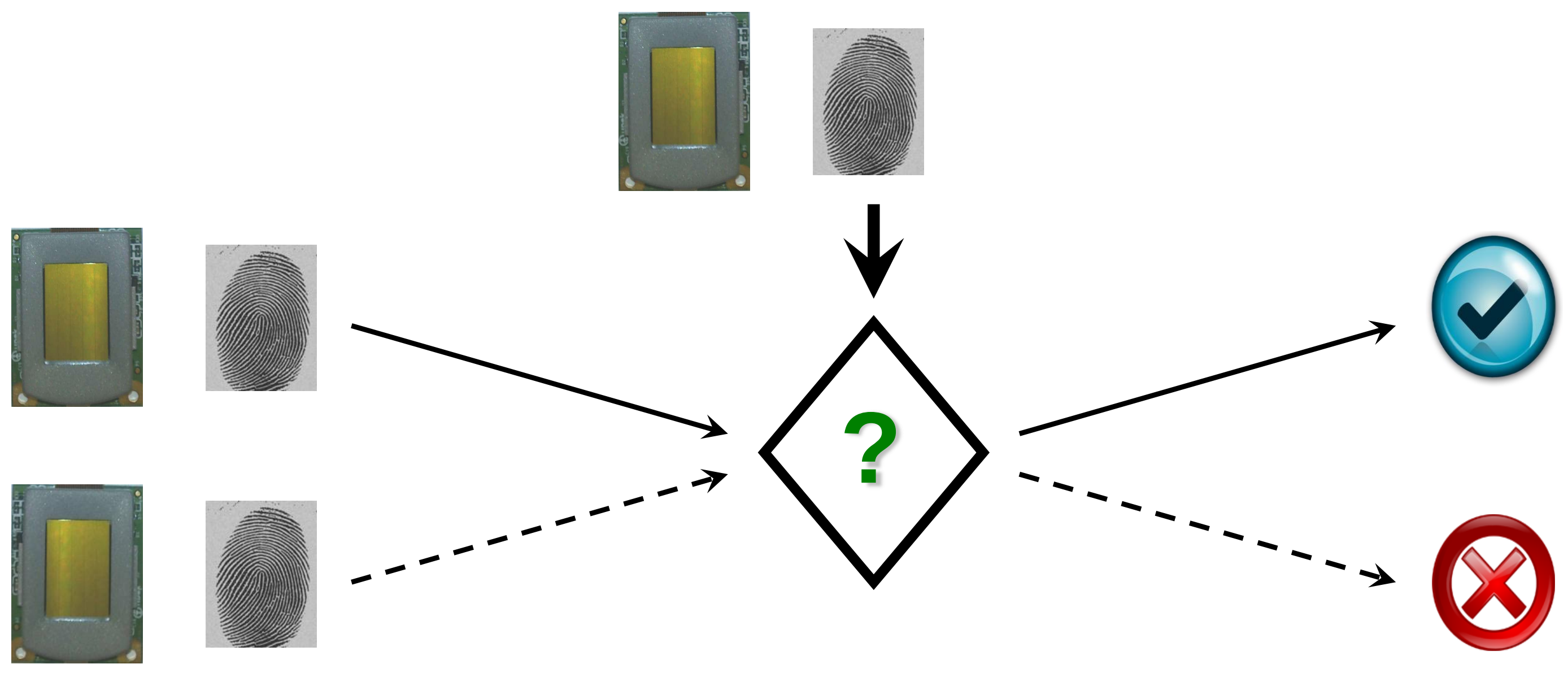
- Attacks of interest
  - malicious replacement of the authentic sensor
  - replay of a stolen image of the authentic fingerprint

- Need to verify the authenticity of the sensor which acquired a particular fingerprint image

- Approach: use the scanner pattern
  - unique, persistent, and unalterable characteristics of the sensors (scanners)

Solution

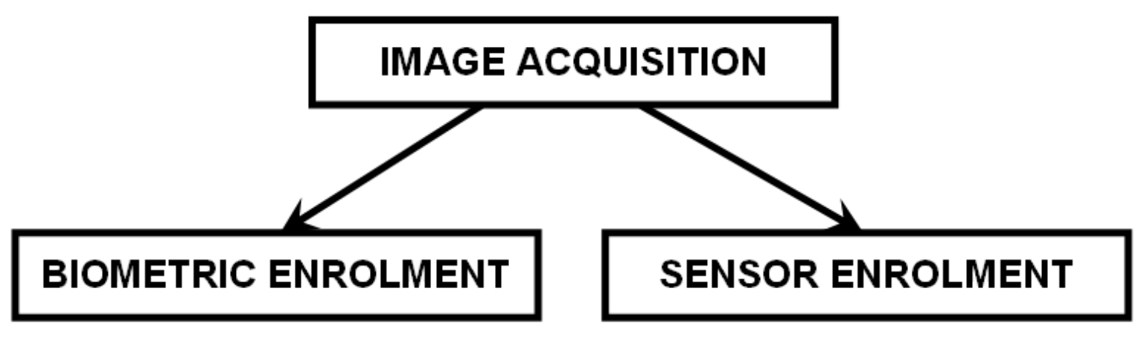
- Sensor authentication
  - determines if two images have been acquired with the same sensor or with a different sensor of the same type, manufacturer, and model
  - sensor enrolment and sensor verification

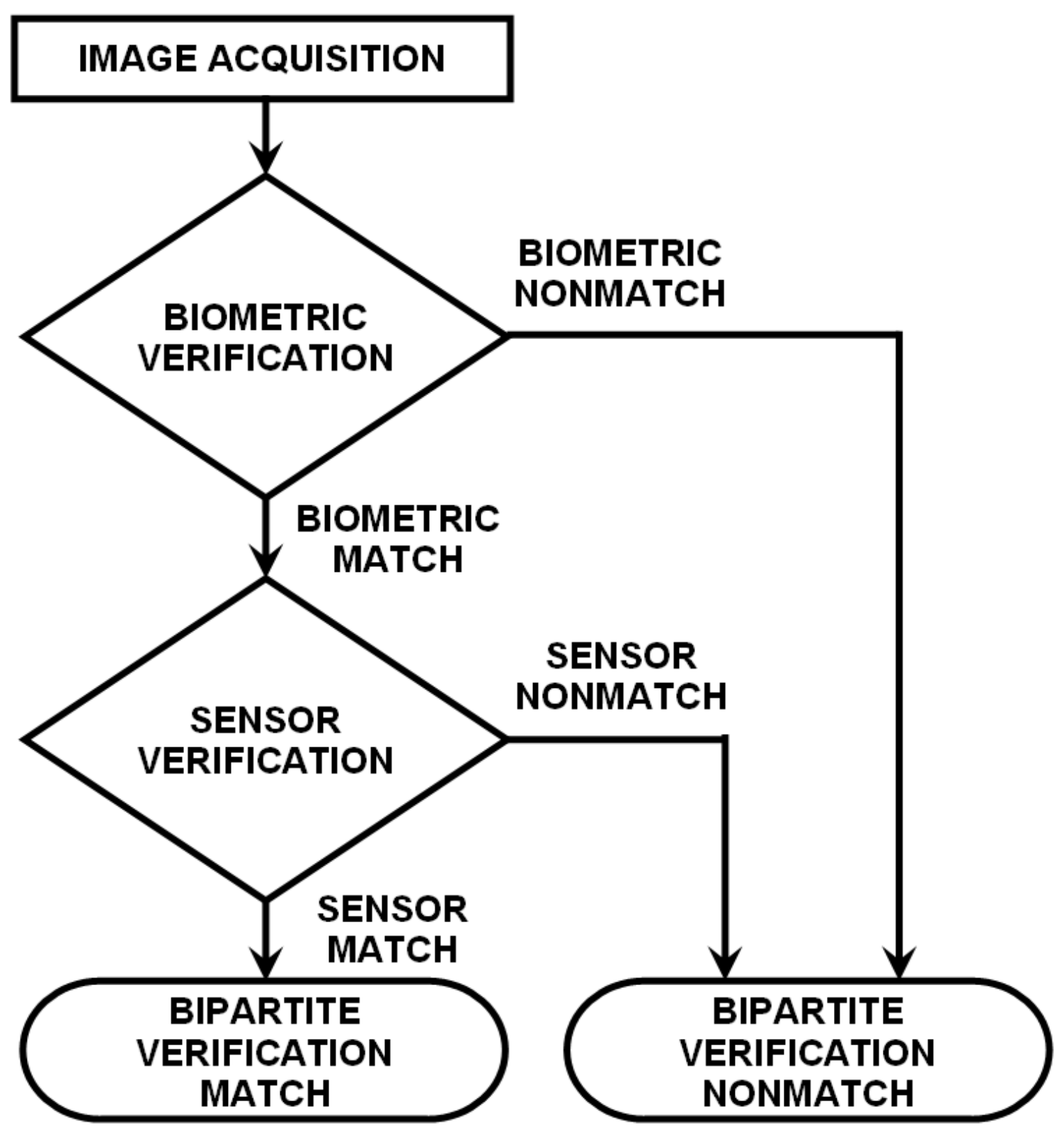


- Our technology
  - accurate, computationally efficient, robust
  - can be added as a software add-on

Applications

- Bipartite authentication
  - biometric authentication and sensor authentication
  - bipartite enrolment
  - bipartite verification





- Directions
  - bind user and device
  - device authentication/identification
  - source of randomness

- Settings
  - mobile wallets
  - access to health care and medical records
  - contextual authentication/user rights
  - asset management