

Lect. 14. Identification

Authentication

❖ Entity Authentication (Identification)

- Over the communication network, one party, Alice, shows to another party, Bob, that she is the real Alice.
- Authenticate an entity by presenting some identification information
- Should be secure against various attacks
- Through an interactive protocols using secret information

❖ Message Authentication

- Show that a message was generated by an entity
- Using digital signature or MAC

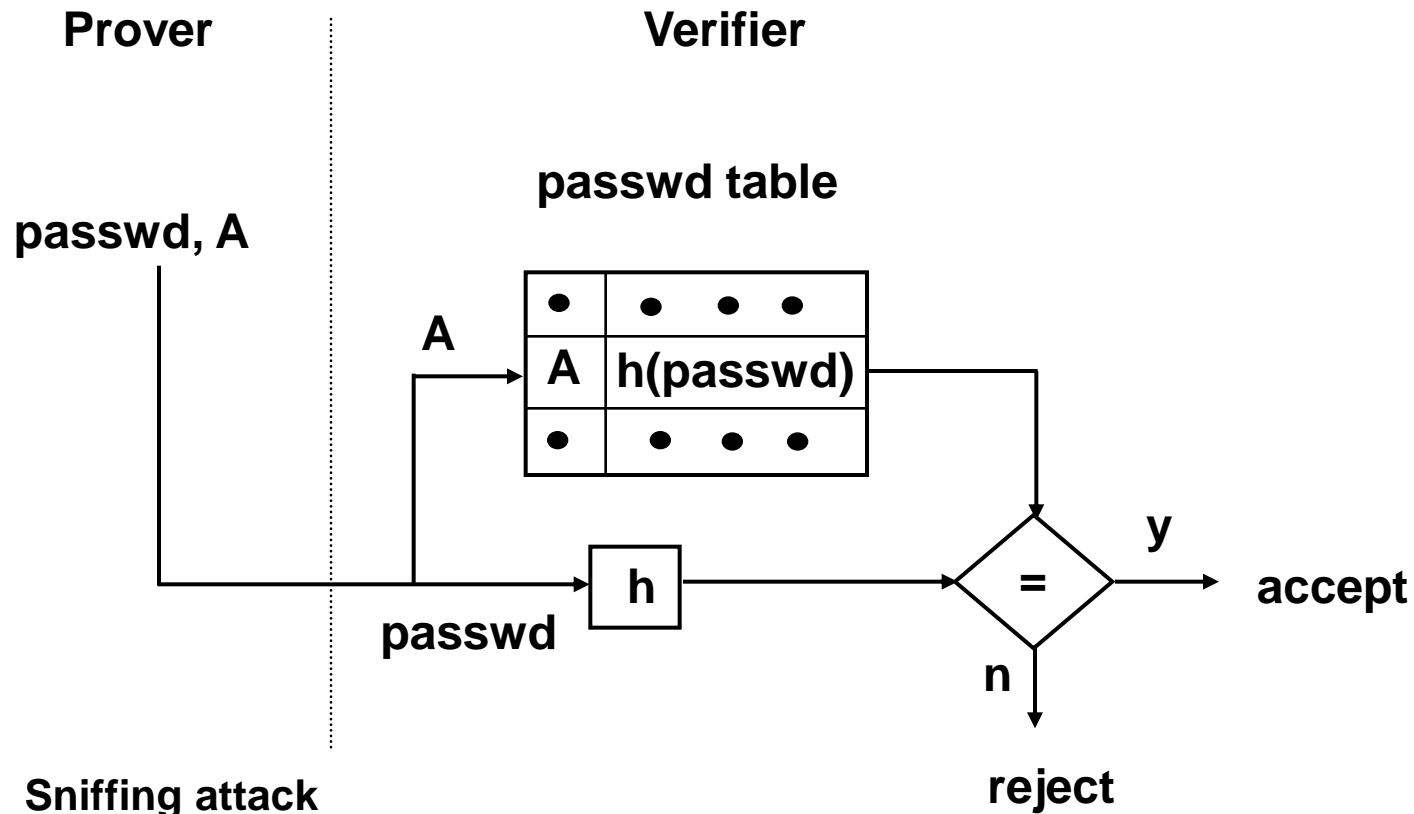
Classification of Identification

Method	Examples	Reliability	Security	Cost
<i>What you Remember (know)</i>	Password Telephone # Reg. #	M/L	M (theft) L (impersonation)	Cheap
<i>What you have</i>	Registered Seal Magnetic Card IC Card	M	L (theft) M (impersonation)	Reasonable
<i>What you are</i>	Bio-metric (Fingerprint, Eye, DNA, face, Voice, etc)	H	H (theft) H (Impersonation)	Expensive

Identification Schemes

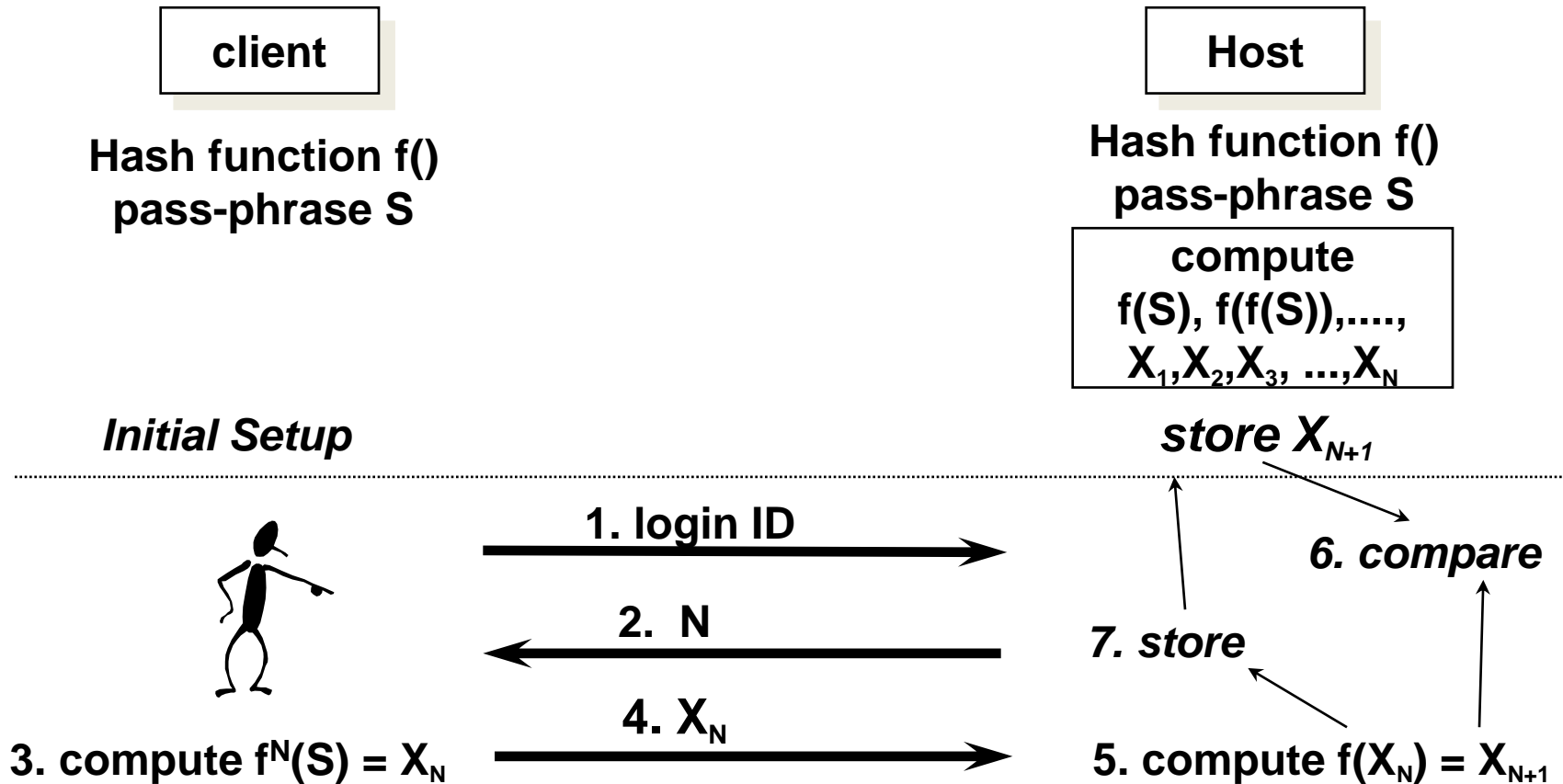
- ❖ **Password-based scheme (weak authentication)**
 - crypt *passwd* under UNIX
 - one-time password
- ❖ **Challenge-Response scheme (strong authentication)**
 - Symmetric cryptosystem
 - MAC (keyed-hash) function
 - Asymmetric cryptosystem
- ❖ **Using Cryptographic Protocols**
 - Fiat-Shamir identification protocol
 - Schnorr identification protocol, *etc*

Identification by Password

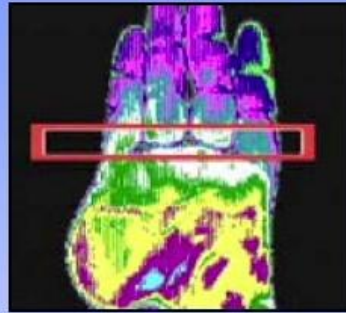


Sniffing attack
Replay attack - Static password

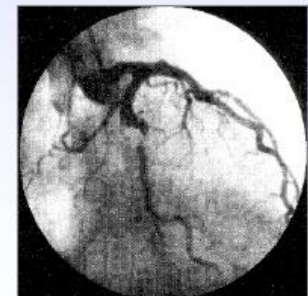
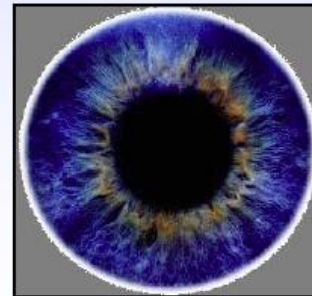
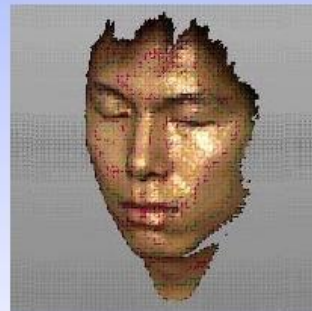
S/Key (One-Time Password System)



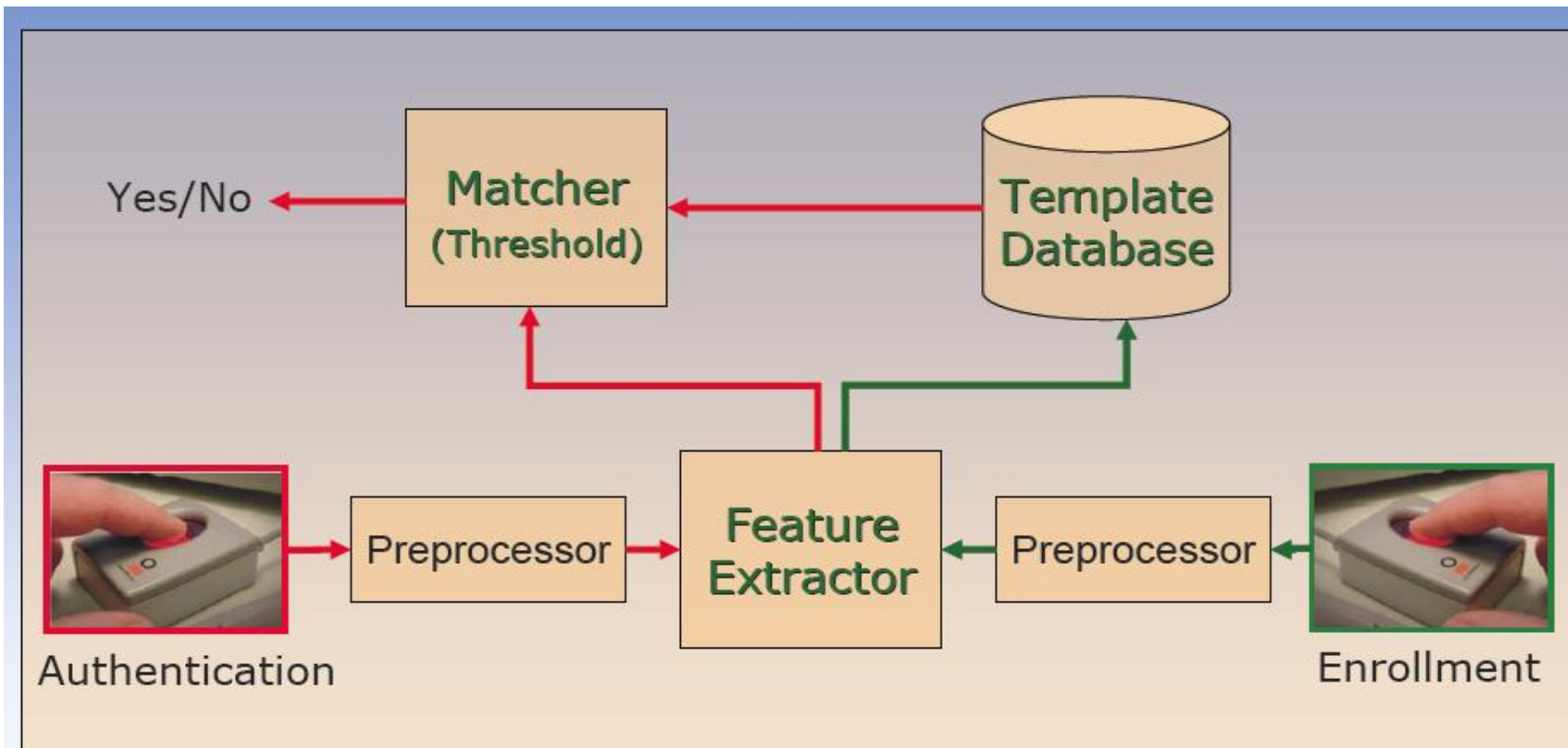
Bio-identification



Joe Smith

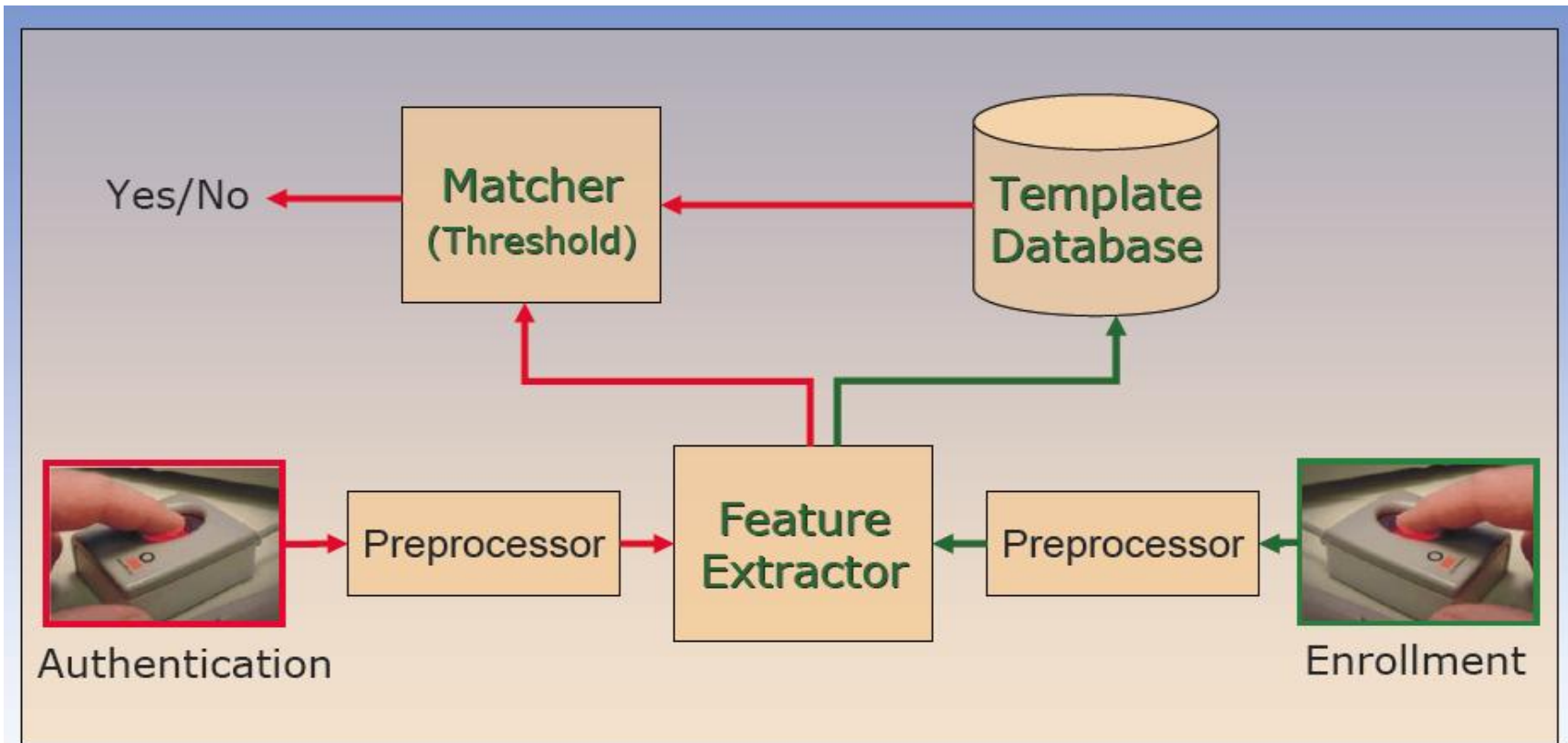


Biometric Recognition System



- False accept rate (**FAR**): Proportion of imposters accepted
- False reject rate (**FRR**): Proportion of genuine users rejected
- Failure to enroll rate (**FTE**): portion of population that cannot be enrolled
- Failure to acquire rate (**FTA**): portion of population that cannot be verified

Biometric Recognition System

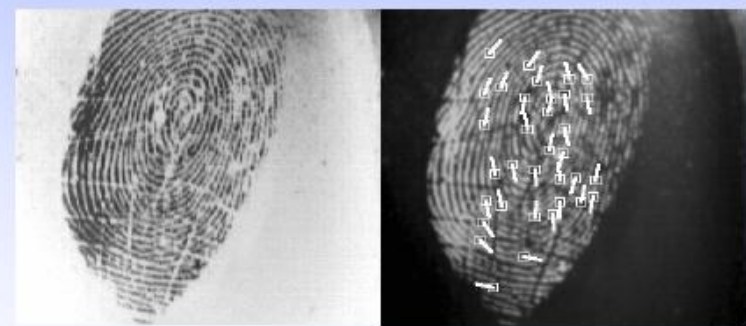


- False accept rate (**FAR**): Proportion of imposters accepted
- False reject rate (**FRR**): Proportion of genuine users rejected
- Failure to enroll rate (**FTE**): portion of population that cannot be enrolled
- Failure to acquire rate (**FTA**): portion of population that cannot be verified

Fake Fingerprint



Live finger



Gummy finger

Access was granted 75% of the time using gummy fingers

Applications

Goal: Automatic & reliable person identification in unattended mode, often remotely



Iris matching:
Heathrow Airport



US-VISIT
Program



Cellular phone:
Siemens



Grocery store
payment: Indivos



Automobile: Audi A8



Disney World

8