Other Authentication Methods

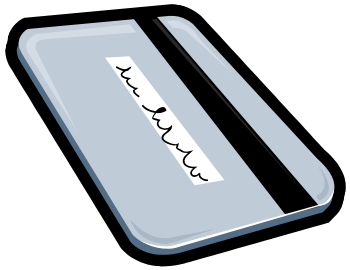
Tokens, Smart Cards, Biometrics

Token Authentication

- object user possesses to authenticate, e.g.
  - embossed card
  - magnetic stripe card
  - memory card
  - smartcard

Types of Cards Used as Tokens

Card Type	Defining Feature	Example
Embossed	Raised characters only, on front	Old credit card
Magnetic stripe	Magnetic bar on back, characters on front	Bank card
Memory	Electronic memory inside	Prepaid phone card
Smart	Electronic memory and processor inside	Biometric ID card
Contact	Electrical contacts exposed on surface	
Contactless	Radio antenna embedded inside	



From Computer Desktop Encyclopedia
Reproduced with permission.

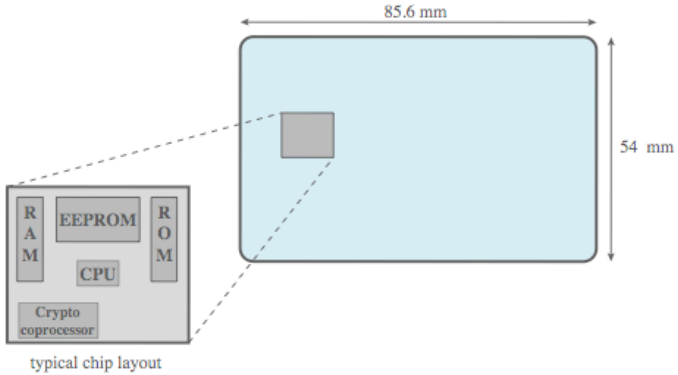
YubiKey by Yubico

Memory Cards

- can store but do not process data
- the most common is the magnetic stripe card
- can include an internal electronic memory
- can be used alone for physical access
  - hotel room
  - ATM

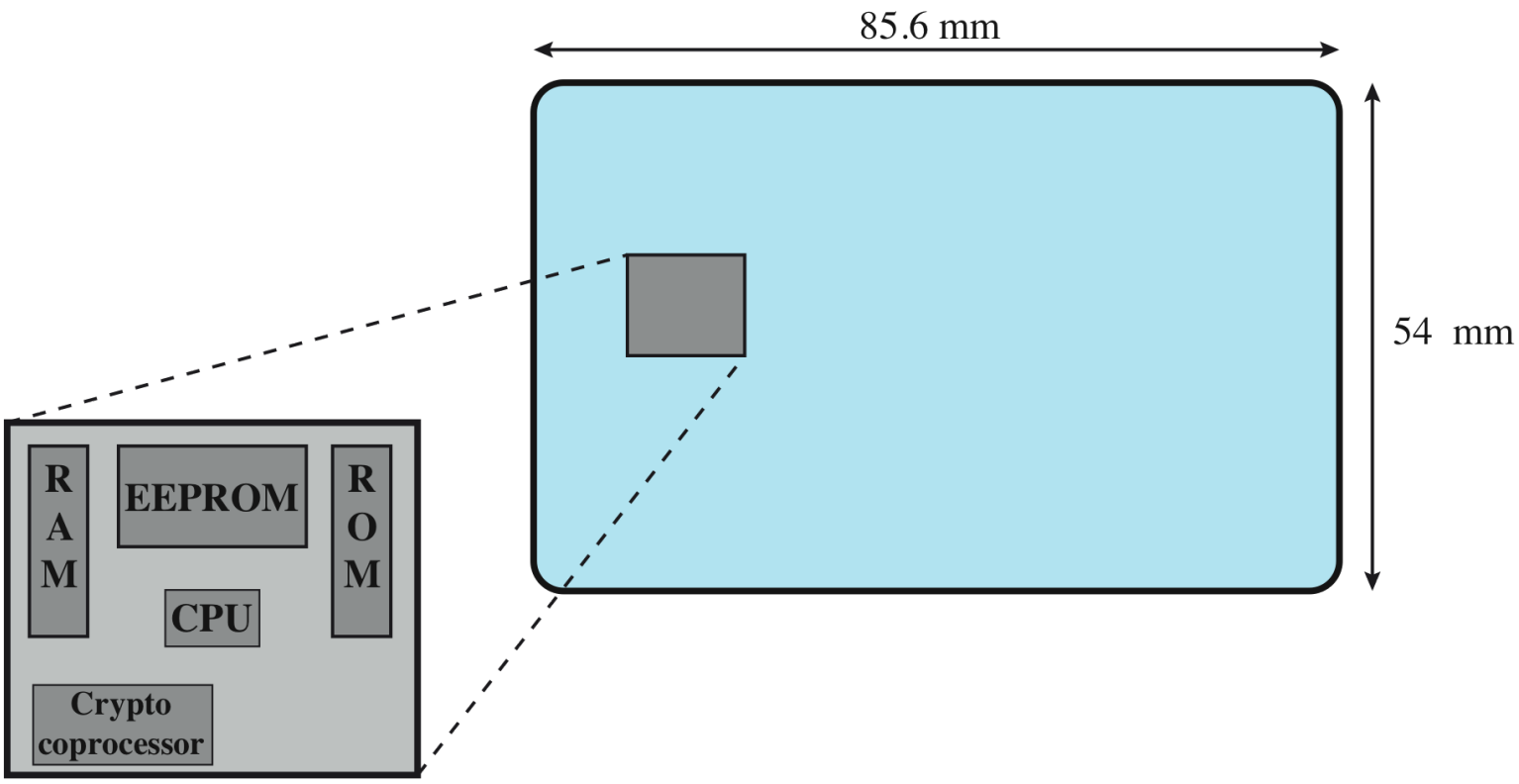
- provides significantly greater security when combined with a password or PIN
- drawbacks of memory cards include:
  - requires a special reader
  - loss of token
  - user dissatisfaction

Smartcard



- credit-card like
- has own processor, memory, I/O ports
  - wired or wireless access by reader
  - may have crypto co-processor
  - ROM, EEPROM, RAM memory
- executes protocol to authenticate with reader/ computer
- also have USB dongles

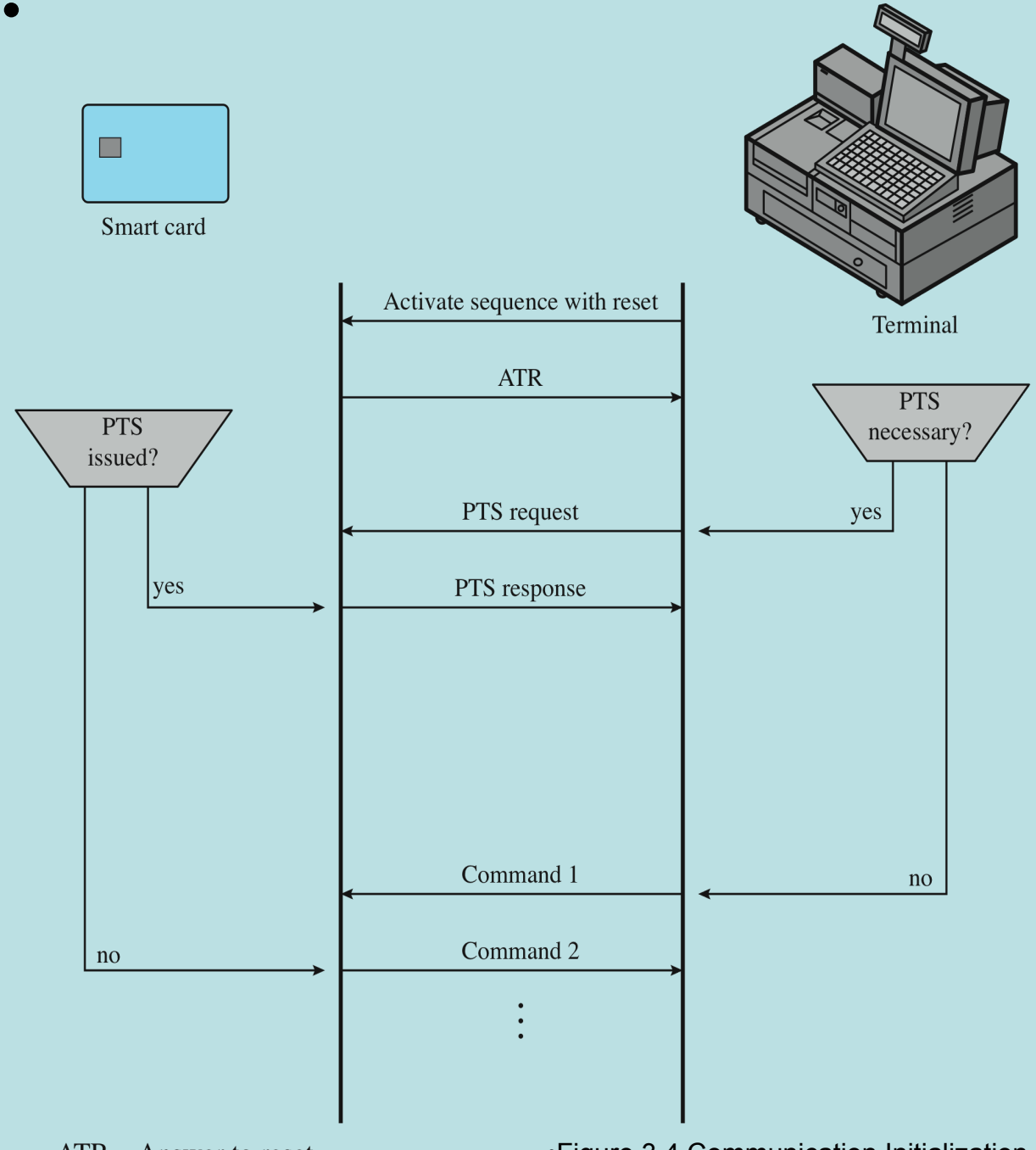
Smart Card Dimensions



typical chip layout

Smart Card Reader

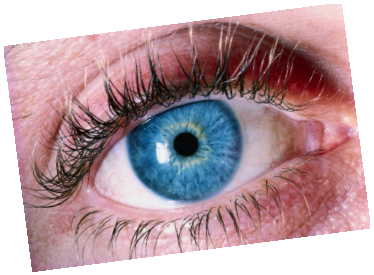
Communication Initialization between a Smart Card and a Reader

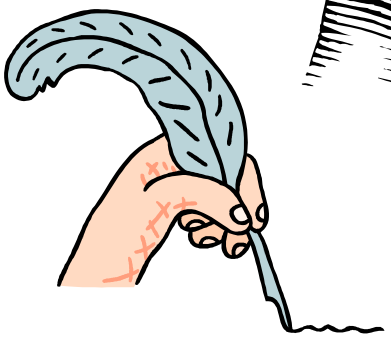


•Figure 3.4 Communication Initialization
• between a Smart Card and a Reader
•*Source: Based on [TUNS06].*

Biometric Authentication

- attempts to authenticate an individual based on unique physical characteristics
- based on pattern recognition
- is technically complex and expensive when compared to passwords and tokens
- physical characteristics used include:
  - facial characteristics
  - fingerprints
  - hand geometry
  - retinal pattern
  - iris
  - signature
  - voice





Common Biometrics

•Fingerprint

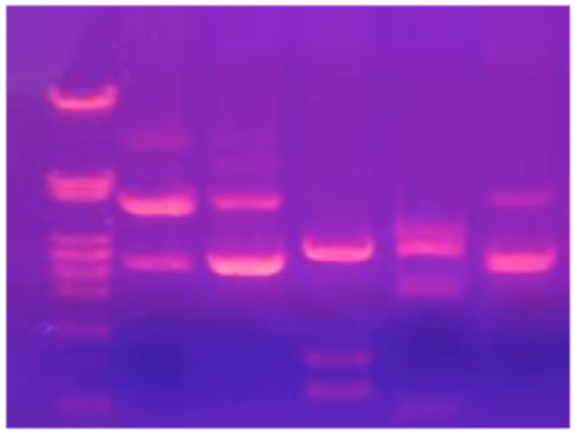
•Iris

•Face

•Signature

•Voice Print

Uncommon Biometrics



•DNA

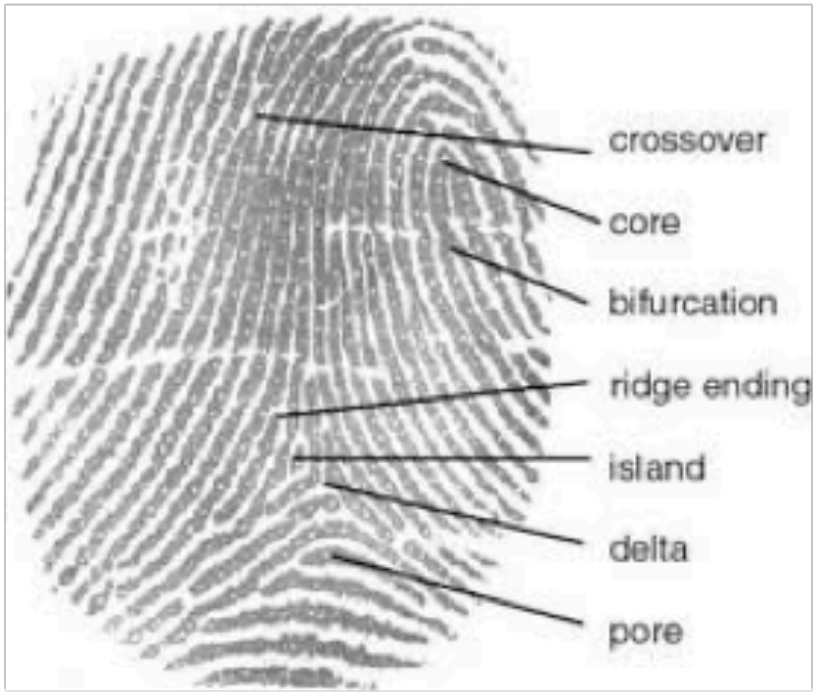
•Gait

•Retina

•Ear

Fingerprints

- Analysis based on discrete features
  - Crossover
  - Island
  - Etc.
- Discrimination power based on combinatorics
  - More matches, more confidence

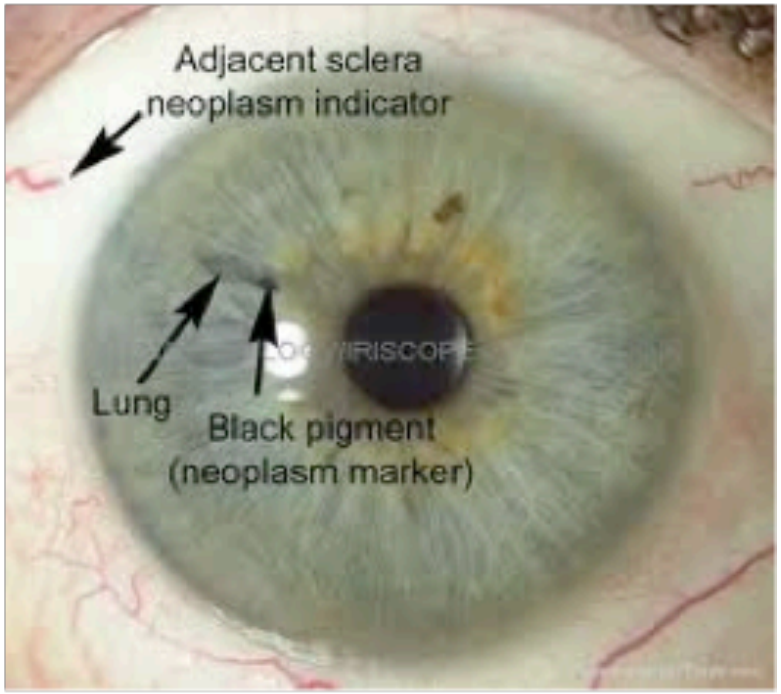


Fingerprints (II)

- Oldest biometric technology
  - Trained experts / court-approved
  - Automatic data base retrieval
- Advantages
  - Reliable, unique (even identical twins)
  - Inexpensive scanners
  - Cooperative subjects ➔ good fingerprints
  - Non-cooperative subjects ➔ latent prints
- Disadvantages
  - 5% of world population has no usable fingerprints
  - Mask-able (gloves / abrasion)
  - Can be faked

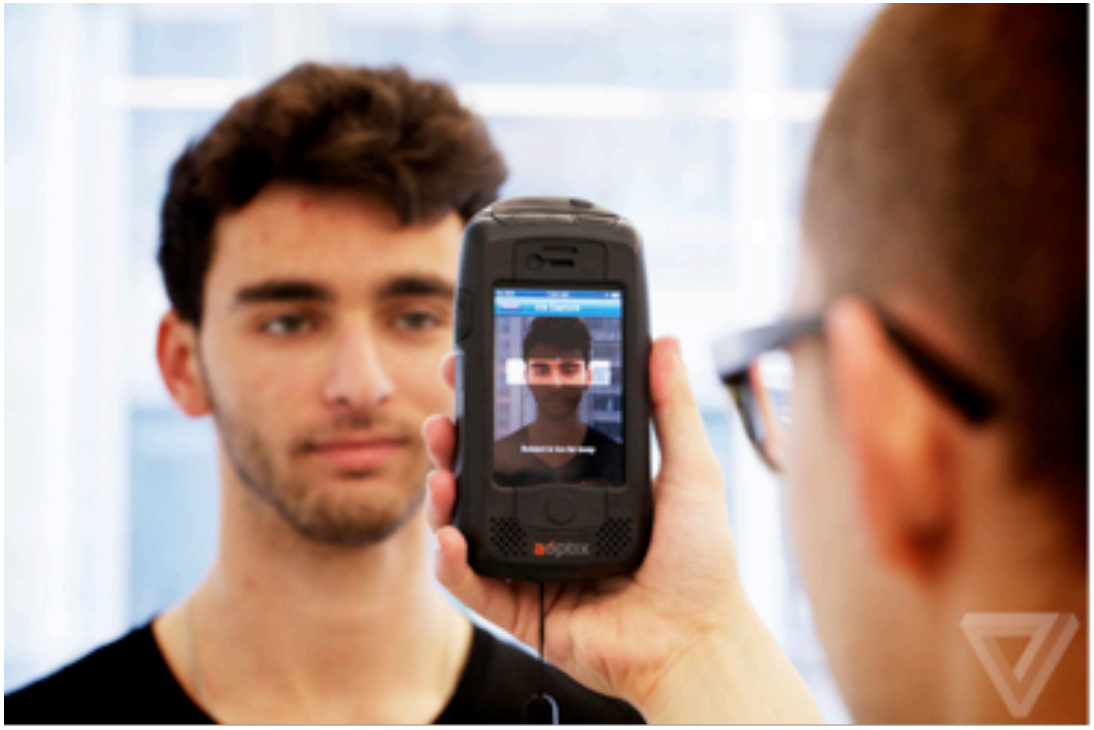
Iris

- Analysis based on discrete features
  - Polar striations
  - Also neoplasms, etc.
- Discrimination power based on combinatorics
  - Similar to fingerprints
- Infra-red lighting
  - Otherwise dark-eyed people can't be matched



Iris

- New biometric technology
- Advantages
  - Reliable /unique (even identical twins)
  - Relatively inexpensive scanners
- Disadvantages
  - No human experts (hard to audit)
  - Cooperative subjects with active sensors only
  - Behavior over time is unclear



Uses of Biometrics

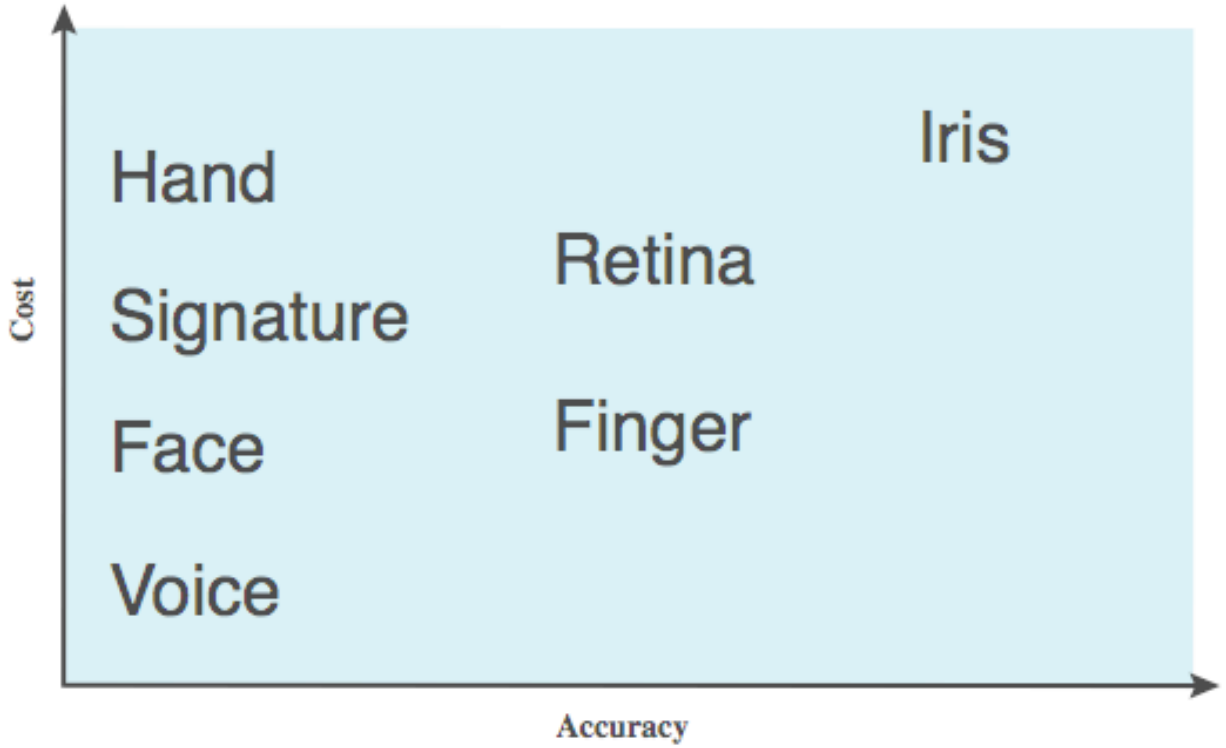
- Forensics (post-hoc identity)
  - Non-cooperative subjects
  - Latent / accidental data
  - Identity search
- Verification (security)
  - Cooperative subjects
  - Verify/reject a single identity
- Intelligence / Surveillance
  - Non-cooperative subjects
  - Biometrics at a distance
  - Watch list

Fearless Predictions

- Currently…
  1. Forensics: Fingerprints, DNA
  2. Security: Fingerprint, Signature, Iris, 2D Face
  3. Intelligence: Human face recognition
- In the near future….
  - Forensics : DNA, Fingerprints, Face
  - High-end Security: Iris, 3D Face
  - Low-end security: Fingerprint, 2D Face
  - Intelligence: Face, gait, ear…

Biometric Authentication

- authenticate user based on one of their physical characteristics



Cost Versus Accuracy

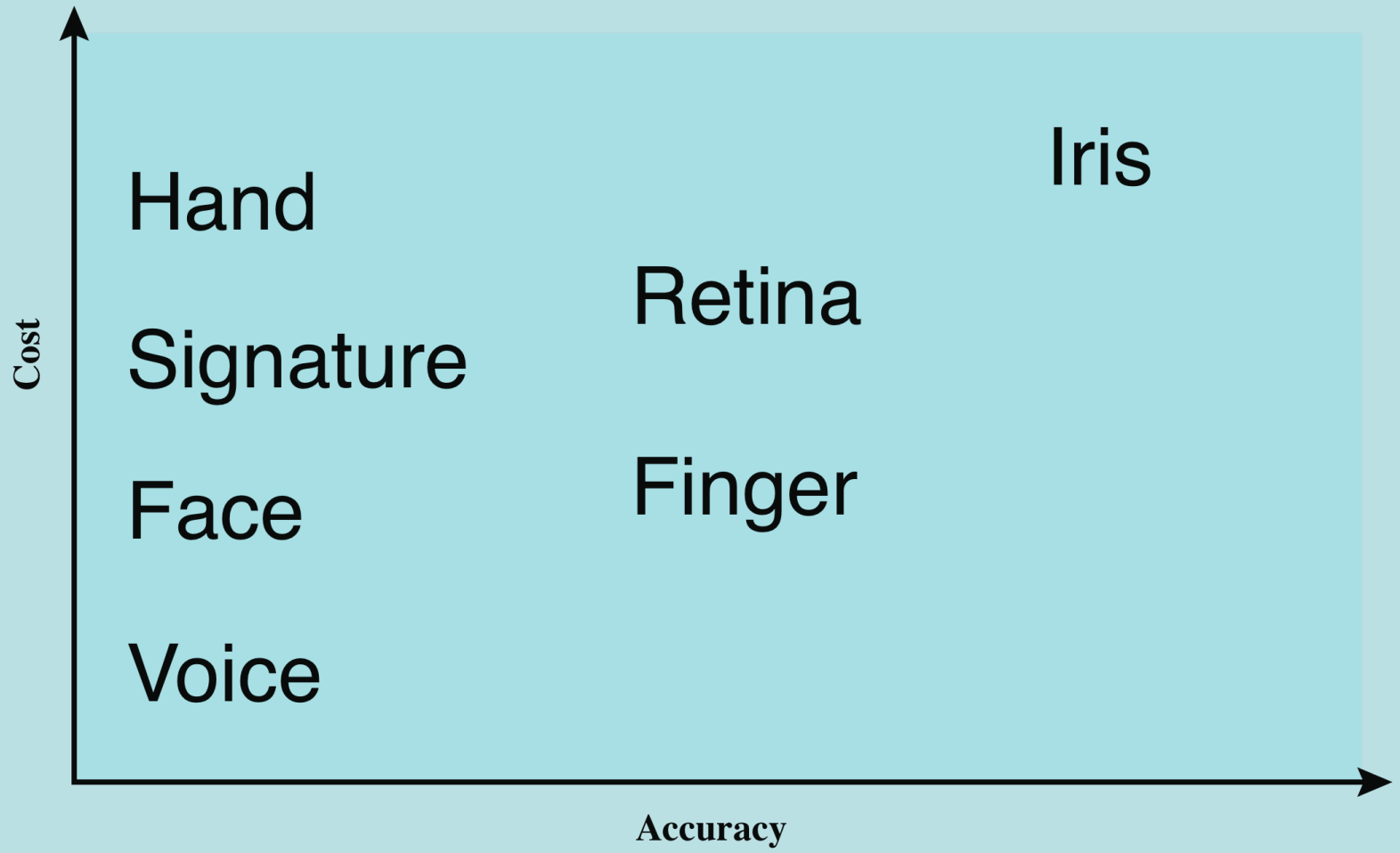
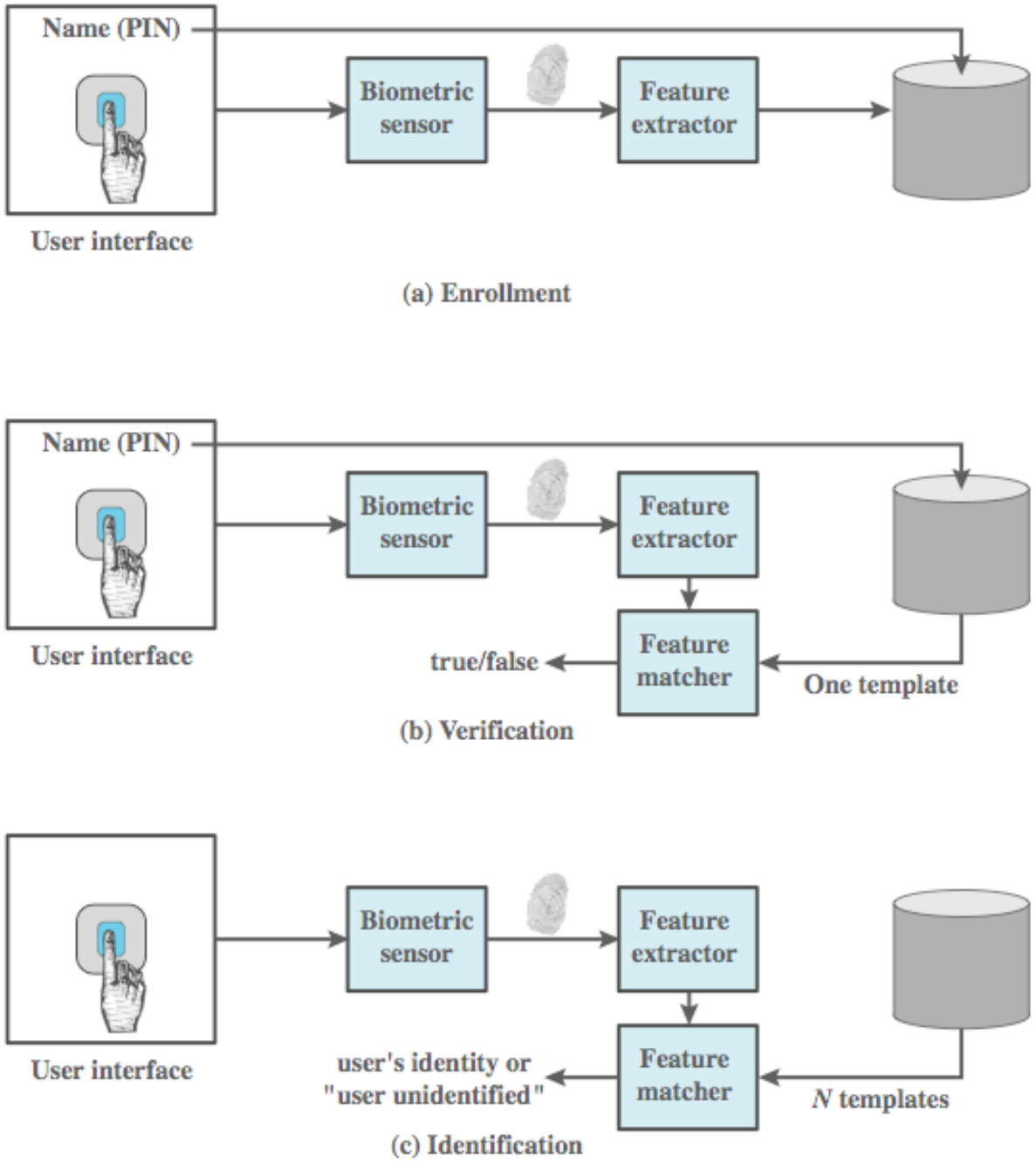


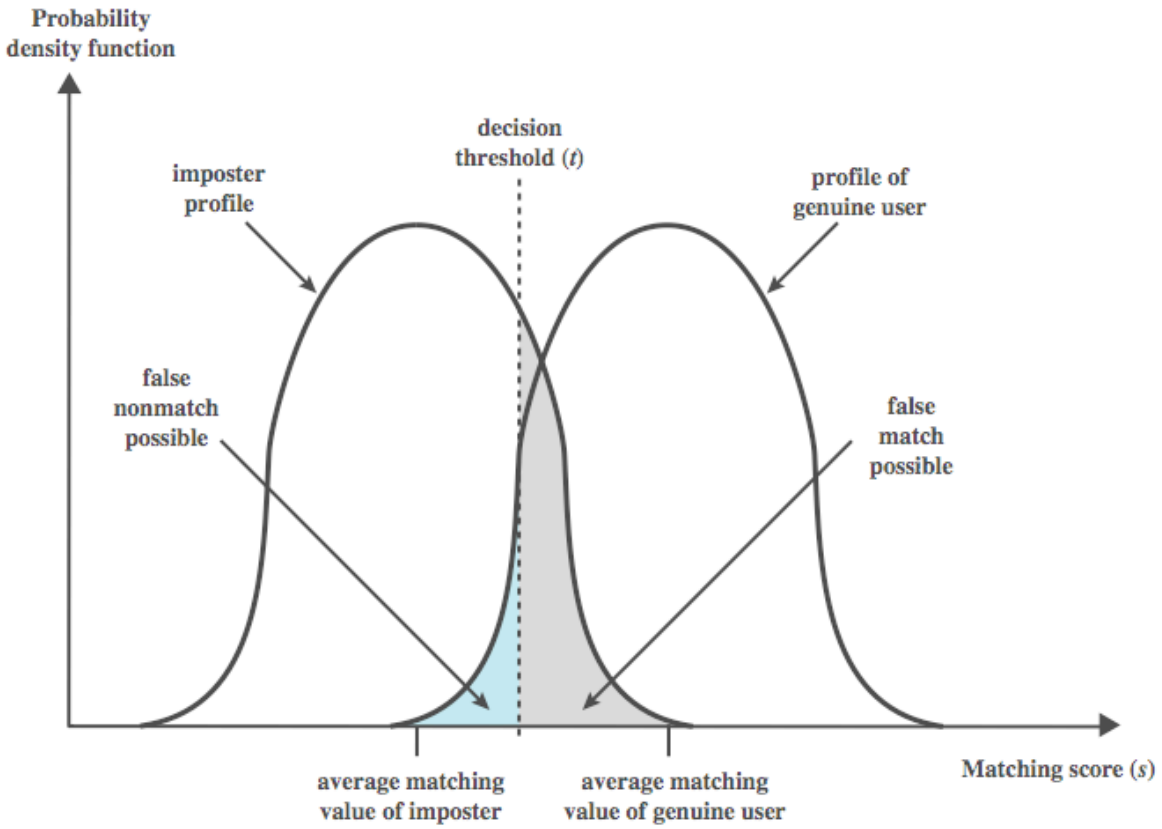
Figure 3.5 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.

Operation of a Biometric System



Biometric Accuracy

- never get identical templates
- problems of false match / false non-match



Biometric Measurement Operating Characteristic Curves

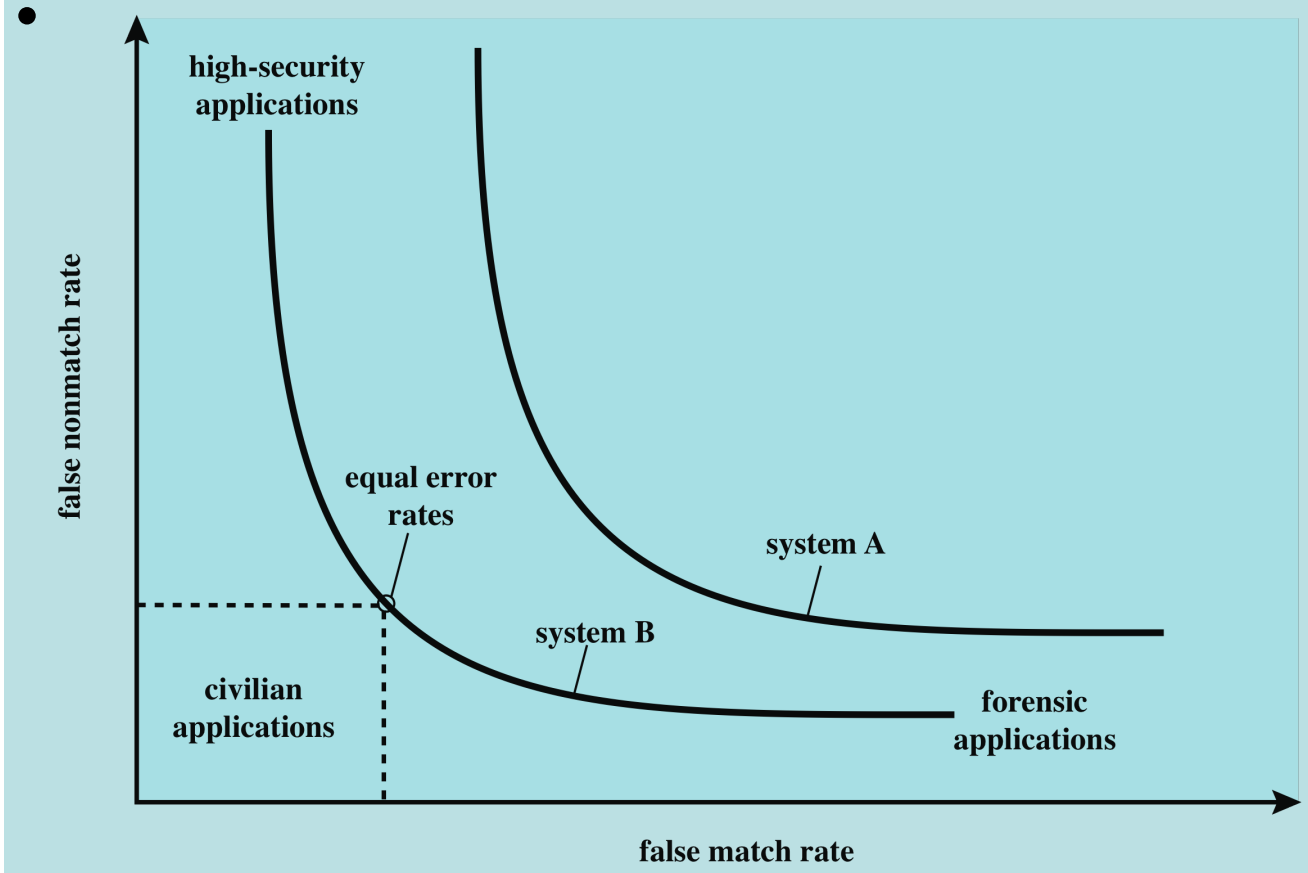
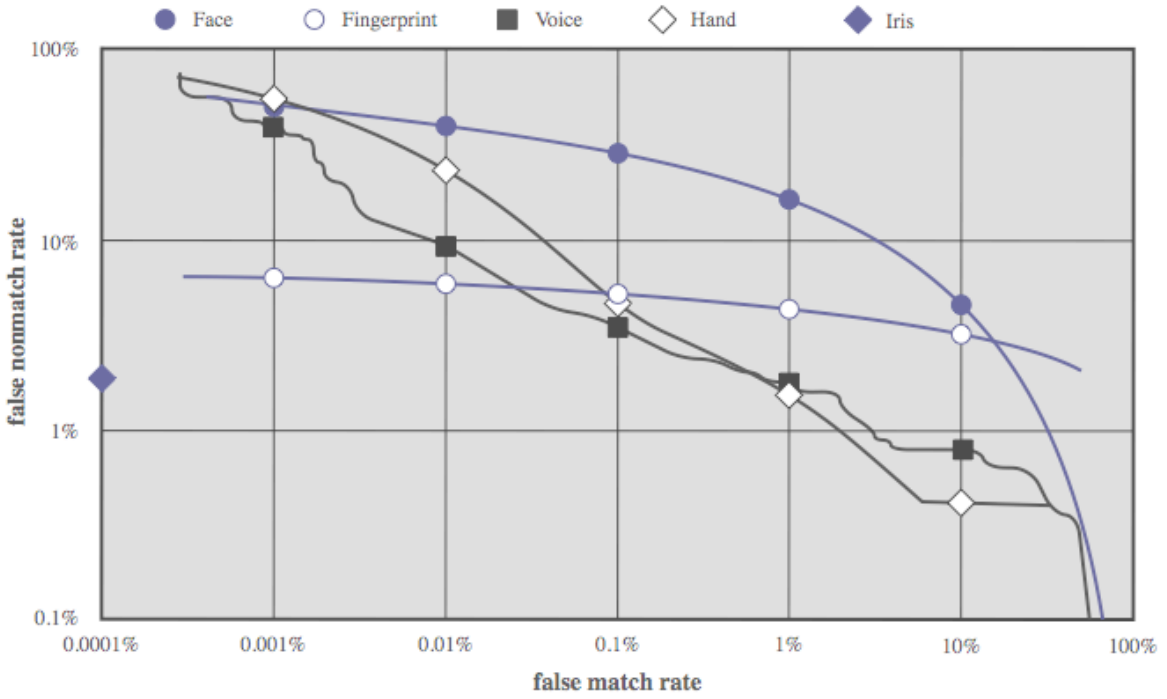


Figure 3.8 Idealized Biometric Measurement Operating Characteristic Curves. Different biometric application types make different trade-offs between the false match rate and the false nonmatch rate. Note that system A is consistently inferior to system B in accuracy performance. [JAIN00]

Biometric Accuracy

- can plot characteristic curve
- pick threshold balancing error rates



Remote User Authentication

- authentication over network more complex
  - problems of eavesdropping, replay
- generally use challenge-response
  - user sends identity
  - host responds with random number
  - user computes f(r,h(P)) and sends back
  - host compares value from user with own computed value, if match user authenticated
- protects against a number of attacks

Password Protocol

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{r, \text{h}(), \text{f}()\}$	random number h(), f(), functions
P' password r', return of r	$\text{f}(r', \text{h}(P')) \rightarrow$	
	$\leftarrow$ yes/no	if $\text{f}(r', \text{h}(P')) =$ $\text{f}(r, \text{h}(P(U)))$ then yes else no

(a) Protocol for a password

- Example of a challenge-response protocol

- user transmits identity to remote host
- host generates a random number (nonce)
- nonce is returned to the user
- host stores a hash code of the password
- function in which the password hash is one of the arguments
- use of a random number helps defend against an adversary capturing the user's transmission

Token Protocol

- user transmits identity to the remote host
- host returns a random number and identifiers
- token either stores a static passcode or generates a one-time random passcode
- user activates passcode by entering a password
- password is shared between the user and token and does not involve the remote host

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{ r, \text{h}(), \text{f}() \}$	r, random number h(), f(), functions
$P' \rightarrow W'$ password to passcode via token r', return of r	$\text{f}(r', \text{h}(W')) \rightarrow$	
	$\leftarrow$ yes/no	if $\text{f}(r', \text{h}(W')) =$ $\text{f}(r, \text{h}(W(U)))$ then yes else no

(b) Protocol for a token

- Example of a
- token protocol

Static Biometric Protocol

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{ r, \mathrm{E}() \}$	r, random number E(), function
$B' \rightarrow BT'$ biometric D' biometric device r', return of r	$\mathrm{E}(r', D', BT') \rightarrow$	$\mathrm{E}^{-1}\mathrm{E}(r', P', BT') =$ (r', P', BT')
	$\leftarrow$ yes/no	if $r' = r$ and $D' = D$ and $BT' = BT(U)$ then yes else no

(c) Protocol for static biometric

- Example of a
- static biometric protocol

- user transmits an ID to the host
- host responds with a random number and the identifier for an encryption
- client system controls biometric device on user side
- host decrypts incoming message and compares these to locally stored values
- host provides authentication by comparing the incoming device ID to a list of registered devices at the host database

Dynamic Biometric Protocol

- host provides a random sequence and a random number as a challenge
- sequence challenge is a sequence of numbers, characters, or words
- user at client end must then vocalize, type, or write the sequence to generate a biometric signal
- the client side encrypts the biometric signal and the random number
- host decrypts message and generates a comparison

- Example of a
- dynamic biometric protocol

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{ r, x, \mathrm{E}() \}$	r, random number x, random sequence challenge E(), function
$B', x' \rightarrow BS'(x')$ r', return of r	$\mathrm{E}(r', BS'(x')) \rightarrow$	$\mathrm{E}^{-1}\mathrm{E}(r', BS'(x')) =$ $(r', BS'(x'))$ extract B' from $BS'(x')$
	$\leftarrow$ yes/no	if $r' = r$ and $x' = x$ and $B' = B(U)$ then yes else no

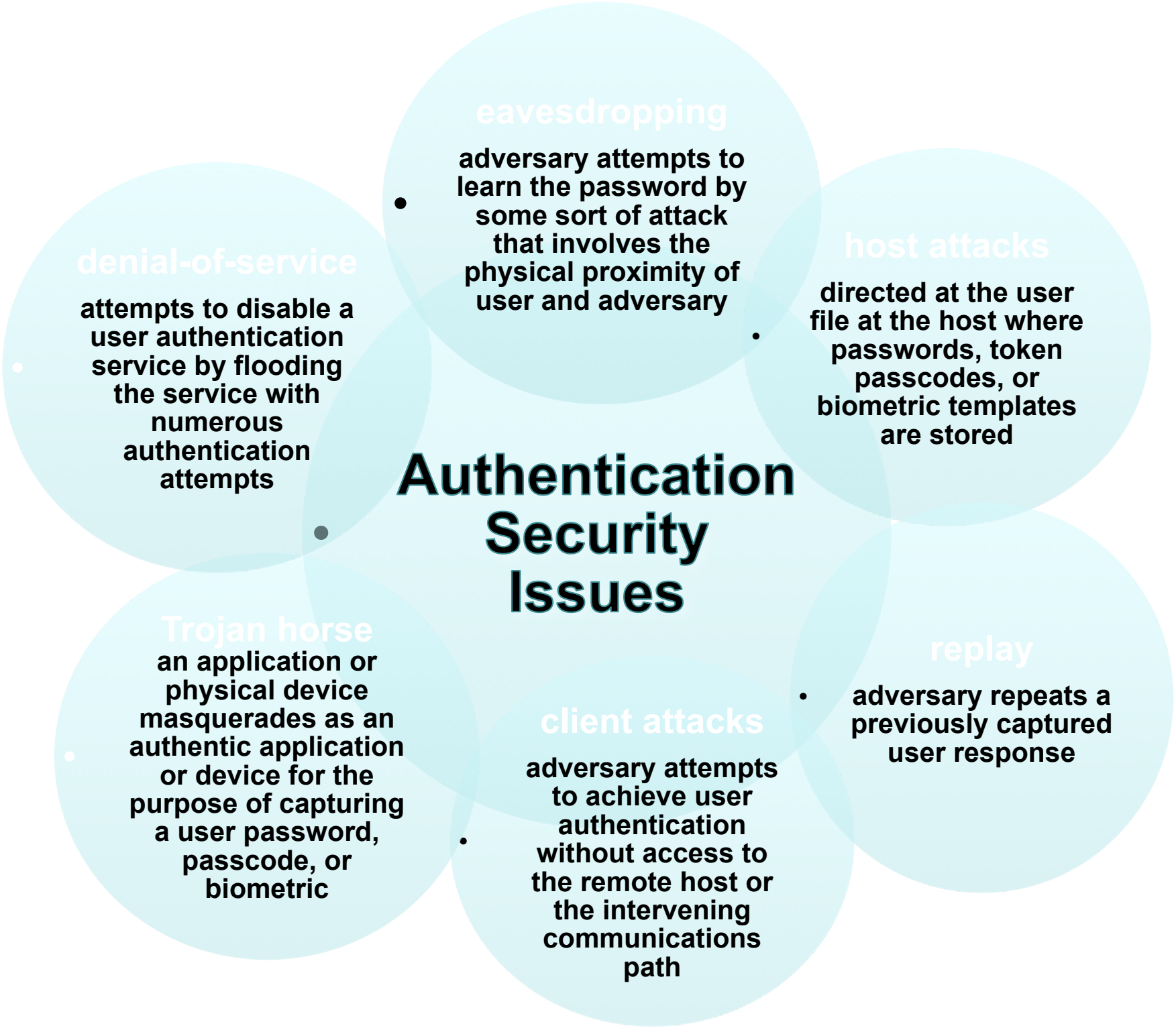
(d) Protocol for dynamic biometric

Attacks	Authenticators	Examples	Typical defenses
Client attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts, theft of object requires presence
	Biometric	False match	Large entropy; limited attempts
Host attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection of password database
	Token	Passcode theft	Same as password; 1-time passcode
	Biometric	Template theft	Capture device authentication; challenge response
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode
	Biometric	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge-response protocol
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of client or capture device within trusted security perimeter
Denial of service	Password, token, biometric	Lockout by multiple failed authentications	Multifactor with token

Potential Attacks, Susceptible Authenticators, and Typical Defenses

Authentication Security Issues

- Client Attacks
- Host Attacks
- Eavesdropping
- Replay
- Trojan Horse
- Denial-Of-Service


Authentication Security Issues
eavesdropping
adversary attempts to learn the password by some sort of attack that involves the physical proximity of user and adversary
host attacks
directed at the user file at the host where passwords, token passcodes, or biometric templates are stored
denial-of-service
attempts to disable a user authentication service by flooding the service with numerous authentication attempts
Trojan horse
an application or physical device masquerades as an authentic application or device for the purpose of capturing a user password, passcode, or biometric
client attacks
adversary attempts to achieve user authentication without access to the remote host or the intervening communications path
replay
adversary repeats a previously captured user response

Practical Application: Iris Biometric System

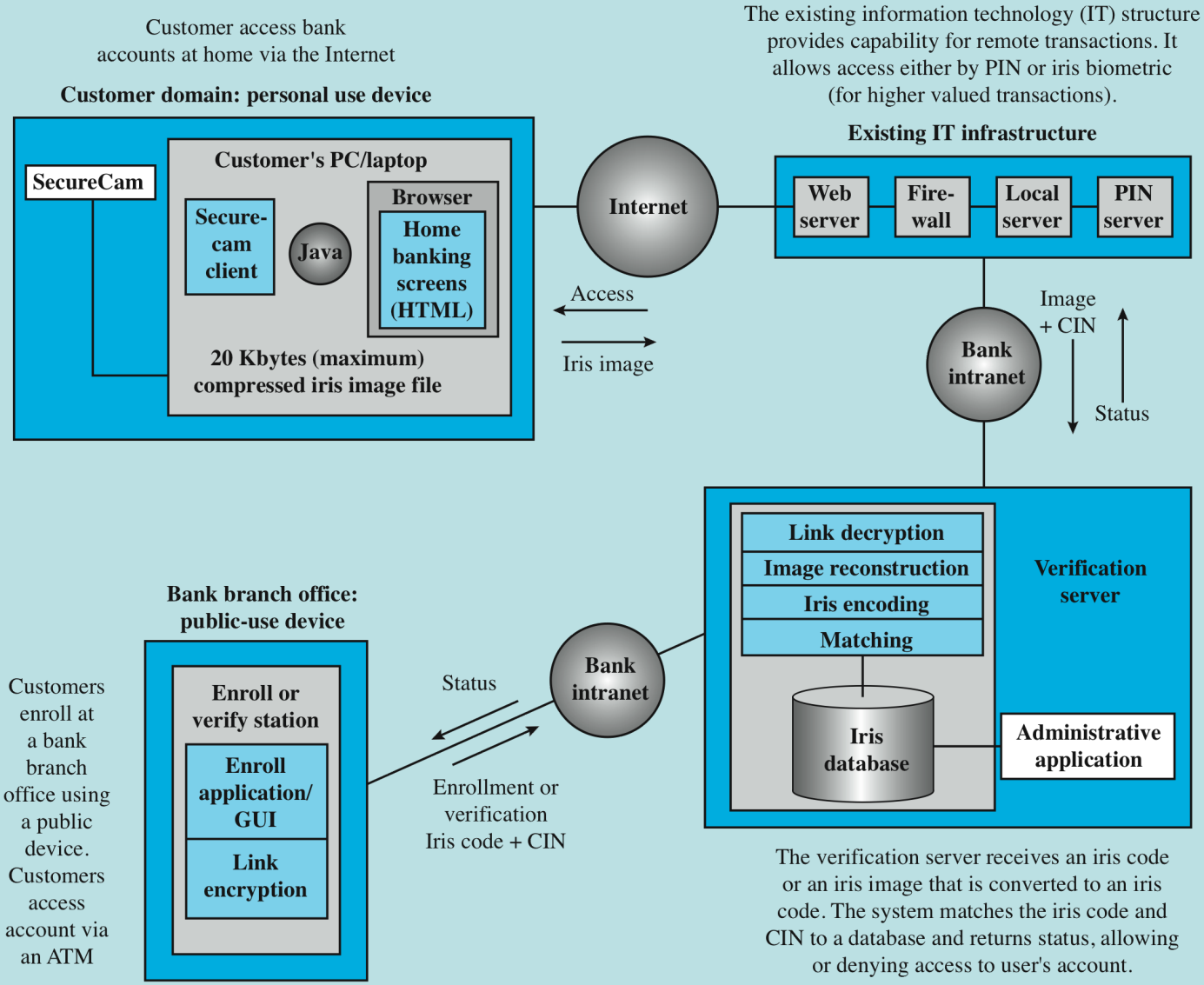
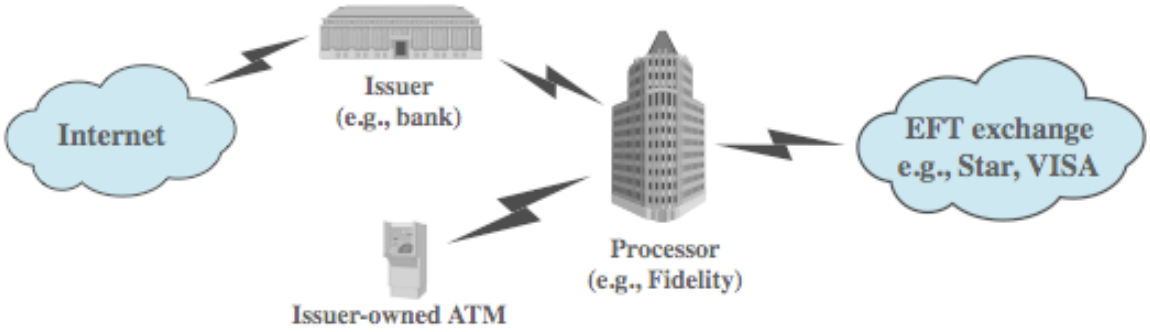
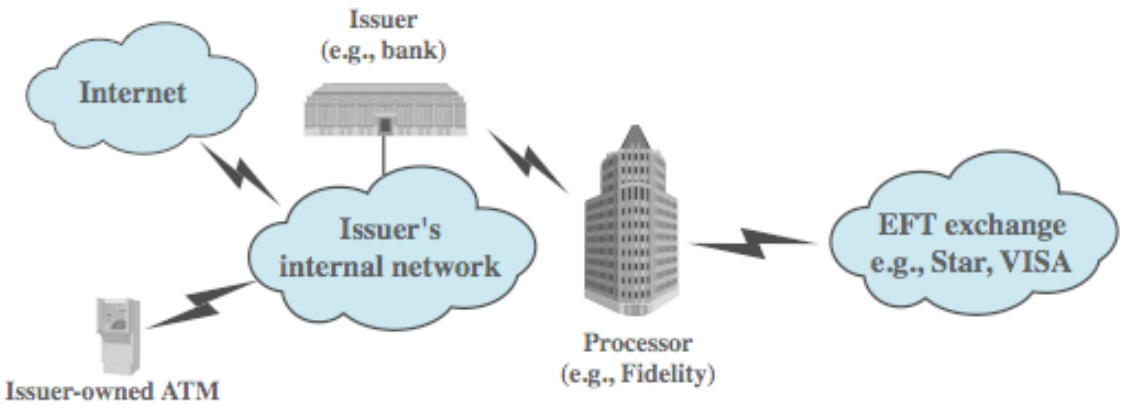


Figure 3.11 Multichannel System Architecture Used to Link Public- and Personal-use Iris Identification Devices via the Internet. The system uses each customer's PIN (personal identification number), iris code, and CIN (customer identification number) to validate transactions. [NEGI00]

Case Study: ATM Security



(a) Point-to-point connection to processor



Summary

- introduced user authentication
  - using passwords
  - using tokens
  - using biometrics
- remote user authentication issues
- example application and case study

Summary

- four means of authenticating a user's identity
  - something the individual knows
  - something the individual possesses
  - something the individual is
  - something the individual does
- vulnerability of passwords
  - offline dictionary attack
  - specific account attack
  - popular password attack
  - password guessing against single user
  - workstation hijacking
  - exploiting user mistakes
  - exploiting multiple password use
  - electronic monitoring
- hashed password and salt value
- password file access control
- password selection strategies
  - user education
  - computer generated passwords
  - reactive password checking
  - proactive password checking
- Bloom filter
- token based authentication
  - memory cards
  - smart cards
- biometric authentication
- remote user authentication
  - password protocol
  - token protocol
  - static biometric protocol
  - dynamic biometric protocol