COMPUTER SECURITY

PRINCIPLES AND PRACTICE

SECOND EDITION

William Stallings | Lawrie Brown

Chapter 3

User Authentication

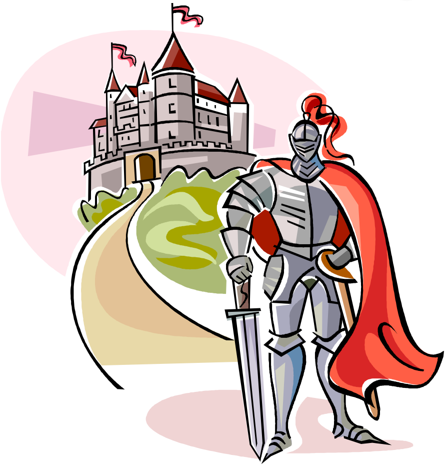
RFC 2828

RFC 2828 defines user authentication as:

"The process of verifying an identity claimed by or for a system entity."

Authentication Process

- **fundamental building block and primary line of defense**
- **basis for access control and user accountability**



- **identification** step
  - presenting an identifier to the security system
- **verification step**
  - presenting or generating authentication information that corroborates the binding between the entity and the identifier

User Authentication

the four means of authenticating user identity are based on:

something the individual knows

- password, PIN, answers to prearranged questions

something the individual possesses (token)

- smartcard, electronic keycard, physical key

something the individual is (static biometrics)

- fingerprint, retina, face

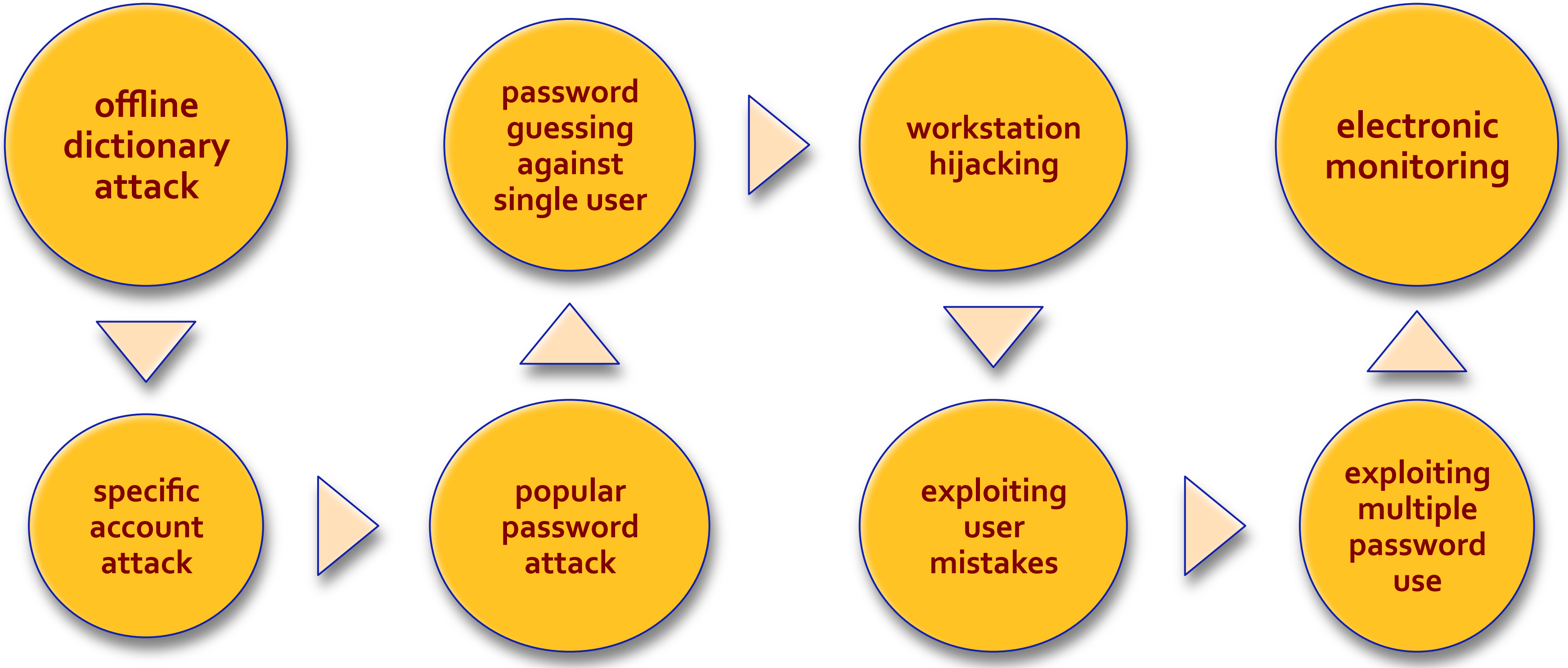
something the individual does (dynamic biometrics)

- voice pattern, handwriting, typing rhythm

Password Authentication

- widely used line of defense against intruders
  - user provides name/login and password
  - system compares password with the one stored for that specified login
- the user ID:
  - determines that the user is authorized to access the system
  - determines the user’s privileges
  - is used in discretionary access control

Password Vulnerabilities



offline dictionary attack

specific account attack

popular password attack

password guessing against single user

workstation hijacking

exploiting user mistakes

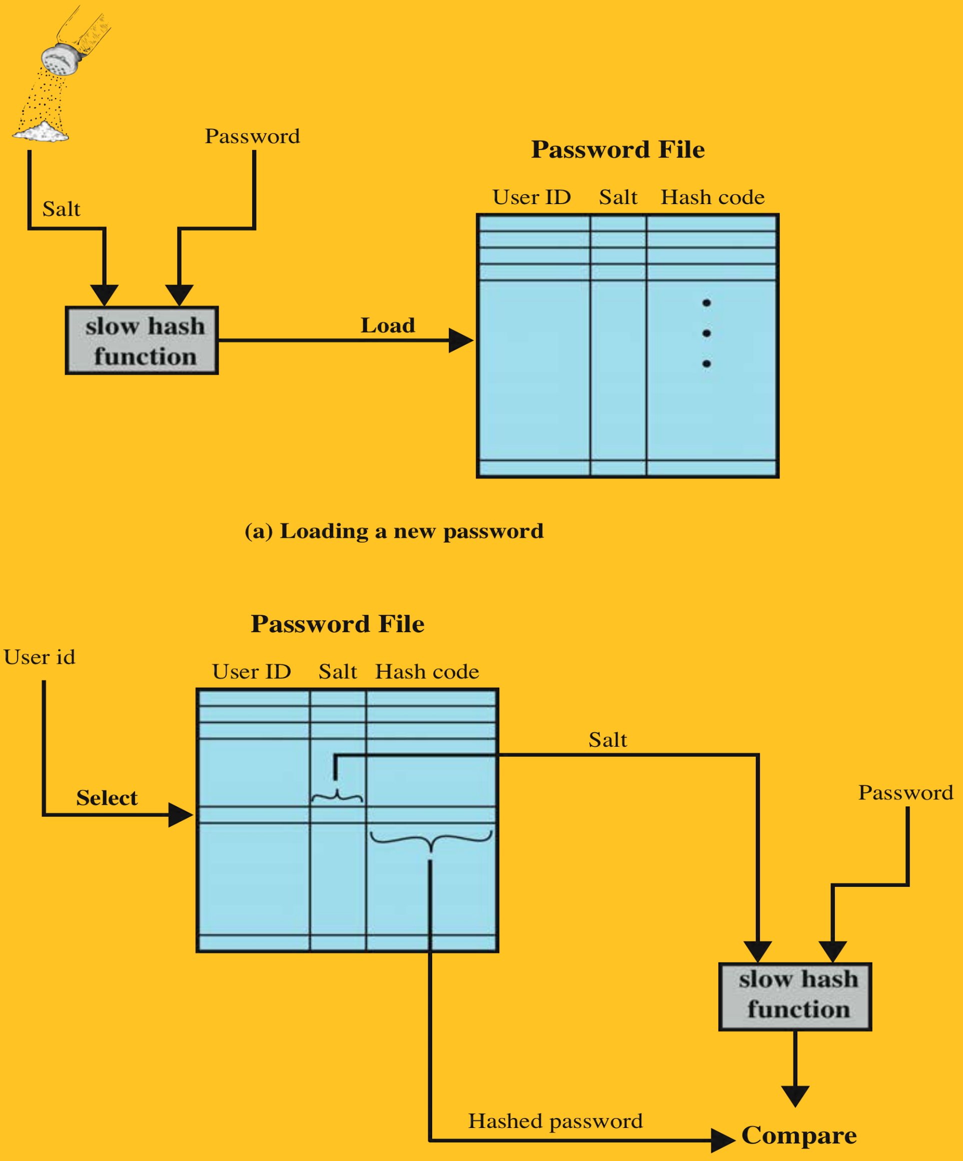
exploiting multiple password use

electronic monitoring

Countermeasures

- controls to prevent unauthorized access to password file
- intrusion detection measures
- rapid reissuance of compromised passwords
- account lockout mechanisms
- policies to inhibit users from selecting common passwords
- training in and enforcement of password policies
- automatic workstation logout
- policies against similar passwords on network devices

Use of Hashed Passwords



(a) Loading a new password

(b) Verifying a password

Figure 3.1 UNIX Password Scheme

UNIX Implementation

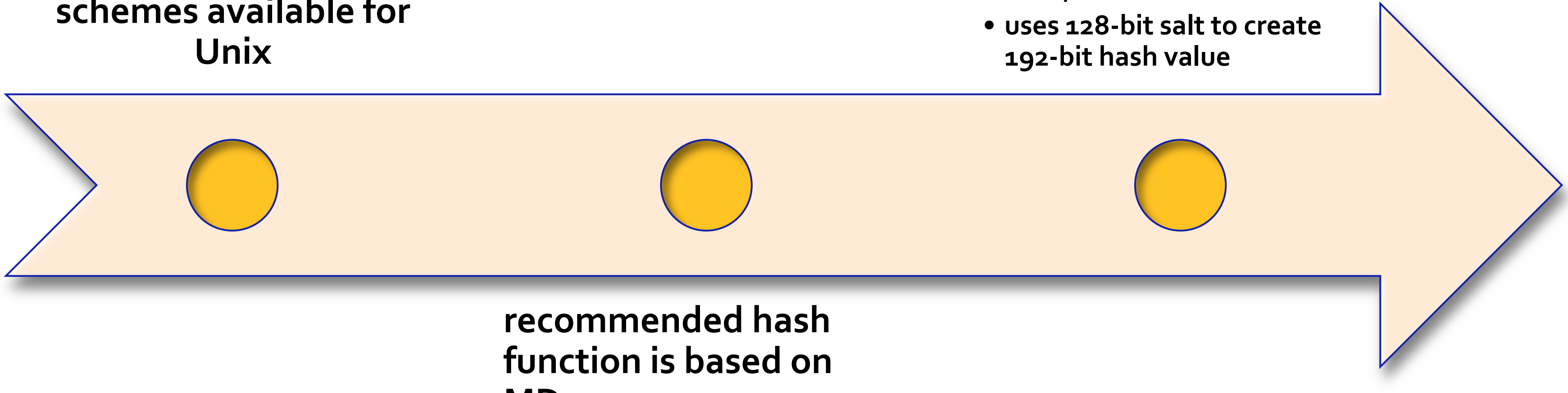
original scheme

- up to eight printable characters in length
- 12-bit salt used to modify DES encryption into a one-way hash function
- zero value repeatedly encrypted 25 times
- output translated to 11 character sequence

now regarded as inadequate

- still often required for compatibility with existing account management software or multivendor environments

Improved Implementations



much stronger hash/salt schemes available for Unix

recommended hash function is based on MD5

- salt of up to 48-bits
- password length is unlimited
- produces 128-bit hash
- uses an inner loop with 1000 iterations to achieve slowdown

OpenBSD uses Blowfish block cipher based hash algorithm called Bcrypt

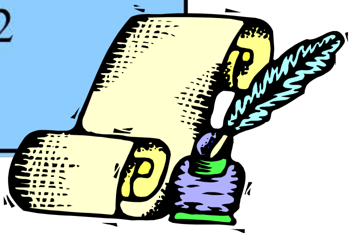
- most secure version of Unix hash/salt scheme
- uses 128-bit salt to create 192-bit hash value

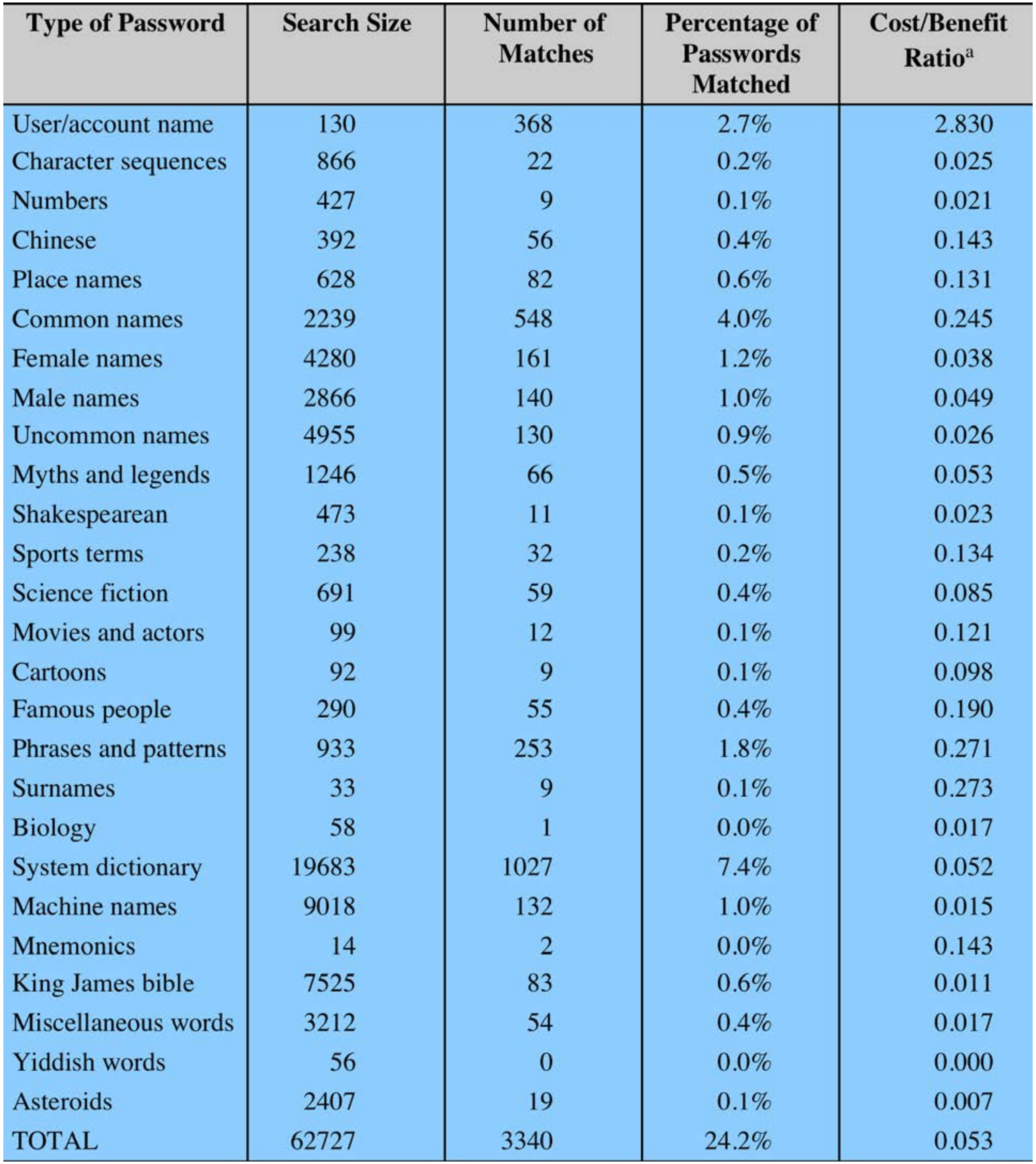
Password Cracking

- dictionary attacks
  - develop a large dictionary of possible passwords and try each against the password file
  - each password must be hashed using each salt value and then compared to stored hash values
- rainbow table attacks
  - pre-compute tables of hash values for all salts
  - a mammoth table of hash values
  - can be countered by using a sufficiently large salt value and a sufficiently large hash length

Table 3.1
Observed Password Lengths

Length	Number	Fraction of Total
1	55	.004
2	87	.006
3	212	.02
4	449	.03
5	1260	.09
6	3035	.22
7	2917	.21
8	5772	.42
Total	13787	1.0





Type of Password	Search Size	Number of Matches	Percentage of Passwords Matched	Cost/Benefit Ratio[a]
User/account name	130	368	2.7%	2.830
Character sequences	866	22	0.2%	0.025
Numbers	427	9	0.1%	0.021
Chinese	392	56	0.4%	0.143
Place names	628	82	0.6%	0.131
Common names	2239	548	4.0%	0.245
Female names	4280	161	1.2%	0.038
Male names	2866	140	1.0%	0.049
Uncommon names	4955	130	0.9%	0.026
Myths and legends	1246	66	0.5%	0.053
Shakespearean	473	11	0.1%	0.023
Sports terms	238	32	0.2%	0.134
Science fiction	691	59	0.4%	0.085
Movies and actors	99	12	0.1%	0.121
Cartoons	92	9	0.1%	0.098
Famous people	290	55	0.4%	0.190
Phrases and patterns	933	253	1.8%	0.271
Surnames	33	9	0.1%	0.273
Biology	58	1	0.0%	0.017
System dictionary	19683	1027	7.4%	0.052
Machine names	9018	132	1.0%	0.015
Mnemonics	14	2	0.0%	0.143
King James bible	7525	83	0.6%	0.011
Miscellaneous words	3212	54	0.4%	0.017
Yiddish words	56	0	0.0%	0.000
Asteroids	2407	19	0.1%	0.007
TOTAL	62727	3340	24.2%	0.053

Table 3.2

Passwords Cracked from a Sample Set of 13,797 Accounts

*Computed as the number of matches divided by the search size. The more words that need to be tested for a match, the lower the cost/benefit ratio.

Password File Access Control

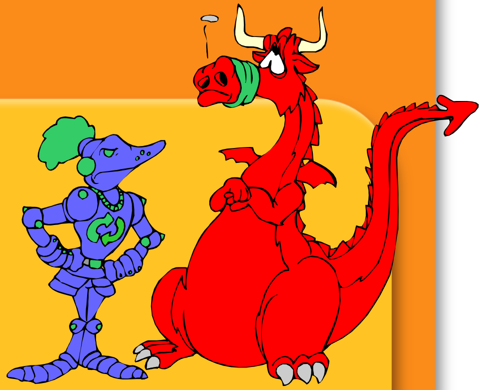
can block offline guessing attacks by denying access to encrypted passwords

make available only to privileged users

shadow password file

- a separate file from the user IDs where the hashed passwords are kept

vulnerabilities



weakness in the OS that allows access to the file

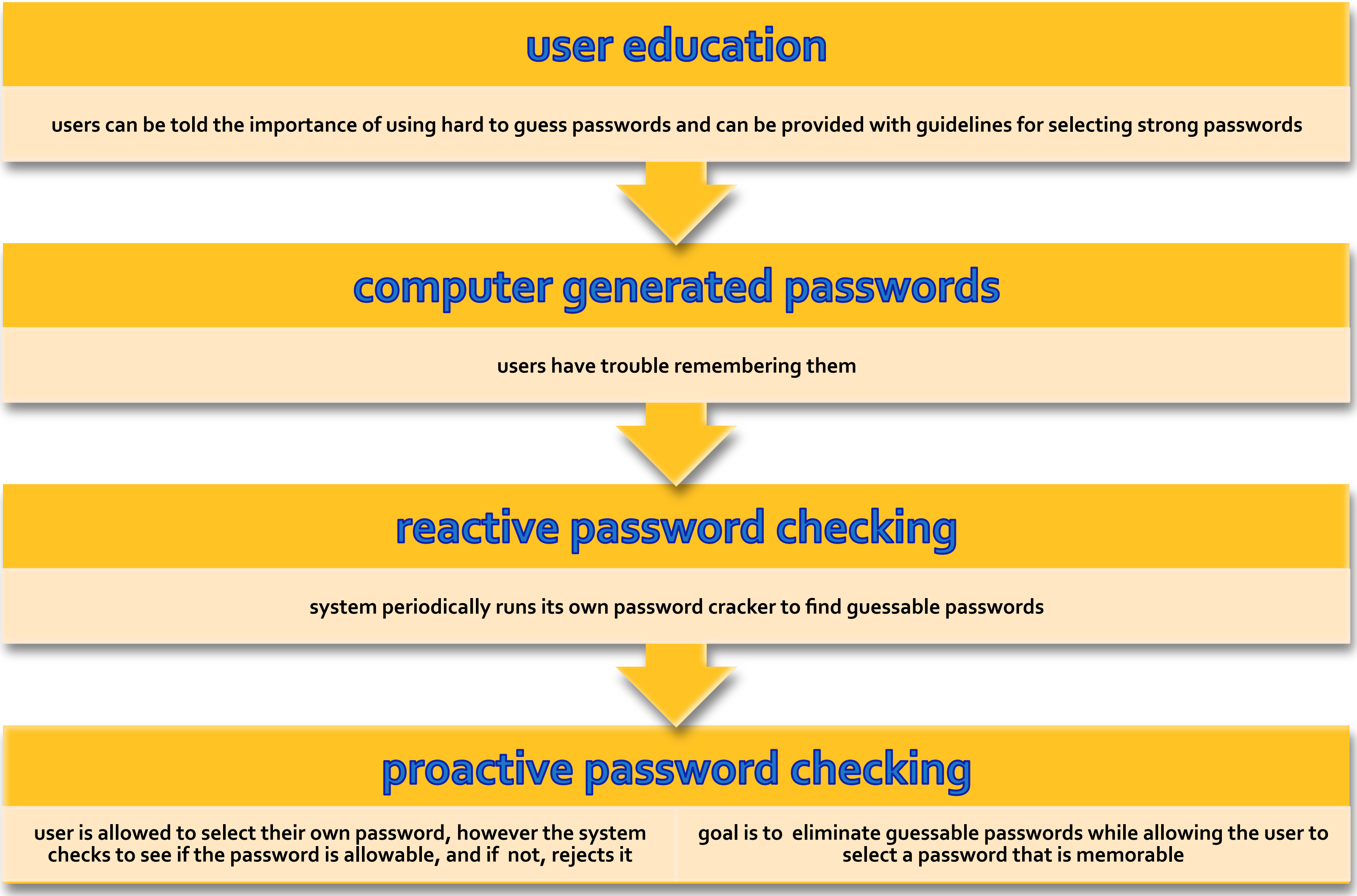
accident with permissions making it readable

users with same password on other systems

access from backup media

sniff passwords in network traffic

Password Selection Techniques



user education

users can be told the importance of using hard to guess passwords and can be provided with guidelines for selecting strong passwords

computer generated passwords

users have trouble remembering them

reactive password checking

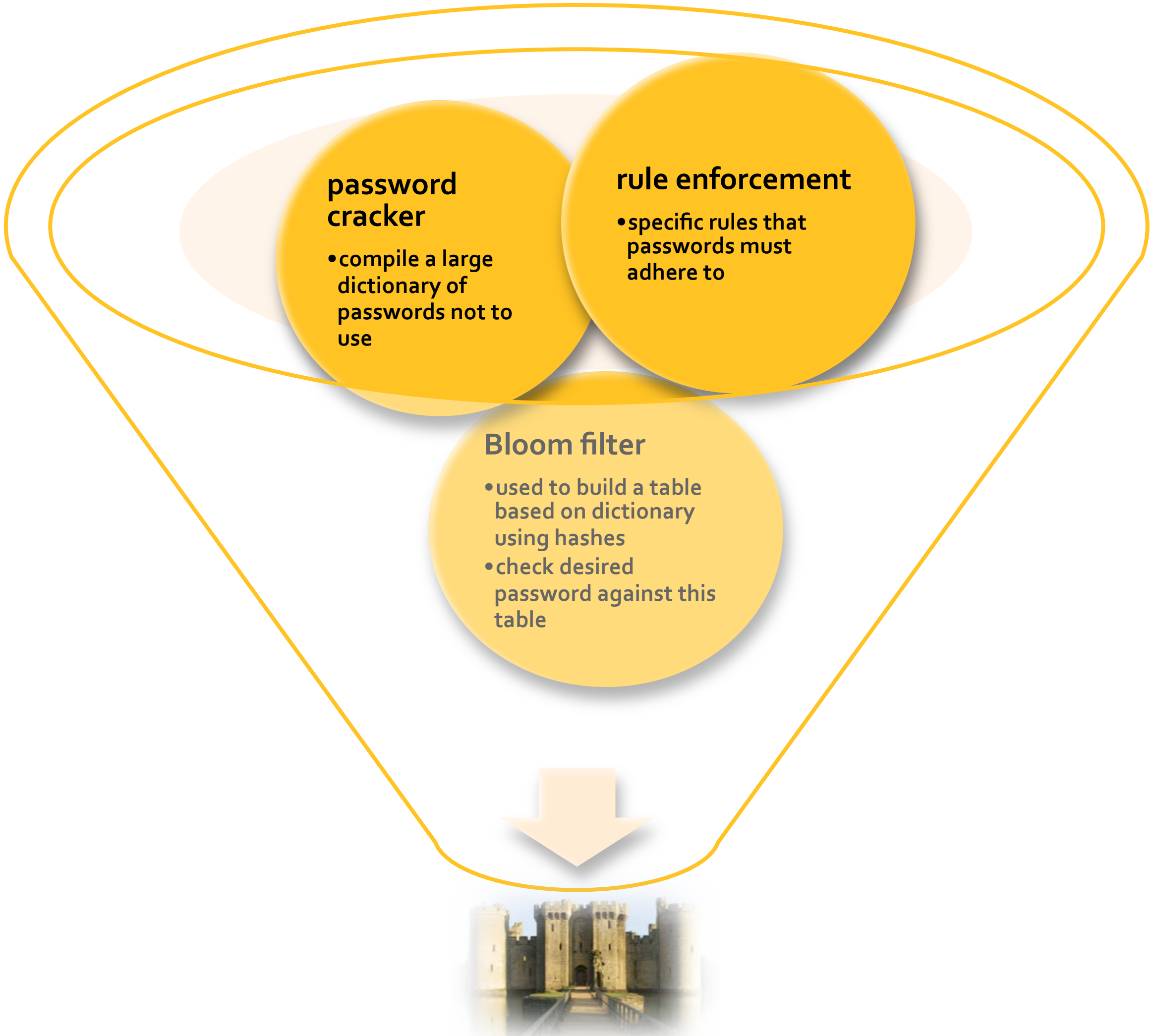
system periodically runs its own password cracker to find guessable passwords

proactive password checking

user is allowed to select their own password, however the system checks to see if the password is allowable, and if not, rejects it

goal is to eliminate guessable passwords while allowing the user to select a password that is memorable

Proactive Password Checking



password cracker

- compile a large dictionary of passwords not to use

rule enforcement

- specific rules that passwords must adhere to

Bloom filter

- used to build a table based on dictionary using hashes
- check desired password against this table

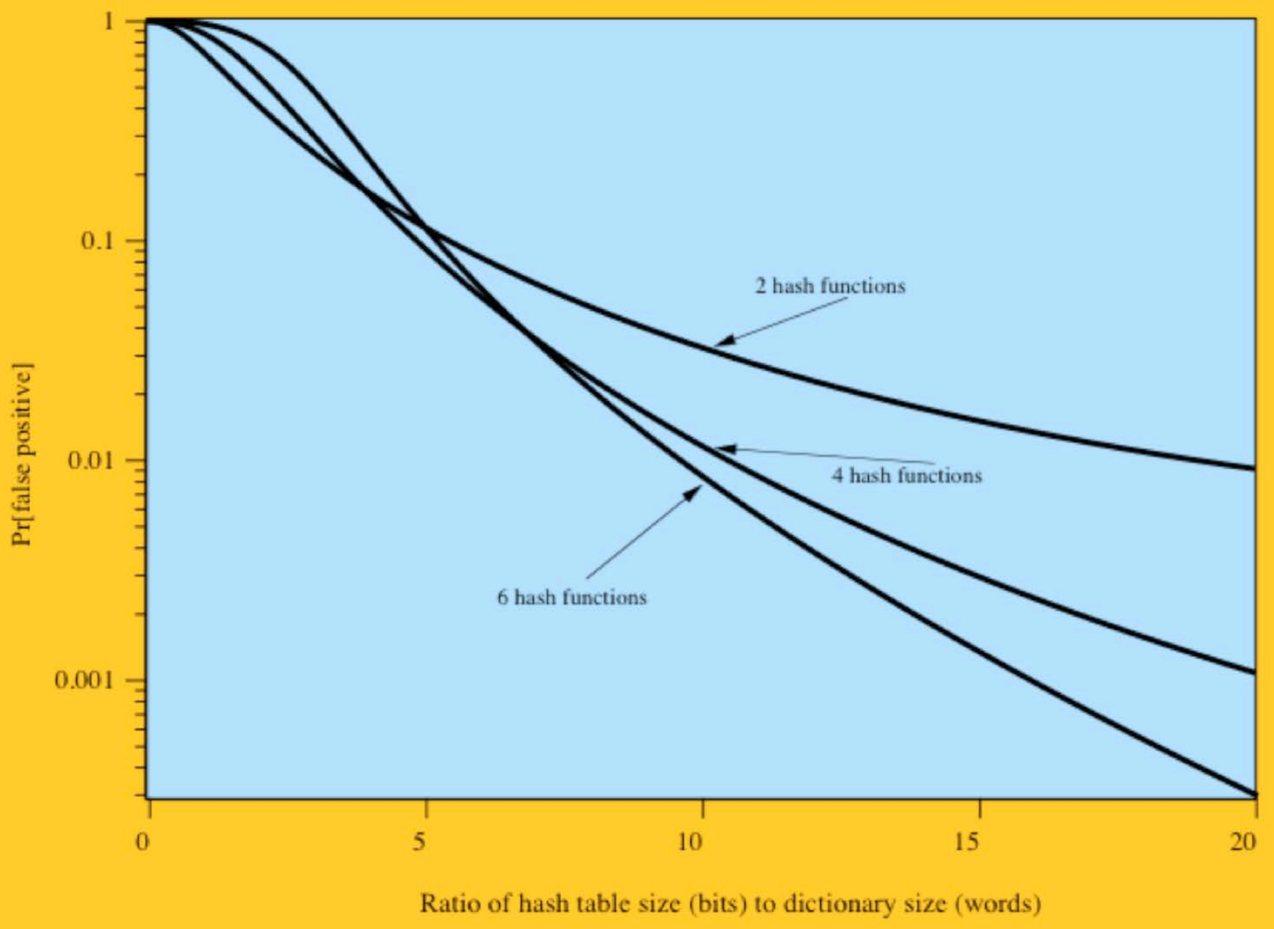


Figure 3.2 Performance of Bloom Filter

Table 3.3
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	

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

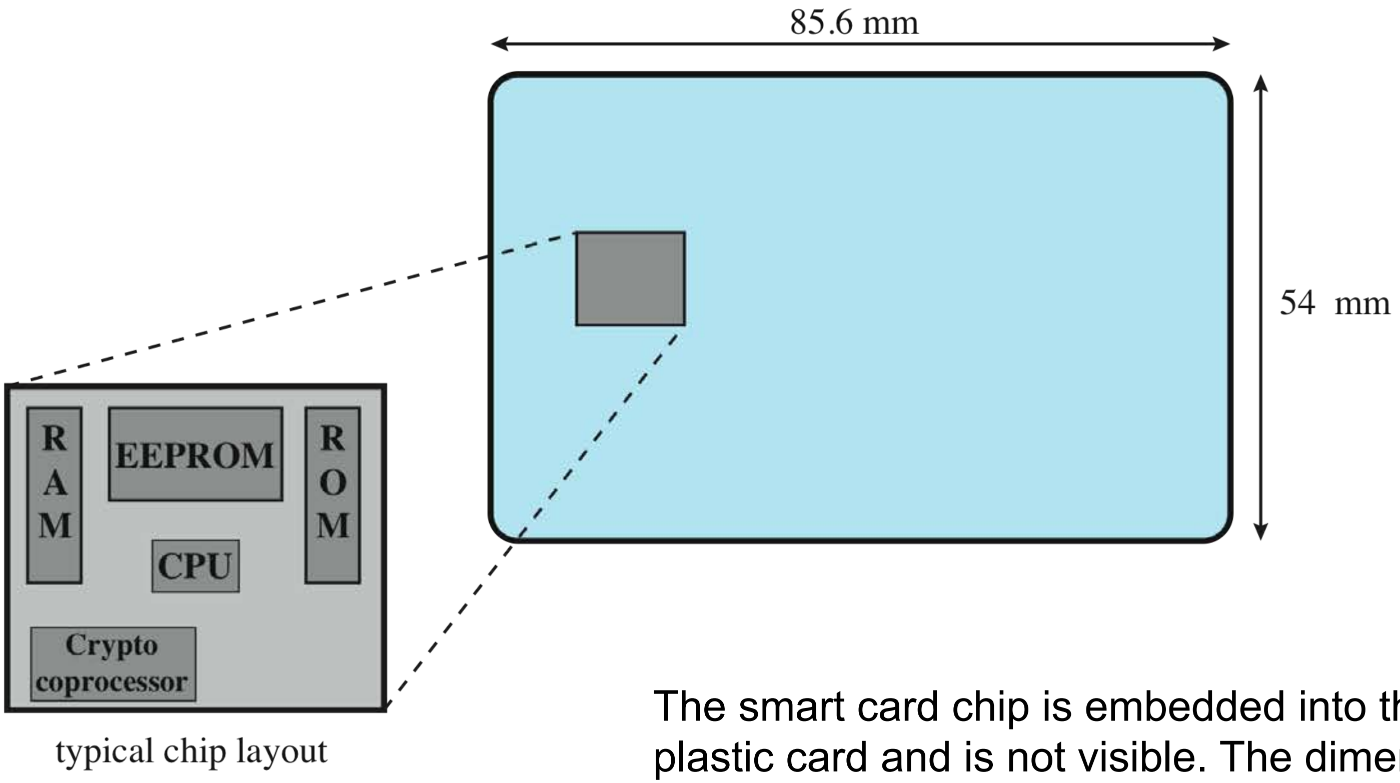
- provides significantly greater security when combined with a password or PIN
- drawbacks of memory cards include:
  - requires a special reader
  - loss of token
  - user dissatisfaction

Smartcard

- physical characteristics:
  - include an embedded microprocessor
  - a smart token that looks like a bank card
  - can look like calculators, keys, small portable objects

- interface:
  - manual interfaces include a keypad and display for interaction
  - electronic interfaces communicate with a compatible reader/ writer
- authentication protocol:
  - classified into three categories: static, dynamic password generator and challenge-response

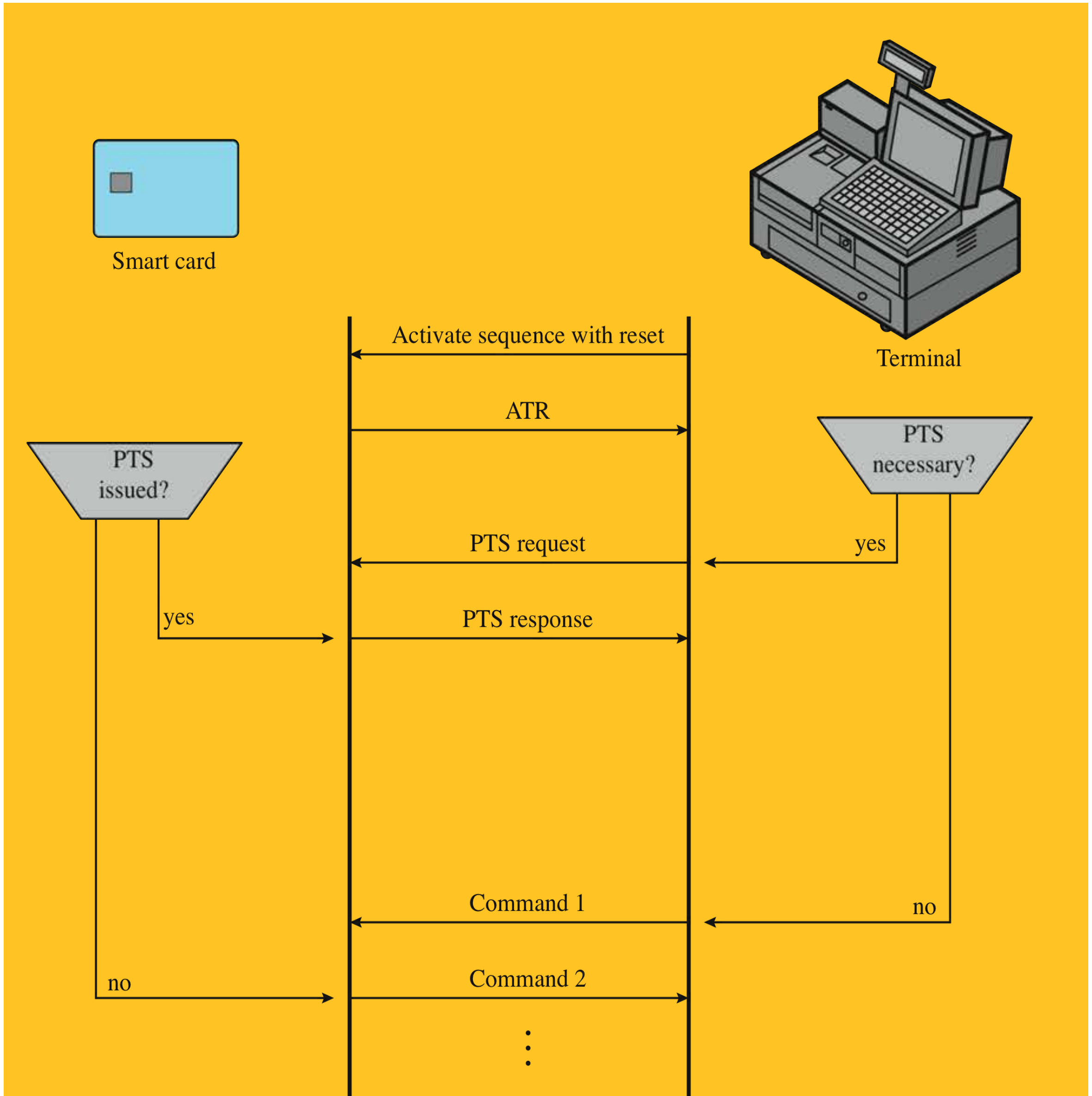
Figure 3.3
Smart Card Dimensions



The smart card chip is embedded into the plastic card and is not visible. The dimensions conform to ISO standard 7816-2.

Figure 3.4

Communication Initialization between a Smart Card and a Reader

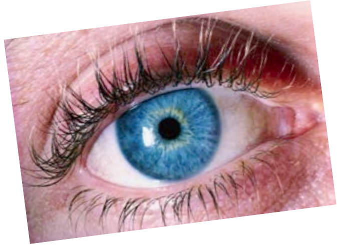


ATR = Answer to reset
PTS = Protocol type selection

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



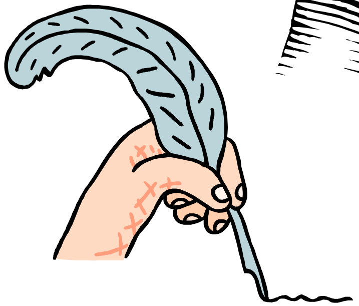


Figure 3.5
Cost Versus Accuracy

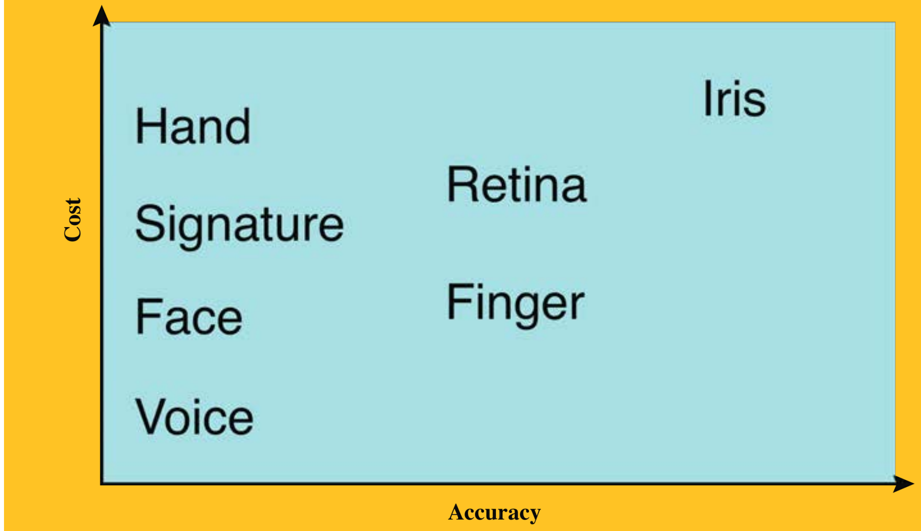


Figure 3.5 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.

Figure 3.6

Operation of a Biometric System

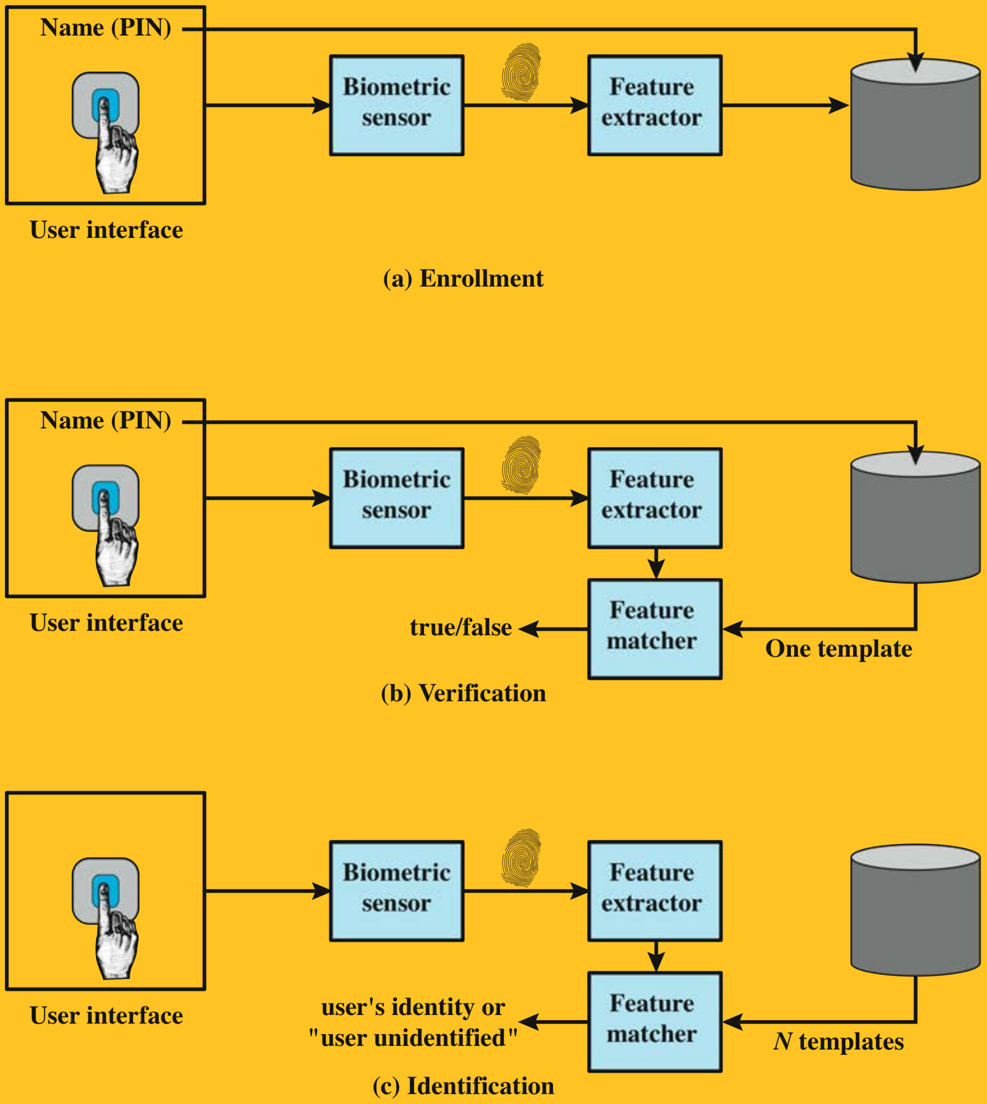


Figure 3.6 A Generic Biometric System Enrollment creates an association between a user and the user’s biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user.

Biometric Accuracy

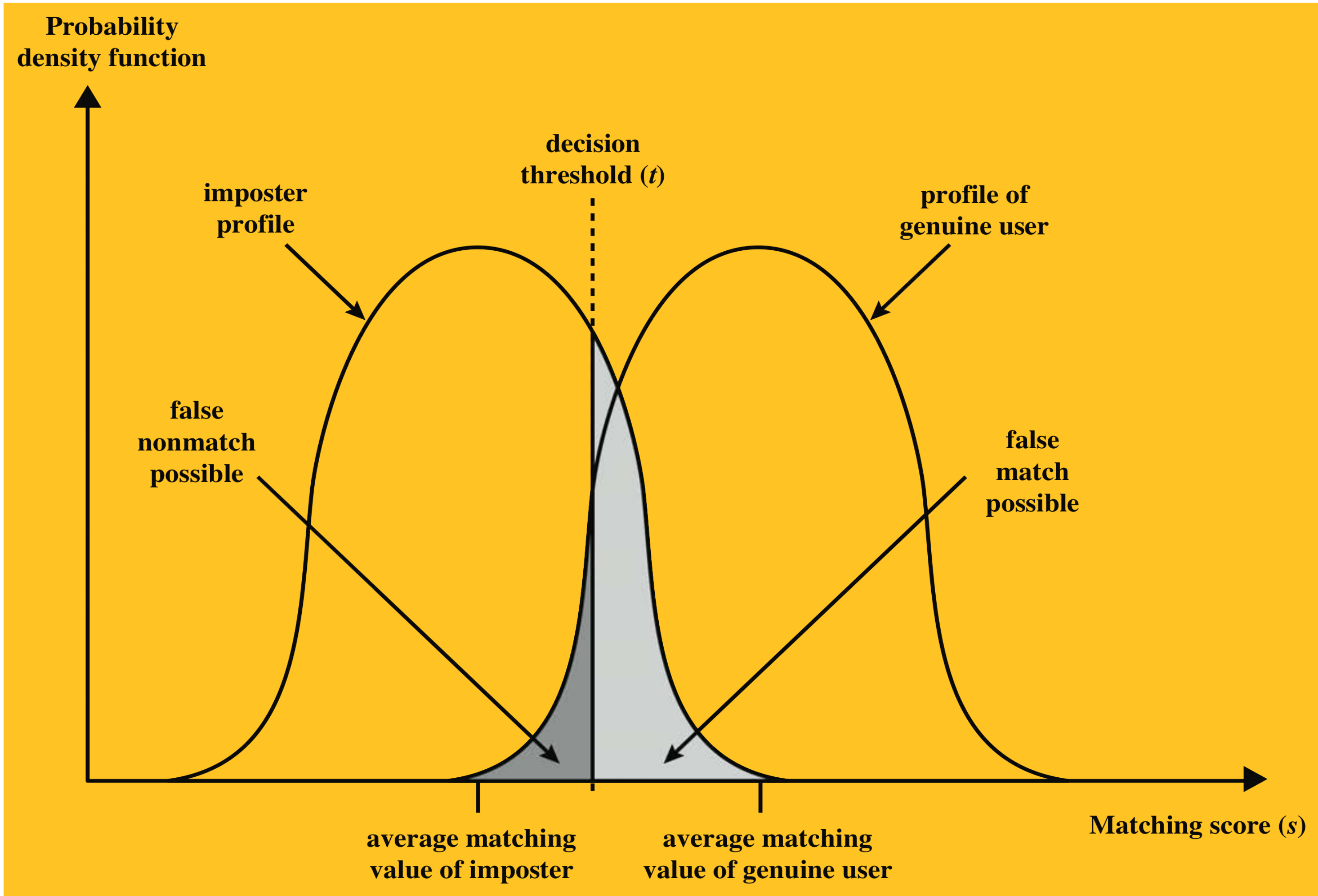


Figure 3.7 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (s) is greater than a preassigned threshold (t), a match is declared.

Biometric Measurement Operating Characteristic Curves

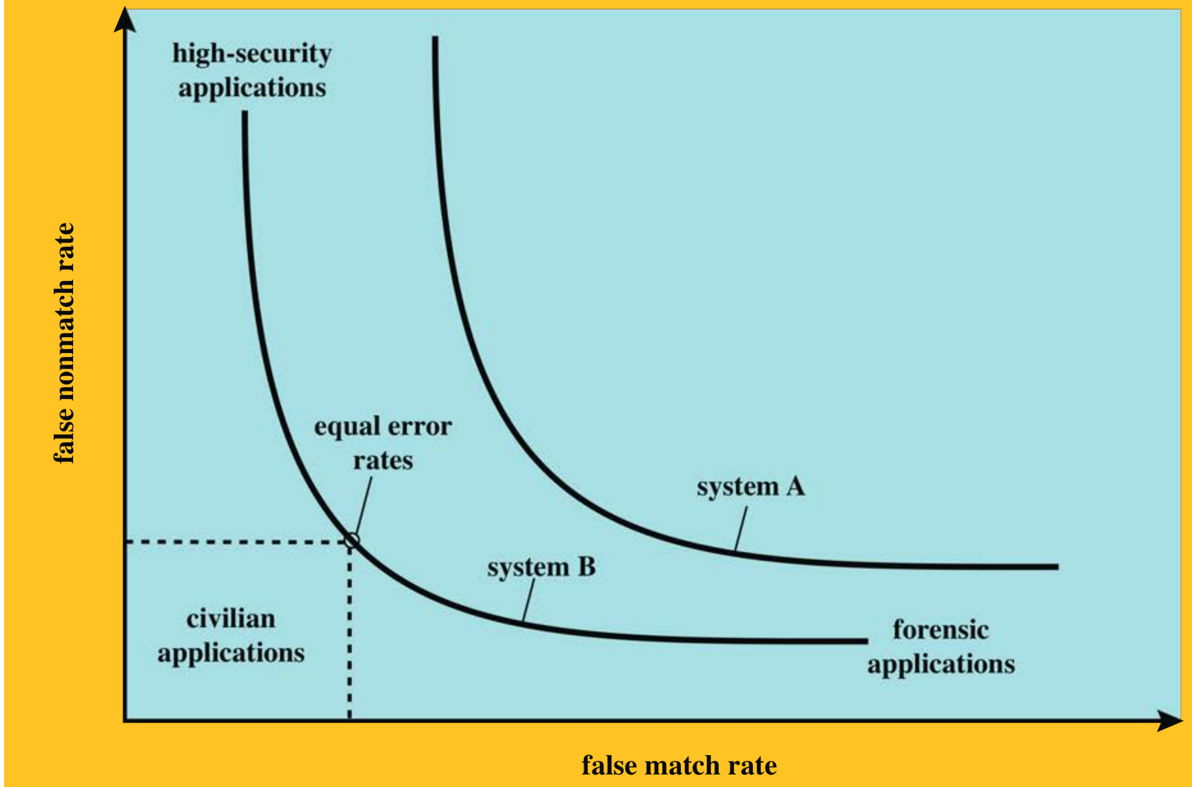


Figure 3.8 Idealized Biometric Measurement Operating Characteristic Curves. Different biometric application types make different trade-offs between the false match rate and the false nonmatch rate. Note that system A is consistently inferior to system B in accuracy performance. [JAIN00]

Actual Biometric Measurement Operating Characteristic Curves

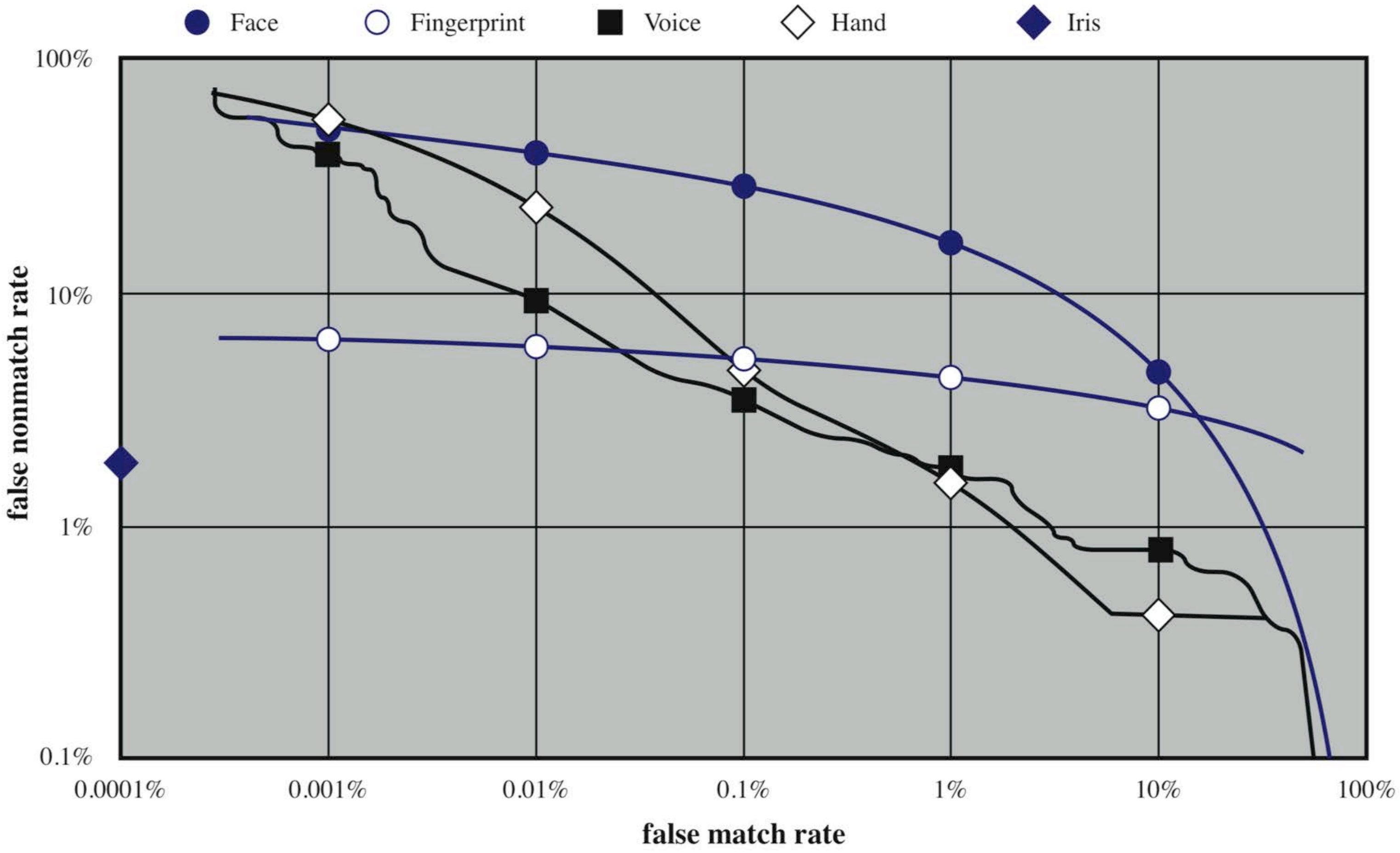
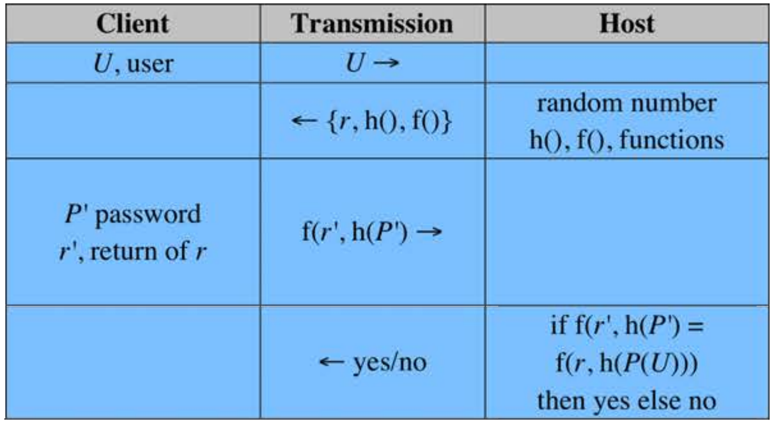


Figure 3.9 Actual Biometric Measurement Operating Characteristic Curves, reported in [MANS01]. To clarify differences among systems, a log-log scale is used.

Remote User Authentication

- authentication over a network, the Internet, or a communications link is more complex
- additional security threats such as:
  - eavesdropping, capturing a password, replaying an authentication sequence that has been observed
- generally rely on some form of a challenge-response protocol to counter threats

Figure 3.10a
Password Protocol



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

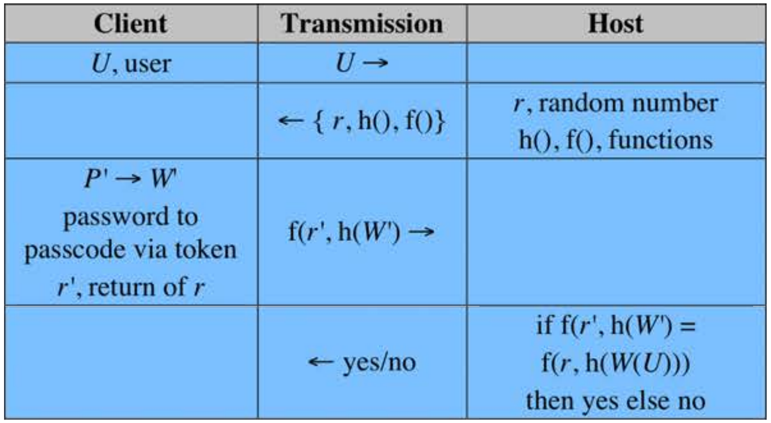
(a) Protocol for a password

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

Figure 3.10b
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

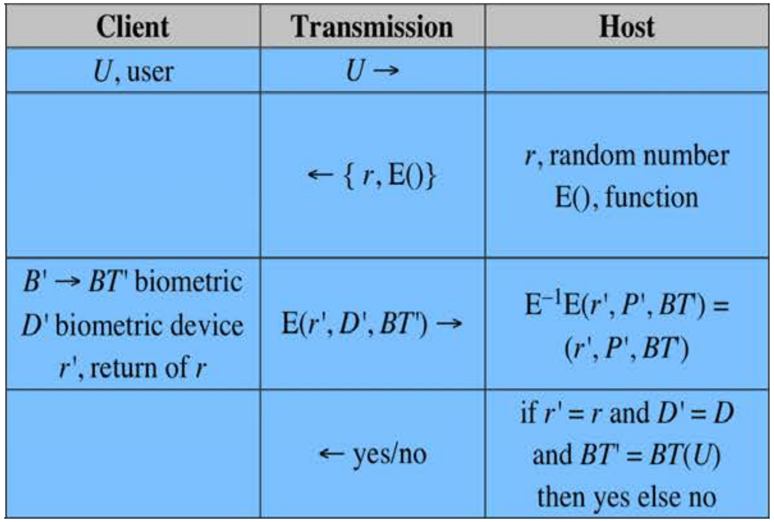


Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{ r, \mathrm{h}(), \mathrm{f}() \}$	r, random number h(), f(), functions
$P' \rightarrow W'$ password to passcode via token r', return of r	$\mathrm{f}(r', \mathrm{h}(W') \rightarrow$	
	← yes/no	if $\mathrm{f}(r', \mathrm{h}(W') =$ $\mathrm{f}(r,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

(b) Protocol for a token

Example of a token protocol

Figure 3.10c
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

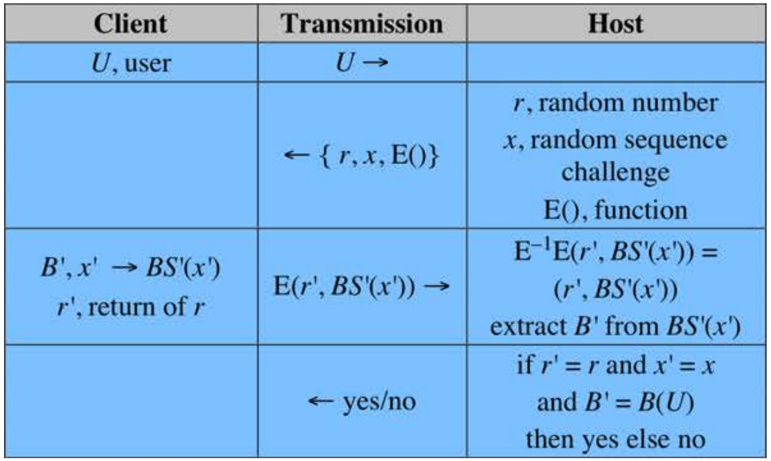
Example of a static biometric protocol

- 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

Figure 3.10d
Dynamic Biometric Protocol

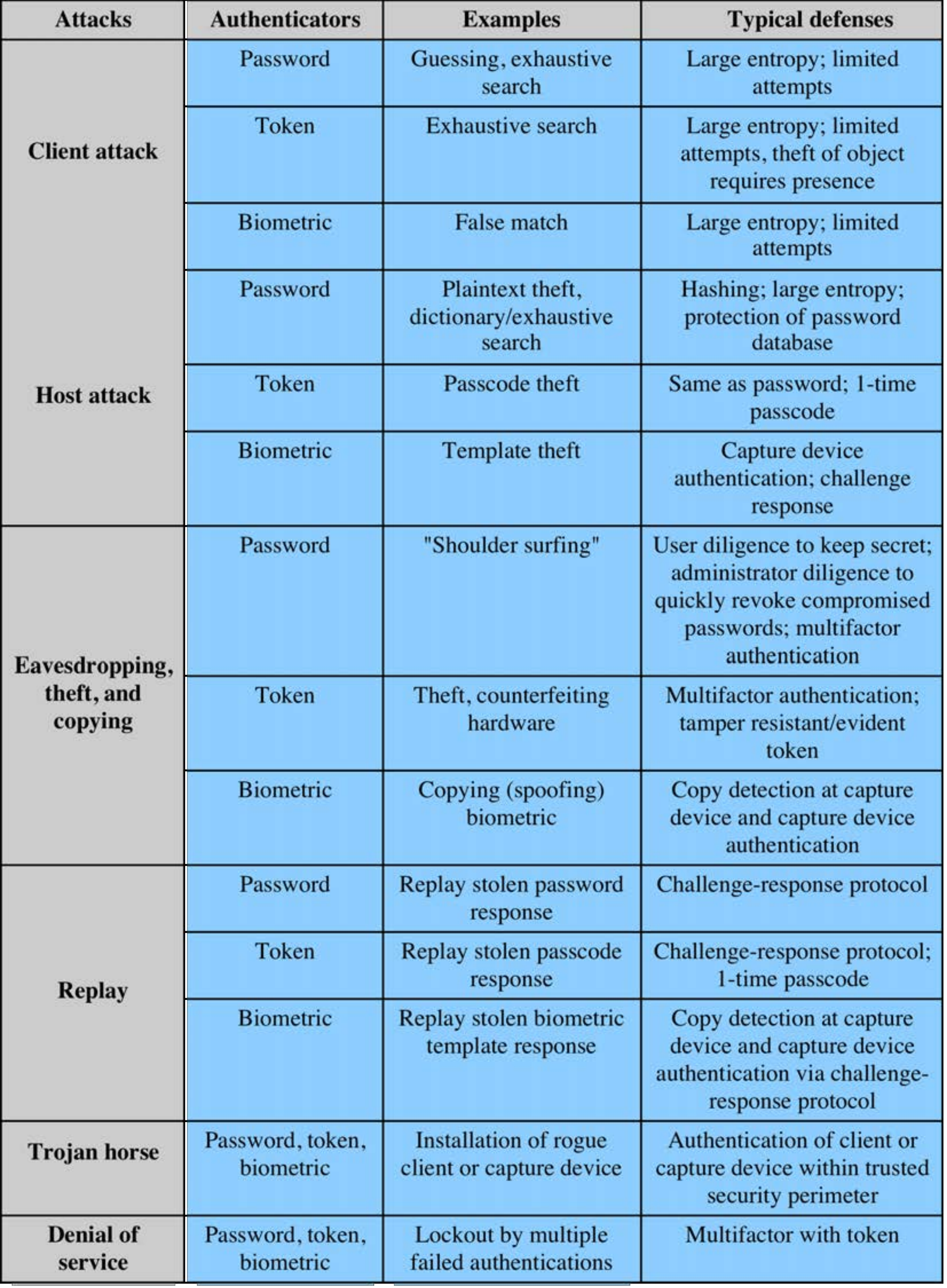
- host provides a random sequence and a random number as a challenge
- sequence challenge is a sequence of numbers, characters, or words
- user at client end must then vocalize, type, or write the sequence to generate a biometric signal
- the client side encrypts the biometric signal and the random number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

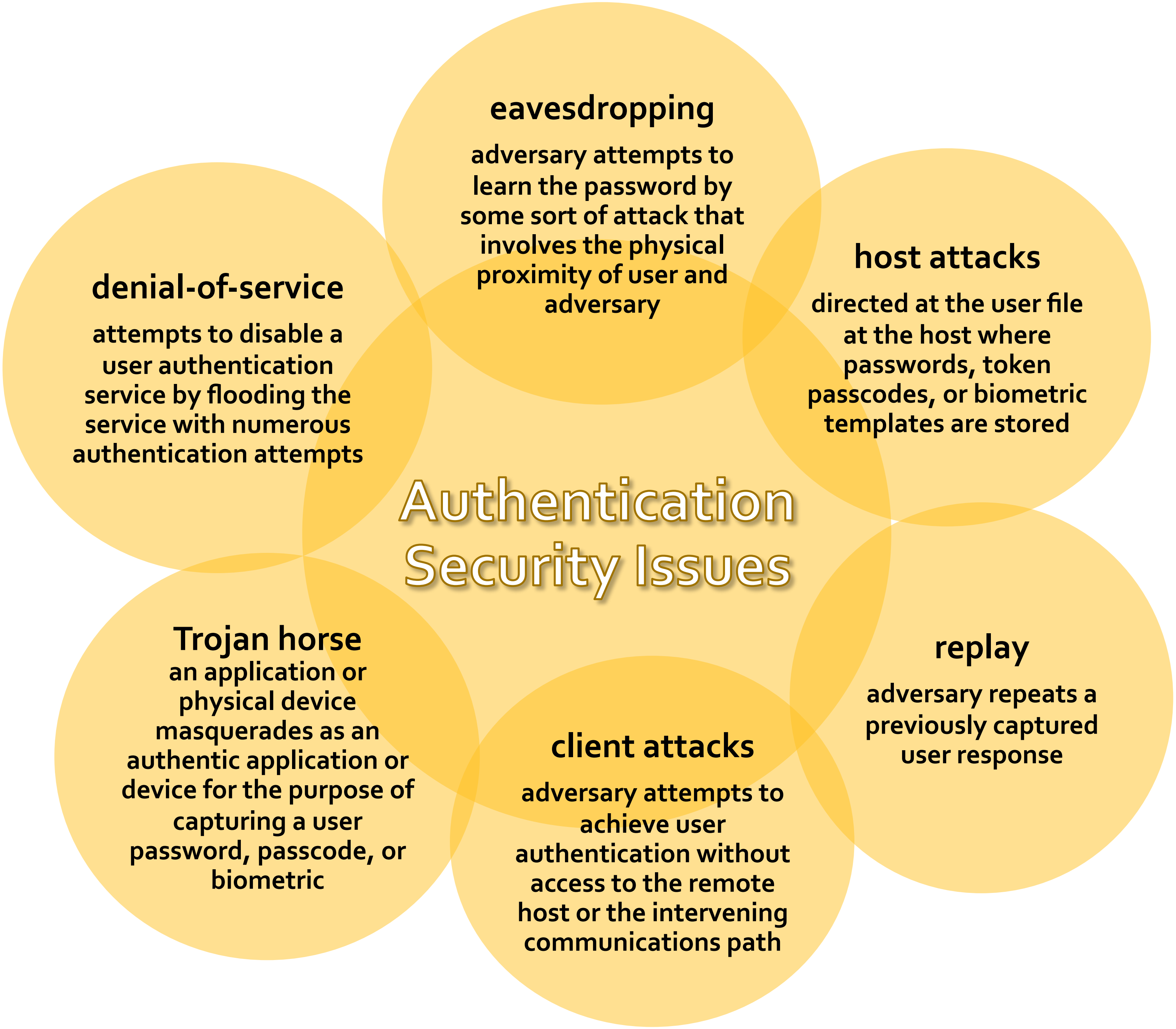
(d) Protocol for dynamic biometric



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

Table 3.4

Potential Attacks, Susceptible Authenticators, and Typical Defenses



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

replay

adversary repeats a previously captured user response

client attacks

adversary attempts to achieve user authentication without access to the remote host or the intervening communications path

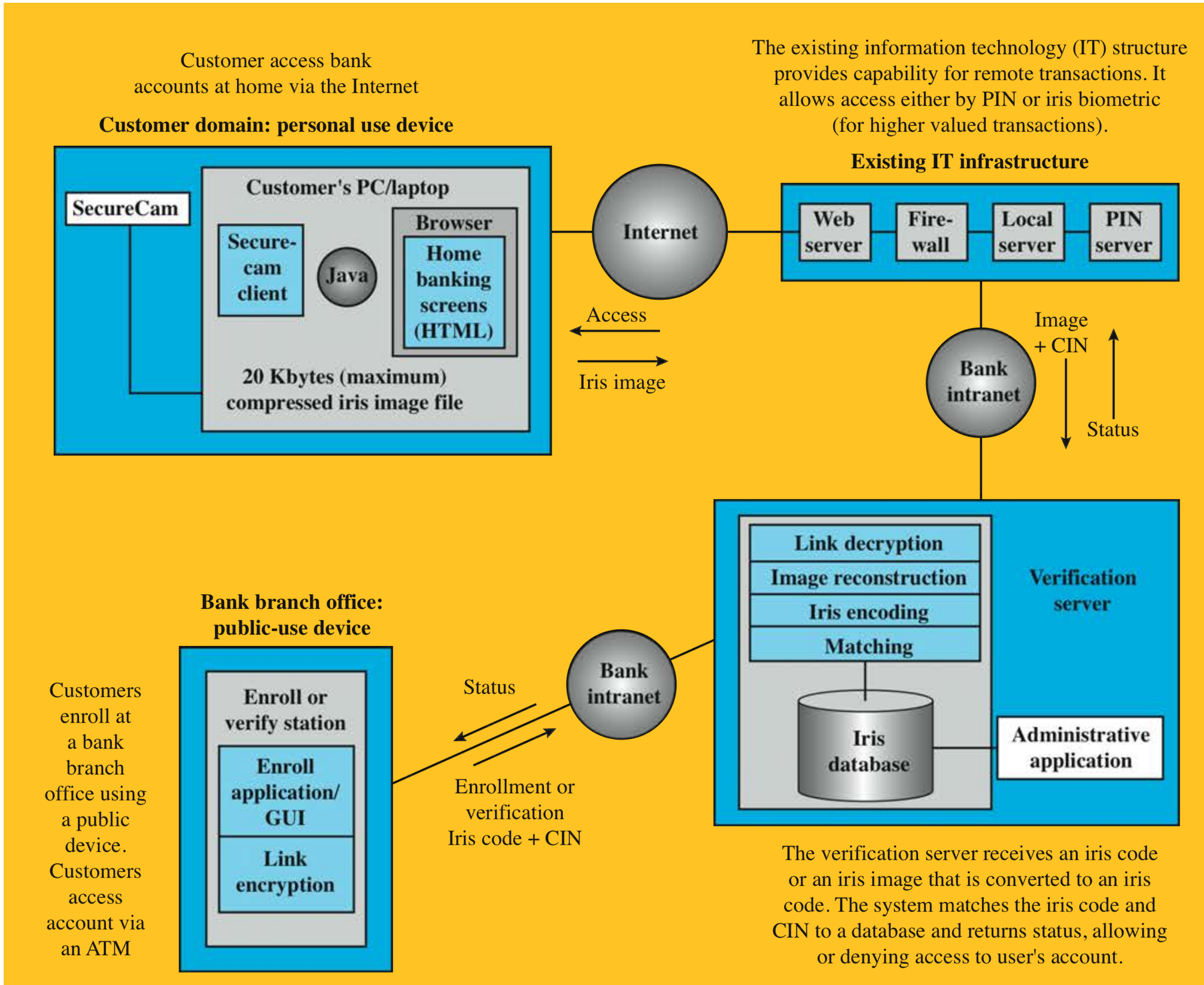
Trojan horse

an application or physical device masquerades as an authentic application or device for the purpose of capturing a user password, passcode, or biometric

denial-of-service

attempts to disable a user authentication service by flooding the service with numerous authentication attempts

Practical Application: Iris Biometric System



Customer access bank accounts at home via the Internet

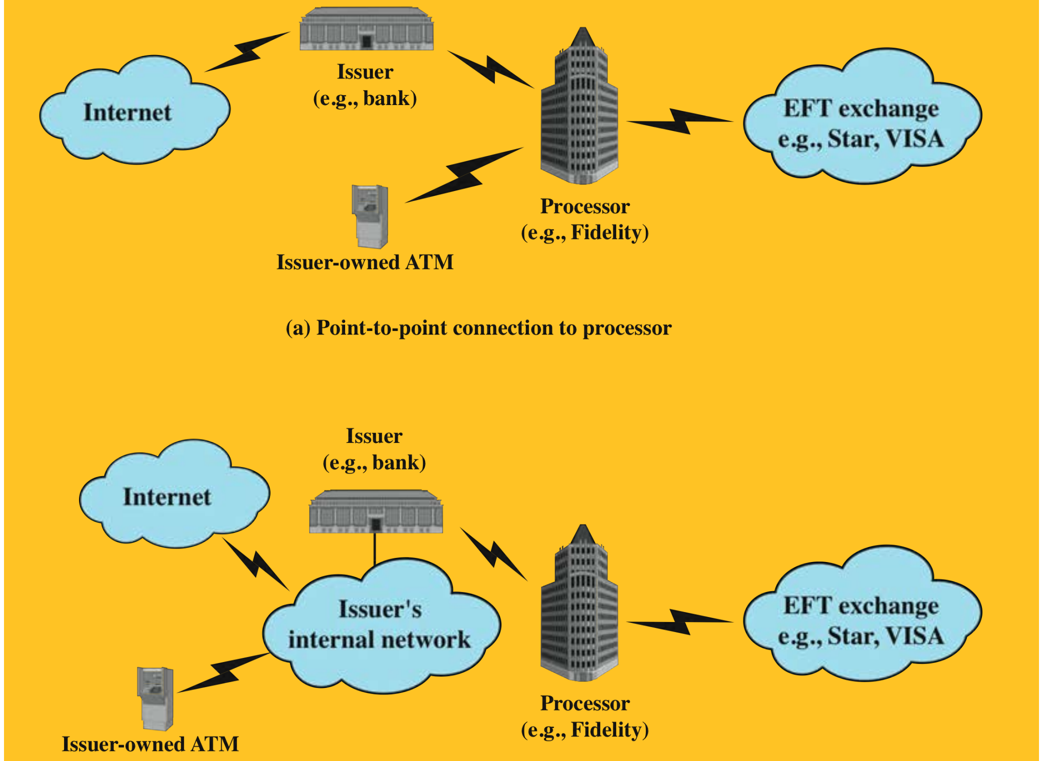
The existing information technology (IT) structure provides capability for remote transactions. It allows access either by PIN or iris biometric (for higher valued transactions).

Customers enroll at a bank branch office using a public device. Customers access account via an ATM

The verification server receives an iris code or an iris image that is converted to an iris code. The system matches the iris code and CIN to a database and returns status, allowing or denying access to user's account.

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 Problems



(a) Point-to-point connection to processor

(b) Shared connection to processor

Figure 3.12 ATM Architectures. Most small to mid-sized issuers of debit cards contract processors to provide core data processing and electronic funds transfer (EFT) services. The bank's ATM machine may link directly to the processor or to the bank.

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