

CS 493

Secure Software Systems

User Authentication



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



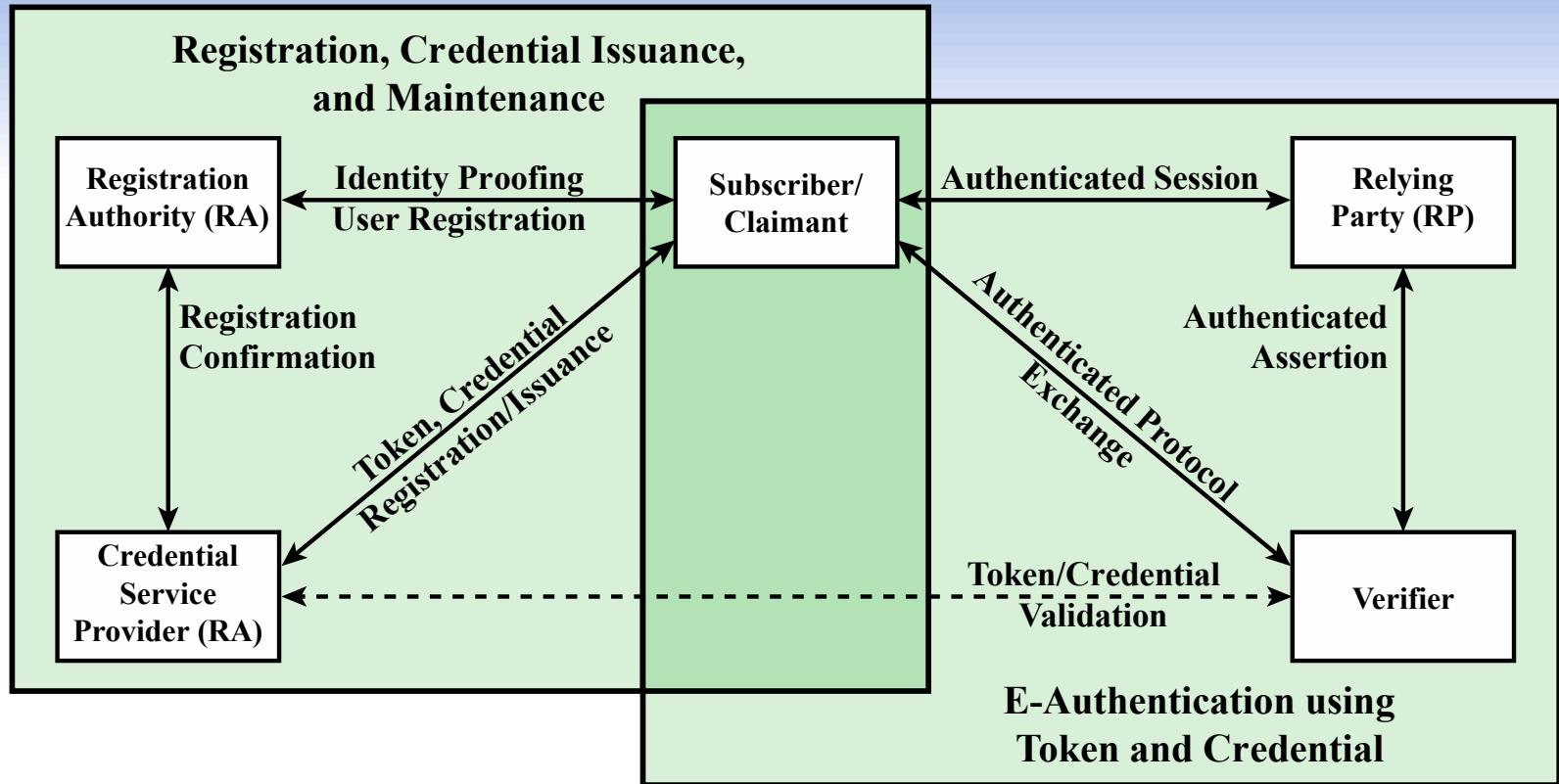


Figure 3.1 The NIST SP 800-63-2 E-Authentication Architectural Model

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)

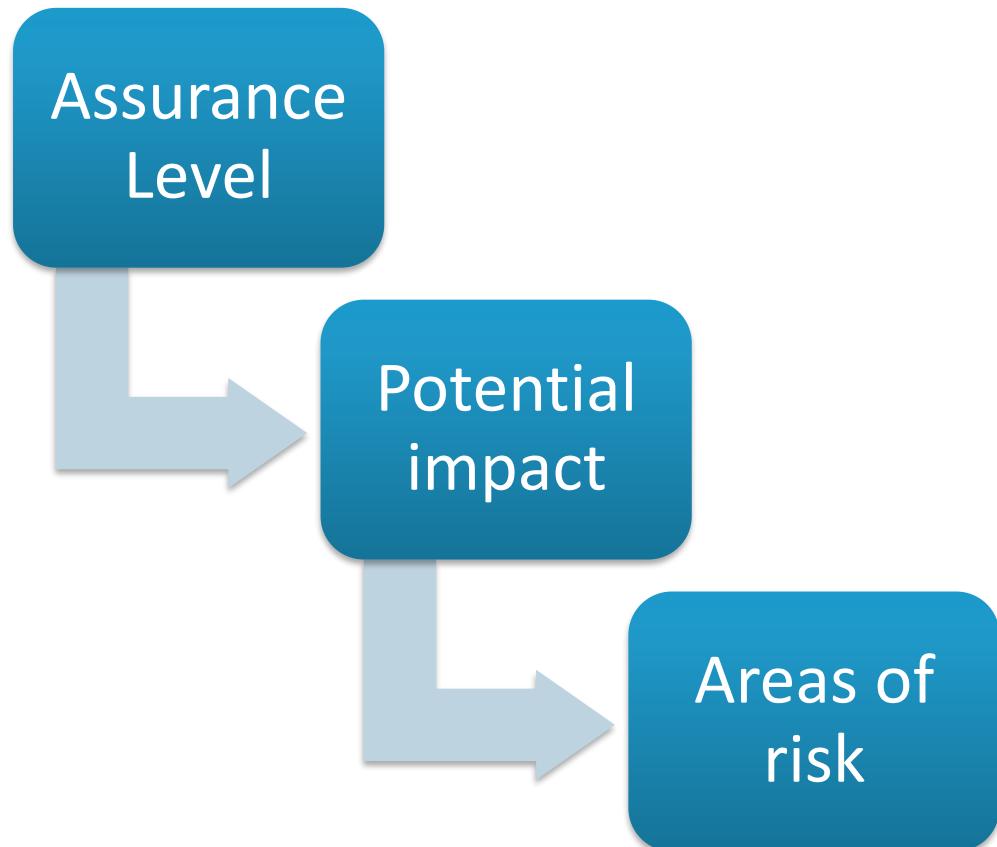
- Fingerprint, retina, face

Something the individual does (dynamic biometrics)

- Voice pattern, handwriting, typing rhythm

Risk Assessment for User Authentication

- There are three separate concepts:



Assurance Level

Describes an organization's degree of certainty that a user has presented a credential that refers to his or her identity

More specifically is defined as:

The degree of confidence in the vetting process used to establish the identity of the individual

The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued

Four levels of assurance

Level 1

- Little or no confidence in the asserted identity's validity

Level 2

- Some confidence in the asserted identity's validity

Level 3

- High confidence in the asserted identity's validity

Level 4

- Very high confidence in the asserted identity's validity

Potential Impact

- FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security:
 - Low
 - An authentication error could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
 - Moderate
 - An authentication error could be expected to have a serious adverse effect
 - High
 - An authentication error could be expected to have a severe or catastrophic adverse effect

Table 3.1

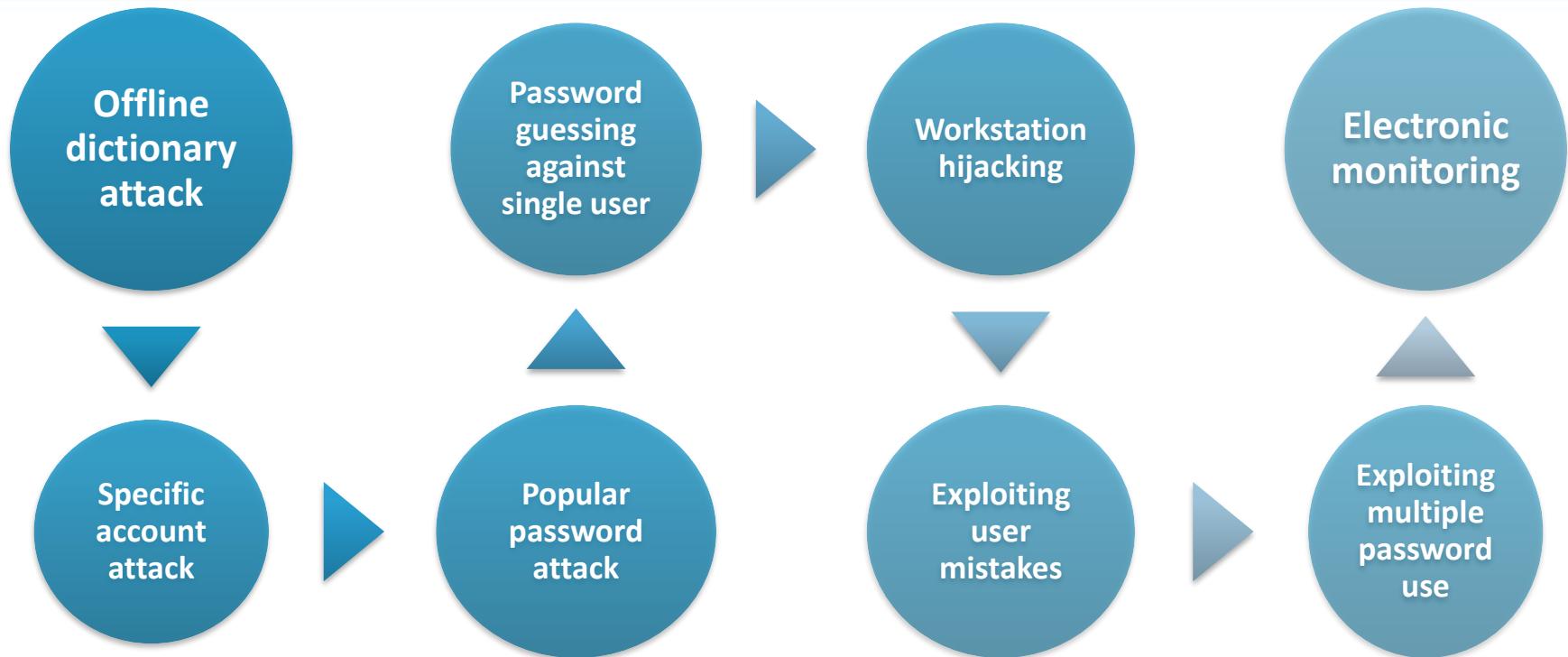
Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
	Low	Mod	Mod	High
Financial loss or organization liability	None	Low	Mod	High
Harm to organization programs or interests	None	Low	Mod	High
Unauthorized release of sensitive information	None	None	Low	Mod/ High
Personal safety				
Civil or criminal violations	None	Low	Mod	High

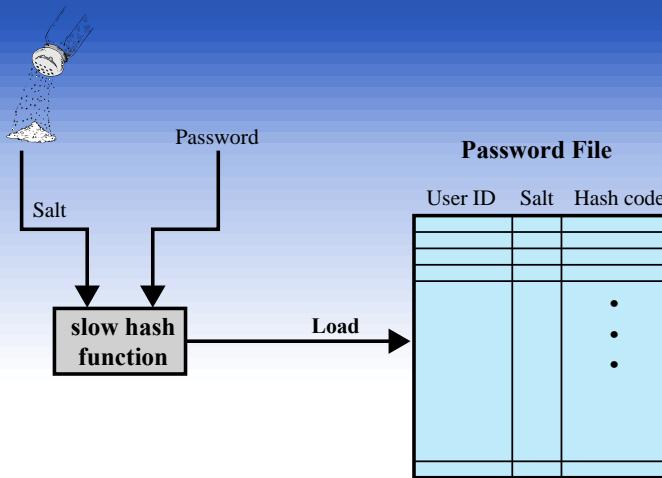
Maximum Potential Impacts for Each Assurance Level

Password Authentication

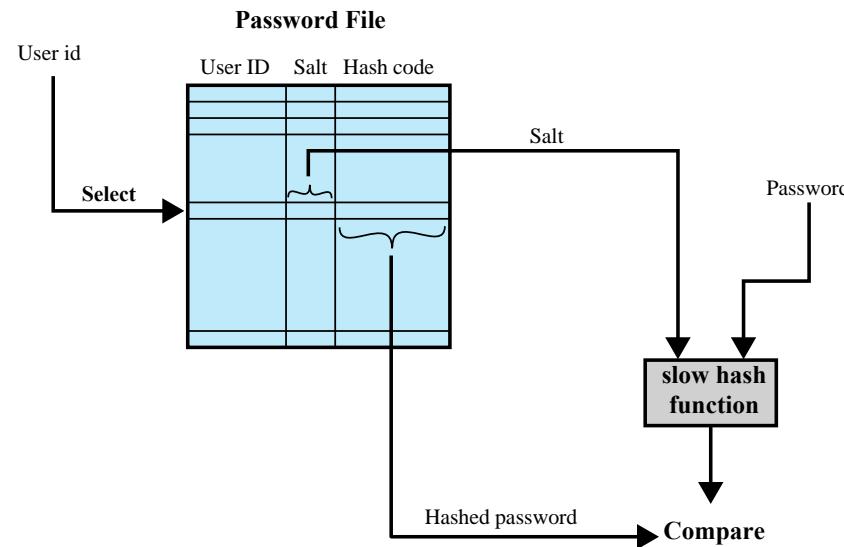
- Widely used line of defense against intruders
 - User provides name/login and password
 - System compares password with the one stored for that specified login
- The user ID:
 - Determines that the user is authorized to access the system
 - Determines the user's privileges
 - Is used in discretionary access control

Password Vulnerabilities





(a) Loading a new password



(b) Verifying a password

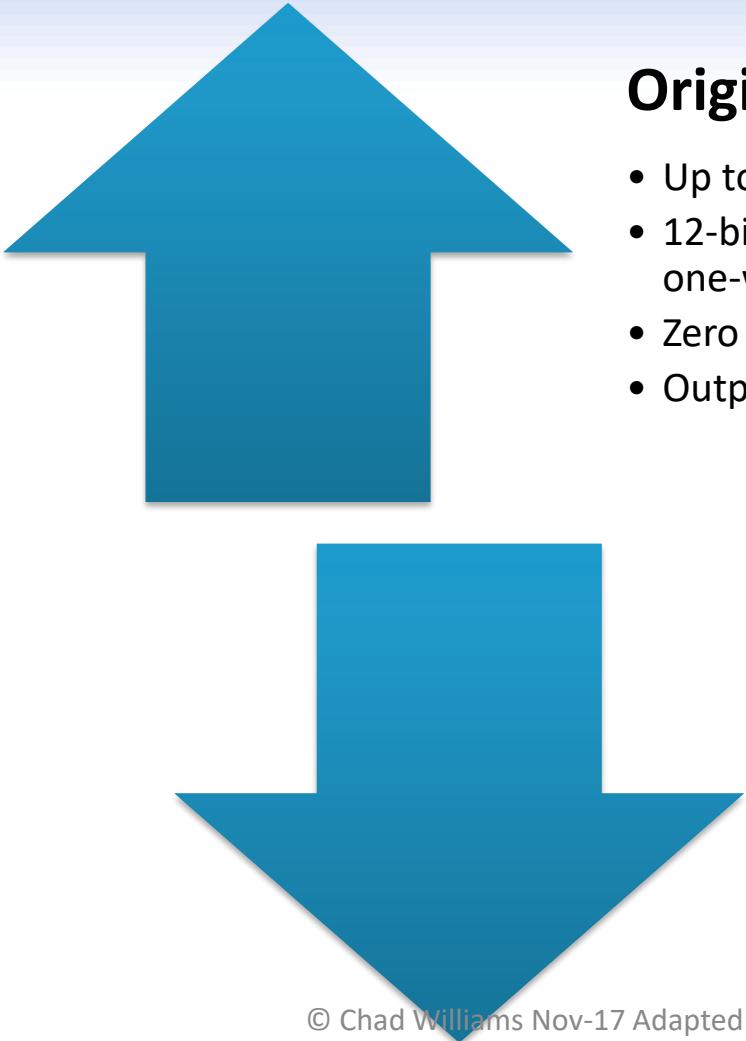
Figure 3.2 UNIX Password Scheme

© Chad Williams Nov-17 Adapted slides from Pearson Higher Ed, copyright 2014

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

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

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

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

Password crackers exploit the fact that people choose easily guessable passwords

- Shorter password lengths are also easier to crack

John the Ripper

- Open-source password cracker first developed in 1996
- Uses a combination of brute-force and dictionary techniques

Modern Approaches

- Complex password policy
 - Forcing users to pick stronger passwords
- However password-cracking techniques have also improved
 - The processing capacity available for password cracking has increased dramatically
 - The use of sophisticated algorithms to generate potential passwords
 - Studying examples and structures of actual passwords in use

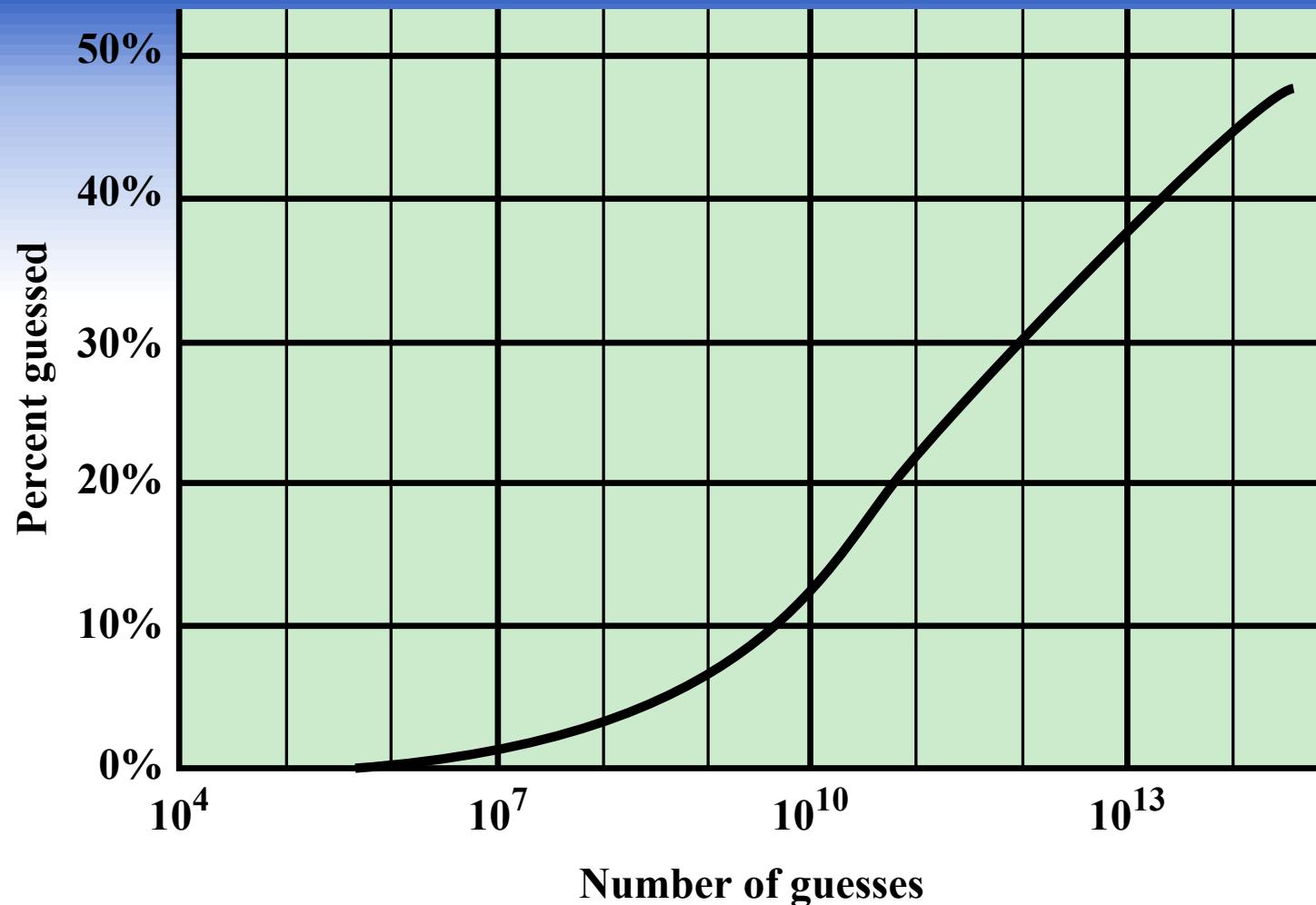


Figure 3.3 The Percentage of Passwords Guessed After a Given Number of Guesses

© Chad Williams Nov-17 Adapted slides from Pearson Higher Ed, copyright 2014

Password File Access Control

Can block offline guessing attacks by denying access to encrypted passwords

Make available only to privileged users

Shadow password file

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 Strategies

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

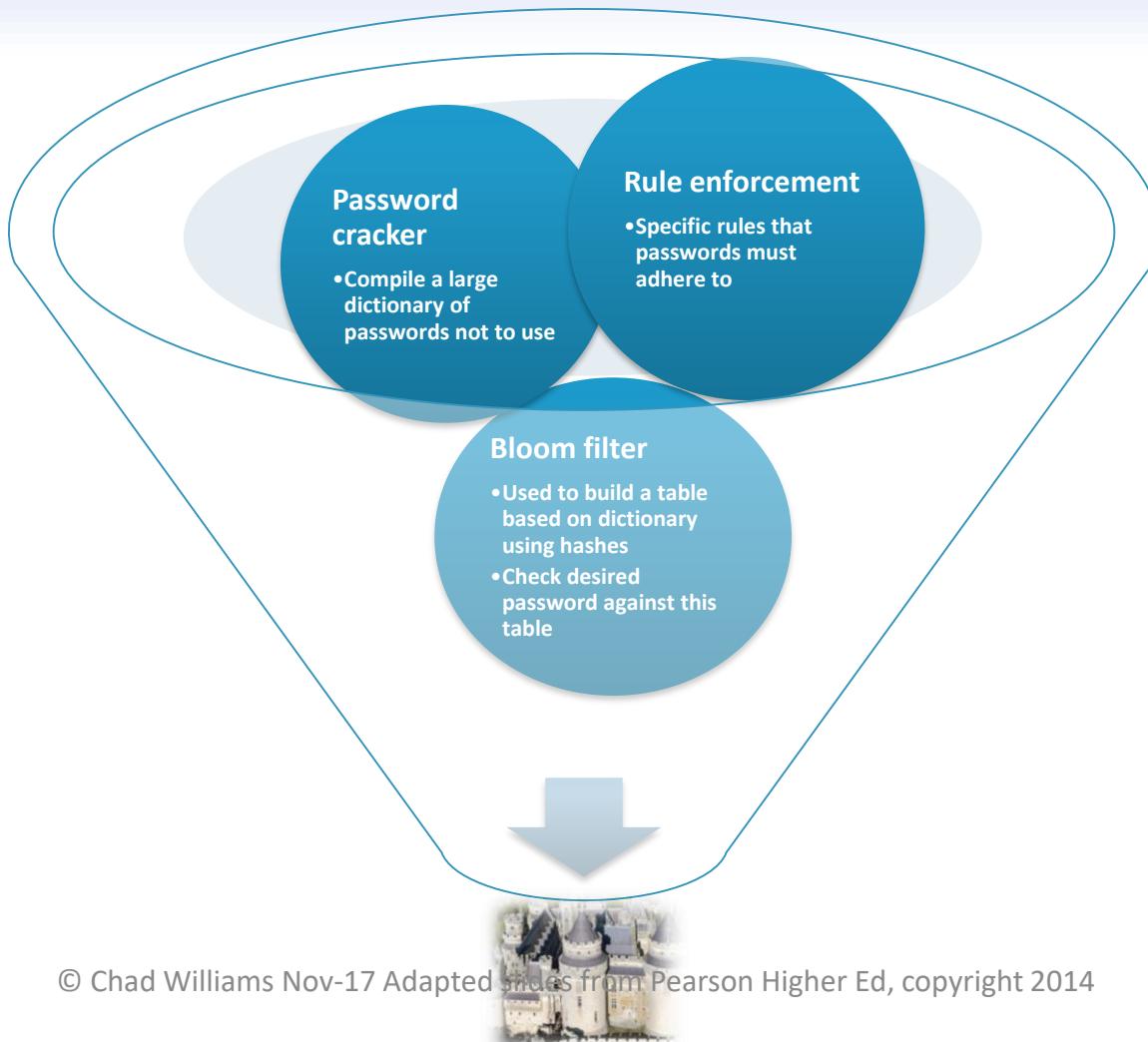


Complex password policy

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



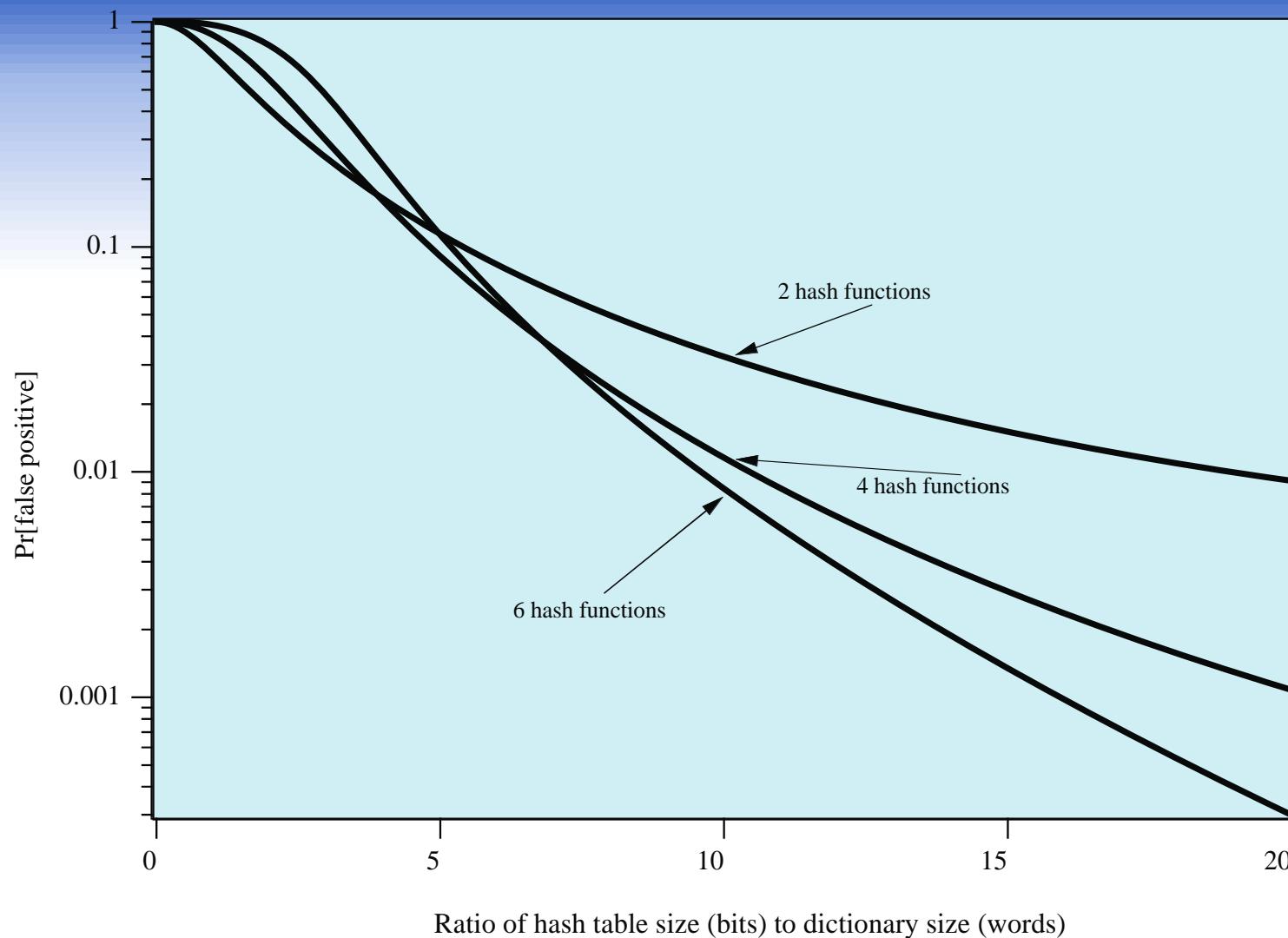


Figure 3.4 Performance of Bloom Filter

© Chad Williams Nov-17 Adapted slides from Pearson Higher Ed, copyright 2014

Table 3.2

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



Smart Tokens

- **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
 - Challenge-response

Smart Cards

- **Most important category of smart token**
 - Has the appearance of a credit card
 - Has an electronic interface
 - May use any of the smart token protocols
- **Contain:**
 - An entire microprocessor
 - Processor
 - Memory
 - I/O ports
- **Typically include three types of memory:**
 - Read-only memory (ROM)
 - Stores data that does not change during the card's life
 - Electrically erasable programmable ROM (EEPROM)
 - Holds application data and programs
 - Random access memory (RAM)
 - Holds temporary data generated when applications are executed

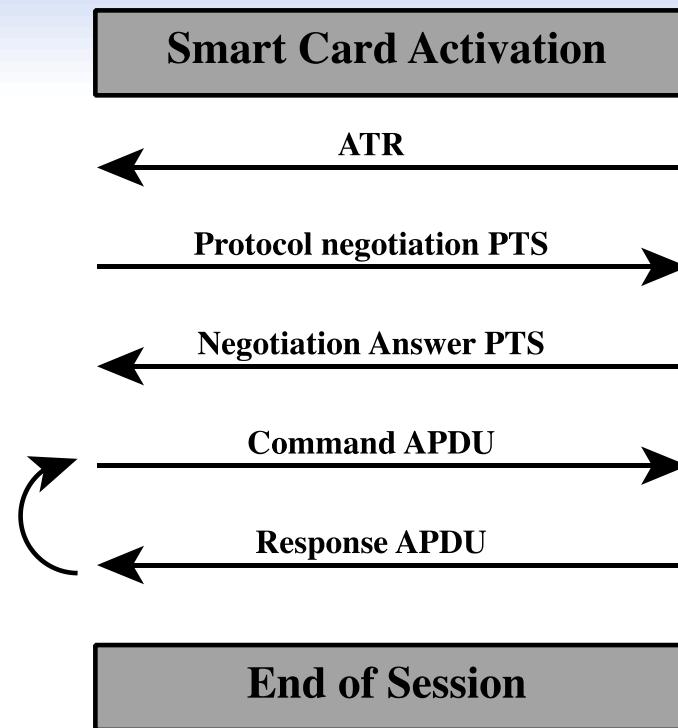




Smart card



Card reader



APDU = application protocol data unit

ATR = Answer to reset

PTS = Protocol type selection

Figure 3.5 Smart Card/Reader Exchange

© Chad Williams Nov-17 Adapted slides from Pearson Higher Ed, copyright 2014

Electronic Identity Cards (eID)

Use of a smart card as a national identity card for citizens

Can serve the same purposes as other national ID cards, and similar cards such as a driver's license, for access to government and commercial services

Can provide stronger proof of identity and can be used in a wider variety of applications

In effect, is a smart card that has been verified by the national government as valid and authentic

Most advanced deployment is the German card *neuer Personalausweis*

Has human-readable data printed on its surface

- Personal data
- Document number
- Card access number (CAN)
- Machine readable zone (MRZ)



Table 3.3

Electronic Functions

Function	Purpose	PACE Password	Data	Uses
ePass (mandatory)	Authorized offline inspection systems read the data	CAN or MRZ	Face image; two fingerprint images (optional), MRZ data	Offline biometric identity verification reserved for government access
eID (activation optional)	Online applications read the data or access functions as authorized	eID PIN	Family and given names; artistic name and doctoral degree; date and place of birth; address and community ID; expiration date	Identification; age verification; community ID verification; restricted identification (pseudonym); revocation query
	Offline inspection systems read the data and update the address and community ID	CAN or MRZ		
eSign (certificate optional)	A certification authority installs the signature certificate online	eID PIN	Signature key; X.509 certificate	Electronic signature creation
	Citizens make electronic signature with eSign PIN	CAN		

CAN = card access number

MRZ = machine readable zone

PACE = password authenticated connection establishment

PIN = personal identification number

© Chad Williams Nov-17 Adapted slides from Pearson Higher Ed, copyright 2014

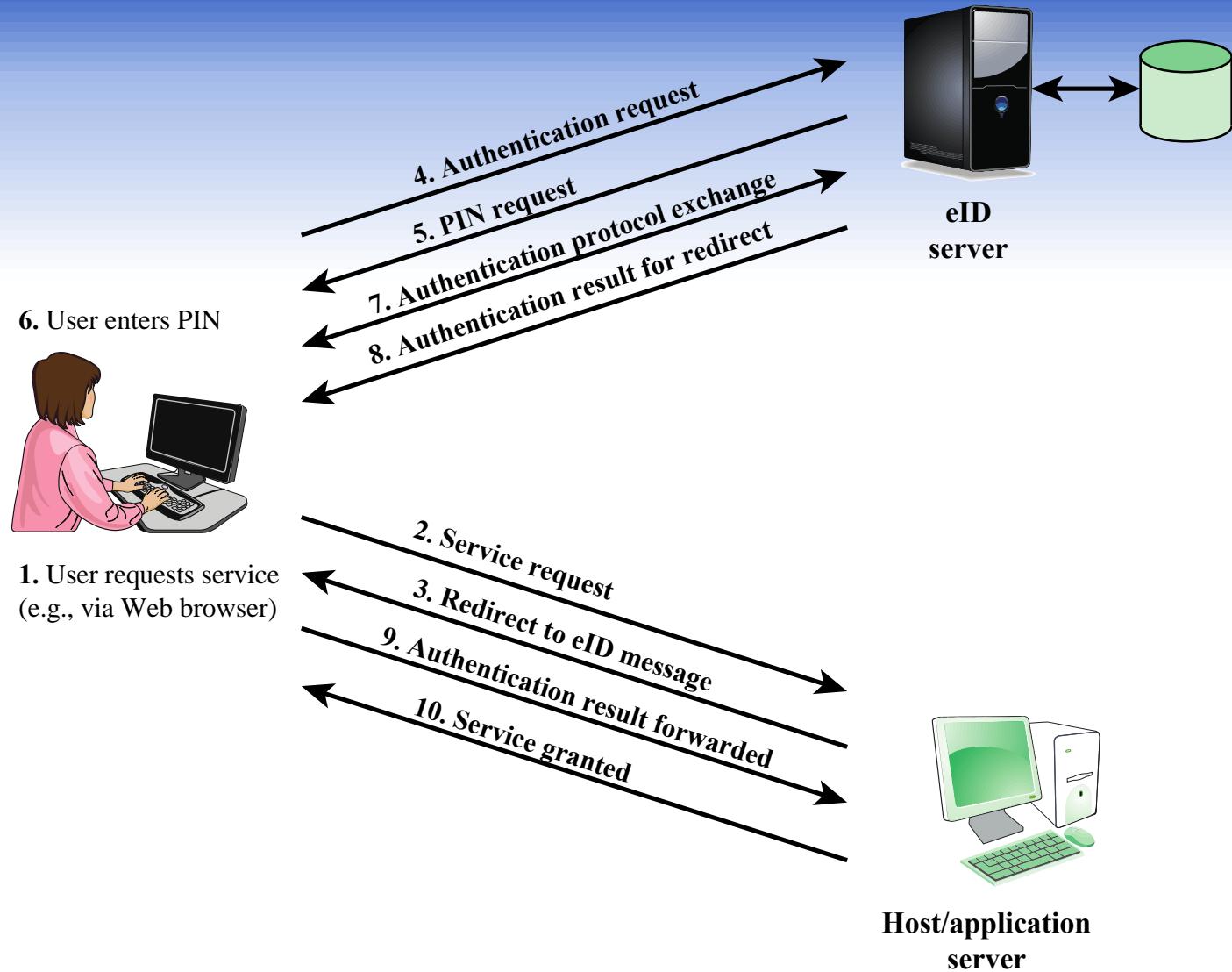
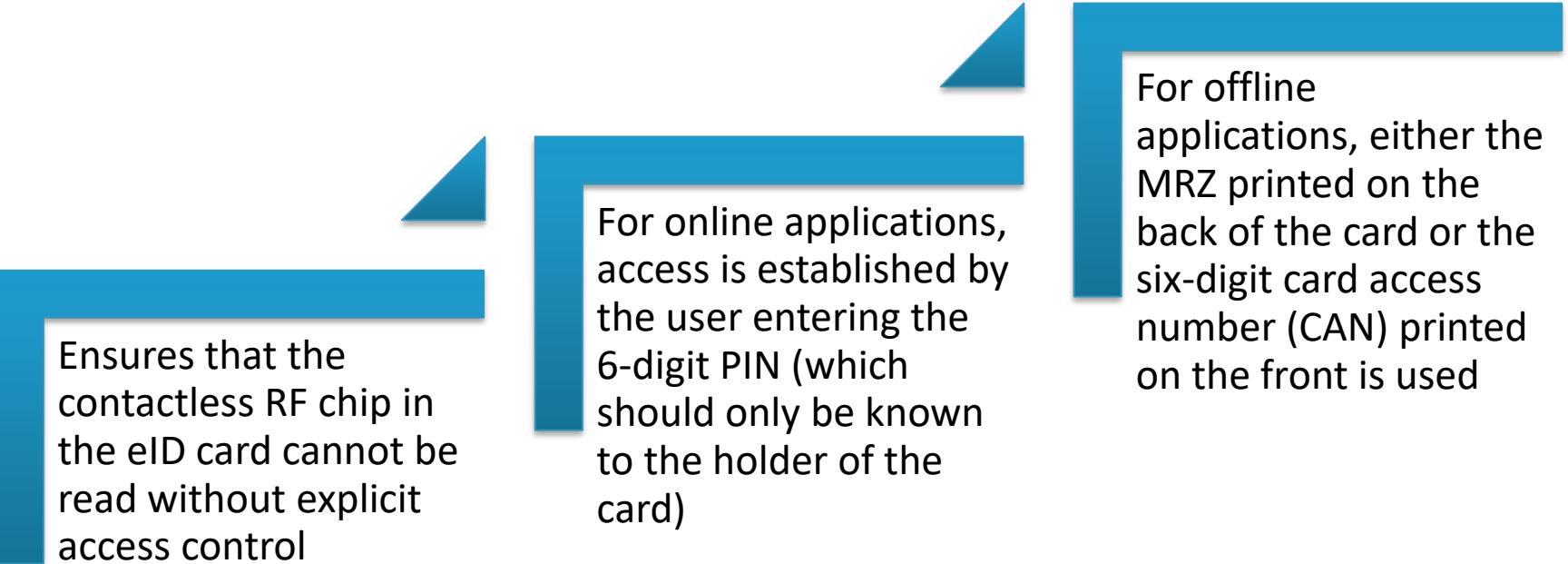


Figure 3.6 User Authentication with eID

© Chad Williams Nov-17 Adapted slides from Pearson Higher Ed, copyright 2014

Password Authenticated Connection Establishment (PACE)



Ensures that the contactless RF chip in the eID card cannot be read without explicit access control

For online applications, access is established by the user entering the 6-digit PIN (which should only be known to the holder of the card)

For offline applications, either the MRZ printed on the back of the card or the six-digit card access number (CAN) printed on the front is used

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



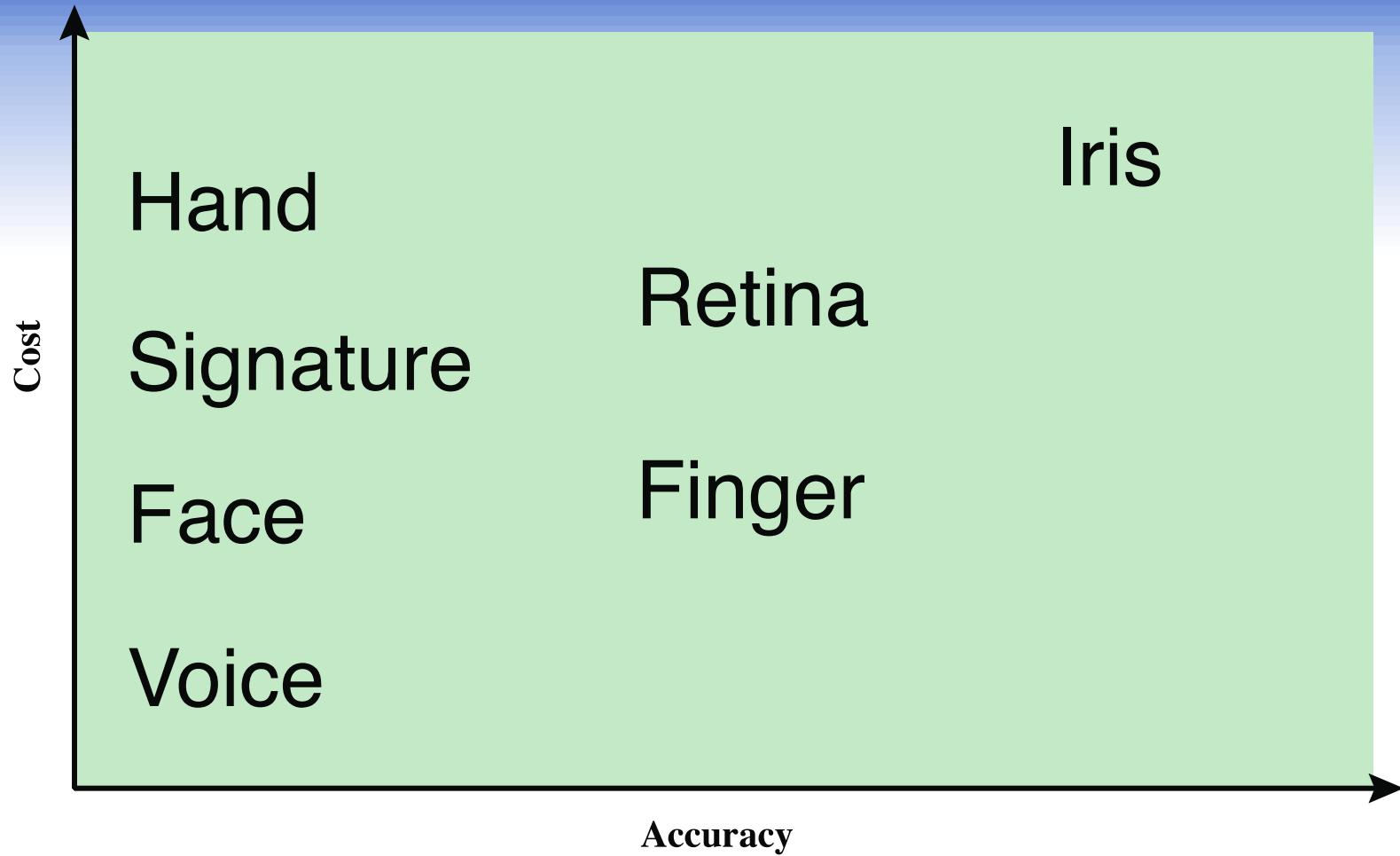
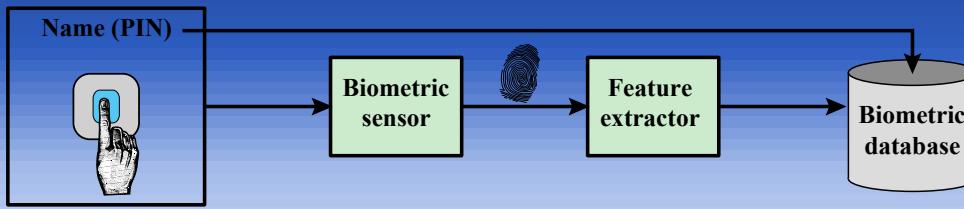
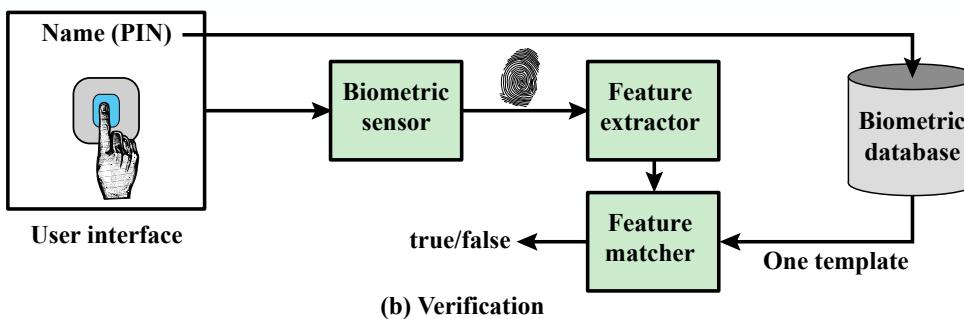


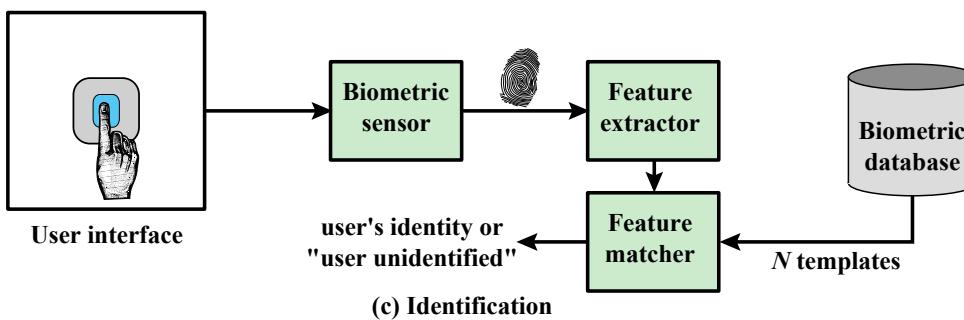
Figure 3.7 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.



(a) Enrollment



(b) Verification



(c) Identification

Figure 3.8 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.

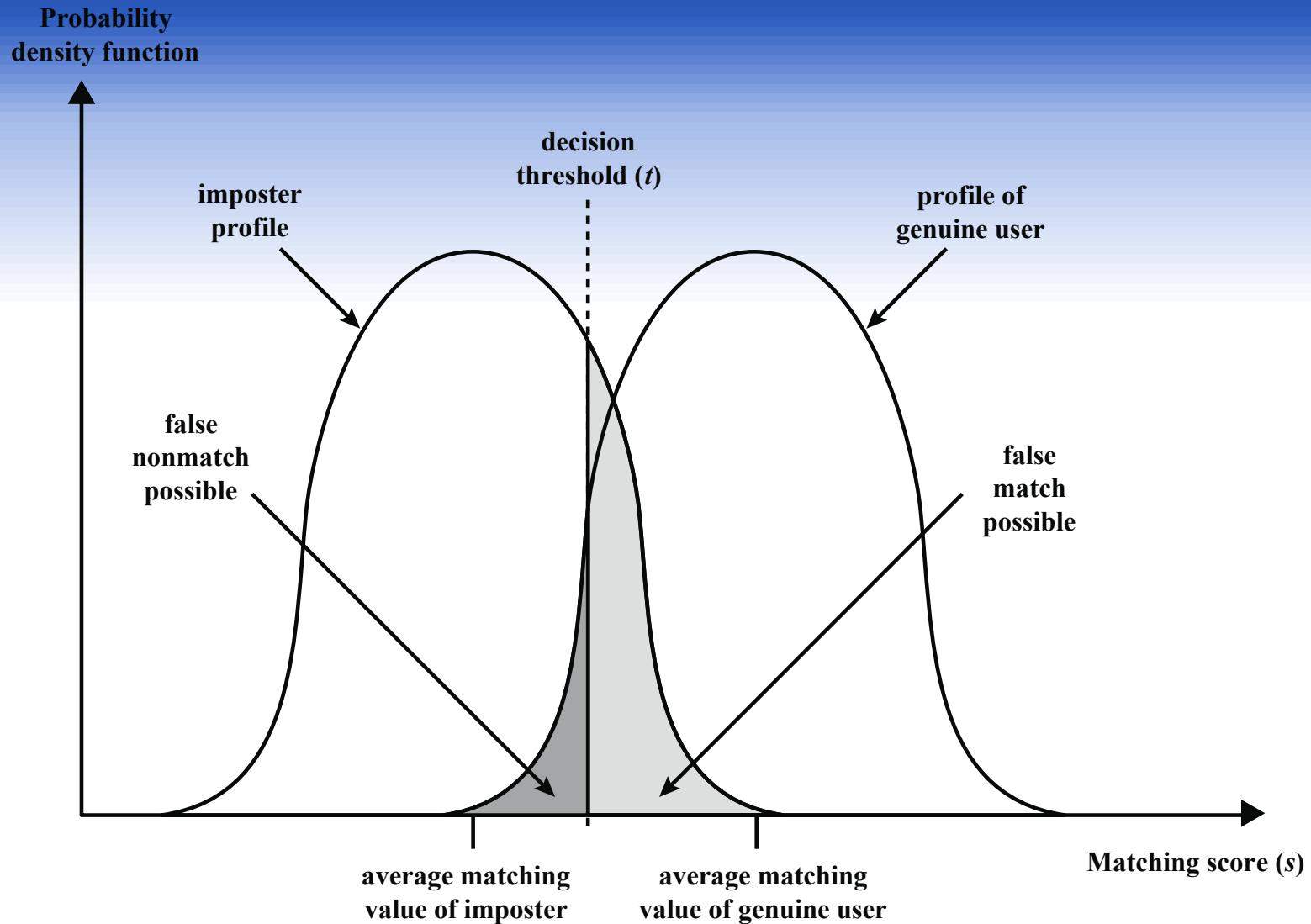


Figure 3.9 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (s) is greater than a preassigned threshold (t), a match is declared

© Chad Williams Nov 17 Adapted slides from Pearson Higher Ed, copyright 2014

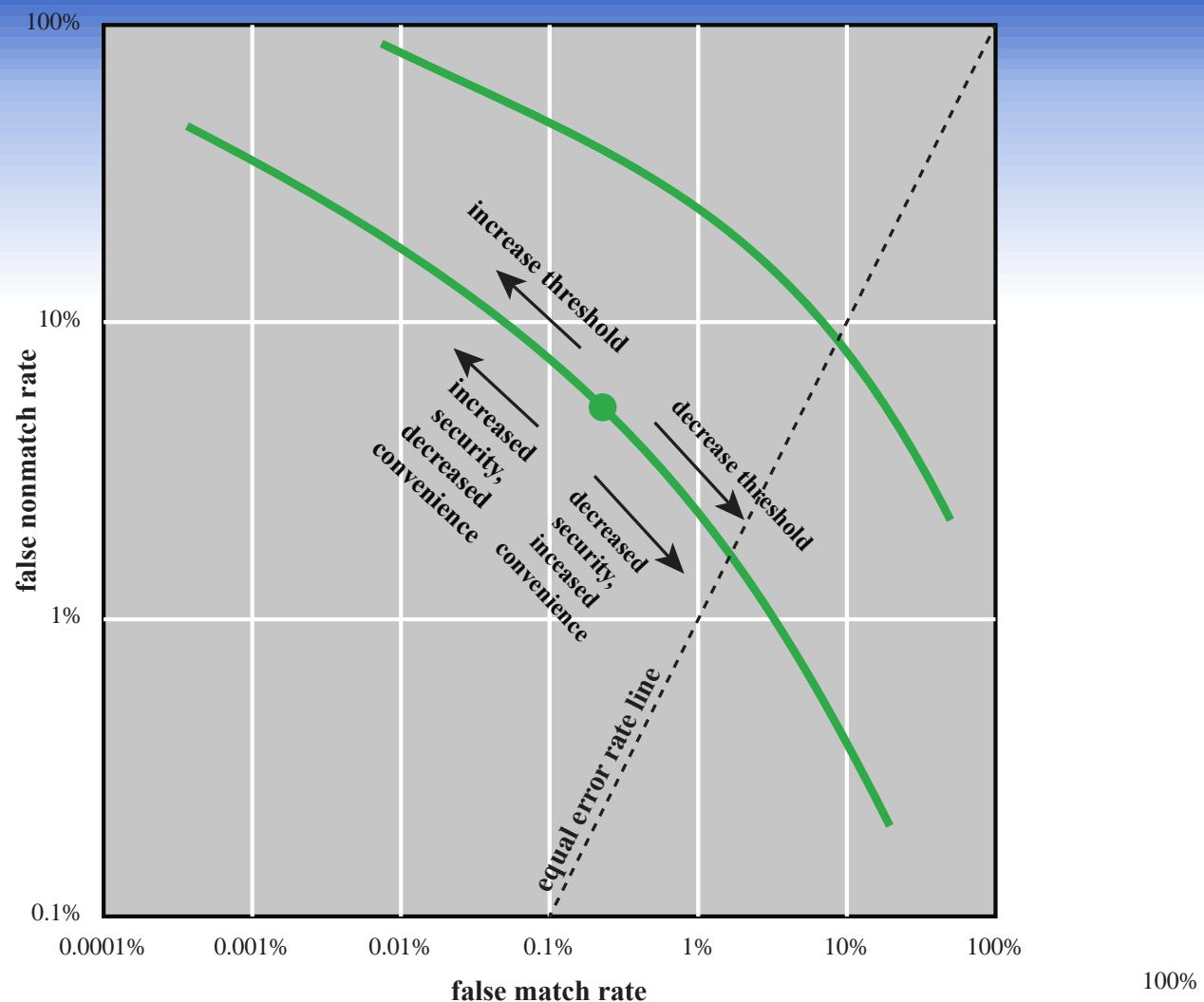


Figure 3.10 Idealized Biometric Measurement Operating Characteristic Curves (log-log scale)

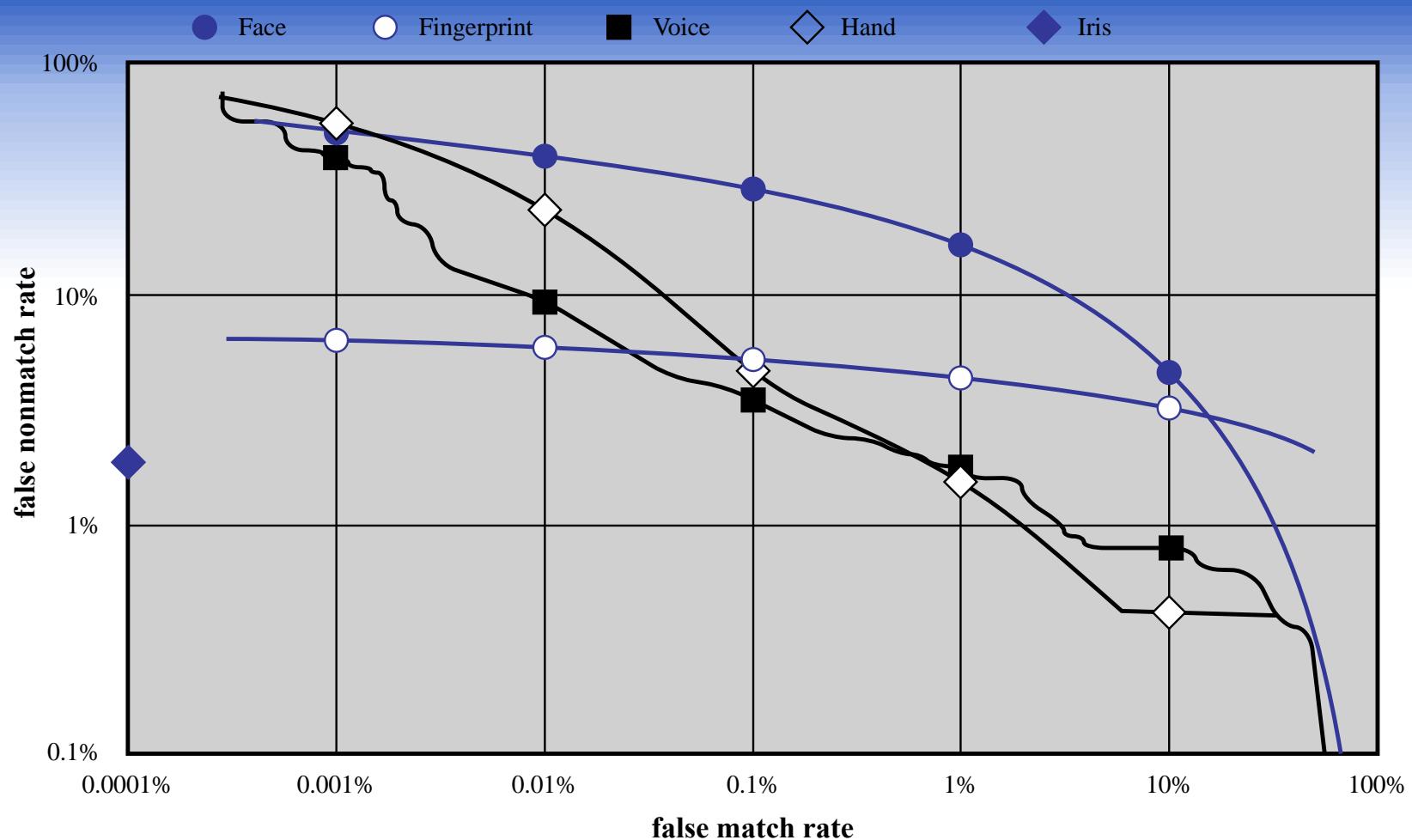


Figure 3.11 Actual Biometric Measurement Operating Characteristic Curves, reported in [MANS01]. To clarify differences among systems, a log-log scale is used.

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



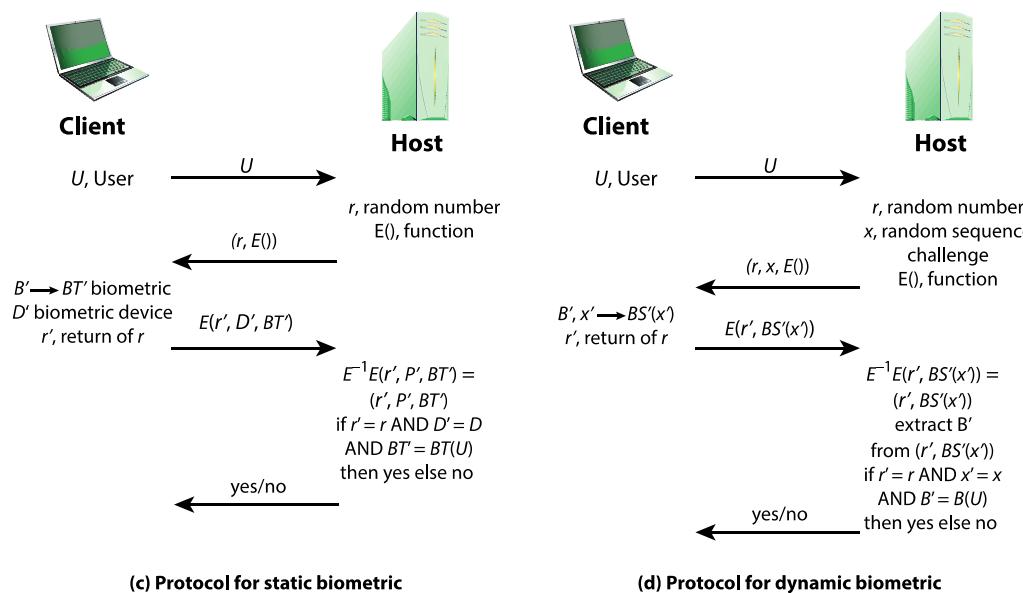
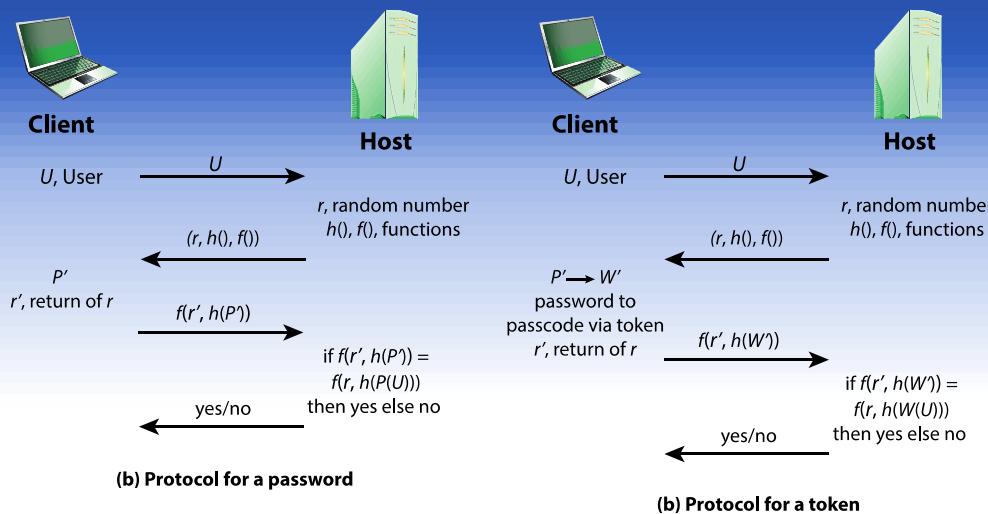


Figure 3.12 Basic Challenge-Response Protocols for Remote User Authentication

© Chad Williams Nov-17 Adapted slides from Pearson Higher Ed, copyright 2014

Table 3.4

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

AUTHENTICATION SECURITY ISSUES

Denial-of-Service

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

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

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

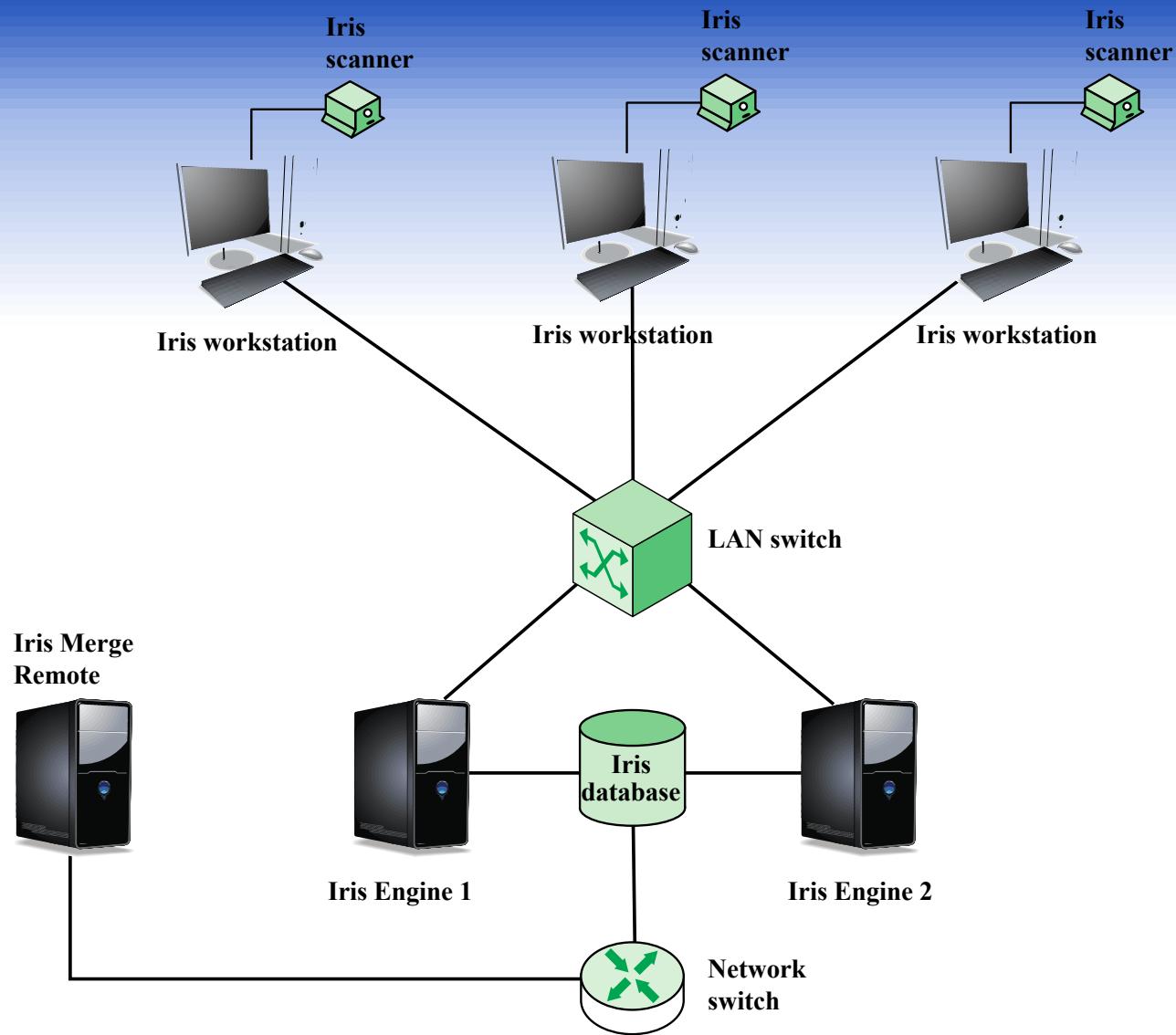


Figure 3.13. General Iris Scan Site Architecture for UAE System

©Chad Williams Nov 17 Adapted稍 from Pearson Higher Ed, copyright 2014

Case Study: ATM Security Problems

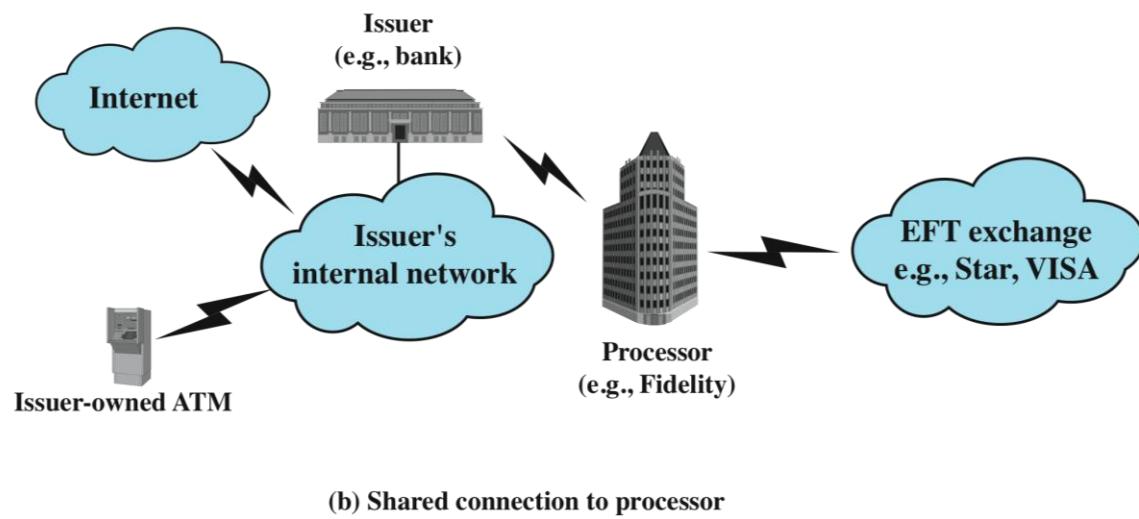
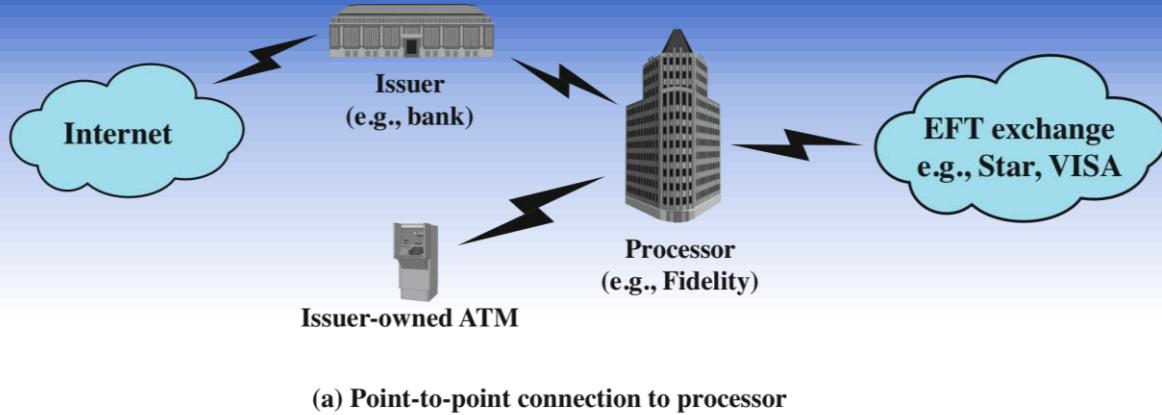


Figure 3.12 ATM Architectures. Most small to mid-sized issuers of debit cards contract processors to provide core data processing and electronic funds transfer (EFT) services. The bank's ATM machine may link directly to the processor or to the bank.

Summary

- Electronic user authentication principles
 - A model for electronic user authentication
 - Means of authentication
 - Risk assessment for user authentication
- Password-based authentication
 - The vulnerability of passwords
 - The use of hashed passwords
 - Password cracking of user-chosen passwords
 - Password file access control
 - Password selection strategies
- Token-based authentication
 - Memory cards
 - Smart cards
 - Electronic identity cards
- Biometric authentication
 - Physical characteristics used in biometric applications
 - Operation of a biometric authentication system
 - Biometric accuracy
- Remote user authentication
 - Password protocol
 - Token protocol
 - Static biometric protocol
 - Dynamic biometric protocol
- Security issues for user authentication



In class exercises revisited

Bob's Pizza Shack

In groups consider this scenario

Bob is a small business owner of Bob's Pizza Shack and wants to create a website to allow online credit card delivery orders

- Identify the languages needed for implementing the case project.
 - What are the known vulnerabilities of these languages and where does the system provide opportunity for misuse?

Alice's Online Bank

In groups consider this scenario

- Alice opens Alice's Online Bank (AOB)
 - Internal use bank employees
 - Interoperates with another bank
 - Interacts with customers
 - Web
 - Mobile app
- Identify the languages needed for implementing the case project.
 - What are the known vulnerabilities of these languages and where does the system provide opportunity for misuse?

Location based social media app

In groups consider this scenario Open source group wants to create a mobile app to allow groups to communicate/find each other in public demonstrations/protests

- Communication internet, as well as, P2P (WiFi/Bluetooth) in case internet cut off – so if person you want to contact is on other side of crowd and no internet as long as P2P network can be established with app can reach somebody outside your immediate vicinity via the P2P network
- Should be able to communicate securely messages and images to people you identify within your group (group as whole or direct)
- Should be able to share GPS location with people in group (group as whole or direct)