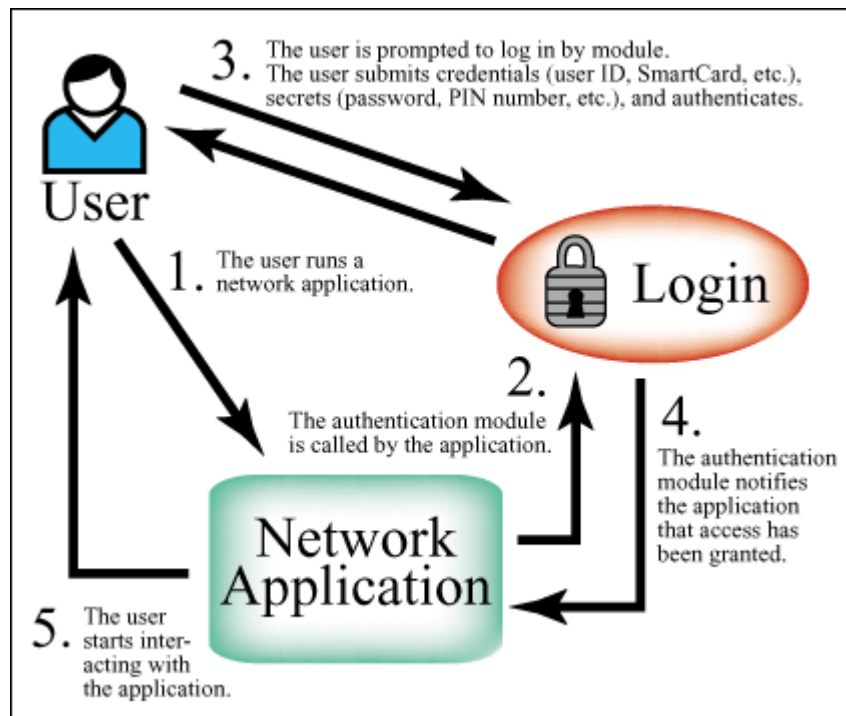


Lecture Outline

- Means of Authentication
- Password-Based
- Token-Based
- Biometric
- Remote Access
- Practical Application



© Novell

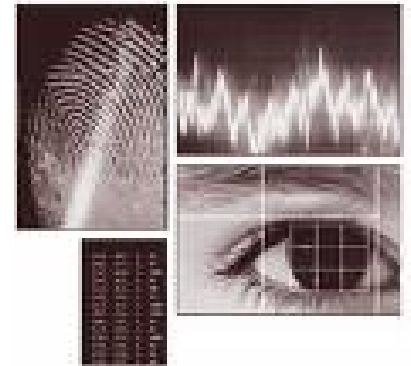


© Madartists

User Authentication

- fundamental security building block
- first line of defense
 - basis of access control & user accountability
- has 3 steps:
 1. enrollment
 2. identification - specify identifier
 3. verification - bind entity (person) and identifier
- login known – why?
- login/password – unique ID unit

Means of User Authentication



- 4 means of authenticating user's identity
- based on something the individual:
 1. knows - e.g. password, PIN, or answers to a prearranged set of questions and pictures (Citizens Bank)
 2. possesses - e.g. keycards, smartcard - tokens
 3. is (static biometrics) - e.g. fingerprint, retina, face, hand vein patterns
 4. does (dynamic biometrics) - e.g. voice, signature, typing rhythm
- can be used alone or combined
- all can provide user authentication
- but all have issues



Password Authentication

- widely used user authentication method
 - user provides name/login and password
 - system compares password with that previously saved for specified login

- authenticates ID of user logging in and
 - that the user is authorized to access system
 - determines the user's privileges – e.g. admin faculty students department
 - is used in discretionary access control – e.g. Blackboard and Senate and UCPRC membership

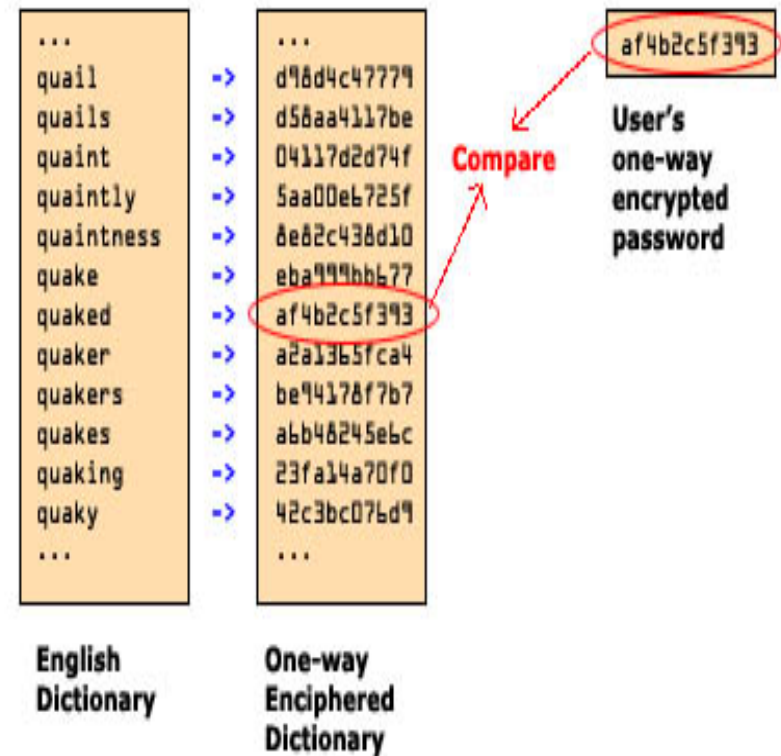
Use of Hashed Passwords

Password Vulnerabilities

- dictionary attack
 - hacker may bypass access controls and gain access to the system password file. The attacker then compares the password hashes against hashes of commonly used passwords

- specific account attack
 - attacker targets a specific account and submits password guesses until the correct password is discovered
 - what is the countermeasure here?

- popular password attack
 - attacker chooses a popular password and tries it against a wide range of user IDs



e.g. news anchor

Password Vulnerabilities

- workstation hijacking/ exploiting user mistakes
 - idle workstation
 - secretarial staff
 - sharing passwords with admins/colleagues

- exploiting multiple password use
 - similar or same password Amazon, eBay, bank, office

- electronic monitoring
 - if password is communicated across network to log on to a remote system, it is vulnerable to eavesdropping
 - Simple encryption will not solve this problem because _____



Salt

- The salt has 3 purposes:
 1. even if 2 users choose the same password, the passwords will be assigned different salt values – thus the hashed values of the 2 users will be different
 2. greatly increases the difficulty of offline dictionary attacks – for a salt of length b , the number of possible passwords is increased by _____
 3. nearly impossible to find out whether a person with passwords on 2 or more systems has used the same password on all of them

Password Cracking

- dictionary attacks
 - try each word then obvious variants in large dictionary against hash in password file
 - each password must be hashed using each available salt value and then compared to stored hash values

- rainbow table attacks
 - precompute tables of hash values for all salts
 - An enormous table of hash values to compare

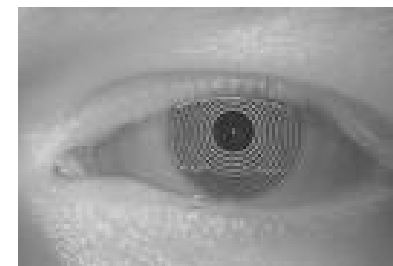
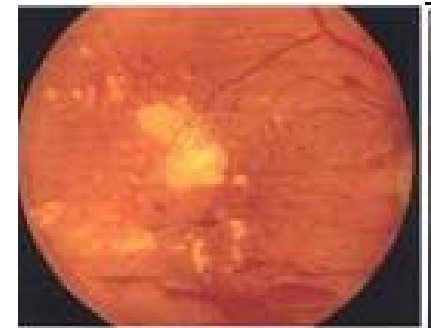
Password File Access Control

- can block offline guessing attacks by denying access to encrypted passwords
 - make available only to privileged users
 - use a separate shadow password file consisting only of the hashed passwords

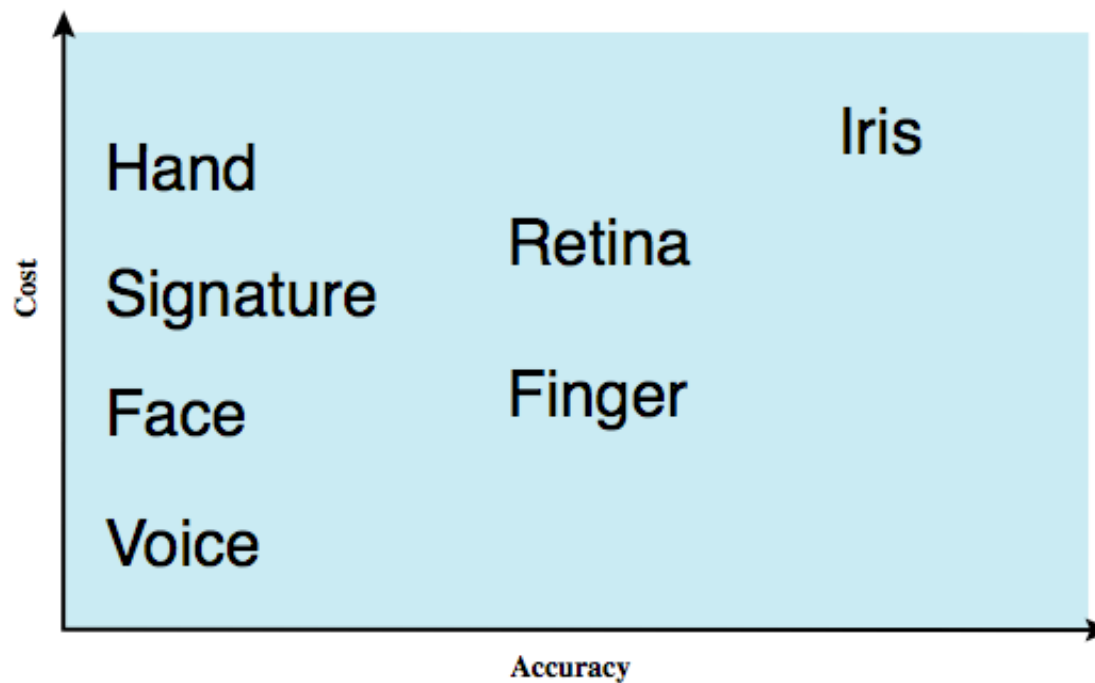
- still have vulnerabilities
 - accident with permissions making it readable
 - users with same password on other systems
 - access from unprotected backup media
 - sniff passwords in unprotected network traffic

Biometric Authentication

- A biometric authentication system attempts to authenticate an individual based on unique physical characteristics.
- Facial characteristics
- Fingerprints:
- Hand geometry:
- Retinal pattern:
 - uses a digital image of the retinal pattern by projecting a low-intensity beam of visual or infrared light into the eye
- Iris:
- Signature:
- Voice:

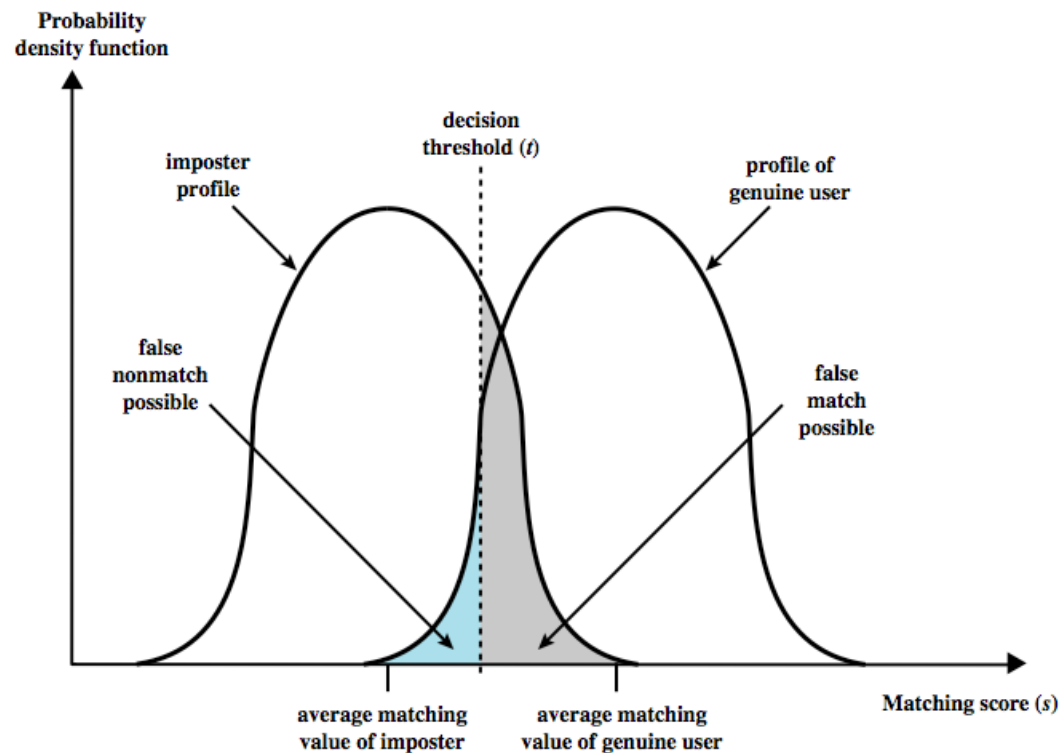


Biometric Authentication – advantages and disadvantages



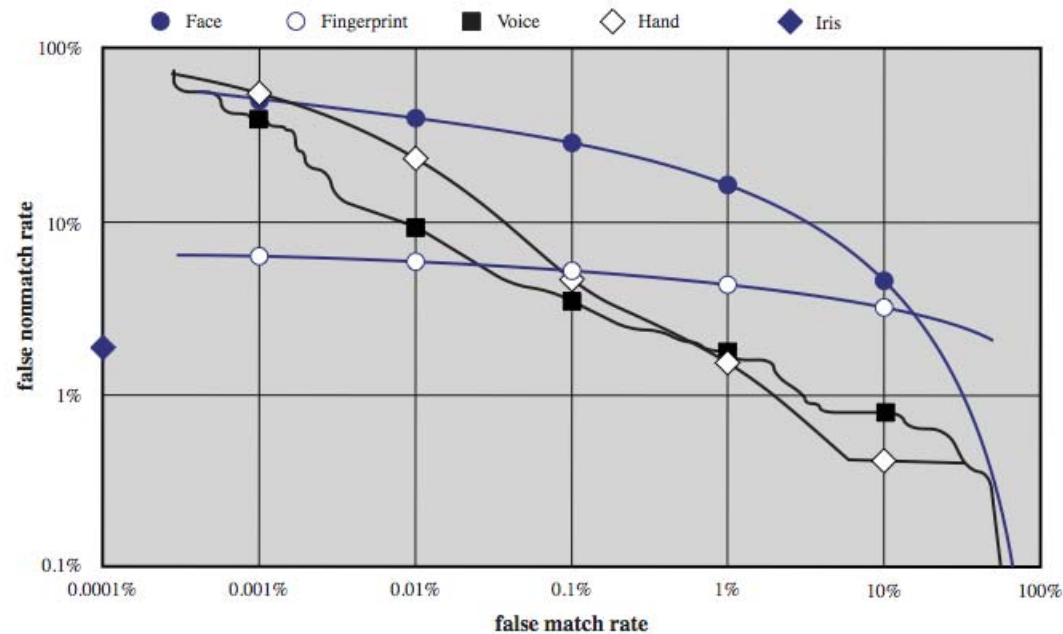
Biometric Accuracy

- the system compares the stored template to the presented template
- never get identical templates
- the system uses an algorithm to generate a matching score (typically a single number) that quantifies the similarity between the input and the stored template
- The difficulty is that the range of matching scores produced by two individuals, one genuine and one an imposter, compared to a given reference template, are likely to overlap - problems of false match / false non-match



Biometric Accuracy

- can plot characteristic curve
- A high-security application may require a very low false match rate, whereas for a forensic application, in which the system is looking for possible candidates, to be checked further, the requirement may be for a low false non-match rate
- The characteristic curves below was developed from actual product testing. The iris system had no false matched in over 2 million cross-comparisons



Remote User Authentication

- authentication over network more complex
 - problems of eavesdropping, replay

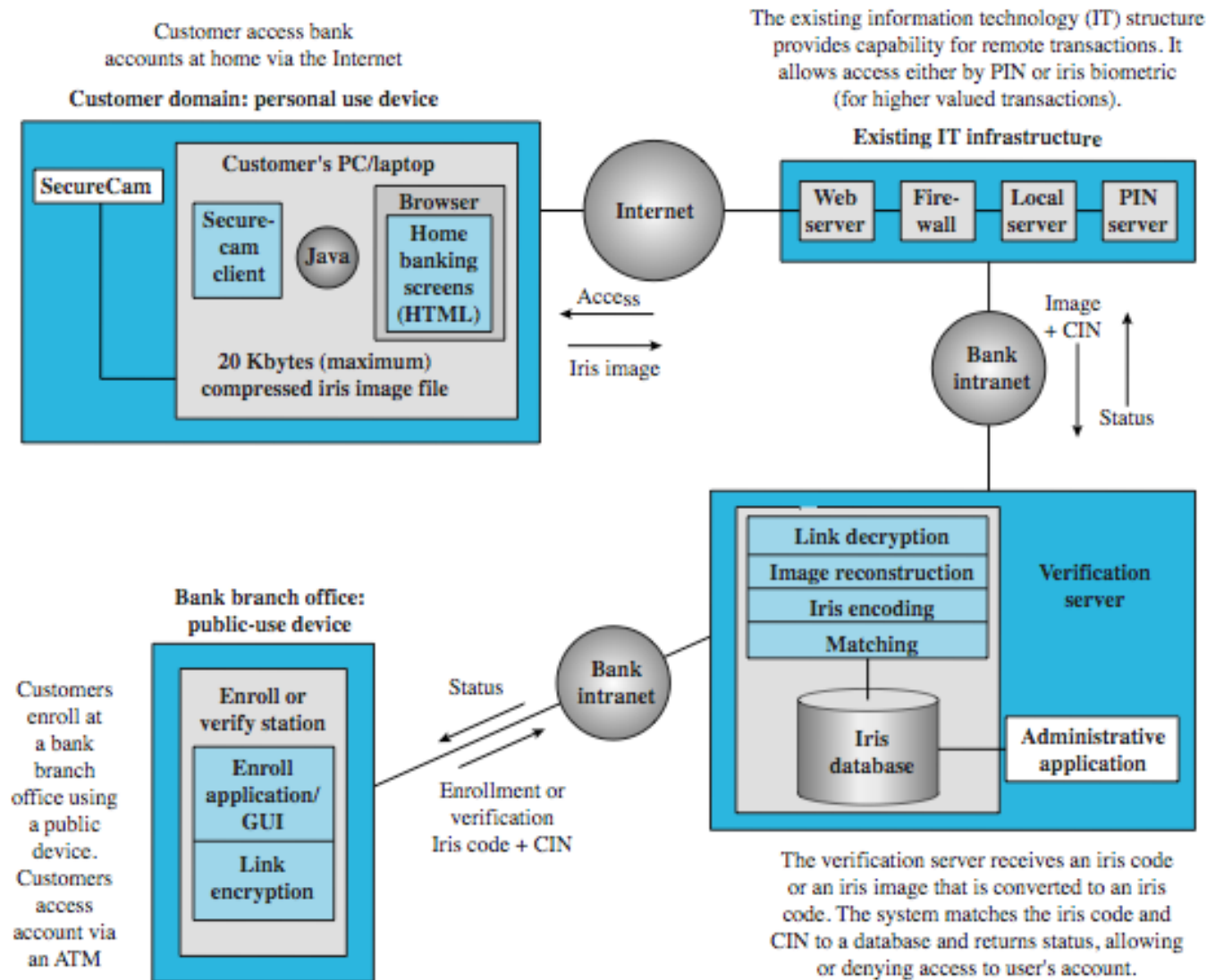
- generally use challenge-response
 - user sends identity
 - host responds with random number
 - user computes $f(r, h(P))$ and sends back
 - host compares value from user with own computed value, if match user authenticated

- protects against a number of attacks

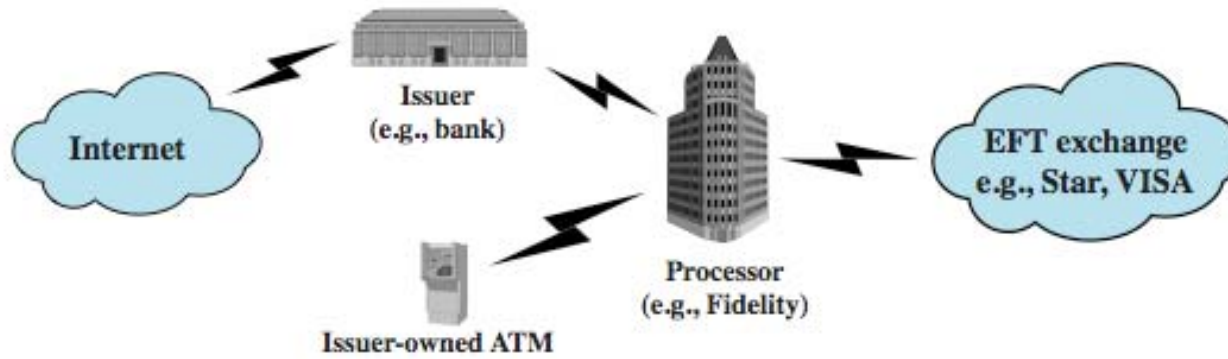
Authentication Security Issues

- client attacks
- host attacks
- Eavesdropping
- Replay
- trojan horse
- denial-of-service

Practical Application



Case Study: ATM Security



(a) Point-to-point connection to processor

