
Lecture 11

# Access Control

# Access Control

- Access Controls
  - Firms must limit access to physical and electronic resources
  - Access control is the policy-driven control of access to systems, data, and dialogues
- Cryptography
  - Many access control tools use cryptography to some extent
  - However, cryptography is only part of what they do and how they work

# Authentication, Authorizations, and Auditing

- **AAA** Protections
  - Authentication-supplicant sends credentials to verifier to authenticate the supplicant
  - Authorization-what permissions the authenticated user will have
  - Auditing-recording what people do in log files

# Authentication

- Credentials Are Based on
  - What you know (e.g., a password)
  - What you have (e.g., an access card)
  - What you are (e.g., your fingerprint)
  - What you do (e.g., speaking a passphrase)

# Two-Factor Authentication

- Two-Factor Authentication
  - Use two forms of authentication for defense in depth
    - Example: access card and personal identification number (PIN)
  - Multifactor authentication: two or more types of authentication
  - Can be defeated by a Trojan horse on the user's PC
  - Can also be defeated by a man-in-the-middle attack by a fake website

# Individual and Role-Based Access Control

- Individual and Role-Based Access Control
  - Individual access control: bases access rules on individual accounts
  - Role-based access control (RBAC)
- Human and Organizational Controls
  - People and organizational forces may circumvent access protections

# Military and National Security Organization Access Controls

- Mandatory and Discretionary Access Control
  - Mandatory access control (MAC)
    - No departmental or personal ability to alter access control rules set by higher authorities
  - Discretionary access control (DAC)
    - Departmental or personal ability to alter access control rules set by higher authorities
  - MAC gives stronger security but is very difficult to implement

# Multilevel Security

- Multilevel Security
  - Resources are rated by security level
  - People are given the same clearance level
  - Some rules are simple
  - Some rules are complex
  - Access control models have been created to address multilevel security

# Physical Access and Security

- Physical Security Perimeter
  - Ideally, only a single point of entry
  - Emergency exits
  - Physical entry controls
  - Securing offices, rooms, and facilities
  - Protecting against external and environmental threats
  - Rules for working in secure areas
  - Public access, delivery, and loading areas

# Physical Access and Security

- ISO/IEC 11.2 Equipment Security
  - Equipment siting and protection
  - Supporting utilities (electricity, water, HVAC)
  - Cabling security (conduits, underground wiring, etc.)
  - Security during off-site equipment maintenance
  - Rules for the removal of property
  - Security of equipment off-premises
  - Secure disposal or reuse of equipment
  - Clear desk and clear screen

# Physical Access and Security

- Terrorism
  - Building set back from street
  - Armed guards
  - Bullet-proof glass
- Piggybacking
  - Following an authorized user through a door
  - Also called tailgating
  - Psychologically difficult to prevent
  - But can and should be done

# Physical Access and Security

- Monitoring Equipment
  - CCTV
  - Tapes wear out
  - High-resolution cameras are expensive and consume a great deal of disk space
  - Low-resolution cameras may be insufficient for recognition needs

# Physical Access and Security

- Trash Bins
  - Protect trash that may contain sensitive information
  - Maintain trash inside the corporate premises and monitor until removed
- Desktop PC Security
  - Locks that connect the computer to an immovable object
  - Login screens with strong passwords

# Passwords

- Reusable password
  - Password used for weeks or months at a time
- One-time password
  - Used only once
- Difficulty of cracking passwords by guessing remotely
  - Account is usually locked after a few login failures
- Password-cracking programs
  - Password-cracking programs exist

# Passwords

- Password Policies
  - Not using the same password at multiple sites
  - Password duration policies
  - Shared password policies (makes auditing impossible)
  - Disabling passwords that are no longer valid
  - Lost passwords (password resets)

# Passwords

- Password Policies
  - Opportunities for social engineering attacks
  - Automated password resets use secret questions (Where were you born?)
  - Password policies must be long and complex
  - Testing and enforcing passwords
  - Passwords must be stored as secure hashes
  - Passwords should be audited regularly

# Common Passwords

The top 20 most commonly used passwords for two real-world data breaches.

| Troy Hunt | | | RockYou.com | | | Gawker.com | | |
|---|---|---|---|---|---|---|---|---|
| Rank | Count | Password | Rank | Count | Password | Rank | Count | Password |
| 1 | 23,174,662 | 123456 | 1 | 290,731 | 123456 | 1 | 2,516 | 123456 |
| 2 | 7,671,364 | 123456789 | 2 | 79,078 | 12345 | 2 | 2,188 | password |
| 3 | 3,810,555 | qwerty | 3 | 76,790 | 123456789 | 3 | 1,205 | 12345678 |
| 4 | 3,645,804 | password | 4 | 61,958 | Password | 4 | 696 | qwerty |
| 5 | 3,093,220 | 111111 | 5 | 51,622 | iloveyou | 5 | 498 | abc123 |
| 6 | 2,889,079 | 12345678 | 6 | 35,231 | princess | 6 | 459 | 12345 |
| 7 | 2,834,058 | abc123 | 7 | 22,588 | rockyou | 7 | 441 | monkey |
| 8 | 2,484,157 | 1234567 | 8 | 21,726 | 1234567 | 8 | 413 | 111111 |
| 9 | 2,401,761 | password1 | 9 | 20,553 | 12345678 | 9 | 385 | consumer |
| 10 | 2,333,232 | 12345 | 10 | 17,542 | abc123 | 10 | 376 | letmein |
| 11 | 2,224,432 | 1234567890 | 11 | 17,168 | Nicole | 11 | 351 | 1234 |
| 12 | 2,194,818 | 123123 | 12 | 16,409 | Daniel | 12 | 318 | dragon |
| 13 | 1,942,768 | 000000 | 13 | 16,094 | babygirl | 13 | 307 | trustno1 |
| 14 | 1,593,388 | iloveyou | 14 | 15,294 | monkey | 14 | 303 | baseball |
| 15 | 1,256,907 | 1234 | 15 | 15,162 | Jessica | 15 | 302 | gizmodo |
| 16 | 1,141,300 | 1q2w3e4r5t | 16 | 14,950 | Lovely | 16 | 300 | whatever |
| 17 | 1,081,655 | qwertyuiop | 17 | 14,898 | michael | 17 | 297 | superman |
| 18 | 1,023,001 | 123 | 18 | 14,329 | Ashley | 18 | 276 | 1234567 |
| 19 | 980,209 | monkey | 19 | 13,984 | 654321 | 19 | 266 | sunshine |
| 20 | 968,625 | dragon | 20 | 13,856 | Qwerty | 20 | 266 | iloveyou |

# Access Cards and Tokens

- Access Cards
  - Magnetic stripe cards
  - Smart cards
  - In selection decision, must consider cost and availability of card readers
- Tokens
  - Constantly changing password devices for one-time passwords
  - USB plug-in tokens

# Access Cards and Tokens

- Proximity Access Tokens
  - Use Radio Frequency ID (RFID) technology
  - Supplicant only has to be near a door or computer to be recognized
- Addressing Loss and Theft
  - Both are frequent
  - Card cancellation
  - Requires a wired network for cancellation speed
  - Must cancel quickly if risks are considerable

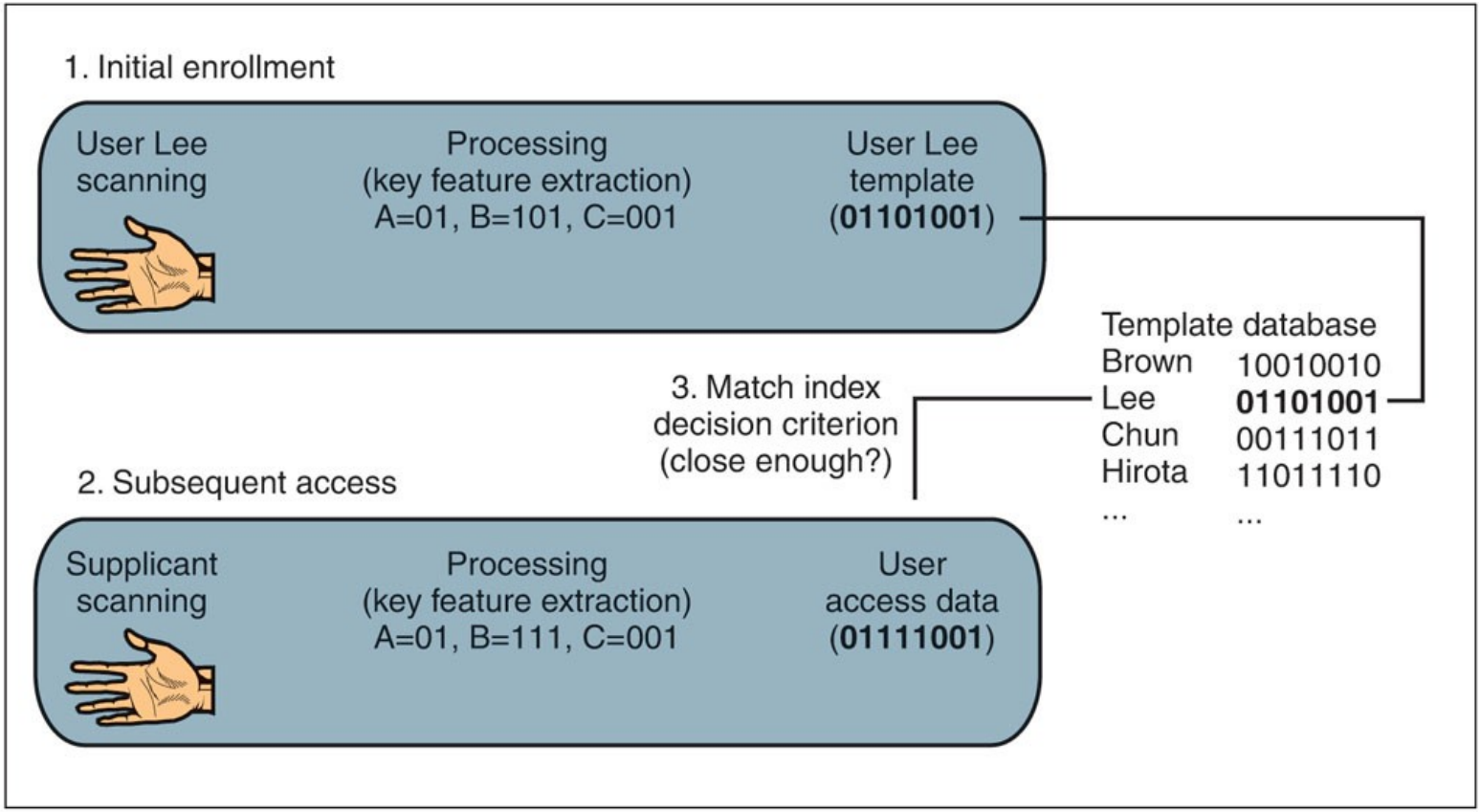
# Access Cards and Tokens

- Two-Factor Authentication Needed because of Ease of Loss and Theft
  - PINs (Personal Identification Numbers) for the second factor
  - Other forms of two-factor authentication

# Biometric Authentication

- Biometric Authentication
  - Authentication based on biological (bio) measurements (metrics)
  - Major promise of biometrics is to make reusable passwords obsolete
- Biometric Systems
  - Enrollment (enrollment scan, process for key features, store template)
  - Later access attempts provide access data, which will be turned into key feature data for comparison with the template
  - There must be configurable decision criteria for deciding how close a match (match index) to require
  - Requiring an overly exact match index will cause many false rejections
  - Requiring too loose a match index will cause more false acceptances

# Biometric Authentication System



# Biometric Authentication

- Errors versus Deception
  - Error rate
    - Refers to accuracy when the supplicant is not trying to deceive the system
  - Deception rate
    - The likelihood that an impostor will be able to deceive the system if he or she tries
- False Acceptance Rates (FARs)
  - Percentage of people who are identified or verified as matched to a template but should not be
- False Rejection Rates (FRRs)
  - Percentage of people who should be identified or verified as matches to a template but are not

# Biometric Authentication

- Vendor Claims for FARs and FRRs
  - Tend to be exaggerated through tests under ideal conditions
- Failure to Enroll (FTE)
  - Subject cannot enroll in system
  - E.g., poor fingerprints due to construction work, clerical work, age, etc.
- Deception
  - Errors: when subject is not trying to fool the system
  - Deception: when subject is trying to fool the system
  - Many biometric methods are highly vulnerable to deception

# Biometric Authentication

- Verification
  - Supplicant claims to be a particular person
  - Is the supplicant who he or she claims to be?
  - Compare access data to a single template (the claimed identity)
  - Verification is good to replace passwords in logins
  - If the probability of a false acceptance (false match) probability is 1/1000 per template match,
    - The probability of a false acceptance is 1/1000 (0.1%)

# Biometric Authentication

- Identification
  - Supplicant does not state his or her identity
  - System must compare supplicant data to all templates to find the correct template
  - If the probability of a false acceptance (false match) probability is 1/1000 per template match,
    - and if there are 500 templates in the database, then
    - the probability of a false acceptance is 500 * 1/1000 (50%)
  - Good for door access

# Biometric Authentication

- Watch Lists
  - Subset of identification
  - Goal is to identify members of a group:
  - More comparisons than verification but fewer than identification, so the risk of a false acceptance is intermediate
  - If the probability of a false acceptance (false match) is 1/1,000 per template match,
    - and if there are 10 templates in the watch list, then
    - the probability of a false acceptance is 10 * 1/1,000 (1%)

# Biometric Authentication

- Fingerprint Recognition
  - Simple, inexpensive, well proven
  - Most biometrics today are fingerprint recognition
  - Often can be defeated with latent fingerprints on glass copied to gelatin fingers
  - Fingerprint recognition can take the place of reusable passwords for low-risk applications

# Biometric Authentication

- Iris Recognition
  - Pattern in colored part of eye
  - Uses a camera (no light is shined into eye, as in Hollywood movies)
  - Very low FARs
  - Very expensive

# Biometric Authentication

- Face Recognition
  - Surreptitious identification is possible (in airports, etc.)
  - Surreptitious means without the subject's knowledge
  - High error rates, even without deception
- Hand Geometry for Door Access
  - Shape of hand
  - Reader is very large, so usually used for door access

# Biometric Authentication

- Voice Recognition
  - High error rates
  - Easily deceived by recordings
- Other Forms of Biometric Authentication
  - Veins in the hand
  - Keystroke recognition (pace in typing password)
  - Signature recognition (hand-written signature)
  - Gait (way the person walks) recognition

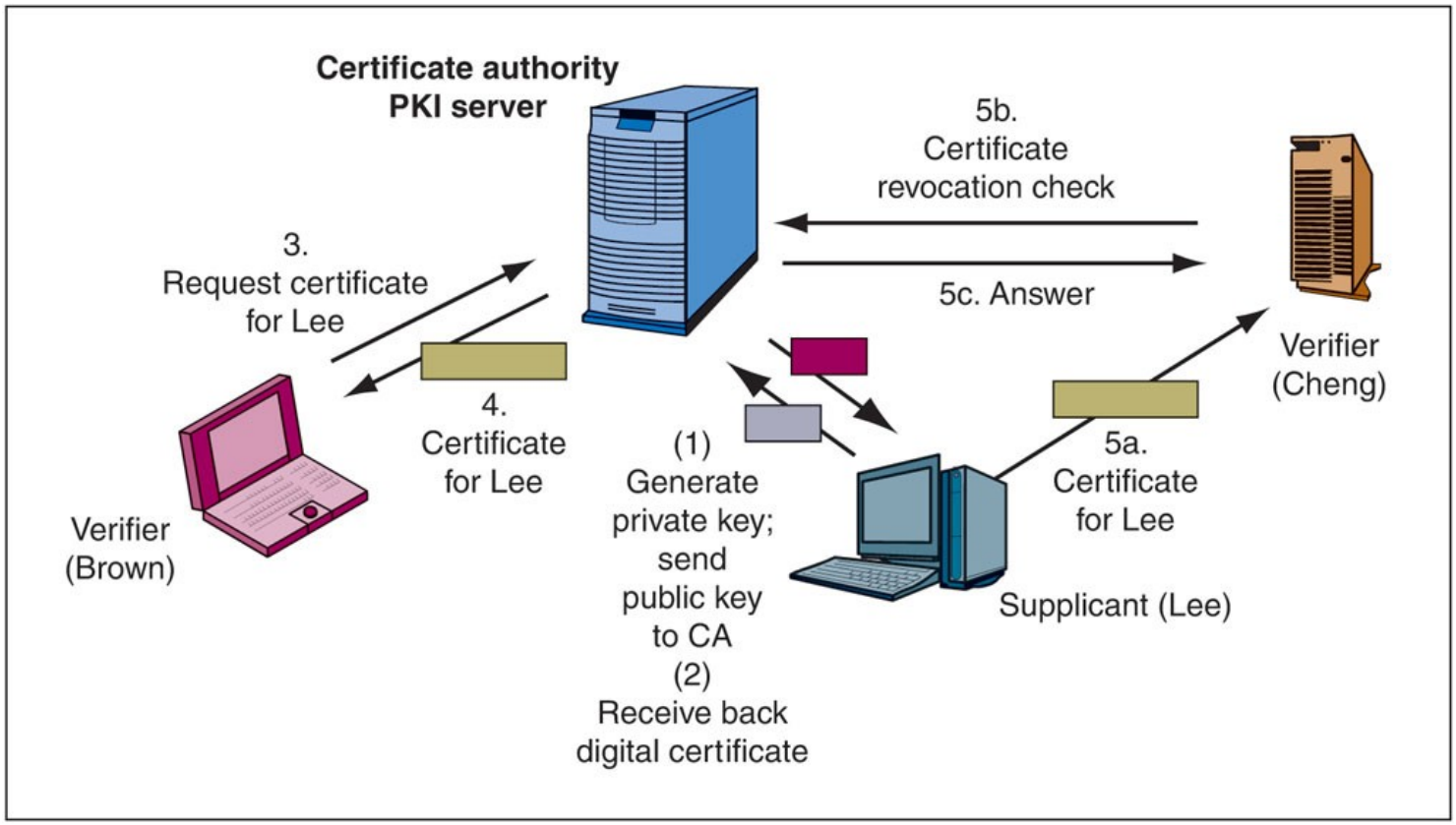
# Cryptographic Authentication

- Public Key Infrastructures (PKIs)
  - Firms can be their own certificate authorities (CAs)
  - Requires a great deal of labor
  - Provisioning
    - Giving the user access credentials

# Cryptographic Authentication

- Public Key Infrastructures (PKIs)
  - Provisioning
    - Human registration is often the weakest link
      - If an impostor is given credentials, no technology access controls will work
      - Limit who can submit names for registration
      - Limit who can authorize registration
      - Have rules for exceptions
    - Must have effective terminating procedures
    - Supervisors and Human Resources department must assist

# Functions of a Public Key Infrastructure (PKI)



# Authorization

- Authorizations
  - Authentication: Proof of identity
  - Authorization: The assignment of permissions  (specific authorizations) to individuals or roles
  - Just because you are authenticated does not mean that you should be able to do everything

# Authorization

- Principle of Least Permissions
  - Initially give people only the permissions a person absolutely needs to do his or her job
  - If assignment is too narrow, additional permissions may be given
  - System has permissions A, B, C, D, E, and F
  - This will frustrate users somewhat

# Authorization

- Giving Extensive or Full Permissions Initially Is Bad
  - User will almost always have the permissions to do his or her job
  - System has permissions A, B, C, D, E, and F
  - Assignments can be taken away, but this is subject to errors
  - Such errors could give excessive permissions to the user
  - This could allow the user to take actions contrary to security policy
  - Giving all or extensive permissions and taking some away does not fail safely

# Auditing

- Auditing
  - Authentication: Who a person is
  - Authorization: What a person may do with a resource
  - Auditing: What the person actually did
- Logging
  - Events
  - On a server, logins, failed login attempts, file deletions, and so forth
  - Events are stored in a log file

# Auditing

- Log Reading
  - Regular log reading is crucial or the log becomes a useless write-only memory
  - Periodic external audits of log file entries and reading practices
  - Automatic alerts for strong threats

# Full Identity Management

- Definition
  - Identity management is the centralized policy-based management of all information required for access to corporate systems by a person, machine, program, or other resource

# Full Identity Management

- Benefits of Identity Management
  - Reduction in the redundant work needed to manage identity information
  - Consistency in information
  - Rapid changes
  - Central auditing
  - Single sign-on (SSO)
    - Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials, for example, a name and password to access multiple applications.
    - With SSO, a user only has to enter their login credentials (username, password, etc.) one time on a single page to access all of their SaaS applications.
  - Increasingly required to meet compliance requirements

# Reference

Chapter 5

Corporate Computer Security, 5th Edition Boyle R.J. & Panko R. R. by Pearson

# Copyright