# Chapter 2:
# Access Control and Site Security

**ACIS 5584 E-Commerce Security**

**Dr. France Belanger**

**Panko, Corporate Computer and Network Security**



## Access Control

- **Definitions**
  - Access control is the policy-driven limitation of access to systems, data, and dialogs
- **What to control?**
- **Who should have access?**
- **What can they do?**



## Access Control

- **Elements of Access Control**
  - User authentication:
    - whether a role or individual should have any access at all
  - User authorization:
    - exactly what the role or individual should be allowed to do to the resource.

## Access Control Tools

- **Physical access control**
  - Locks, monitoring tools, personnel, etc.
- **Logical access control**
  - User profiles (IDs and passwords)
  - Firewalls (Chapter 5)
  - Biometrics



## Physical Access Control: Building Security Basics

- **Single point of (normal) entry to building**
- **Fire doors with closed-circuit television (CCTV) and alarms**
- **Security centers**
- **Interior doors: avoid piggybacking**
- **Training security personnel AND employees**
- **Dumpster diving**
- **Drive shredding programs for discarded disk drives that do more than reformat drives**
- **Data Wiring Security**



## Physical Access Control: Access Cards

- **Technologies**
  - Magnetic Stripe Cards
  - Smart Cards
  - Tokens
- **Card Cancellation**
  - Requires a central system
- **PINs**
  - Can be short
  - Provide two-factor authentication (PIN + card)

## Access Control Tools

- **Physical access control**
  - Locks, monitoring tools, personnel
- **Logical access control**
  - User profiles (IDs and passwords)
  - Firewalls (Chapter 5)
  - Biometrics



## Logical Access Control: User Profiles:

- **Cracking Passwords Difficult**
- **Hacking Super accounts**
  - UNIX: Hacking root
  - Windows: administrator
  - NetWare: supervisor
  - Hacking root rare; usually can only hack ordinary user account
  - May elevate privileges of user account to take root action



## Physical Access Password Cracking

- **10phtcrack**
- **Brute-force password guessing**
  - Alphabet, without case is fast
  - Alphabet, with case takes much longer
  - Alphanumeric (letters and digits) takes longer still
  - All keyboard characters takes longest of all
- **Dictionary attacks**
  - Try common words, or all words. Several languages
  - There are only a few thousand of these
  - Very rapidly cracked
- **Hybrid attacks**
  - Common word with single digit at end, etc.

## Figure 2-3: Password Length

| Password Length In Characters | Alphabetic, No Case (N=26) | Alphabetic, Case Sensitive (N=52) |
|---|---|---|
| 1 | 26 | 52 |
| 2 | 676 | 2,704 |
| 4 | 456,976 | 7,311,616 |
| 6 | 308,915,776 | 19,770,609,664 |
| 8 | 2.08827E+11 | 5.34597E+13 |
| 10 | 1.41167E+14 | 1.44555E+17 |



## Figure 2-2: Password Length

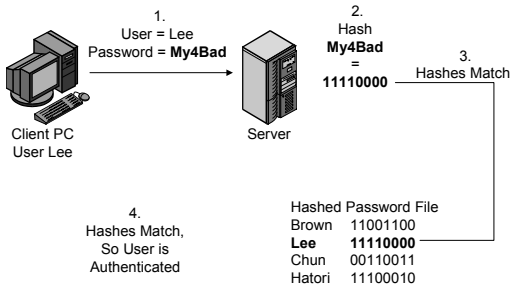
| Password Length In Characters | Alphanumeric: Letters And Digits (N=62) | All Keyboard Characters (N=80) |
|---|---|---|
| 1 | 62 | 80 |
| 2 | 3,844 | 6,400 |
| 4 | 14,776,336 | 40,960,000 |
| 6 | 56,800,235,584 | 2.62144E+11 |
| 8 | 2.1834E+14 | 1.67772E+15 |
| 10 | 8.39299E+17 | 1.07374E+19 |



## Password Policies

- Password duration
- Password sharing
- Disabling passwords no longer valid
- Lost passwords (password resets) issues
  - Opportunities for social engineering attacks
  - Leave changed password on answering machine
  - Automated password resets (easily-guessed questions)
- Testing and enforcing password policies

## Figure 2-4: Password Hashing [Encryption]






## UNIX/etc/passwd File Entries

*Without Shadow Password File*

User Name | User ID | GCOS | Shell

**plee:6babc345d7256:47:3:Pat Lee:/usr/plee/:/bin/csh**

Password | Group ID | Home Directory

*With Shadow Password File*

**Plee:x:47:3:Pat Lee:/usr/plee/:/bin/csh**

Asterisk instead of x indicates that the password is stored in a separate shadow password file



## Password Policies (Cont.)

- **Windows passwords**
  - Obsolete LAN manager passwords (7 characters maximum) should not be used
  - Windows NTLM (NT LAN Manager) passwords are better
  - Option (not default) to enforce strong passwords
- **Avoid Shoulder Surfing**
- **Check for Keystroke Capture Software**
  - Professional versions of windows protect RAM during password typing
    - Consumer versions do not
  - Trojan horse throws up a login screen later, reports its finding to attackers

## Windows Client PC Software

- BIOS passwords allow boot-up security
  - Can be disabled by removing battery
- Screen savers with passwords allow away-from-desk security
- Windows professional provides some security with required login

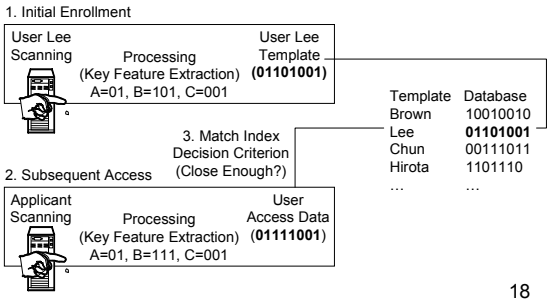


## Logical Control: Biometrics

- **Biometric Authentication**
  - Based on body measurements and motions
- **Biometric Systems (Figure 2-10)**
  - Enrollment
  - Later access attempts
  - Acceptance or rejection



## Figure 2-10: Biometric Authentication System



## Figure 2-9: Biometric Authentication

- **Verification Versus Identification**
  - Verification: Are applicants who they claim to be? (compare with single profile)
  - Identification: Who is the applicant? (no claim of identify; compare with all profiles stored)
    - More difficult than verification
  - Verification is good to replace passwords in logins
  - Identification is good for door access (no need to enter ID)



## Figure 2-9: Biometric Authentication

- **Precision**
  - False acceptance rates (FARs): Percentage of unauthorized people allowed in
  - False rejection rates (FRRs): Percentage of authorized people rejected
  - Vendor claims tend to be exaggerated through tests under ideal circumstances
- **User Acceptance is Crucial**
  - Fingerprint recognition has a criminal connotation
  - Some methods difficult to use, require disciplined group



## Figure 2-9: Biometric Authentication

- **Biometric Methods**
  - Fingerprint recognition
    - Simple, inexpensive, well-proven
    - Can be defeated with copies
  - Iris recognition
    - Very low FARs
    - High FRR rate can harm acceptance
  - Signature recognition
    - Pattern and writing dynamics

## Figure 2-9: Biometric Authentication

- **Biometric Methods**
  - Face recognition
    - Can be in public places for surreptitious identification
  - Hand geometry
  - Voice recognition
  - Keystroke recognition
    - Rhythm of typing
    - Normally restricted to passwords



## Figure 2-9: Biometric Authentication

- **Biometric Standards**
  - Poor standardization (ltd interoperability)
- **Biometrics Effectiveness**
  - Airport face recognition mostly has false positives
    - 4-week face recognition trial at Palm Beach International Airport
    - Scanned 958 times; Only recognized 455 times
    - Recognition rate fell if wore glasses (especially tinted), looked away
    - Would be worse with larger database (250 pictures)
    - Would be worse if photographs were not good



## Figure 2-9: Biometric Authentication

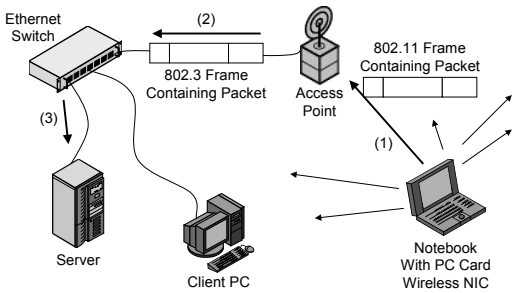
- **Can Biometrics be Fooled?**
  - DOD 270-person test indicates poor acceptance rates when subjects not attempting to evade
    - Face recognition recognized person only 51 percent of time and Iris recognition only 94 percent of the time.
  - Other research: evasion often successful for some methods
    - German magazine fooled most face & fingerprint recognition systems
    - Prof. Matsumoto fooled fingerprint sensors 80% of time with gelatin finger created from latent print on a glass

## Biometrics Authentication

- **The Revocation Problem**
  - What happens if the database template for a person is stolen?
  - Cannot base design on confidentiality of the database

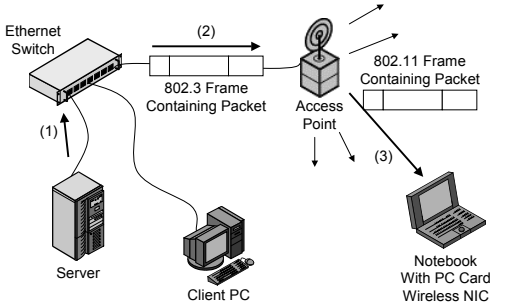


## Wireless LAN (WLAN) Security: 802.11 Wireless LAN






## 802.11 Wireless LAN



## Multiple 802.11 Standards

| Standard | Rated Speed (a) | Unlicensed Radio Band | Effective Distance (b) |
|---|---|---|---|
| 802.11b | 11 Mbps | 2.4 GHz | ~30-50 meters |
| 802.11a | 54 Mbps | 5 GHz | ~10-30 meters |
| 802.11g | 54 Mbps | 5 GHz | ? |

Notes: (a) Actual speeds are much lower and decline with distance. (b) These are distances for good communication; attackers can read some signals and send attack frames from longer distances.

28

## Wireless LAN (WLAN) Operations

- **Uses Spread Spectrum transmission**
  - Signal spread over a broad range of frequencies
    - Methods used by military are hard to detect
    - But in 802.11 does not provide security
    - 802.11 methods easy to detect so devices can find each other; used to prevent frequency-dependent propagation problems rather than for security
- **SSIDs (service set identifier)**
  - Mobile devices must know access point's SSID

29

## Wired Equivalent Privacy (WEP)

- **Early WLAN security**
- **Not enabled by default!!**
- **Uses 40-bit or 128-bit encryption keys**
  - 40-bit too small; 128-bit OK
- **Uses shared passwords (All stations – AP)**
  - Difficult to change, so rarely changed
- **Flawed security algorithms**

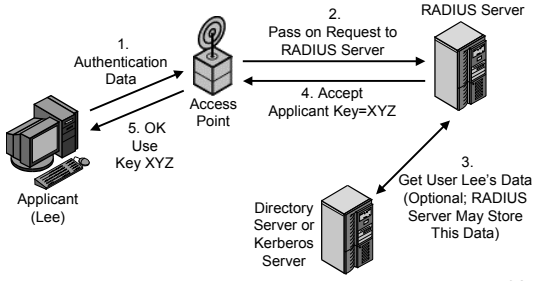
30

## 802.1x and 802.11i (Figure 2-14)

- **Basic Operations**
  - Authentication server: access decisions
  - User data server: holds data on individuals
  - Access point: gives out individual keys for secure exchange
- **Authentication:**
  - Uses Extensible Authentication Protocol (EAP)
    - Offers many options for authentication
      - (MD5 CHAP, TLS, TTLS)



## Figure 2-14: 802.1x Authentication for 802.11i WLANs






## Assignments

- **Thought Questions 2 and 4**