Learning Objectives

After completing this module, you should be able to:

- Recognize the purposes of entry control
- Identify the fundamental criteria of entry control
- List some of the advantages and disadvantages of coded credentials
- Discuss the most common types and use of biometrics
- Recognize the features of a good entry control system
INFCIRC/225/Revision 5

• 4.17 Technical means and procedures for access control, such as keys and computerized access lists, should be protected against compromise
• 4.26 Effective access control measures should be taken to ensure the detection and prevention of unauthorized access
• 4.27 The identity of authorized persons entering the protected area should be verified. Passes or badges should be issued and visibly displayed inside the protected area

Purposes of Entry Control

• A perimeter security system is designed to provide a boundary around each protection area to prevent or detect unauthorized penetrations
• Entry control is designed to allow authorized persons and materials to move in and out through that boundary in a balanced secure way
• The system must:
  ▪ Allow entry of authorized persons
  ▪ Prevent entry of unauthorized persons
  ▪ Allow exit of authorized persons
Definitions for Entry Control

**Access Authorization:** An administrative determination that an individual is eligible for access to enter a secure area or to access a secure cyber space. For instance, he/she is eligible to enter an area where nuclear materials are stored or where classified material is stored.

**Badge:** Credential an individual is provided once access authorization is determined.

**Verification:** Determination of access authorization at the entry control point:
- Accepts authorized persons
- Rejects unauthorized persons

Basis of Personnel Entry Control

- **Something you know**
  - Personal Identification Number (PIN)
  - Password

- **Something you have**
  - Key
  - Credential

- **Something you are**
  - Biometric feature (e.g., fingerprints)
Types of Personnel Entry Control

Personnel Authorization Verification

Manual (Protective Force Guards)
- Have - Credential (Photo)
- Exchange Credential

Automated (Machines)
- Have - Credential (Coded)
- Know - Memorized Number (PIN)
- Are - Personal Characteristics (Biometric)

Combination of Criteria
- Combining two or all three factors greatly increases security

- Badge swipe and PIN
- Hand-geometry Biometrics
Personal Identification Numbers (PINs)

- Easy to use if not more than 6 digits
- Disadvantages
  - Employee may forget the number
  - Employee may write it down
  - Adversary may obtain it or guess it
- Best used with other types of verification

Types of Credentials

- Verified by protective force guards
  - Take-home photo credential
    - Photo compared to individual
    - Photo compared to photo in database
  - Exchanged photo credential
- Verified by machine
  - Coded credential
  - Best used with other types of verification
Badge Exchange System

- The badge exchange system relies on two credentials
- One credential is take-home while the other stays within the secure area
- These credentials must look different

Take-Home | Exchange

Personnel Credentials

- Coded Credentials
  - Bar Code
  - Magnetic Stripe
  - Weigand
  - Proximity
  - "Smart"

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Controls access by area and time</td>
<td>● Identifies badge, not person</td>
</tr>
<tr>
<td>● Logs each access (or exit)</td>
<td>● Requires maintenance</td>
</tr>
<tr>
<td>● Has low false rejection rate</td>
<td>● May be defeated by counterfeit badge</td>
</tr>
<tr>
<td>● Performs consistently</td>
<td></td>
</tr>
</tbody>
</table>
Characteristics of Bar Code

- Image of varying width lines (bars) and spaces
  - Linear barcode or one-dimensional (1D)
  - Two-dimensional (2D) barcode
- Commonly used
- Easy to make
- Disadvantage
  - Susceptible to reproduction

1D Bar Code  
2D Bar Code

Characteristics of Magnetic Stripe Badges

- Polarized magnetic particles, similar to cassette tape
- Widespread use, as on credit cards
- Easy to use
- Easy to make
- Disadvantage
  - Erased by common magnet
Characteristics of Wiegand Cards

- Uses series of embedded wires with special magnetic properties
- Widespread use, output format is an industry standard
- Easy to use, card is read via a “swipe” action similar to magnetic stripes
- More difficult to make

Characteristics of Proximity Badges

- Radio Frequency identification card
  - Induction powered
  - Coded RF transmitter
- Widespread use
- Easy to use
  - Hands free operation
  - Compatible with protective clothing
- Purchased, not made at site
  - Options for programming
    - Pre-programmed
    - Programmed at site
- Disadvantage
  - Multiple badges in range of reader
Characteristics of Smart Cards

- Credit-card-sized device with microcomputer
  - Allows storage of identification information, including
    - PIN / password
    - Biometric template
  - Some capable of encrypting data
  - Contact or contactless
  - May include magnetic stripe and/or barcode
- Increasing use
- Usually not made onsite

Verification vs. Recognition

- Most biometric systems verify identity
  - You claim to be someone by presenting a card or PIN
  - The system compares the recorded template with the live biometric (one-to-one)
- Some biometric systems recognize you
  - No claim of identity is made
  - The system searches through its entire database to find a match (one-to-many)
# Biometric Verification

<table>
<thead>
<tr>
<th>Type</th>
<th>Use</th>
<th>Verification or Recognition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>Common</td>
<td>Verification</td>
</tr>
<tr>
<td>Hand geometry</td>
<td>Common</td>
<td>Verification</td>
</tr>
<tr>
<td>Iris pattern</td>
<td>Not common</td>
<td>Recognition or Verification</td>
</tr>
<tr>
<td>Voice</td>
<td>Not common</td>
<td>Verification</td>
</tr>
<tr>
<td>Face</td>
<td>Not common</td>
<td>Verification</td>
</tr>
<tr>
<td>Finger Vein pattern</td>
<td>New</td>
<td>Verification</td>
</tr>
</tbody>
</table>

## Fingerprint Identity Verification

- Captures the ridges and valleys of the fingerprint

### Fingerprint Capture Methods

- **Ultrasonic Capture**
- **Solid State Capture**
- **Video Capture**
Hand Geometry Identity Verification

• Uses CCD camera to image hand using near infrared illumination

Iris Identity Verification or Recognition

• Video camera captures image of the iris
• Iris structure is highly unique to an individual
Voice Recognition Identity Verification

- Uses microphone to collect a spoken phrase

Facial Identity Verification

- Uses cameras to capture facial features
- Special cameras

Thermogram

Two Dimensional

Two Dimensional with Parallax

Three Dimensional
Blood Vein Identity Verification

- Images the vein pattern on finger, palm, or the back of the hand

Factors Impacting Biometric Capture

<table>
<thead>
<tr>
<th>Environmental Factors</th>
<th>Personnel Characteristic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lighting—Both artificial and natural</td>
<td>Fingerprint: Cold, dry, oily, cuts</td>
</tr>
<tr>
<td>Dust and debris</td>
<td>Face: Hair, glasses, light, clothing, camera, presentation</td>
</tr>
<tr>
<td>Background noise</td>
<td>Hand: Jewelry, bandages, weight change</td>
</tr>
<tr>
<td>Electromagnetic noise</td>
<td>Eye: Glasses, head movement,</td>
</tr>
<tr>
<td></td>
<td>Voice: Speaker volume, illness</td>
</tr>
</tbody>
</table>

Picture courtesy of Hitachi Finger Vein Products
Levels of Entry Control

<table>
<thead>
<tr>
<th>Level</th>
<th>Verification</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>One type</td>
<td>Credential OR PIN OR Biometric</td>
</tr>
<tr>
<td>2</td>
<td>Two Types</td>
<td>Credential AND PIN OR Credential AND Biometric OR Biometric AND PIN</td>
</tr>
<tr>
<td>3</td>
<td>Three Types</td>
<td>Credential AND PIN AND Biometric</td>
</tr>
</tbody>
</table>

Features of Biometric Systems

- **Ease of Integration**
  - A factor of how many different systems support a specific technology and if the biometric has a flexible system interface
- **Verification times**
  - 2 to 20 seconds
- **Enrollment**
  - 1% to 3% of population is incompatible
  - 30 seconds to 10 minutes required to enroll
- **Cost**
  - $1,000 to $5,000 per terminal
Personnel Entry Control Errors

- Performance - Expressed as error rates associated with the specific technology
  - False rejection
    - Authorized persons are not allowed to enter
    - A small number may be an acceptable trade-off for high security situation
    - Easy to quantify
  - False acceptance
    - Unauthorized persons are allowed to enter
    - A small number may be an acceptable trade-off for low security situation
    - Difficult to quantify

Characterizing Error Rates

![Error Rates Graph]
Features of a Good Entry Control System

- Integration with boundary
  - Cannot be bypassed
  - Block individuals until access authorization verified
  - Interfaces with the alarm system
- Integration with the guards/response force
  - Protects guard
  - Area is under surveillance
- Personnel integrate with system
  - Easy to use for entry and exit
  - Accommodates peak throughput (loads)
  - Accommodates special cases

Application of Good Design Criteria

- Turnstiles with card readers and PIN pads
- CCTV Camera
- Metal Detectors
- Secondary Inspection Area
- Hardened Guard Booth
Summary

• The purpose of entry control is to allow authorized persons to move in and out through a protected area boundary
• Entry control verification techniques depend on verifying what you: Know, Have, and Are
• Biometric systems verify who you are by means of a unique physical characteristic, such as fingerprint or hand geometry
• A good entry control system addresses interface with the protected area boundary, the guard force, and personnel