

Physical Threats & Protecting the Information Infrastructure

CSH5 Chapters 22 & 23

“Physical Threats to the Information Infrastructure” & “Protecting the Information Infrastructure”

Franklin Platt



1

Copyright © 2011 M. E. Kabay. All rights reserved.

Selected Topics in Facilities Security (1)

- Location of building
- Location within building
- Layout
- Doors
- Windows
- Electrical power supply
- Air conditioning
- Electromagnetic radiation
- Fire detection and prevention
- Water damage

NOTE:

These lecture notes do *not* correspond to the content or sequence of material in CSH5 Chapters 22 & 23



2

Copyright © 2011 M. E. Kabay. All rights reserved.

Location of Building

If possible, safe area: avoid

- Earthquakes
- Tornadoes
- Hurricanes
- Civil unrest
- Gasoline storage
- Aircraft flyways
- Train tracks
- Heavily-traveled highways (esp. raised)



3

Copyright © 2011 M. E. Kabay. All rights reserved.

Location of Building (cont'd)

- Ensure dual access paths
 - Fire emergency teams
 - Ambulances
 - Police
- If possible, avoid labeling building function
- Avoid forcing outside lineups of staff at starting time

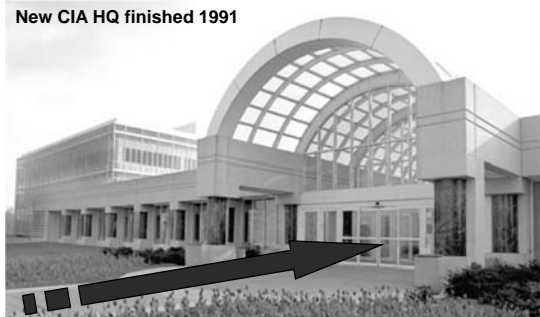


4

Copyright © 2011 M. E. Kabay. All rights reserved.

Building Design (1)

- Defend against car/truck bombs
 - ❑ Avoid large areas of unprotected glass at ground level
 - ❑ Place obstructions at entranceways
 - ✓ Anchored planters
 - ✓ Reinforced seats



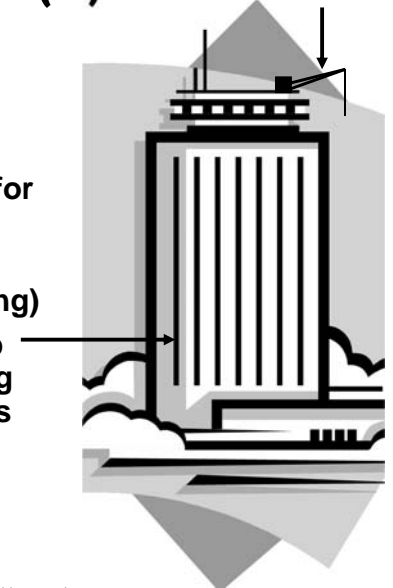
New CIA HQ finished 1991

Copyright © 2011 M. E. Kabay. All rights reserved.

5

Building Design (2)

- Provide for entry of large equipment
 - ❑ roof cranes
 - ❑ Wide or double doors for technical areas
- Eliminate large chases (indents on side of building)
 - ❑ Make it harder to climb building using climbing equipment / techniques



Copyright © 2011 M. E. Kabay. All rights reserved.

6

Location Within Building

- Access to building affects computer room security
- Involve EDP security staff in design of new building
- No external walls
- Inconspicuous yet allowing easy access for fire department
- Far from hazardous areas

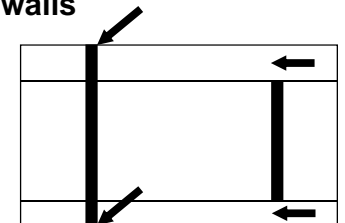


Copyright © 2011 M. E. Kabay. All rights reserved.

7

Layout

- Separate functions
- Tape vaults/safes
- Security equipment in secure, separate room
- Rest rooms, food areas near center
- Substantial walls
- Avoid closets in common walls
- Slab-to-slab construction:
- Make provision for secure but effective maintenance access

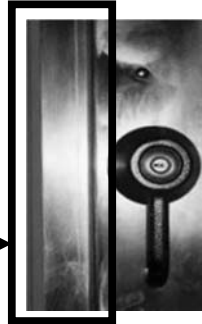


Copyright © 2011 M. E. Kabay. All rights reserved.

8

Doors

- As few as possible
- Formal exiting study to set minimum
- Put alarms and signs on doors which are not essential during normal work
- Solid wood or metal (avoid glass: 64% burglaries through glass)
- Secure frames
- Hidden or inward hinges
- Non-removable hinge pins
- Astragals (protector on door edge)



Windows

- None! Cover with bricks if facing outside
- Eliminate internal *vision panels*
- If impossible, at least move security equipment out of sight
- Cover sensors in room during visitor tours
- Security glazing
- Gratings, bars, fastenings
- Breakage sensors connected to alarm system
- Closed circuit TV monitoring motion sensors



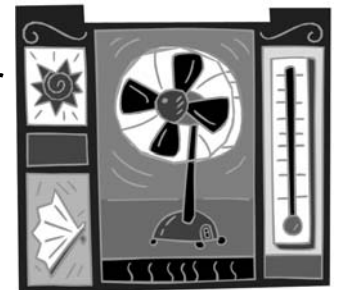
Electrical power supply

- Disturbances: monitors, power conditioners
- Outages: UPS, motor alternator w/ flywheel, battery/rectifier, diesel generators (fuel)
- Plan for peak load, minimum time required, graceful shutdown
- Emergency lighting (fixed, portable)
- Protect electrical equipment from tampering



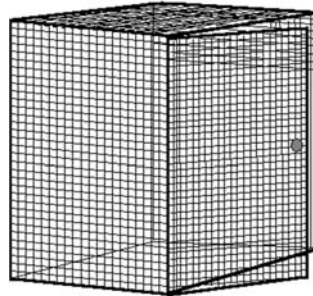
Air Conditioning

- Protect external air intakes for air conditioners
 - ❑ Susceptible to gas attack "or disabling"
- Temperature ~21C +/- 2C
- Humidity ~50% +/- 5%
- Positive pressure
- Risks: dust, condensation, curling paper, static charge
- Keep computer air conditioning separate from that of rest of building
- Non-combustible ducts
- Link to fire suppression system (auto shutoff)



Electromagnetic Radiation

- Magnets
 - ❑ Bulk tape erasers
 - ❑ Speakers on sound systems
- Radio transmitters
 - ❑ (e.g., nearby public radio or TV stations)
 - ❑ Walkie-talkies
 - ❑ Cellular (mobile) phones are a threat
- Aluminum mesh if needed on windows (if any) to create *Faraday cage*



Faraday cage

13

Copyright © 2011 M. E. Kabay. All rights reserved.

Fire Prevention & Detection (1)

- Keep DP separate from rest of building if possible
- Non-combustible materials in walls
- Restrict openings in walls
- Self-closing fire enclosures
- Duct work, cables to be cemented into walls w/ fire-resistant materials
- Appropriately placed smoke, heat detectors
- Full-time monitoring and alerts by *trained people*



14

Copyright © 2011 M. E. Kabay. All rights reserved.

Fire Detection and Prevention (2)

- Fire-resistant raised floors
- Suction cups handy



15

Copyright © 2011 M. E. Kabay. All rights reserved.

Fire Detection and Prevention (3)

- Detectors in suspended ceilings
- Systems approach integrates information from multiple sensors
- HALON systems forbidden because of laws on environmental protection passed in 1990s
- Keep combustibles (e.g., paper) out of computer room
- Best system in world is useless without trained staff: *practice fire drills*



16

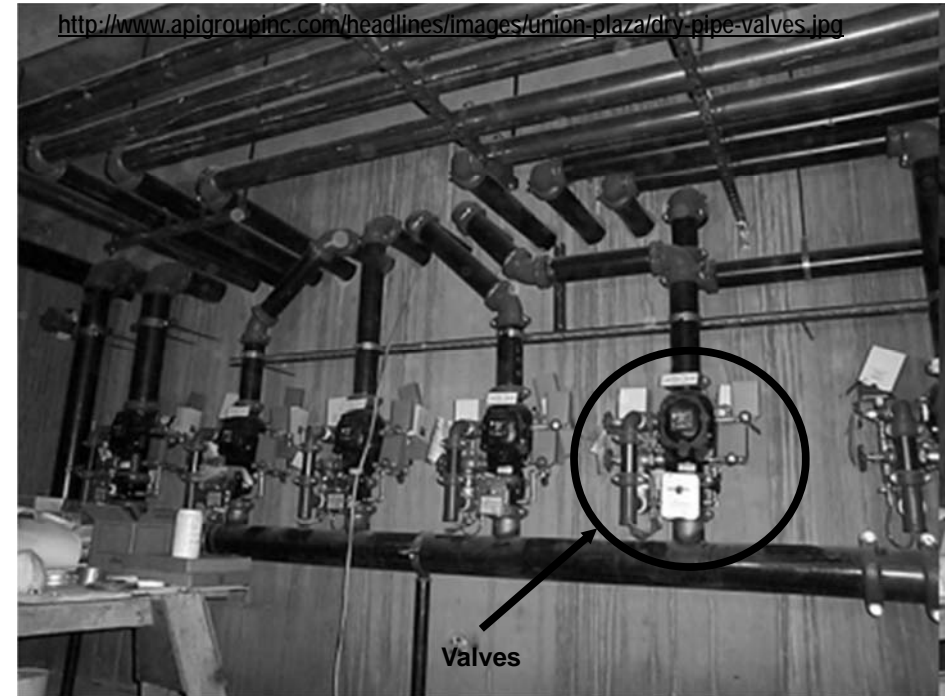
Copyright © 2011 M. E. Kabay. All rights reserved.

Water Damage

- Install water detectors below raised flooring
- Link water detectors to building's central alarm systems
- Use dry-pipe sprinkler systems (see also large picture next page)
- Floors above computer room to be waterproof
- Install rolls of non-flammable plastic sheets ready to cover equipment against water



Copyright © 2011 M. E. Kabay. All rights reserved.



Selected Topics in Facilities Security (2)

- Guards, Gates and Guns
- Surveillance
- Access Controls
- Protective Technologies



Copyright © 2011 M. E. Kabay. All rights reserved.

Guards, Gates and Guns



Guards



- Usually contractors
 - ❑ Choose companies with bonded employees
- Define expectations / policies clearly
- Train extensively & rehearse emergencies
- Monitor performance – no exceptions, no tailgating
- Teach to examine outbound equipment
 - ❑ Become aware of high-density storage media such as flash drives

21

Copyright © 2011 M. E. Kabay. All rights reserved.

Fences

- Primarily for delay
- Psychological barrier
- Serious assailant not deterred
- Improvements: barbed wire, razor wire, electrification
- Surveillance essential (see later)

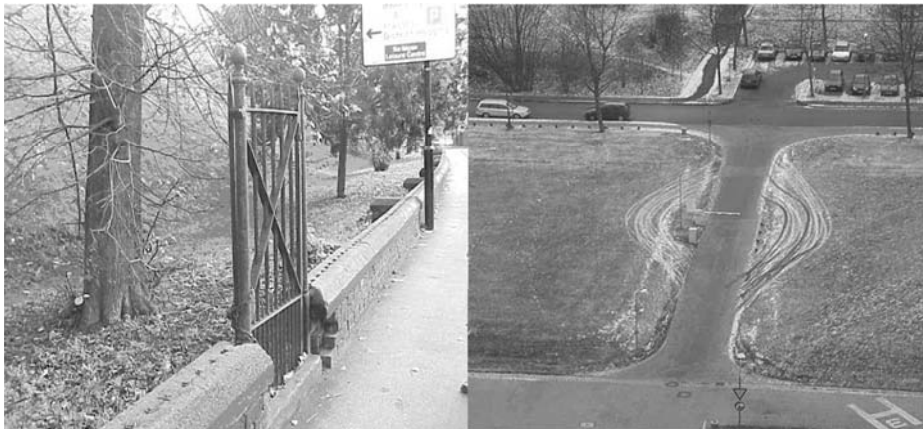


22

Copyright © 2011 M. E. Kabay. All rights reserved.

Gates

- Gates cannot compensate for weak perimeter:



- Some secure installations have double gates (external and internal)

23

Copyright © 2011 M. E. Kabay. All rights reserved.

Other Barriers

- Obstruct penetration by bombers
 - ❑ Concrete pillars in front of entrances or other weak points (as mentioned in part 1)
 - ❑ Prevent stopping / parking in front of buildings (seal of access roads)
- Slow down attack vehicles – zig-zag barriers
- High-security installations have guards who check vehicles inside and out
 - ❑ All passengers out for positive ID and verification of authorized business
 - ❑ Mirrors to look under vehicles



Mayur Industrial Corp.
Under-Vehicle Bomb Search Mirrors
<http://preview.tinyurl.com/nz2jhe>

24

Copyright © 2011 M. E. Kabay. All rights reserved.

Weapons

- Armed guards require special training & licensing
 - ❑ Much more expensive than ordinary guards
- High-security government installations use military forces
 - ❑ High-powered personal weapons (e.g., machine guns)
 - ❑ Artillery (armored vehicles, RPGs)



Surveillance

- Cameras more effective than watchmen alone
 - ❑ Motion detectors + digital recorders
 - ❑ Must protect recording equipment
 - ❑ Archive tapes/disks safely and for > 1 month
- Guards must monitor activity carefully
- Ethical and legal issues about *concealed* cameras
- May use *dummy* cameras among real ones
 - ❑ Deception is tool of good security

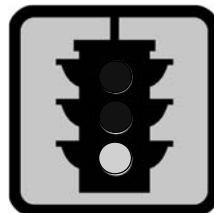
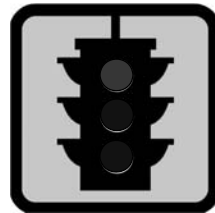


Dummy camera



Access Controls

- Principles
- Mechanical Locks
- Keypads
- Features of Electronic Access Control Systems
- Cards
- Biometric Methods



Access Control Principles

- Normally only one controlled, monitored access point
- Audit trail is valuable
- Staff responsibilities
 - ❑ Wear badges in restricted areas
 - ❑ Accompany visitors
 - ❑ Challenge unbadged people and call security at once
- Put in positive light: protect employees against trouble, disruption, loss of business, loss of employment
- Apply rules even handedly and consistently to avoid doubts about individual's integrity

Mechanical Locks

- Appropriate only for small sites
- Infrequent use (2-3 times/day)
- Beware wedges and tape blocking doors open
- Keys easily duplicated
 - ❑ Many unregistered locksmiths (e.g., hardware store clerks) ignore DO NOT DUPLICATE warnings
- Cannot be individually inactivated
- Loss of a master key can cost \$1000s to replace ALL keys in set for everyone
- Special locks (e.g., Abloy) more secure



Michael Zemanek 2012:
Key covers obscure
DO NOT DUPLICATE

Keypads

- Fixed keypads must be secured against observation (e.g., by sleeve over keypad)
- Be sure you can set multiple-key combinations
- Variable-position keypads harder to read by observers
- Watch out for patterns of wear that would give away smaller key space



Features of Electronic Access-Control Systems

- Antipassback (system remembers who's in area)
- Time-open limit (alarms for doors kept open)
- Duress signal (e.g., Putting in card upside down)
- Degraded mode (if CPU goes down)
- Audit features (records of movements, violations)
- Computer-room alarms linked to building alarms
- Building alarms audible in computer room



Image used with permission of
United Security Systems Inc.
<http://www.ussinational.com>

Cards

- Wiegand: wires generate magnetic pulses

HID Wiegand cards

SENSORCARD WIEGAND

SensorCard Wiegand uses Wiegand Wire, a highly-secure technology which uses short lengths of special alloy wire on a unique strip which is embedded in the card's core. Wiegand is virtually impossible to counterfeit, cannot be altered and is immune to external magnetic fields or RF interference. Databac is a certified manufacturer of Wiegand cards. SensorCard Wiegand can be printed using direct card printers. It has a two-year warranty.

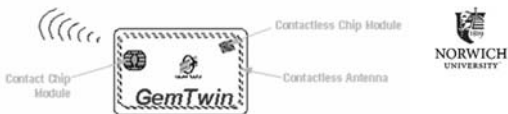
Code: HID-1201

[View spec sheet](#)

- Barium ferrite: polarized magnetic fields
- Bar codes
- Infrared-readable embedded bar codes
- Magnetic stripe
- Proximity (radio frequency signatures)



Smart Cards



- Include microprocessor
- Can serve as I&A unit
- Also for digital signatures
- Interact with software
- Many *form factors*
 - ❑ Cards
 - ❑ Cards with keypads for PINs
 - ❑ Calculators
 - ❑ USB keyfob



Biometric Methods

- Hand geometry
- Fingerprints
- Retinal scan
- Iris scan
- Face recognition
- Voice verification
- Signature dynamics
- Keystroke dynamics
- Weight/height cabinets
- Combinations even more effective



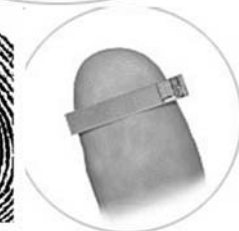
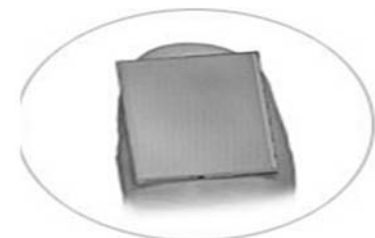
Hand Geometry

- Easy to use
- No need for tokens, cards
- Extremely low errors
 - ❑ Few false positives (allowing wrong person in)
 - ❑ Few false negatives (preventing right person from entering)
- Contrary to movies, does NOT respond to dead hands!



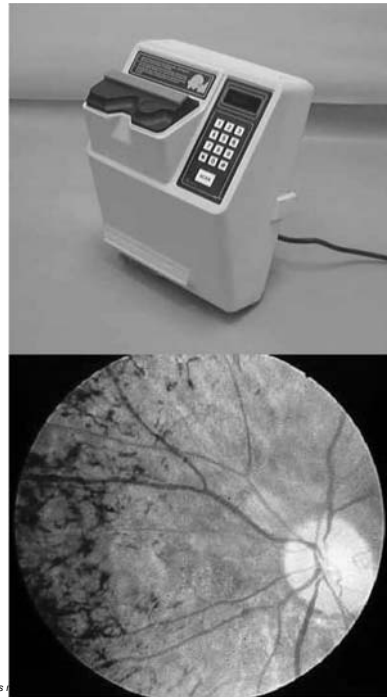
Fingerprints

- High accuracy*
- Sensors available for static image (middle image) and also for dynamic swipe (lower image)
- *But Japanese scientists showed that fake fingers easy to create from fingerprints
 - ❑ Used crazy glue to enhance ridges
 - ❑ *Gummy Bears* candy
 - ❑ Fooled sensors 80%



Retinal Scan

- Viewed with suspicion by general public
- Hygiene issues due to physical contact with sensor sleeve
- Highly reliable
- As with all biometric systems, data generally stored in *one-way* encrypted form

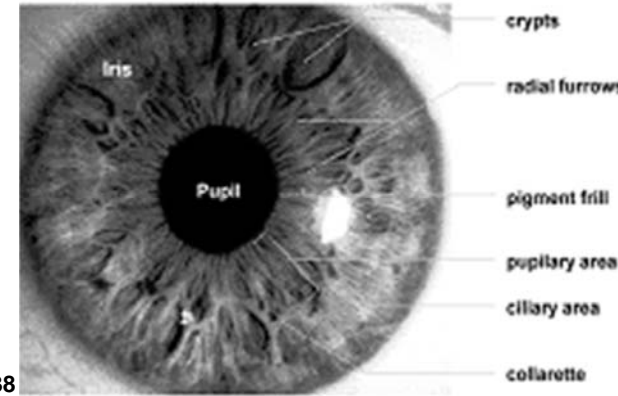


37

Copyright © 2011 M. E. Kabay. All rights reserved.

Iris Scan

- Highly reliable
- Easy enrolment process
- Non-invasive readers
 - ❑ No direct contact required



38



Enrolment unit

Remote unit



Face Recognition



- Two distinct applications:
 - ❑ Recognizing *authorized* personnel for I&A
 - ❑ Recognizing *unregistered* people using photos*
- *Developing bad reputation for high error rates; e.g., Tampa PD dropped sample system in Aug 2003 after > 2 year trial w/out single capture of a criminal



39

Copyright © 2011 M. E. Kabay. All rights reserved.

Protective Technologies



- “Special tamper-evident features and materials employed for the purpose of detecting tampering and deterring attempts to compromise, modify, penetrate, extract, or substitute information processing equipment and keying material.”
 - ❑ CNSS Instruction 4009 (Glossary)
 - ❑ <http://tinyurl.com/na6yab>
- E.g.,
 - ❑ Tapes
 - ❑ Special screws
 - ❑ Seals
 - ❑ Photographic Logs



40

Copyright © 2011 M. E. Kabay. All rights reserved.

Tapes



- Detecting opening of equipment or containers
- Used in forensic work for chain of custody
- Tape splits into two parts when opened

Courtesy J&S Industrial (HK) Co.



<http://www.j-n-s-ind.com.hk/security.htm> Used with permission.

Copyright © 2011 M. E. Kabay. All rights reserved.

Special Screws

- Can substitute screws or bolts requiring special drivers with restricted distribution
- E.g., Tamperproof Screw Co, Inc. of New York

☐ <http://www.tamperproof.com/index.cfm?fuseaction=products>



Images used by kind permission of Tamperproof Screw Co.

Copyright © 2011 M. E. Kabay. All rights reserved.

Seals

- Use soft metal (e.g., lead) or plastic units to prevent opening containers or enclosures without discovery
 - ☐ Use serial numbers or unique patterns
 - ☐ E.g., everyone will have seen seals on electric utility boxes and meters;
 - ☐ E.g., from American Casting & Manufacturing, <http://www.americancasting.com>



©American Casting & Manufacturing

Images used by kind permission of AC&M

Seals (cont'd)

- Examples from ULINE Shipping Supply Specialists http://www.uline.com/Group_47



High Security Seal

CLASSIFIED BY U.S. CUSTOMS AS HIGH SECURITY

Lock your **high value cargo** up tight.

- Absolute protection from tampering and theft.
- Sequentially numbered on both bolt and body.
- C-TPAT and ISO 17712 compliant.

http://www.uline.com/Browse_Listing_2302.asp
Image used by kind permission of ULINE Shipping Supply.

Copyright © 2011 M. E. Kabay. All rights reserved.

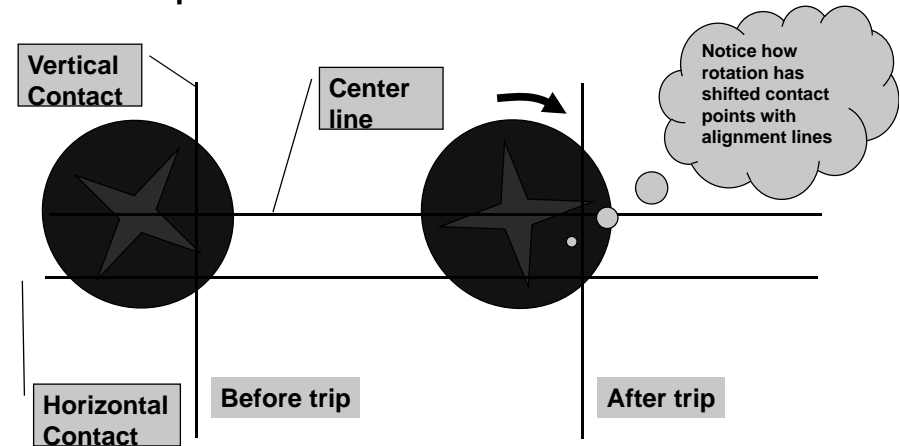
Photographic Logs (1)

- Use process of careful photography of computer equipment before allowing it to be taken overseas
- Record details such as
 - Exact distances of movable parts
 - Scratches, nicks especially around screws
 - Wipe fingerprints from inner components that should not have to be removed such as batteries and memory chips
 - Orientation of screws and bolts (see next slide)



Photographic Logs (2)

- Philips Head screw has rotated:



DEFCON 17: Invisible Access

- *Electronic Access Control, Audit Trails, and "High Security"*
- 47 minute discussion of physical access control device vulnerabilities



- <http://www.youtube.com/watch?v=wsvQtlU5a4>

DISCUSSION