Greater Lafayette Security Professionals, January 2011

Physical Security

Keith A. Watson, CISSP CISA
CERIAS, Purdue University

Overview

- The need
- Policy
- Safe versus Security
- Design of Physical Protection Systems
- Assessments
- Penetration Tests
- Lock Picking
- Examples

The Need for Physical Security

- Stealing a physically unprotected computer system or storage device is easier than breaking in over a network
- As computing devices become "commuting" devices more sensitive data is at risk
- Large and small installations of computing systems require environmental support
- Users in an office environment often put sensitive information at risk

Physical Security Components

- Policy
- Deterrence
- Adversaries
- Design of Physical Protection Systems
- Assessment
- Penetration Testing
- Lock Picking

Policy

- Physical Security Policies are sometimes hard to find
  - Few organizations have them
  - Most geared toward building access
- Regulated industries may have specific requirements for policies
  - NERC-CIP

Policy

- Policies should cover
  - Perimeter
  - Critical facility definitions, protection and access
  - Employee, contractor responsibilities
  - Monitoring of contractors and employees
  - Logging of access
  - Retention of access, alarm logs, surveillance
  - Response to access violations and alarms

Safety versus Security

- Protect life above all else
- Safety is the operation of systems during abnormal events
  - Fire, flood, weather, electrical faults, etc.
- Security is the operation of systems to prevent or detect attack by malevolent adversaries
- During safety critical events, security must also be considered

Deterrence

- Deterrence reduces the likelihood of attack by increasing the difficulty of attack and lowering the reward motive for attackers
- Methods
  - Locked doors
  - Lighting
  - Signage
  - Guard force

Adversaries

- Motivated individuals and groups
  - Organized
  - Have a plan
  - Have a reward in mind
- Opportunistic individuals
  - No plan
  - Have an opportunity

Design of Physical Protection Systems

- Objectives
  - Facility characterization
  - Threat definition
  - Target identification
- Functions
  - Detection
  - Delay
  - Respond

Detection

- Discovery of an adversary action
- Measure of effectiveness of detection function
- Measure of probability of sensing adversary action
- Measure of time required for reporting
- Measure of time required for alarm assessment

Detection Components

- Exterior Sensors
  - Passive, Active, Covert, Visible
- Interior Sensors
- Alarm Assessment
  - Humans are poor detectors
  - Good at assessment
- Alarm and Communication Display
- Entry Control
  - Biometrics, Locks, Scanners, Badges

Delay

- Slowing down of adversary progress
- Accomplished by
  - Personnel
  - Locks
  - Barriers
  - Response personnel
- Effectiveness measured by the time required by an adversary to bypass each element
  - After detection

Delay Components

- Defense in Depth
  - Diversification of detection and protection
- Access Delay
  - Barriers (Perimeter, Vehicle, Structural)
  - Fences
  - Dispensable Barriers (Foam, Smoke, Sticky Stuff)

Response

- Actions taken to prevent adversary success
- Interruption
  - Sufficient response personnel arriving at the appropriate location to prevent progress
  - Accurate communication to and by response force
- Neutralization
  - Actions and effectiveness of responders after interruption
- Measurement is response time

Response Components

- Response Force
  - Contingency Planning
  - Training
  - Outside Agencies
- Response Force Communications
  - Normal
  - Survivability (Jamming)
  - Duress Alarms

Physical Security Assessment

- It's traditional Risk Assessment
- Facility and System Characterization
- Threats
- Vulnerabilities
- Likelihood
- Impacts
- Determine Risk
- Make Recommendations

Threats

- Develop threat profile
  - Asset, access, actor, motive, outcome
- Determine the value of the asset to the organization and the actors
- Look for groups that promote extremism or protests against the organization
  - Research labs: animal rights organizations
- Classify actors
- Document the threats

Finding Vulnerabilities

- Walk around with and without a "guide"
- Ask questions of the guide for background info
- Observe the physical environment
- Take photos (if permitted) and notes
- Write down location of finding and details
- Repeat the tour without the guide
- Observe the operational environment

Facility Vulnerabilities

- Location and quantity of windows and doors
- Quality and durability of doors and locks
- Placement of alarm sensors
- Life safety sensors and equipment
- Surveillance systems
- Barriers and access delay points (DiD)
- Lack of entry controls
- Environmental control quality, maintenance, redundancy, and protection

Interior Vulnerabilities

- Converted offices for server space
- Critical systems in open spaces
- Locked down or cabled equipment
  - Check for default lock codes
- Lack of visitor logs
- Media vaults or cabinets
- Sticky notes with sensitive info
- Document storage and protection
- Operations and procedures for handling sensitive systems and information

Exterior Vulnerabilities

- Crime data
- Response times
- Facility perimeters and setbacks
- Fences
- Areas of concealment
- Employee entrances and access points
- Delivery and load dock locations, monitoring and procedures
- Location and cover for redundant power

Vulnerability Assessment

- Quantitative
  - Test Data
  - Error rates
  - Delay measurements
  - Response times
- Qualitative
  - Presence of physical protection system
  - Adherence to principles
  - Expert opinion

Likelihood

- Nature of the vulnerability
- Location of the vulnerability
- Skills required by and motivation of threat actor
- Probability and speed of detection
- Levels of delay
- Response and response time

Impacts

- Theft of equipment of equipment and data
- Disclosure of data
- Destruction of equipment or data
- Modification or corruption of data
- Insertion of monitoring devices or software
- Destruction of or damage to facility
- Release of toxins, diseased animals, pathogens, pests into environment
- Reputation, Public Relations, Financial

Determine Risk

- Risk is calculation of likelihood and impact
- High likelihood and high impact is high risk
- With test data as proof, risks can be more accurately calculated

Recommendations

- Move to a more secure facility
- Add alarms, surveillance, and monitoring
- Add delay
- Isolate critical systems and data behind barriers and perimeters
- Provide redundancy
- Hire guard force; work with local L.E.
- Develop response plans
- Rehearse response
- Test detection systems

Penetration Testing

- Gaining physical access to a secure facility or location within a facility
- Involves a team of people with different skills and roles
- Includes definition of scope prior to test
- Legal issues and risks must be evaluated

Pre-Test Procedures

- Gathering intel
  - HUMINT (human)
  - SIGINT (signals)
  - OSINT (open source)
  - IMINT (imagery)
- Determining risk
- Creating a test plan
- Get-out-of-jail-free papers

Surveillance Methods

- Dumpster Diving
- Satellite imagery
- Photos of facility, personnel, guards
- Snooping on radio communications
- Monitoring scheduled activities

Test Methods

- Social Engineering
  - Dress the part
  - Talk the talk
  - Create badges and business cards
  - Tailgating
  - Visiting non-existent or vacationing personnel
  - Delivery Boy
  - Security Guard

Test Methods

- Repeatedly triggering alarms
- Copy key fobs and badges
- Pick locks
- Compromise doors
- Explore suspended ceiling spaces

Lock Picking

- Lock Picking takes advantage of loose tolerances in manufacturing to open a lock without the appropriate key
- Lock Picking requires lots of practice and simple tools
- Locks are essentially puzzles that can be opened with knowledge of how they work
- In IN, there are no specific laws that prohibit lock picks

References

- Mary Lynn Garcia, **Vulnerability Assessment of Physical Protection Systems**, Elsevier Butterworth-Heinemann, 2006
- Mary Lynn Garcia, **The Design and Evaluation of Physical Protection Systems**, Elsevier Butterworth-Heinemann, 2008
- Deviant Ollam, **Practical Lock Picking**, Syngress, 2010
- Wil Allsop, **Unauthorised Access: Physical Penetration Testing For IT Security Teams**, Wiley, 2009