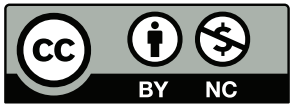
Physical and Procedural Security



Physical Security

- Another line of defense
- Violations sometimes lead to cyber breaches
- Remember: the usual goal of cybersecurity is to protect the *data*
- The attackers just want to win; they don't care about how

General Principles

- Who is the enemy?
- What are their resources?
- What are you trying to protect?
- The same as before!

Enemies

- Teenagers and other joy hackers — don't rule them out!
- Criminals — more likely after the hardware, but not always
- Governments
- Note well: physical attacks are much riskier for the attacker; there is no anomymity if detected. Physical attacks can be a high-stakes game.

Enemy Resources

- Technical skills: lock-picking, alarm neutralization, radio jammers, climbing, etc.
- Detailed knowledge of the facility
- Insider assistance?

Assets

- Direct access to computers
- Access to telecommunications lines
- Access to internal LANs
- Access to internal offices
- Information — hard-copy, removable media, etc.

Computer Access

- Remove the disk?
- Probe the RAM?
- Use the debugger to gain root privileges?
- Scan for cryptographic keys?
- Replace the BIOS?
- Install a keystroke logger?
- Physical access wins — always

Lines and LANs

- Plant wiretaps?
- Bypass firewall?
- Denial of service?

Information!

- Manuals
- Phone books
- Organizational charts
- Learn enough to sound like an insider
- The garbage is interesting, too. . .

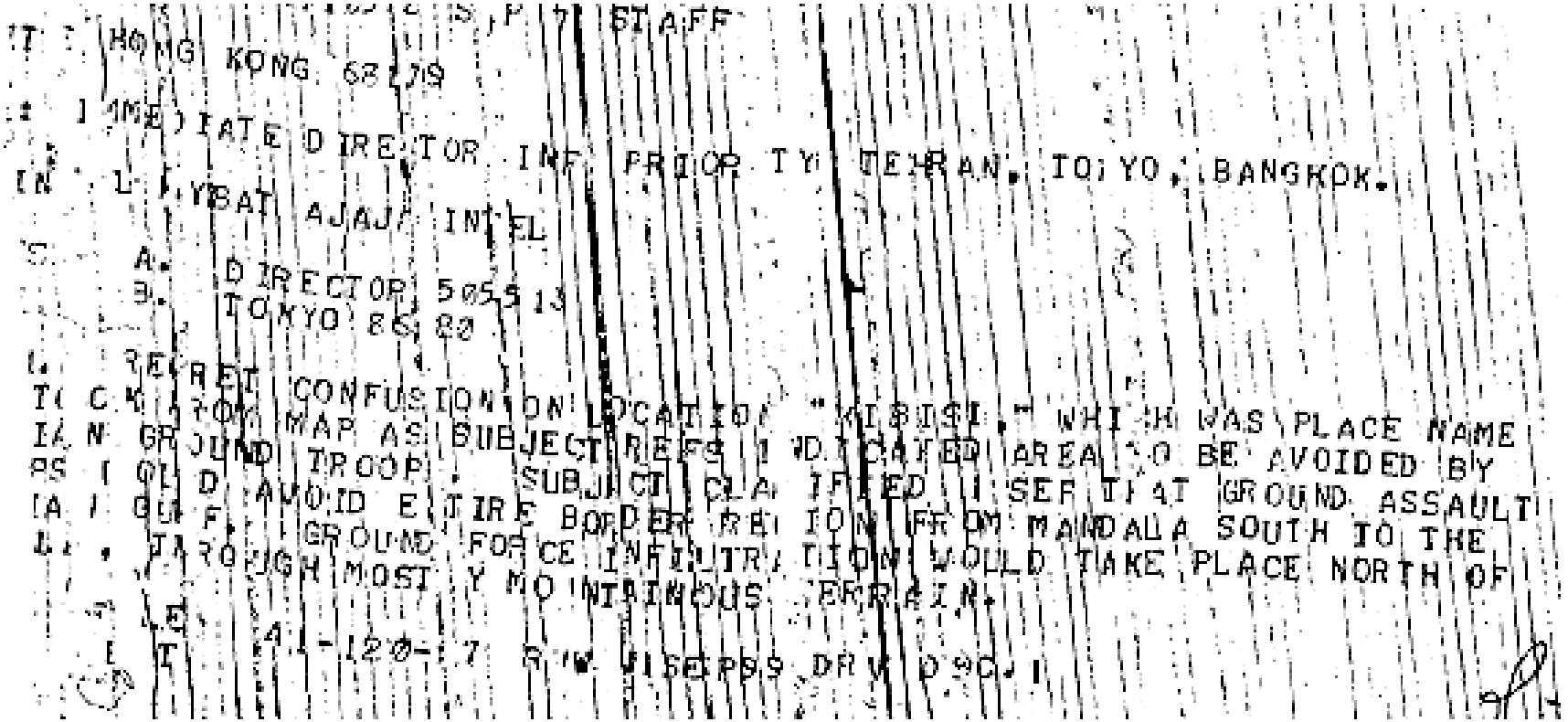
Dumpster Diving

- Raid your outside trash bins
- Discarded information is often almost as useful
- Probably legal under US law, if no trespassing is involved

Shredding

- Best defense: shredding
- Interim step: internal locked garbage cans
- Use “cross-cut shredder”
- (NSA has standards for such things. . .)
- Alternative: use *reliable* outside contractor

Shredding Done Poorly



Shredded CIA Cable reporting on information provided by an Iranian contact, *secret*.

Source: National Security Archive, George Washington University

Employees

- How are employees authenticated when they arrive?
- Badges? How are they checked?
- Guards? Turnstiles? PINs or chips?
- What links the employee to the badge?

Are Badge Rules Enforced?

- How are badges authenticated?
- Does the guard verify the picture?
- Is it possible to “tailgate”?
- What happens in abnormal situations, i.e., fire drills or fire alarms?
- What about holiday parties?
- What about external service personnel?

Locks

- Locks are not always as strong as they appear
- Experts have many ways to bypass locks
- Does your lock match your security needs?
- What about key control?

Pin and Tumbler Locks

- Most common form of lock
- Generally very easy to pick
- Guides and videos freely available on the Internet
- “Keep honest people honest”

Better Key Locks Exist

- Used for high-threat situations (i.e., bike locks in New York)
- (Not always as good as they seem — see the story of the Kryptonite bike lock and the Bic pen)
- Much harder to get duplicate keys made
- People frequently trade security for convenience

Combination Locks

- Often trivial to crack (i.e., most combination padlocks)
- But — safes often have *much* better ones
- High-end safes have electronic combination locks — turning the dial generates enough power
- If users pick their own combinations, are they guessable? Of course. . .

Richard Feynman on Safes

"I opened the safe that contained the secret of the atomic bomb — all the secrets, the formulas, the rates at which neutrons are liberated from uranium, how much uranium you need to make a bomb, how much was being made and available, all the theories, all the calculations, the WHOLE DAMN THING! . . .

"I remembered in the book about the psychology, and I said, 'You know, it's true. Psychologically, DeHoffman is just the kind of a guy to use a mathematical constant for his safe combination. And the other important mathematical constant is e.' So I walk back to the safe. 27–18–28 — click, clock, it opens.

"I checked, by the way, that all the rest of the filing cabinets had the same combination."

Los Alamos From Below: Reminiscences 1943–1945, by Richard Feynman

Electronic Locks

- Many types
- Mag stripe (hotels; this CS department)
- RFID (this university)
- Keypads
- More

Key Control

- How easy is it to get a key or combination?
- (Note the analogy to cryptographic keys)
- Many different threat vectors

Key Labels

- Many common keys or locks have numbers stamped on them, i.e., “S-100” for file cabinets
- Most car keys have such numbers
- Combination locks used for school lockers have such numbers
- Anyone with access to the database can create a key
- The database isn’t hard to get. . .

Rekeying

- Home locks: generally must disassemble the lock
- Offices: remove just the cylinder, via a “control key”
- Hotels: put a “combination” on a magstripe; change the combination via a new mag stripe that lists the previous one

Other Issues

- The spare key safe
- Employees (or family members) who lose keys
- Fire department keys
- “Hidden” keys to houses and cars

Attacking Locks

- Lock picks and “bump keys”
- Drilling the lock
- Plastic or metal shims
- Many other techniques

Going Around Security

- “You don’t go through strong security, you go around it”
- Many ways to evade locks
- Physical security is also a systems property

Attacks

- Remove the hinges
- Break nearby glass and unlock from the inside
- Break down the door
- Pry off the door jamb

Attacking Electronic Locks

- Bug the cable?
- Hack the control computer!
- Often have modem access, default passwords, unpatched software
- Pry the door from the magnetic catch just a little bit — it's an inverse cube law
- Insiders: put transparent tape on the strike plate

Fool the Motion Detector

- Slide paper under the door
- Squirt Silly String in the gap
- Easier with glass doors

Evading Detection

- Locks are often rated by time-to-crack with and without power tools
- Power tools are *noisy* — use will be noticed
- Frequently, then, the goal is to combine the lock with surveillance or alarms

Process Helps

- Logs
- ID checks
- Protocols
- Disclosure
- But — don't just go through the motions

Logs

- Keep track of who enters and leaves
- Sometimes automated, via electronic keys (hackable?)
- Guard should match log entry against ID
- Look at the logs!

Chain of Evidence

- Do not separate authorization from entry
- Example: separation of ID check from actual gate
- Photo ID-checking not very useful for authorization unless matched against external data

Protocols

- Make sure everyone understands and follows the process
- Don't let someone talk you into something
- Education helps — make sure your employees know how they can be fooled, and why each part of the process exists

Social Engineering

- Talk your way into someplace
- Act and sound as if you belong
- Know the terminology (see dumpster diving, above)

Why it Works

- Constant verification is too clumsy
- Most of the time, you're not being scammed
- But the bad guys know this

Data Matching

- Reconcile data after the fact
- Make sure that all records agree
- Doesn't prevent fraud; can detect it, and perhaps deter it
- That's how the fraudulent Microsoft code-signing certificates were discovered (CERT Advisory CA-2001-04)

Data Auditing

- In a large-scale system, you can't check all transactions in detail
- Pick a random subset, and investigate them carefully
- Check *all* links in the process — does everyone know about the transaction and have the same details recorded?

Risk Management

- We can't prevent all security problems
- What are the odds of a failure? What will one cost us?
- Easier in the physical world — we have a much better sense of the strength of security systems
- Electronic locks and access control systems turn a well-understood problem into a software security problem — and we don't know how to solve that very well. . .

Is This Computer Science?

- Many of the thought processes and techniques are the same
- Computer systems can be part of the problem
- Computer systems have to support the solutions