CIS551: Computer and Network Security

Jonathan M. Smith

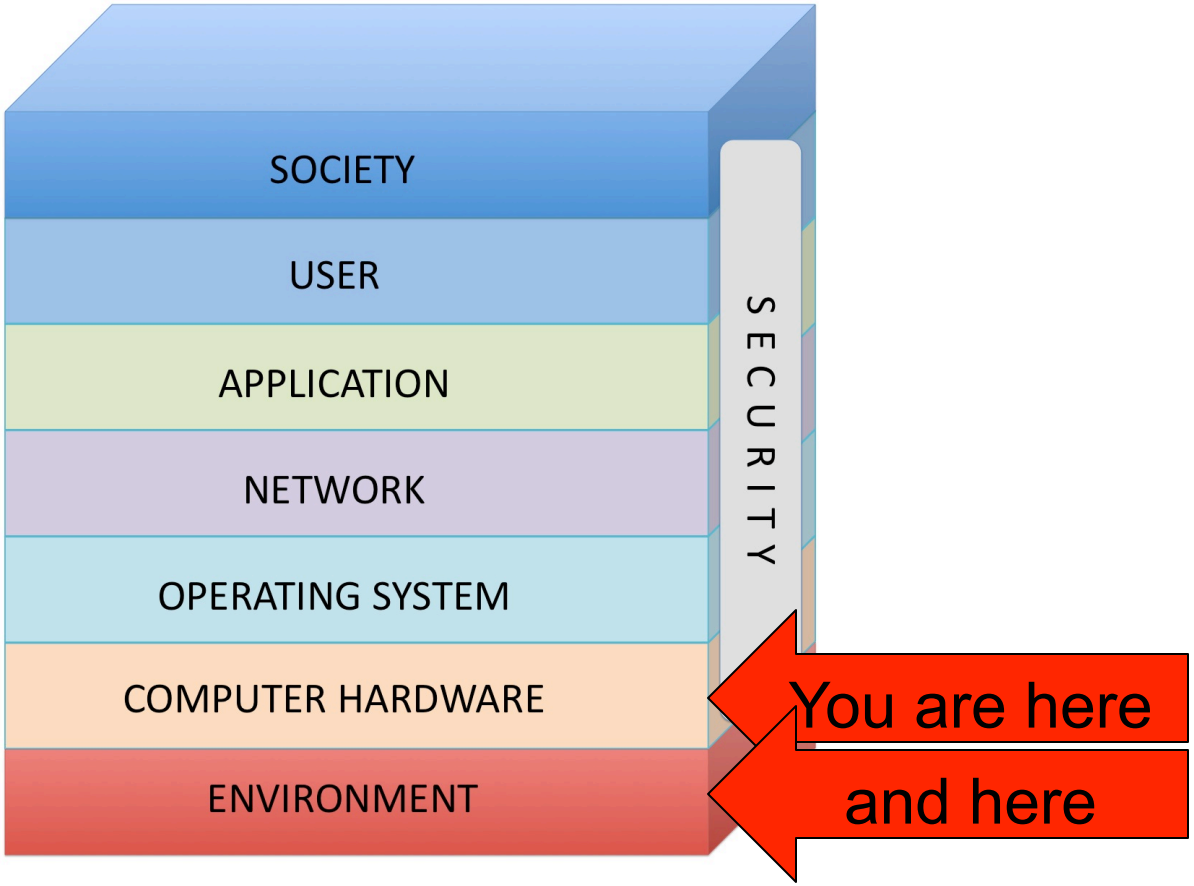
jms@cis.upenn.edu

04/07/2014

CIS551 Topics

- Computer Security
  - Software/Languages, Computer Arch.
  - Access Control, Operating Systems
  - Threats: Vulnerabilities, Viruses
- Computer Networks
  - Physical layers, Internet, WWW, Applications
  - Cryptography in several forms
  - Threats: Confidentiality, Integrity, Availability
- Systems Viewpoint
  - Users, social engineering, insider threats

Sincoskie NIS model

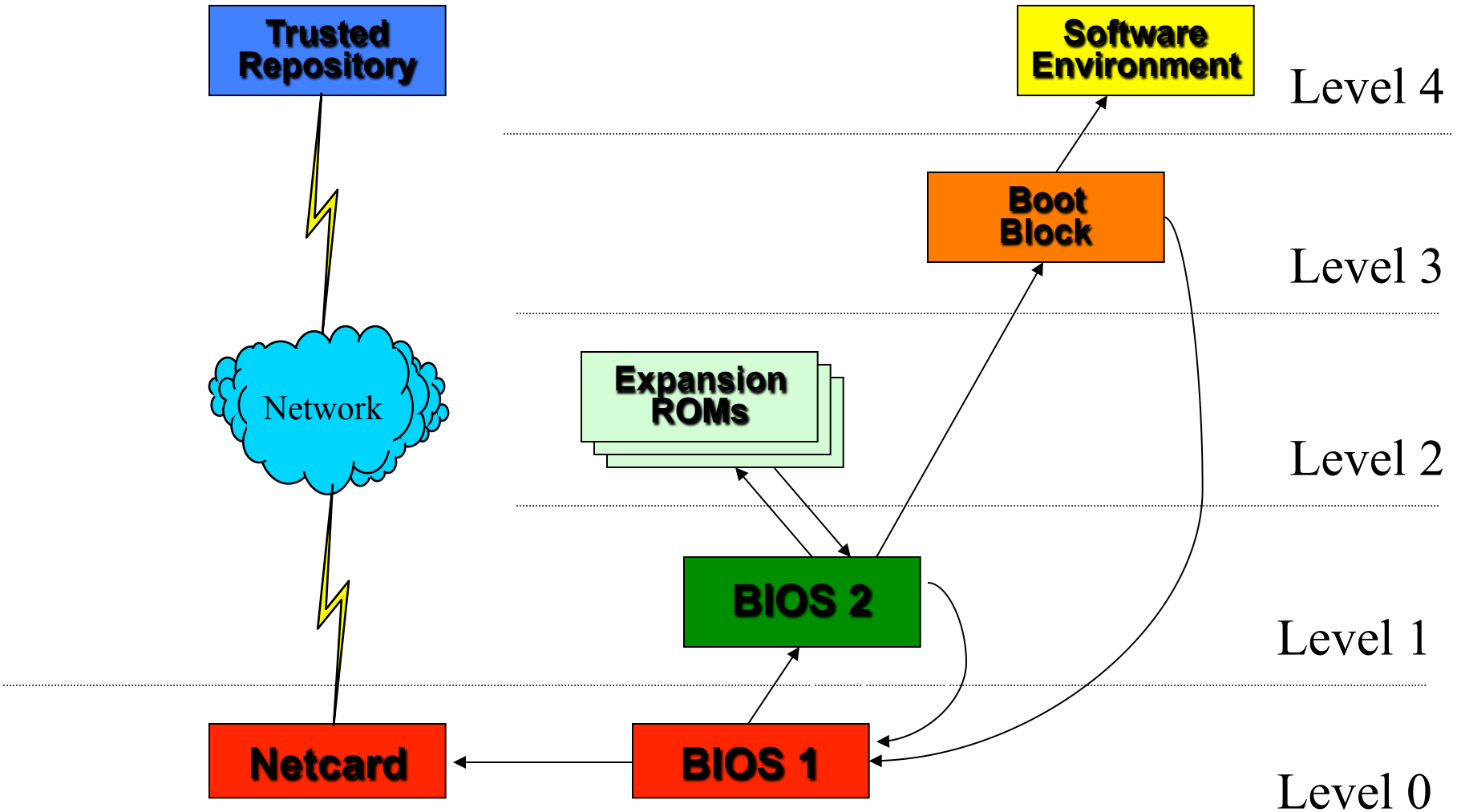


W.D. Sincoskie, *et al.* “Layer Dissonance and Closure in Networked Information Security” (white paper)

Trust refresher

- **Trust** is the *expectation* that the right thing will happen for the right person at the right time and at the right place
- Trust is often based on *transitive* trust
  - I trust Alice since I trust Bart and Bart trusts Alice
- Trust is often based on *assumptions* of trust
  - This creates a chain of dependencies
  - See K. Thompson, “Reflections on Trusting Trust”
- Most SW systems assume HW trusted
  - “FPGA Viruses”, Hazdic, Udani, Smith, FPL ‘99
  - “Overcoming an untrusted TCB”, Hicks, Finnicum, King, Martin, Smith, S&P ’10
- Can we minimize dependencies
  - And minimize “attack surface”?

Root of Trust – Arbaugh's AEGIS (Oakland '97)



Trusted Platform Module

- Standardized hardware “root of trust”
- Stores keys, performs attestation, etc.
- Can be used for secure boot, DRM, etc.
- Widely deployed in servers

Desiderata for Trust Evidence

- Multiple independent sources for *attestation*
  - E.g., voting TPMs with secured access (crypto)
- Minimal dependent sources
  - Rely as much as possible on *differential* integrity
  - Secure Boot on TPM
- Robust integrity checks
  - Chaining Layered Integrity Checks (Arbaugh)
- Recovery strategies using independence

Tamper Resistance

- Presume unsupervised access to multiple instances of device
- Desirable for *trust*
- Idea: A *component* you can trust
- Why?
  - Store cryptographic keys
  - Integrity check other components
  - Permit unsupervised access
- Usually implemented in hardware

How?

- Packaging
  - Lid switches
- Detection
  - Circuitry which interrupts power to memory
    - Erase key material
- Examples (from Anderson and Kuhn)
  - VISA Security Module
  - Smartcards
  - Subscriber Identity Modules (SIMs)

Non-Invasive Attacks (A&K)

- Early Pay-TV smartcard
  - 8-bit uproc. with ROM, RAM, EEPROM
  - Buy full service, store code in EEPROM
  - EEPROM updated via pins
  - Tape across pins
- Other attacks
  - Cycling, anomalous voltages, clock glitches
  - Single-stepping for forensics
  - Sophisticated attacks on operating silicon
- Cat and mouse game!

Invasive Attacks (Anderson & Kuhn)

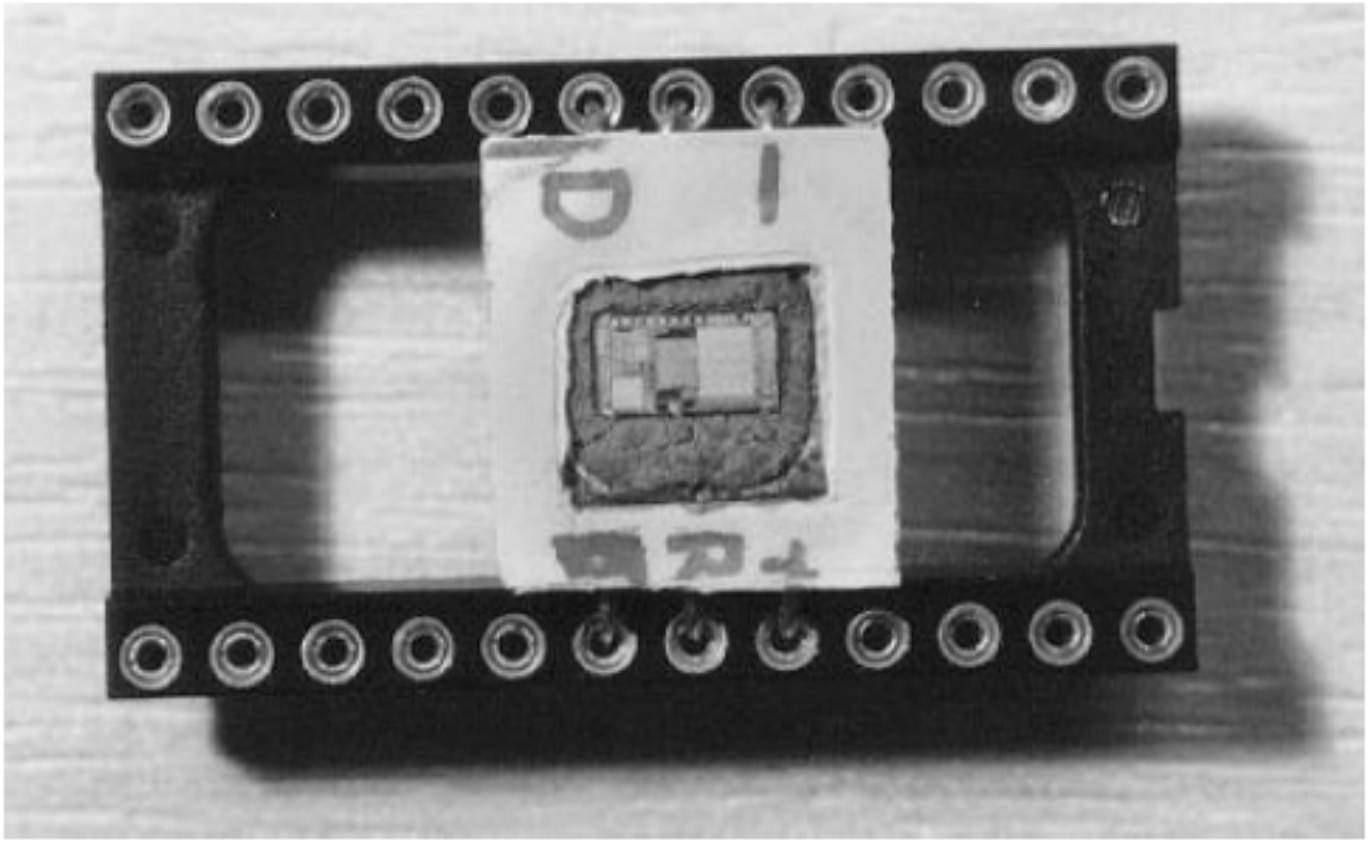


Figure 1: Fully functional smartcard processor with covering plastic removed for microprobing experiments. All tools necessary for this preparation were obtained for US$30 in a pharmacy.

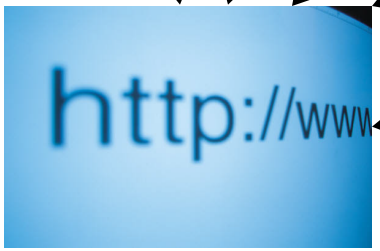
Defenses

- Opacity (make observation of operation hard, e.g., through choice of materials)
- Obscuration (e.g., through introduction of dummy elements as silicon features to increase attacker work factor)
- Dummy accesses / bus encryption
- Systems approaches
  - E.g., cause 10min delay, as in GSA safes
- Speculative discussion of PALs

Access Models

User

?



App
Web
Browser

Client
Computer

E-mail
client

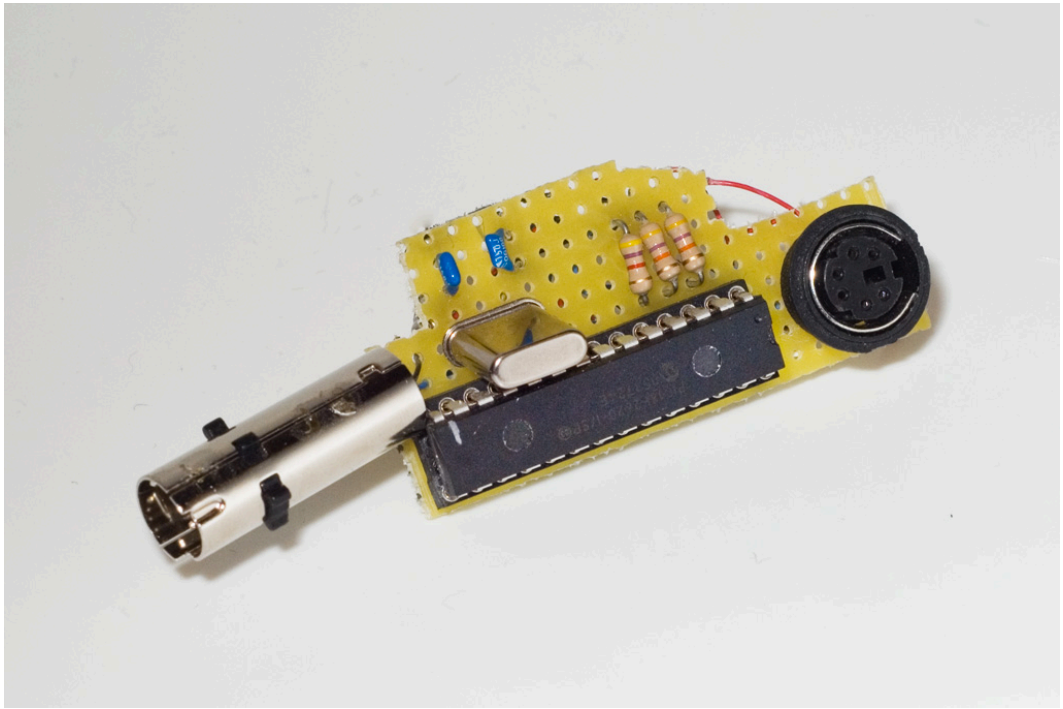
Covert Channels

- *Indirect* system information leakage
- Examples:
  - Timing of password entry on Tenex
  - Send bits as sizes of files
- Key idea: a mechanism which can encode information
  - Information can be *encoded* or *modulated*

Timing Channels

- Particularly pernicious
- If (A or B) and B takes longer, measure and deduce which occurred
- Ultimately present in all systems which can be measured
  - Goal: minimize timing channel *bit rate*
- Major problem: computers and networks are fast – low % still a lot (voice: 2.4Kbps)

“Jitterbug” Timing Channel (Shah)



- Inserted between keyboard and computer
- Modulates characters with controlled delays, creating a timing channel
- Recovered typing via Internet

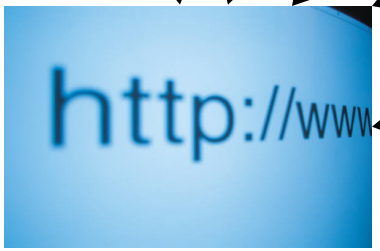
Defenses

- Control physical access
  - What about the custodian?
- Defeat/attenuate modulation
  - Make all timing constant (hard to “jitter”)
  - Randomize timing (force extremely low bit rate – could be done with gateway box)
- Isolate machines
  - No way to get out (“air gap”)
  - Not particularly successful against Stuxnet…

Access Models

User

?



App
Web
Browser

Client
Computer

E-mail
client

Unintended emissions

- Displays (CRTs) *radiate*
- Kuhn and Anderson paper
  - Read display via RF emissions
    - Sometimes called “phreaking”
  - Surprising that it works!
  - Allows getting user data (if you’re close)
- Paper exploits font characteristics

Defenses

- Reduce emissions by design
  - Components that emit less RF
- Shielding of components
  - Attenuate emissions
  - Shield computers or shield rooms
    - TEMPEST
- Make information harder to extract
  - Kuhn and Anderson use special fonts
  - Fonts intended to be hard to recover

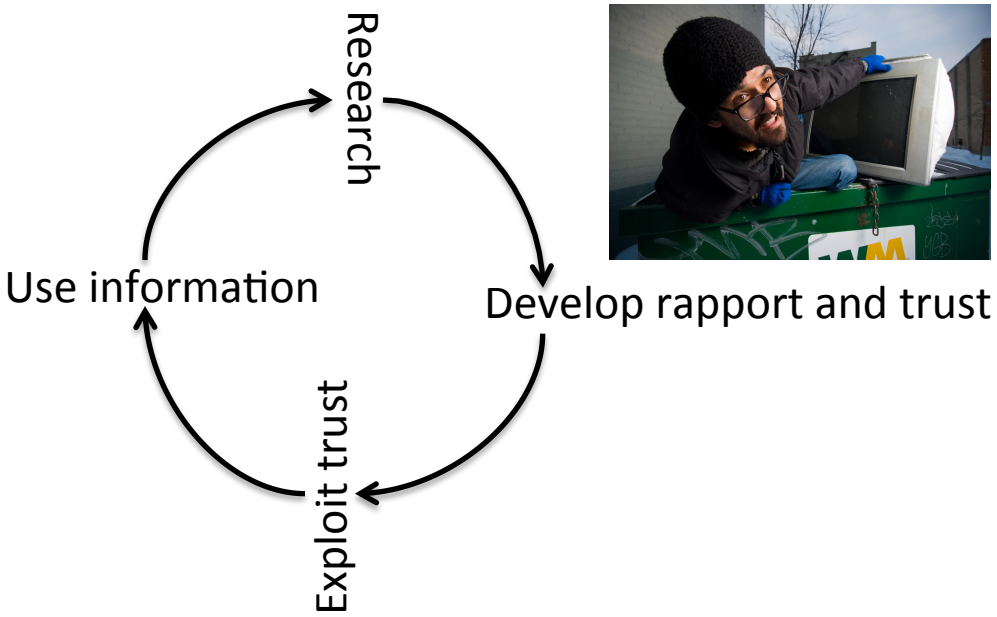
Social Engineering

- Security systems have “human element”
- Some people in the system:
  - Have access to valuable information
  - Use computers that contain information
  - Can alter software or passwords
  - Can be fooled
- The social engineer’s goal is to convince people to hand over information and control

Social Engineers

- Computer/information-focused variety of "con(fidence) men"
  - See David W. Maurer, "*The Big Con: The Story of the Confidence Man and the Confidence Game*" (ISBN 0-385-495380-2)
- Modern Era: Kevin D. Mitnick and William L. Simon, "*The Art of Deception*", Wiley 2002.
  - Will use Mitnick's "Security at a Glance"

“The Social Engineering Cycle”



ACTION	DESCRIPTION
Research	SEC filings, marketing, web content, dumpsters…
Develop support and trust	Insider information, misrepresenting identity, cite those known to victim, ask for help, cite authority
Exploit trust	Information or action from victim (ask attacker for help!)
Use information	If a step, repeat cycle until goal achieved

Mitnick: “Common Social Engineering Methods”, I

- Posing as a fellow employee
- Posing as an employee of a vendor, partner company, or law enforcement
- Posing as someone in authority
- Posing as a new employee requesting help
- Posing as a vendor or systems manufacturer with a system patch or update

Mitnick: “Common Social Engineering Methods”, II

- Offering help if a problem occurs, then make the problem occur: victim calls for help
- Sending free software or patch to install
- Sending virus/Trojan as an attachment
- False pop-up window asking for login/PW
- Capturing keystrokes with expendable system or program
- Leaving CD/memory stick with malware

Mitnick: “Common Social Engineering Methods”, III

- Use insider lingo/terminology to gain trust
- Offer a prize to register with username/PW
- Leave document(s) at company mailroom for intraoffice delivery (“it’s from *us*”!)
- Modify FAX machine heading to appear internal
- Ask receptionist to receive, then forward, a FAX

Mitnick: “Common Social Engineering Methods”, IV

- Ask for a file to be transferred to an (apparently) internal location
- Get a voice mailbox set up so callbacks perceive attacker as internal
- Pretending to be from remote office and asking for e-mail access locally

Mitnick: “Warning signs of an attack”

- Refusal to give callback number
- Out-of-ordinary request
- Claim of authority
- Stresses urgency
- Threatens consequences of noncompliance
- Shows discomfort when questioned
- Name dropping
- Compliments or flattery
- Flirting

Mitnick: “Common Targets of Attacks”

TARGET TYPE	EXAMPLES
Unaware of value of information	Receptionists, telephone operators, administrative assistants, security guards
Special privileges	Help desk or technical support, system administrators, computer operators, telephone system administrators
Manufacturer/vendor	Computer hardware, software manufacturers, voice mail systems vendors
Specific departments	Accounting, human resources

Mitnick: “Factors that Make Companies More Vulnerable to an Attack”

- Large number of employees
- Multiple facilities
- Information on employee whereabouts (“I’m on vacation”) left in voice mail messages
- Phone extension information made available
- Lack of security training
- Lack of data classification system
- No incident reporting/response plan in place

Mitnick: Defenses

- Verification of Identity
- Verification of Employment Status
- Criteria for verifying Non-Employees
- Data Classification

Mitnick: “Verification of Identity”

ACTION	DESCRIPTION
Caller ID	Verify call is internal, and name or extension matches identity
Callback	Look up requester in company directory and call their #
Vouching	Ask a trusted employee to vouch for requester’s identity
Shared common secret	Request enterprise-wide shared secret, such as a password or daily code
Supervisor or manager	Contact employee’s immediate supervisor and request verification of identity and employment status
Secure e-mail	Request a digitally signed message
Personal voice recognition	For a caller known to employee, validate by caller’s voice
Dynamic passwords	Verify against a dynamic password solution (such as SecureID or other token)
In person	Require requester to appear in person with a badge/ID

Mitnick: “Verification of Employment Status”

ACTION	DESCRIPTION
Employee directory check	Verify that requester is listed in on-line directory
Requester’s manager verification	Call requester’s manager using phone number listed in company directory
Requester’s department or workgroup verification	Call requester’s department or workgroup and determine that requester is still employed by company

Mitnick: “Determine Need to Know”

ACTION	DESCRIPTION
Consult job title/workgroup/ responsibilities list	Check published lists of which employees are entitled to specific classified information
Obtain authority from manager	Contact your manager, or the manager of the requester, for authority to comply with the request
Obtain authority from the information owner or designee	Ask owner of information if requester has a need to know
Obtain authority with an automated tool	Check proprietary software database for authorized personnel

Mitnick: “Verifying Non-Employees”

CRITERION	ACTION
Relationship	Verify that requester’s firm has a vendor, strategic partner or other relationship
Identity	Verify requester’s identity and employment status at the vendor / partner firm
Nondisclosure	Verify that the requester has a signed NDA on file
Access	Refer the request to management when the information is classified above “Internal” (*see next slide*)

Mitnick: “Data Classification”

CLASSI-FICATION	DESCRIPTION	PROCEDURE
Public	Can be freely released to the public	No need to verify
Internal	For use within the company	Verify Identity of requester as active employee; verify NDA and management approval for non-employees
Private	Information of a personal nature intended for use only within the organization	Verify identity of requester as active employee, or nonemployee with authorization. Check with HR to disclose Private information to authorized employees or external requesters
Confidential	Shared only with an absolute need to know within the organization	Verify identity of requester and need to know from designated information owner. Release only with prior written consent of manager, or information owner or designee. Check for NDA on file. Only management personnel may disclose to non-employees

Insider Threats

- Social Engineering is an attempt by an *outsider* to gain trusted status
  - Primarily to gain information or access
- Insider threats are from trusted *insiders*
  - People who already have information or access and (may) need it for their jobs
  - Example: Heath MS Thesis
  - Example: “Wikileaks” leaker

Existence of insider threat?

- Clues:
  - Unexplained information in public domain
  - Unexplained behavior changes by competitors that might rely on information
- Forensics:
  - Who had access to it?
  - Who had incentives to leak?
- This requires continuing analysis
- In national security, sometimes called a “mole”.

Types of insider threat

- Divided loyalties
  - Uses corporate information for gain
  - Example: Walker spy ring
  - Example: Insider trading
- Disgruntled employee
  - Wishes to damage enterprise while inside
- Former employee (fired or laid off)
  - Not really insider anymore, *but* retains information and *might* retain access / passwords

The human element

- Insiders know:
  - Corporate information
  - Who knows what
  - Corporate defenses
- Insiders can:
  - Alter systems and practices
  - Hide from / avoid systems and practices
  - Gain increasing access (no revocation…)

Need to know

- Careful identification of what information people need to do their jobs
- Policies and procedures can enforce
- One example: “compartmentalization”
  - Idea warship’s watertight compartments
    - Torpedo/mine can’t sink ship
  - Like “privilege separation” in O.S.
- Careful documented procedures for information access and termination

Examples of trusted employees

- System Administrators
- Security guards
- Executives
  - And their Administrative Assistants
- Financial departments
- Human resources
- Janitors ☺

Personnel Security – the first line of defense

- If people must be trusted, check:
  - Complete resume and notes from interviews
  - References from previous jobs
  - Neighbors
  - Criminal record
  - Financial record
- Grant accesses gradually
  - Revoke when no longer needed

Dynamic Personnel Security

- Require trusted employees to report adverse circumstances (divorce, bankruptcy, arrest)
- Monitor logs/ accesses to information
- Sudden changes in behavior
  - 9-5 employee starts working late + on weekends
- Peer / supervisor information
- Privacy & work/life separation an issue

Trusted employee management

- If terminations / layoffs are necessary
  - Ideal: accesses revoked at notice time
  - Quickly gather possessions and escort from building
  - Fired -> disgruntled -> insider threat (minimize risk)
- Pay (at least) adequately; address concerns promptly

Legal protections

- Non-disclosure Agreements (NDAs)
  - Best if identify specific types, or “marked” information
- Non-compete Agreements
- These minimize risk of information misuse
- They have to have “teeth” (penalties) to be meaningful if violated
  - And you have to detect it…

Technical Approaches

- Mainly, logging and anomaly detection
  - E.g., attempted access to privileged information
  - E.g., unusual off-hours access
  - E.g., large data outflows
- Careful, continuing review of privileges
- Numbered copies (for backtracing)
- Can also use forensics, post-hoc

Walker Spy Ring - Heath Thesis

- Untrustable person in trusted position
  - History of criminal actions
  - Financial Stresses
- Major weaknesses in US Navy Fleet Broadcast System (FBS)
  - Too much trust in too-many personnel
  - Few limitations on damage from leaks
  - Inadequate auditing
  - Decentralized responsibility for security

Summary

- Bad guys can be surprisingly inventive
- There are different classes of attackers
- Need defensive *systems* and *policies*
  - Defend, Delay, Detect
  - Recovery strategy