CIS551: Computer and Network Security

Jonathan M. Smith

jms@cis.upenn.edu

04/09/2014

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: Walker (see: Maj. Heath MS Thesis)
    - Example: Manning “Wikileaks”
    - Example: Snowden “NSA”

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