Combatting Insider Misuse

Peter G. Neumann

Computer Science Laboratory

SRI International

Theme

- The only way to address insider misuse sensibly is to make significant improvements to system and networking trustworthiness:
  - Architecturally
  - Developmentally
  - Operationally

Definitions

- Insider: a system user that can misuse certain privileges
  - Determined relative to the boundaries of interest
- Other definitions in the literature:
  - Exclude outsiders who become insiders
  - Assume the reader "knows" what an insider is
  - Assume a perimeter separates "insider" and "outsider"
- Notion of a single perimeter unrealistic

Assumptions

- Physical presence irrelevant
  - – Insider can be remote; outsider can be local
- Outsiders can become insiders
  - – Break in (social engineering, holes, ...)
- Distinction between malicious, accidental misleading
  - – Do something deliberately, other events accidentally occur

Classes of Insiders

- Entities can be both insiders and outsiders
  - Depends on frame of reference
- Example: system with partitioned administrator privileges
  - Trusted Xenix
- Implication: “insider” multidimensional

Classes of Insider Misuse

- Obviousness
  - Obvious vs. stealthy
- Intent
  - Accidental vs. intentional

Threats

Attribute	Outsiders	Insiders
Access controls	Unprivileged exploitation of inadequate controls	Privileged manipulation of access controls
Confidentiality	Unencrypted password capture	National security leaks
Integrity	Untrustworthy Web code	Putting Trojan horses in trusted components
Denial of Service	Flooding, physical harm to exposed equipment	Disabling protected components
Authentication	Penetrations, attacks on PKI/ authentication infrastructures	Usurpation of superuser, access to root keys
Accountability	Masquerading, attacks on accounting infrastructures	Hacking beneath the audit trails, altering audit logs
Other misuses	Planting pirated software on web	Running covert business, insider trading

Role of Knowledge

- Outsiders: direct info and inferences from web info (such as penetration scripts), help files, social engineering; chats helpful
- Ordinary insiders: experience gained from normal use and experiments; familiarity with sensitive files, project knowledge; collusion easy
- Privileged insiders: deep knowledge from experience; ability to change and abuse privileges; ability to create invisible accounts; collusion dicier?

Exploiting Vulnerabilities

- Insider: attack may be close to expected behavior
  - Gradually shift statistical profile, defeating anomaly IDS
  - Better system security improves situation

Resulting Risks

- Differ between outsiders, insiders; but ***effects*** can be similar
- Examples
  - – Outsiders becoming insiders may do as much, less, or more damage than existing insiders
  - – Outsiders can create major havoc or damage especially if firewall, authentication, and server security is weak

Examples:
High Tech, Detailed Knowledge

- Autotote ex-programmer hacked willing Breeders' Cup Pick Six horserace off-track betting system
- Hackers penetrated Russian Gazprom, controlled pipeline flow
- Rogue code in Microsoft software included rogue password to allow access to thousands of Web sites

Examples:
Low Tech, Government Privileges

- Aldrich Ames, spy in the US CIA
- Browsing by US IRS employees for curiosity, fraud
- Danish mailman intercepted postal mail, led to credit card fraud
- Nova Scotia worker deleted her speeding ticket

Examples: Low Tech, Other Privileges

- Laptop stolen, financial records of customers for 4 banks compromised
- 4000-person AIDS database leaked to press
- Bank executive in Malaysia transferred $1,500,000
- Pakistani outsourcee of UCSF health-care group threatened to release personal data files unless paid back wages

Prevention

- Saltzer-Schroeder principles of secure design
  - Especially psychological acceptability
- Need meaningful, stated security policy
  - Must be implementable with existing security mechanisms
  - Fine-grained access controls critical to minimizing insider misuse

Security Policies

- Explicitly define both insider misuse and proper behavior
- Need to be appropriate to application domain
  - So that domain must be understood
- Existing audit trails generally inadequate for insider misuse detection

Detection, Analysis, Identification

- What to analyze depends on several things
  - Where insiders can come from
  - Goals of analysis
- Unknown types of insider attacks require new uses of statistical analysis
  - Emphasis on correlation on a wide-area (enterprise-wide) basis
  - Need to design, implement tools to do this
- ***DANGER***: *false accusations*!

Responses

- Cut off attacks or let them continue?
  - Depends on goals
- If allowed to continue, must deal with continuing compromise of system
  - Simply restoring may not be enough

Decomposition of Insider Problem

- Development stages: system architecture and design
- Operational aspects: system administration, support; enterprise management
- Security issues: authentication, intrusion detection
- Psychological and other factors
  - Critical as detection relies on knowing expected normal behavior
  - Are there psychological traits that could be revealing?
- Responses: tailored to the misuse detected

Observations

- Gap between intended allowed uses and uses thought to be allowed
- Gap between what is though to be allowed and what is actually possible
- Without a security policy, how do you know what constitutes misuse?
  - – What does “unauthorized use” mean when everything authorized

Example: High-Integrity Elections

- Good paradigm that illustrates "insider" is hierarchical, distributed, context-dependent
- Many requirements;
  - Registration, authentication, authorization, voter information
  - Polling place availability, accessibility
  - Vote casting, counting
  - Monitoring (auditing), remediation of detected irregularities

Election Integrity Principles (see Saltzer and Schroeder, 1975)

- Don’t use an OS, or minimize OS functions
- Security controls cannot be bypassed
- Do not depend on secrecy for security
- Keep vendor, election official privileges separate
- Apply least privilege
- Make systems easy to use, both for voters and election officials
- Provide pervasive, forensic-quality auditing
- If policy may need to be altered, do not embed that policy in a mechanism

Research and Development Directions

- Recognize commonalities in insider, outsider misuse
- Effort to define characteristic types of insider misuse
- Need fine-grained access policies, mechanisms
- Move focus of commercial tools to detecting unknown misuse, not just known misuse
- Address hierarchical, distributed correlation of results aggregated across different sensors, analytic tools, and systems
- Integrate this all with network management
- Systems used to manage this must be tamperproof and spoofproof
- Extend profiles to include extrinsic individual characteristics

What This Workshop Can Do

- Explore idiosyncracies of insider misuse
- Elaborate on the above, and other, research directions

Parting Thought

- COTS intrusion detection systems not useful for detecting unrecognized forms of insider misuse
- Proprietary monocultures dangerous in the long run
  - – Just look at e-voting systems and how dependent counties and states are on the single vendor
- Robust, open source software could have tremendous payoffs
  - – May inspire COTS developers to produce better systems
  - – Here, “robust” is critical