CSci530: Computer Security Systems
Intrusion Detection
5 November 2003

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute

Administrative

- All proposals replied to. If you do not have a response send a follow-up message to csci530@usc.edu.
- End-of-term exam on last regular lecture day.
- Research paper officially due the same day, but no penalty if turned in up to one week late.
- Out of town Friday, see me after class if you would otherwise need to meet me during my Friday office hours.

Intrusion Detection

- Security Enforcement Mechanisms are not foolproof, so we need a way of knowing when they are not working.
  - Or even better, before they stop working
- We need ways to detect insider misuse

Taxonomy for Intrusion Detection

- What is detected
  - Signature based approaches
  - Anomaly detection
- Where detected
  - Network Based
  - Host Based
  - Application Based
- When attack is detected
  - Real time
  - After the fact

Basis for detecting attack

- Systems operating normally
  - Activity conforms to statistically predictable patterns.
  - Actions do not include attempts to subvert policy.
  - Actions of processes conform to the policies regarding what they are allowed to do.

Rating ID systems

- False positives
  - Normal activity flagged as intrusion
    - Affects adminstrator workload
  - E.g. spam filtering
- False Negatives
  - Attacks that are not detected

Anomaly Detection

- How it works
  - Analyze baseline characteristics of system or user behavior and record.
  - Compare current characteristics and behavior against baseline.
  - Flag differences
- Why it is hard
  - Deciding how to characterize behavior so that changes reflect intrusions and not normal changes in activities.

Metrics

- Threshold metrics
  - Number of failed access attempts.
  - Bandwidth consumed.
- State change probabilities (Markov models)
  - Requires training by analyzing normal traces
  - Looking for transitions that don't seem to follow the normal pattern

Misuse detection

- Whether activities or code is violate site policy.
  - Rule based
  - Signature based.
- Problems
  - Can only detect attacks known in advance.
  - Virus checkers are usually signature based.
  - Many more false negatives (subject to definition)
- Strengths
  - Tend to have fewer false positives.

Collecting Input Data

- Audit vs. Intrusion Detection
- Network Based ID
- Host Based ID
- Application based ID

Network Based ID

- Often based on network sniffing
  - Listening to network traffic as it goes by a sensor node
    - Could be placed in routers or other network components
  - Issues?
    - Placement
    - Load
    - Encrypted traffic
    - Determining intent

Host Based ID

- Scan system and application logs
- Report on system state
- Report activity to ID system
- Issues
  - Only get what applications already put into logs
  - Might not understand the intent of an action.

Application Based ID

- Application determines what to report to ID system.
  - Based on a policy
- Drawbacks
  - Requires application involvement. Some applications will not report.
    - Authorization functions like GAA-API can help address this limitation.
- Benefits
  - Application understands the objects and entities to which policies apply.

Issues in Intrusion Detection

- Collecting data on and reporting events
  - Languages, e.g. CIDF
    - Dr. Tung will talk about in his lectures.
- Reducing Data
  - To reduce network traffic consumed
    - Consider overhead
  - Summarize data
    - Finding relationships

Components of ID systems

- Collectors
  - Gather raw data
- Director
  - Reduces incoming traffic and finds relationships
- Notifier
  - Accepts data from director and takes appropriate action

Advanced IDS models

- Distributed Ditection
  - Combining host and netwror monitoring (DIDS)
  - Autonomous agents (Crosbie and Spafford)

Intrusion Response

- Intrusion Prevention
  - (marketing buzzword)
- Intrusion Response
  - How to react when an intrusion is detected

Possible Responses

- Notify administrator
- System or network lockdown
- Place attacker in controlled environment
- Slow the system for offending processes
- Kill the process

Phase of Response (Bishop)

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow up

PREPARATION

- Generate baseline for system
  - Checksums of binaries
    - For use by systems like tripwire
- Develop procedures to follow
- Maintain backups

IDENTIFICATION

- This is the role of the ID system
  - Detect attack
  - Characterize attack
  - Try to assess motives of attack
  - Determine what has been affected

CONTAINMENT

- Passive monitoring
  - To learn intent of attacker
  - Learn new attack modes so one can defend against them later
- Constraining access
  - Locking down system
  - Closing connections
  - Blocking at firewall, or closer to source
- Combination
  - Constrain activities, but don't let attack know one is doing so (Honeypots, Jail).

ERADICATION

- Prevent attack or effects of attack from reoccuring.
  - Locking down system (also in containment phase)
  - Blocking connections at firewall
  - Isolate potential targets

RECOVERY

- Restore system to safe state
  - Check all software for backdoors
  - Recover data from backup

FOLLOWUP

- Take action against attacker.
  - Find origin of attack
- Notify other affected parties
  - Some of this occurs in earlier phases as well
- Assess what went wrong and correct procedures.
- Find buggy software that was exploited and fix