A Layered Approach to Insider Threat Detection and Proactive Forensics

Phillip G. Bradford, Ning Hu
University of Alabama
Tuscaloosa, AL 35487
Insider threats

Definition
- Menaces to computer security as a result of unauthorized system misuses by users of an organization.

Insider threats are potentially more destructive than external ones:
- Knowledge about the target
- Easy access to the target

Consequences for targeted organizations:
- Financial losses
- Denial of service
- Reputation damage
- Individual victims
IDS deficiencies

- Given the prevalence and destruction of insider sabotages, early detection and documentation of such threats is vital to the stakeholder’s interest.
- The IDS alone does not offer a satisfactory solution:
  - Detection accuracy
    - SID is known for false negatives.
    - AID is prone to false positives.
  - Costs
    - Lee et. al.’s classification: [5] damage, response and operational costs
    - It is an art to balance between detection cost and accuracy.
  - Applicability
    - Intrusion vs. extrusion
    - Insiders may often enjoy advantages.
Proactive forensics

- Imperfect proactive security
  - Need to collect and retain important evidence that for further investigation and legal actions

- Proactive forensics
  - A way to augment insider threat detection with a mixture of ID and CF tools & techniques.
  - Definition:
    - PF is a process of “the design, construction and configuring of (computer) systems to make them most amenable to digital forensics in the future.” [6]
Objectives

- An effective model that monitors user activities persistently to identify potential insider threats in a timely, precise, and efficient manner.

- The target system performs:
  - Online monitoring of user activities to detect potential system misuses and abuses
  - Proactive collection and analysis of important evidence concerning insider threats

- Currently concerned with monitoring general user processes
  - Non-critical and incremental threats
  - Low-and-slow deviations
Approaches

- Use the IDS as a black box to drive forensic tools
  - The coarse-grained output of the IDS can be input to an appropriate forensic tool set (e.g. TCT) for further analysis.

- Build statistical metrics for fleshing out long term changes in user behavior
  - Li et. al. [7] provides a theoretical model for intrusion detection
    - Feature vector: observables
    - Three feature ranges:
      - \{suspicious\} = \{normal\} \cap \{anomalous\}.
    - Feature vectors are gradually aggregated into one of the three ranges.
    - How to select the appropriate features?
      - Use GAs to select the relevant features
We propose a layered architecture in implementing a Proactive Process Monitor (PPM). The current design contains three layers:

- The top layer quickly spots unauthorized user processes by process name with minimal overhead.
- The middle layer utilizes a GA-generated rule base to capture the unauthorized processes associated with particular user roles with reasonable overhead.
- The bottom layer performs statistical analysis over the remaining processes for any “low-and-slow” deviations from the expected process patterns associated with user roles.
- Suspicious or resource-draining processes from the above three layers are logged securely at a separate site for offline analysis by forensic tools.
The small-user-world principle [6]

- Users in same job functions are expected to perform similar authorized actions on an organization’s computer systems.
- User roles can be mapped to user actions, which can be turned into observables for the detector.
- The recurrence of deviations as observed in users’ actions (e.g. processes) may trigger an alarm in the detector.
Further research

- Completing our work on mappings from user roles to actions in line with organization-specific computer security policies:
  - Role-Based Access Control (RBAC [9])

- Improving the statistical approach:
  - Refine process metrics
  - Avoid indiscriminate system call tracing for cost concerns

- Validating our approach with experiments:
  - Lacking good test data for insider threat detection
  - Budget, time and legal constraints for using human subjects
  - Simulation?
References