The Need for a Standard for the Format and Content of Audit Trails

Katherine Price

Purdue University

COAST Computer Security Lab

kep@cs.purdue.edu

Topics of Discussion

- Problem of No Widely Accepted Standard
- Difficulties with Lack of Content
- Difficulties with Tool Migration
- Difficulties with Data Reconciliation
- Some Proposed Standards
- Current Work to Develop a Standard

No Widely Accepted Standard

- Each audit source creates its own ad-hoc standard for format and content
  - the format for the audit trails varies greatly from system to system
  - each system gathers different data based on what the developer believed was important
- Disparity in format and content of audit data impedes progress in intrusion detection

Impediments to Progress in Intrusion Detection Methods

- Three major difficulties face intrusion detection techniques
  - difficulties with lack of content
  - difficulties with tools migration
  - difficulties with data reconciliation
- A standard for format and content would help overcome these impediments

Difficulties with Lack of Content

- Many current auditing systems do not supply enough data
  - lack of record activities
  - lack of detail
- Intrusions are not being detected because of insufficient evidence in audit trail

Bindings and Lack of Detail

- Audit data often does not contain enough information to resolve bindings
  - files names are transient bindings that may change over the life of the file
  - file descriptors, such as inode numbers in UNIX, are fixed throughout the life of the file
- Race condition attacks often take advantage of binding resolution problems

Difficulties with Tool Migration

- Many detection tools are designed for a particular audit source
- Difficulties in changing audit source
  - disparity in types of data available
    - » algorithms tailored for particular data may become ineffective
  - converting between formats is difficult
- Disparity in audit data makes it difficult to migrate tools to new audit sources

Difficulties with Data Reconciliation

- Detection systems must analyze data from multiple sources to uncover new, sophisticated attacks
- Many possible sources of information
  - applications and operating systems
  - firewalls and routers
- Disparity in audit data makes it difficult to reconcile multiple audit sources

Some Proposed Standards

- Standards for Content
  - C2 Level Audit
    - » standard is too broad
    - » different interpretations of “security relevant event”
- Standards for Format
  - ASAX’s NADF
  - Bishop’s Format
    - » Both handle UNIX OK, but difficulties may arise with other sources, especially with hierarchical data