A Privacy-Preserving Interdomain Audit Framework

Adam J. Lee, Parisa Tabriz, and Nikita Borisov

Abstract

Recent trends in Internet computing have led to the popularization of many forms of virtual organizations. E.g., data and resources are often shared across organizational boundaries and we have seen an increase in businesses outsourcing tasks to third parties. This creates more points of vulnerability and allows attackers to carry out more widely distributed forms of attacks. A process that coordinates information from each organization could detect correlated attacks, but the privacy concerns of each entity often restrict this level of information flow. We present a privacy-preserving framework for distributed audit that allows collaborating organizations to detect distributed attacks without requiring the release of excessive private information.

Step 1: Audit Group Formation

Audit Group: Organizations with a mutual interest to detect correlated attacks

Practical Scenarios
Research labs
Grid computing
Virtual organizations
Depts. in large corporations

Organization Trust
Organizations have some pre-existing trust
• Loose coalitions
Shared key protects log entries:
• Each organization knows key
• Does not share it with auditor
Organizations may probe for information with false log entries
• Detect this during alert reporting

Step 2: Log Obfuscation

The General Log Obfuscator (GLO) accepts audit logs, a group key, and a policy defining obfuscation methods for each data item to be disclosed to the auditor.

Log Data Formats
Identifiers (e.g. DEBUG, WARN)
Numbers (e.g. 80, 3.14)
Trees (e.g. 192.168.0.1, /usr/bin)
Partial Order (e.g. Role hierarchy)
Lists (e.g. Packet header fields)

Obfuscation Methods
Full disclosure
Local exact match
Portion dropping
Local prefix match
Local greater-than
Basic numeric transformations
Local blinded arithmetic
Complete obfuscation

Step 3: Detection

Auditor: Chosen by audit group
• Runs code submitted by alert group
• Operates on obfuscated records only
• Generates alerts

Step 4: Alert Generation

If an auditor detects a correlated attack, he sends an alert to those organizations that were involved.

How do you catch a bad auditor?
• Fake alerts: sign log records
• Detect invalid alerts
• Missing alerts: plant fake log sequences
• Probabilistic guarantee of completeness
• Ongoing work

Obfuscation Methods:
Data items in logs are disclosed at different levels of granularity.

Examples:

Portion Dropping

Local Exact Match

Local Greater Than

Local Prefix Match

Local Blinded Summation

Obfuscation details…