Measuring the Forensic-ability of Audit Logs for Nonrepudiation

Jason King :: jtking@ncsu.edu
Advisor: Laurie Williams :: laurie_williams@ncsu.edu

Problem

Repudiation Threats: users who deny performing an action without other parties having any way to prove otherwise

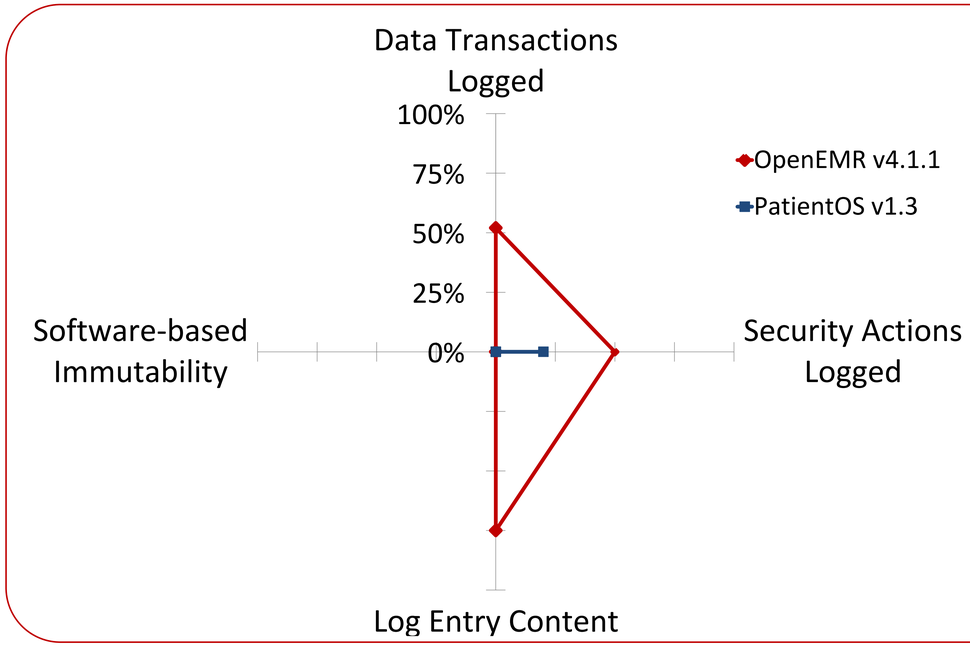
"Modifying Without a Trace"

Initial Findings

- **Inconsistent Logging Mechanisms** fail to log some actions, such as:
  - Data views
  - Granting user privileges
  - Access to audit log files
- **Inadequate Organizational Procedures** for securing log file integrity

Objective

Measure the degree to which a given audit log file captures the data necessary to allow for meaningful forensic analysis of user behavior within the software system



Related Publications

J. King, B. Smith, and L. Williams, "Audit Mechanisms in Electronic Health Record Systems: Protected Health Information May Remain Vulnerable to Undetected Misuse," International Journal of Computational Models and Algorithms in Medicine, vol. 3, p. 19, April-June 2012.

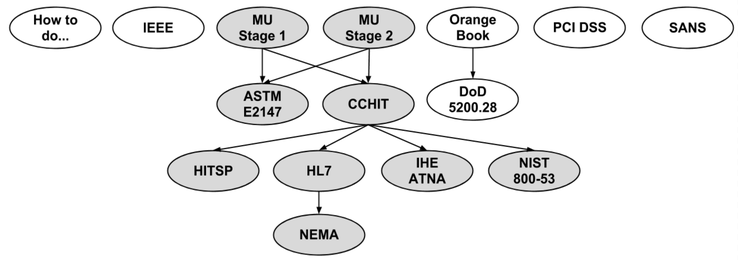
J. King, B. Smith, and L. Williams, "Modifying Without a Trace: General Audit Guidelines are Inadequate for Electronic Health Record Audit Mechanisms," presented at the ACM SIGHIT International Health Informatics Symposium, Miami, Florida, USA, 2012.

J. King, L. Williams, "Secure Logging and Auditing in Electronic Health Records Systems: What Can We Learn from the Payment Card Industry," 3rd USENIX Workshop on Health Security and Privacy, Bellevue, Washington, USA, 2012.

Validation

- Demonstrate practicality, economic productivity, usability, predictability, meaningfulness
- User studies

Initial Research



The following components affect forensic-ability:

- **Data Transactions Logged**
  Currently cataloged: 11 data transactions
- **Security Actions Logged**
  Currently cataloged: 77 security events
- **Log Entry Content**
  Currently cataloged: 22 log entry content
- **Software-driven Immutability**
  Prevent modifications of log entries
- **Timestamp Reliability**
  Synchronize timestamps system-wide
- **Log Backups**
  How often to perform backups
- **Log Retention**
  How long to keep log files
- **Policy-driven Immutability**
  Prevent modifications of log entries