
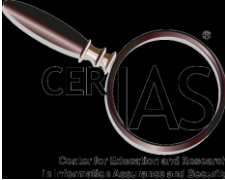


PURDUE
UNIVERSITY

CS62600: Advanced
Information Assurance

Logging and Audit
September 3, 2009
Prof. Chris Clifton



What is Auditing?

- Webster: a methodical examination and review
- Information Security: An a-posteriori technique to identify security violations
 - How does this help maintain security?

Fall 2009 CS626 2



Issues



- What information do we need?
 - After the fact – current state of system isn't enough
 - *logging*
- How do we perform an Audit?
 - Audit methodology
- What do we do with the results?

Fall 2009

CS626

3



Logging



- Goal: Record all information that might be needed for an audit
 - Authentication attempts
 - Failed only?
 - Access to trusted resources
 - All? Just failed attempts?
- Log must enable detection of security violations
 - Is this enough?

Fall 2009

CS626

4



Example: Bell-LaPadula



- What must be logged?
 - Action (read/write)
 - Level of subject
 - Level of object
- Can now check
 - Read: $S \geq O$
 - Write: $O \geq S$
- Is this necessary?
 - What if system validated as not allowing illegal read/write?
- What about change of security level?

Fall 2009

CS626

5



Logging *Trusted* Operations



- Secure system *prevents* security violations
- Trusted components: those that *can* violate security
 - Assumptions made to justify system secure
- Log actions by trusted components
 - Change in security level
 - Operations performed while not at maximum level

Fall 2009

CS626

6



Logging: Implementation



- Log must be protected
 - Doesn't do any good if security violations erased from log
- Sanitization
 - Remove sensitive information from log
 - Why?
 - Before or after logging?

Fall 2009

CS626

8



Audit



- Detect security violation
 - State-based auditing: identify if state at prior time is valid
 - Transition-based auditing: Identify if prior transition would lead to unauthorized state
- Detect attempts to breach security
 - Not necessarily violations

Fall 2009

CS626

9



Example: Sarbanes-Oxley



- Goal: Financial transparency
- Method: Audit
- Information Assurance Mandates
 - Little encoded in law
 - Authority given to Public Company Accounting Oversight Board
 - Requirements for internal controls, maintenance of audit information
 - *Jail time for failure*
- Outcome: Significant investment in data integrity and provenance

Fall 2009

CS626

13



SOX – The Hype



- “Solution providers looking to assist public companies coping with the complexities of the Sarbanes-Oxley Act might find peace of mind with new tools from Microsoft and Oracle.” ([CRN, March 30, 2004](#))
 - “Section 404 also gives companies a mere 48-hour window to disclose material events”
- The crux of this list and SoX is protecting “sensitive user information” ([JasonKolb.com](#))

Fall 2009

CS626

14



Internal Controls requirement

- (a) **RULES REQUIRED.**—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—
- (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
 - (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
- (b) **INTERNAL CONTROL EVALUATION AND REPORTING.**—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

[15 USC 7213 Sec. 404](#)



Internal Controls requirement

- (II) an evaluation of whether such internal control structure and procedures—
- (aa) include maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer;
 - (bb) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer; and

[15 USC 7213 Sec. 103\(a\)\(2\)\(A\)\(iii\)](#)

- Discussion: What must be Logged?



Teeth (1)



- **§ 1519. Destruction, alteration, or falsification of records in Federal investigations and bankruptcy**

Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.

[18 USC 73 Sec. 1519](#)

Fall 2009

CS626

17



Record Maintenance



- **§ 1520. Destruction of corporate audit records**

(a)(1) Any accountant who conducts an audit of an issuer of securities to which section 10A(a) of the Securities Exchange Act of 1934 (15 U.S.C. 78j– 31(a)) applies, shall maintain all audit or review workpapers for a period of 5 years from the end of the fiscal period in which the audit or review was concluded.

(2) ... (including electronic records) ...

(b) Whoever knowingly and willfully violates subsection (a)(1), or any rule or regulation promulgated by the Securities and Exchange Commission under subsection (a)(2), shall be fined under this title, imprisoned not more than 10 years, or both.

[18 USC 73 Sec. 1520](#)

- Discussion: What does this mean for IA?

Fall 2009

CS626

18