Data Exchange for Audit Information

Joshua Franklin

Peter Zelechoski

VVSG View on Audit Logs

- **VVSG 2005 Volume 1 Requirement 2.1.5**

  Election audit trails provide the supporting documentation for **verifying the accuracy** of reported election results. They present a concrete**, indestructible archival record of all system activity** related to the vote tally, and are **essential for public confidence** in the accuracy of the tally, for **recounts**, and for **evidence** in the event of criminal or civil litigation.

(Emphasis added)

VVSG View on Audit Logs (continued)

- Audit records shall be prepared for all phases of election operations performed using devices controlled by the jurisdiction or its contractors.
- The timing and sequence of audit record entries is as important as the data contained in the record.
  - systems shall provide the capability to create and maintain a real-time audit record
  - All audit record entries shall include the time-and-date stamp
  - Voting systems shall provide a capability for the status messages to become part of the real-time audit record.
  - (for shared computing environments) operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object

VVSG View on Audit Logs (continued)

- **Pre-election Audit Records**, the log shall include:
  a. The allowable number of selections a contest
  b. The combinations of voting patterns permitted or required by the jurisdiction
  c. The inclusion or exclusion of contests as the result of multiple districting within the polling place
  d. Any other characteristics that may be peculiar to the jurisdiction, the election or the polling place location
  e. Manual data maintained by election personnel
  f. Samples of all final ballot formats
  g. Ballot preparation edit listings

VVSG View on Audit Logs (continued)

- **System Readiness Audit Records**, minimum requirements include:
  a. Prior to the start of ballot counting ... generate a readiness audit record ... shall include the identification of the software release, the identification of the election to be processed, and the results of software and hardware diagnostic tests
  b. systems used at the polling place ... shall include polling place identification
  c. record the correct installation of ballot formats on voting devices
  d. record the status of all data paths and memory locations to be used in vote recording
  e. Upon the conclusion of (System Readiness) tests ... the audit record (shall record) that the test data have been expunged
  f. results of the ballot reader and arithmetic-logic accuracy test
  g. systems that use a public network (for sending ballots) report the test ballots ... include: the number of ballots sent, when each ballot was sent, the machine from which each ballot was sent, specific votes or selections contained in the ballot

VVSG View on Audit Logs (continued)

- **In-process Audit Records** document system operations during diagnostic routines and the casting and tallying of ballots. At a minimum they shall contain:
  a. Machine generated error and exception messages
  b. Critical system status messages ... include, but are not limited to: diagnostic and status messages upon startup; the “zero totals” check conducted before opening the polling place or counting a precinct centrally; for paper-based systems, the initiation or termination of card reader and communications equipment operation; for DRE machines, the event (and time, if available) of activating and casting each ballot
  c. Non-critical status messages that are generated by the machine's data quality monitor or by software and hardware condition monitors
  d. all normal process activity and system events that require operator intervention

Types of Logs

- AUDIT LOG
- CONFIGURATION LOG
- CONSOLE LOG
- INTERNAL AUDIT LOG
- MAINTENANCE LOG
- OPERATING SYSTEM LOG
- PROBLEM LOG
- SOFTWARE IDENTIFICATION VERIFICATION LOG
- SOFTWARE INTEGRITY VERIFICATION LOG
- VOTING SYSTEM CONFIGURATION LOG

Our Focus

Audit Logs

- A time-stamped record of significant events that occur during an election.
  Source: Electronic Voting Glossary, Michael Shamos
- "A system generated record, in either machine readable or printed format, providing a record of activities and events relevant to initialization of election software and hardware, identification of files containing election parameters, initialization of the tabulation process, processing of voted ballots, and termination of the tabulation process."
  Source: Florida Voting System Standards Appendix
- An "electronically stored record of events and ballot images from which election officials may produce a permanent paper record with a manual audit capacity for a voting system using voting machines."
  Source: Ark. Code §7-1-101(2). Cf. AUDIT TRAIL (def. 2)

Items to Remember

- Not logging in XML
- Platform dictates logging methodology
- Data exchange of log information
- Not for older equipment

Some Goals of Logs

- A tool to reconstruct an election
- A tool for providing information not just data
- A way to identify faulty machines and poor election practices
- Provide a legally defensible continual chain of custody of their unaltered records
- A public record to support public confidence in the voting system

Poor Practices

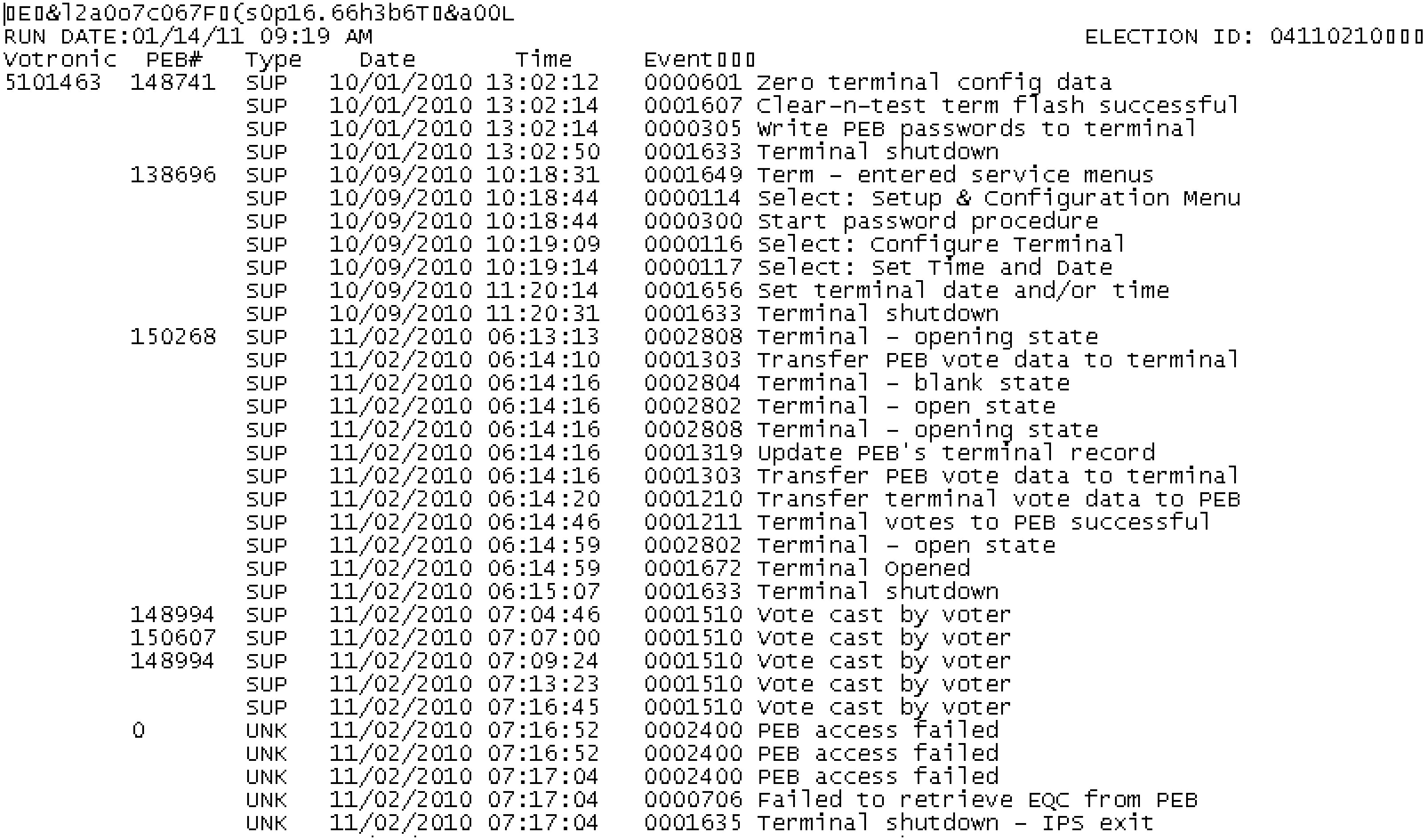
- Not recording important/significant events (e.g., ballot cast)
- Difficult to access (e.g., encrypted, requires specialized knowledge, nonexistent) << encryption may be necessary when logging confidential information, it is not always a bad practice
- Ambiguous events (e.g., error)

Non-exhaustive List of Events

- Booting and shutting down of a system.
- Logging into and signing off of a system.
- Failed attempts at logging onto a system.
- Session connections by operators or sub-systems.
- Starting and stopping of a program (also when launched from a menu).
- Reading of precinct media into the central system.
- Data transfer from one machine or program to another machine or program by any means.
- Write operation to a data file or database
- Creation or modification of a ballot definition.
- Transfer of the ballot definition.
- Generation of reports.
- Manual inserts or modifications to election results.
- Error messages.
- Recovery from a power or component failure.
- Password changes.
- Readiness testing.
- Opening and closing of polls.
- Adding or removing precinct machines to the election setup and/or operational status

Source: EAC Request for Interpretation 2009-04 (Audit Log Events)

2010 General, Anderson Co., SC



```
▯E▯&l2a0o7c067F▯(s0p16.66h3b6T▯&a00L
RUN DATE:01/14/11 09:19 AM                                                  ELECTION ID: 04110210▯▯▯
Votronic  PEB#    Type    Date       Time      Event▯▯▯
5101463  148741   SUP   10/01/2010 13:02:12   0000601 Zero terminal config data
                  SUP   10/01/2010 13:02:14   0001607 Clear-n-test term flash successful
                  SUP   10/01/2010 13:02:14   0000305 Write PEB passwords to terminal
                  SUP   10/01/2010 13:02:50   0001633 Terminal shutdown
         138696   SUP   10/09/2010 10:18:31   0001649 Term - entered service menus
                  SUP   10/09/2010 10:18:44   0000114 Select: Setup & Configuration Menu
                  SUP   10/09/2010 10:18:44   0000300 Start password procedure
                  SUP   10/09/2010 10:19:09   0000116 Select: Configure Terminal
                  SUP   10/09/2010 10:19:14   0000117 Select: Set Time and Date
                  SUP   10/09/2010 11:20:14   0001656 Set terminal date and/or time
                  SUP   10/09/2010 11:20:31   0001633 Terminal shutdown
         150268   SUP   11/02/2010 06:13:13   0002808 Terminal - opening state
                  SUP   11/02/2010 06:14:10   0001303 Transfer PEB vote data to terminal
                  SUP   11/02/2010 06:14:16   0002804 Terminal - blank state
                  SUP   11/02/2010 06:14:16   0002802 Terminal - open state
                  SUP   11/02/2010 06:14:16   0002808 Terminal - opening state
                  SUP   11/02/2010 06:14:16   0001319 Update PEB's terminal record
                  SUP   11/02/2010 06:14:16   0001303 Transfer PEB vote data to terminal
                  SUP   11/02/2010 06:14:20   0001210 Transfer terminal vote data to PEB
                  SUP   11/02/2010 06:14:46   0001211 Terminal votes to PEB successful
                  SUP   11/02/2010 06:14:59   0002802 Terminal - open state
                  SUP   11/02/2010 06:14:59   0001672 Terminal opened
                  SUP   11/02/2010 06:15:07   0001633 Terminal shutdown
         148994   SUP   11/02/2010 07:04:46   0001510 Vote cast by voter
         150607   SUP   11/02/2010 07:07:00   0001510 Vote cast by voter
         148994   SUP   11/02/2010 07:09:24   0001510 Vote cast by voter
                  SUP   11/02/2010 07:13:23   0001510 Vote cast by voter
                  SUP   11/02/2010 07:16:45   0001510 Vote cast by voter
         0        UNK   11/02/2010 07:16:52   0002400 PEB access failed
                  UNK   11/02/2010 07:16:52   0002400 PEB access failed
                  UNK   11/02/2010 07:17:04   0002400 PEB access failed
                  UNK   11/02/2010 07:17:04   0000706 Failed to retrieve EQC from PEB
                  UNK   11/02/2010 07:17:04   0001635 Terminal shutdown - IPS exit
```

Source: http://www.scvotinginfo.com/wp/data/

System Clock Integrity

What’s wrong with these log entries recorded during a May 18 primary?

- **5/18/2010 05:36 AM - Polls Opened**
- **1/18/2019 04:44 AM - Security Disengaged**
- **5/18/2010 05:36 AM - Diagnostics**

Detecting Problems

What's wrong with these log entries recorded during a May 8 primary?

Machine 1

- 5/8/2010 01:00 AM Polls Opened

Machine 2

- 5/7/2010 09:13 PM Polls Opened

EML 480* (part 1)

```
•    <?xml version="1.0" encoding="UTF-8"?>
•    <EML xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
•      xsi:schemaLocation="urn:oasis:names:tc:evs:schema:eml ../../480-auditlog-v7-0.xsd"
•      xmlns="urn:oasis:names:tc:evs:schema:eml"   xmlns:ts="urn:oasis:names:tc:evs:schema:eml:ts"
•      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
•      xmlns:al="urn:oasis:names:tc:ciq:xal:4“ xmlns:nl="urn:oasis:names:tc:ciq:xnl:4"
•      Id="480” SchemaVersion="7.0">
•      <!--you will need to point the xsi at a server\folder where the schemas are available
         in this example, we use the ../../ to point it at 2 folders up from where this document is stored -->
•    <EMLHeader>
•        <TransactionId> 480</TransactionId> <!--a static value that is always 480 for this EML message -->
•        <SequenceNumber>1</SequenceNumber> <!--This is the first message in this EML480 set -->
•        <NumberInSequence>2</NumberInSequence> <!--There are 2 EML480 messages in the set -->
•    <SequencedElementName>Set20120309ABC</SequencedElementName>
     <!--name for the set == the creator can make it anything they want but it needs to match across the set-->
•        <OfficialStatusDetail>
•          <OfficialStatus>Official</OfficialStatus>
•          <StatusDate>2012-03-09</StatusDate> <!-- The current date when it is generated -->
•        </OfficialStatusDetail>
•        <!--The "SEAL" which contains a digital signature for the message goes here -->
•      </EMLHeader>
```

EML 480* (part 2)

- <AuditLog>
  - <!--would like either a Type attribute or an AuditLogType child element -- allow for an enumeration that can be localized-->
  - <!-- Log types might include AUDIT LOG, CONFIGURATION LOG, CONSOLE LOG, INTERNAL AUDIT LOG, MAINTENANCE LOG, OPERATING SYSTEM LOG, PROBLEM LOG, SOFTWARE IDENTIFICATION VERIFICATION LOG, SOFTWARE INTEGRITY VERIFICATION LOG, VOTING SYSTEM CONFIGURATION LOG -->
- <EventIdentifier IdNumber="12345"/>
- <ElectionIdentifier IdNumber="X45N234”>
  <ElectionName>2012 Primary Election for Jurisdiction Alpha</ElectionName></ElectionIdentifier>
- <Update>no</Update>
  <!--this is a yes or no value (case sensitive); no means it is the first issuance; yes means it updates a previous issuance -->
- <LoggedSeal>
  <!--Logged Seal is a required element right now ; would like to make this not required, since we are “encouraging” use of the SEAL in the header -->
- <Seal><ds:Signature><ds:SignedInfo>
- <ds:CanonicalizationMethod Algorithm=""></ds:CanonicalizationMethod>
- <ds:SignatureMethod Algorithm=""></ds:SignatureMethod>
- <ds:Reference><ds:DigestMethod Algorithm=""></ds:DigestMethod>
- <ds:DigestValue></ds:DigestValue></ds:Reference>
- </ds:SignedInfo>
- <ds:SignatureValue></ds:SignatureValue>
- </ds:Signature>
- </Seal>
- </LoggedSeal>

EML 480* (part 3)

- <Message>log record 1</Message><!--This is an actual log record ;
- in many other spots we have the Messages structure which allows for multiple Message children;
- We need to modify this to use this parent/child structure-->
- <!--Also want to allow for some structure in the individual Message elements -->
- <!--attributes needed include:
- MachineIdentifier
- Phase (pre-election, system-readiness, in-process, other?),
- Type (EAC RFI 2009-04 listing, possibly others),
- UserId (identification code of the user, might be the system if it is a system level task),
- MessageCode ()
- Message Severity ()
- DateTime ()-->
- <!--child elements needed include: ??? -->
- <!--content needed include: TextualMessage -->
- </AuditLog>

EML 480* (part 3 sample)

- <Messages>
- <Message Type=“Boot” Phase=“pre-election” MachineIdentifier=“B2-E1-15-BE-1C-5B”
  UserId=“none” MessageCode=“A0001A01” MessageSeverity=“Informational”
  DateTime=“20120308T11:20:11.987”>System Booted</Message>
- <Message Type=“Login” Phase=“pre-election” MachineIdentifier=“B2-E1-15-BE-1C-5B”
  UserId=“j2345” MessageCode=“E1234C98” MessageSeverity=“Informational”
  DateTime=“20120308T11:21:22.876”>Log In Failed</Message>
- <Message Type=“Login” Phase=“pre-election” MachineIdentifier=“B2-E1-15-BE-1C-5B”
  UserId=“j2345” MessageCode=“A5467B21” MessageSeverity=“Informational”
  DateTime=“20120308T11:22:33.765”>User Logged In</Message>
- <Message Type=“ElectionDefinition” Phase=“pre-election” MachineIdentifier=“B2-E1-15-BE-1C-5B”
  UserId=“j2345” MessageCode=“B98967A11” MessageSeverity=“Informational”
  DateTime=“20120308T11:23:44.654”>Open Election Definition</Message>
- </Messages>
- </AuditLog>