



Automating Voting Terminal Event Log Analysis

Tigran Antonyan, Seda Davtyan, Sotirios Kentros, Aggelos Kiayias,
Laurent Michel, Nicolas Nicolaou, Alexander Russell,
Alexander A. Shvartsman

Voting Technology Research (VoTeR) Center
University of Connecticut

<http://voter.engr.uconn.edu>

Presented by Nicolas Nicolaou

Work funded by the Connecticut Secretary of the State Office

Why Auditing?



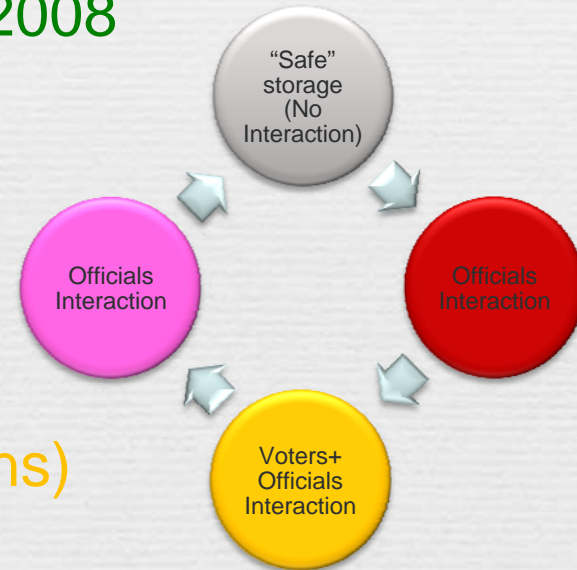
[<http://www.statehousereport.com>]

Motivation

- Electronic Voting Technologies
 - Direct Recording Electronic (DRE)
 - Optical Scan (OS) tabulator
 - ❖ VVPAT – Voter Verifiable Paper Audit Trail
 - ❖ Used in over 50% of counties in 2008

- Terminal Usage in Election Procedures

- “Safe” Storage
 - ❖ No Interaction (?)
- Polling Place
 - ❖ Officials (Before Election)
 - ❖ Voters + Officials (During Elections)
 - ❖ Officials (After Elections)



- **Is the interaction with the terminal benign and does it follow the election procedures?**

Question

How can someone check the **Actions and **their Validity**, performed on an E-Voting Terminal during an Election Process?**

Can we devise an **Automated Procedure to perform this check?**

The Event Log

- What is an Event Log
 - A list of **Timestamped Entries**
 - ❖ Actions performed on the terminal, and
 - ❖ Time/Date associated with any recorded action
 - ❖ What actions are recorded?

- Where an Event Log is found
 - In every **E-voting Terminal with Logging Capabilities**
 - ❖ Usually **Dedicated Memory Space**

- Event Logs are useful for:
 - **Monitoring actions on e-voting terminals**
 - ❖ **Before, During and After the elections**
 - **Report environmental effects**
 - ❖ **i.e. Power Failure**

Why Auditing the Event Log?

- Detect **Expected** Event Histories
 - Compliant with electoral procedures
- Detect **Irregular** Event Histories
 - Deviation form electoral procedures
 - Malfunction of machines
 - Reveal any malicious intent
- To **Improve** Electoral Procedures
 - Minimize procedural uncertainties
 - Increase the chance of detecting malicious actions

Event Log Audit is Essential for any Election Process



Every E-Voting System should provide an Event Log

The Need for Independent Log Audit

- E-Voting Systems with Logging Capabilities
 - Print Event Log
 - Provide Software to read and analyze the Event Log
 - ❖ Usually Developed by the Vendor

- Issues
 - Printing Module
 - ❖ Module Defects
 - Wrong Sequence of events
 - ❖ Manual Parse of the printout
 - Time Consuming and Inaccurate
 - Vendor Software
 - ❖ Reliability
 - What are the analysis criteria?
 - ❖ Conflict of Interest?
 - Is it trustworthy?

Our Approach

- **Understand and Parse** the Log
 - Input: **Event Log raw data and format**
 - Output: **Exact Action sequence recorded in the Log**
- **Examine** log sequences in light of predefined Action Rules
 - Rules can be customized by
 - ❖ **Voting Terminal: Actions it can record**
 - ❖ **Election Process: Sequence of Actions it contains**
- **Report** whether Log Sequences satisfy the Rules

Case Study: AccuVote (AV-OS)

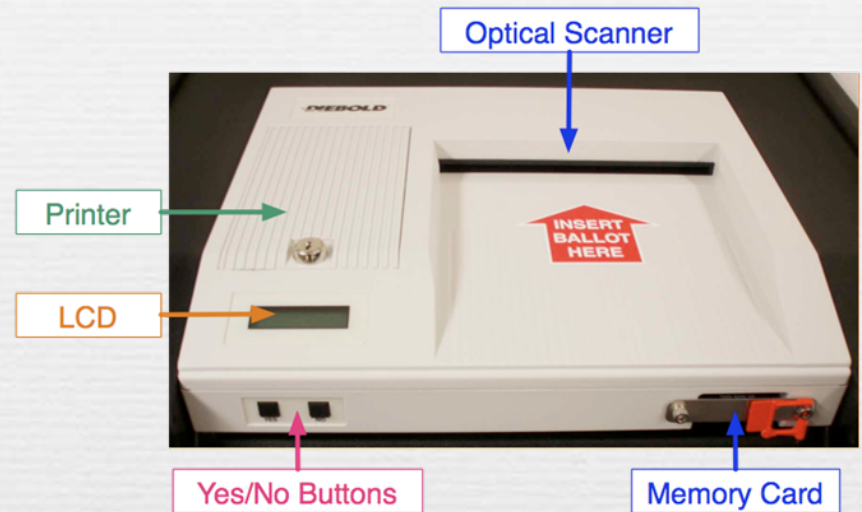
- Premier's Accu-Vote Optical Scan tabulator
 - Provides inherent VVPB/VVPAT
 - But is not perfect:
 - ❖ Tampering with Memory cards [Hursti'05], [EVT'07]
 - ❖ Firmware manipulations [SAC'09]
 - ❖ Reports by others and CA, CT, FL, AL,...

- Provides **Logging Capabilities**
 - Printing the Event Log for Auditing
 - ❖ Print Module is Defective
 - Suffers from other Deficiencies

Case Study: AccuVote OS (AV-OS)

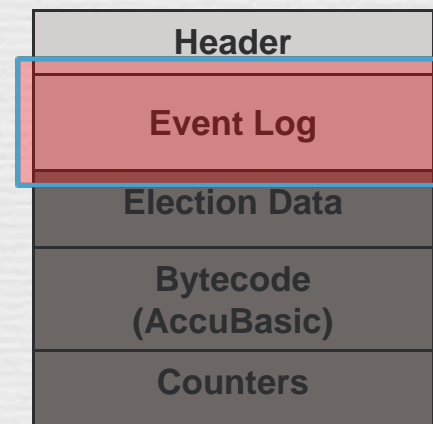
Physical Characteristics

- Firmware Version 1.96.6
- Input Devices
 - ❖ Yes/No Buttons
 - ❖ Optical Scanner
- Output Devices
 - ❖ Printer
 - ❖ LCD



Memory Card

- Contains Election Data
- Divided in 5 sections
- Contents of the MC obtained by build-in extraction module



Applying Our Approach: AV-OS Logs

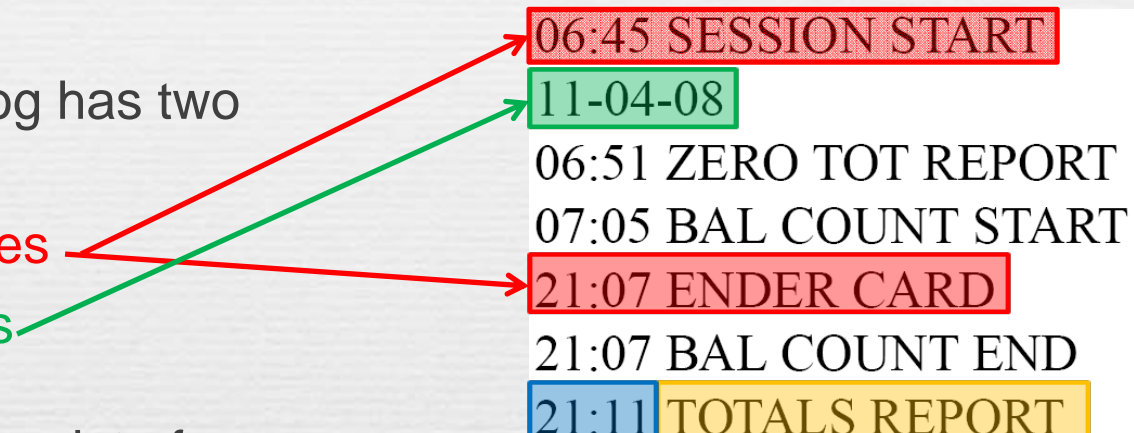
- Design and Implement a Procedure for AccuVote OS Event Log Audit
 - Parse, analyze and evaluate event logs
 - ❖ Automated Log Analyzer
 - General for other E-Voting Systems
- Discover AV-OS event log Defects and Deficiencies
- Used in the Event Log Audit in the CT Presidential Elections of November 2008

Log Audit Procedure at a Glance

1. Understand the contents of the AV-OS Event Log
2. Model AV-OS as a finite state machine (FSM)
 - AV-OS states
 - State transitions (Actions)
 - Logged Events
3. Specify the electoral process
 - Augment FSM Actions with Time-Sensitive information based on the definition of the electoral process.
4. Develop Analysis Tool
 - Parse AVOS Event Log
 - Compare the Event Action Sequence over Time-Sensitive Action Sequence Rules

AV-OS Event Log Entries

- ❑ Log entries: 512
 - Circular Buffer
- ❑ AV-OS Event Log has two types of entries:
 - Action entries
 - Date entries
- ❑ Action entries consist of
 - Time of occurrence
 - Action name
- ❑ Date entries only follow:
 - INITIALIZED action
 - SESSION START action



06:45 SESSION START
 11-04-08
 06:51 ZERO TOT REPORT
 07:05 BAL COUNT START
 21:07 ENDER CARD
 21:07 BAL COUNT END
 21:11 TOTALS REPORT

Event Types Recorded by AV-OS

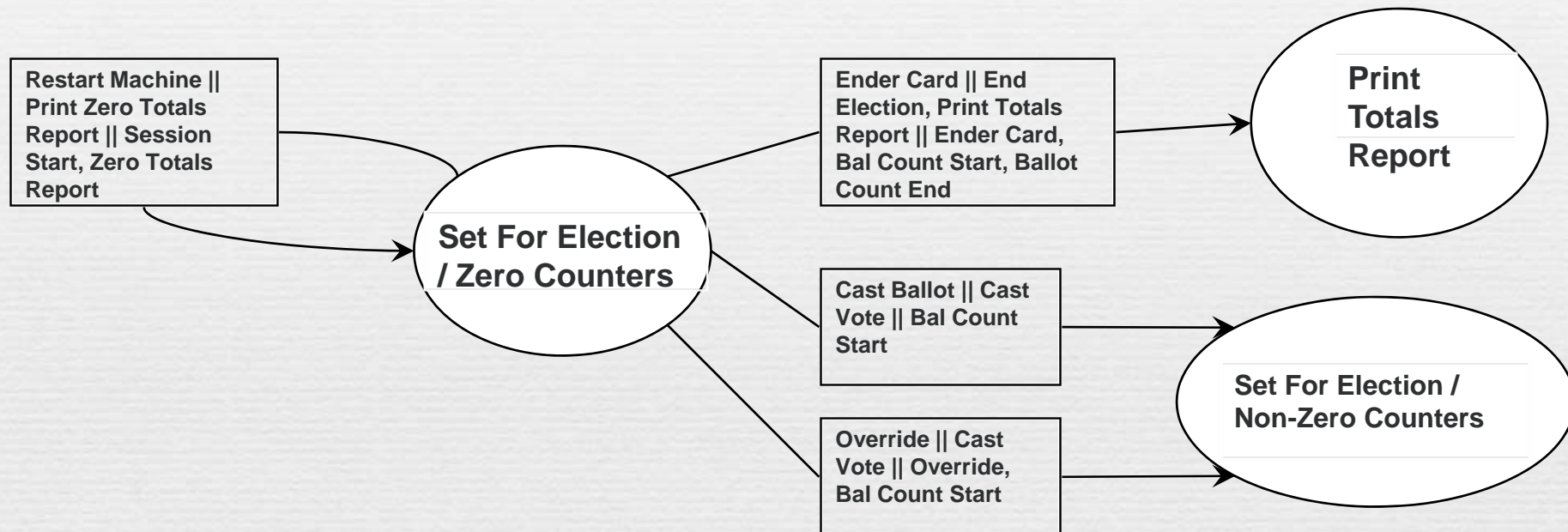
Action Name	Action Description
AUDIT REPORT	Appears when an Audit Report is printed.
BAL COUNT END	After the ender card is inserted in an election, this action appears.
BAL COUNT START	Appears when the first ballot is cast in an election.
BAL TEST START	Records the beginning of a test election.
CLEAR COUNTERS	Appears when the counters are set to zero.
COUNT RESTARTED	Appears if the machine is reset during an election, after at least one ballot is cast.
DOWNLOAD END	Recorded during the download of data is ended.
DOWNLOAD START	Recorded during the download of data is started.
DUPLICATE CARD	Appears when a card is duplicated. Present in the master card and the copy.
ENDER CARD	Records when an ender card is inserted, signifying the end of an election.
INITIALIZED	The 1st action in the Log. Date action appears when one programs the card.
MEM CARD RESET	A memory card reset returns a card in 'not set' status, if it was set for election.
OVERRIDE	Records an override by a poll worker. Used for the insertion of overvoted ballots.
POWER FAIL	If the machine is unplugged or a power failure occurs, this action is recorded.
PREP FOR ELECT	Recorded when the card is set for election.
SESSION START	Date action. Appears every time you reset the machine.
TOTALS REPORT	Appears when a Totals Report is printed.
UNVOTED BAL TST	Appears when an unvoted ballot test is performed.
UPLOAD END	When an upload is completed, this action is recorded.
UPLOAD ERROR	Appears when an upload error is detected.
UPLOAD STARTED	Marks the beginning of an upload.
VOTED BAL TEST	Appears when an voted ballot test is performed.
ZERO TOT REPORT	Appears when a Zero Totals Report is printed.

Modeling AV-OS as a FSM

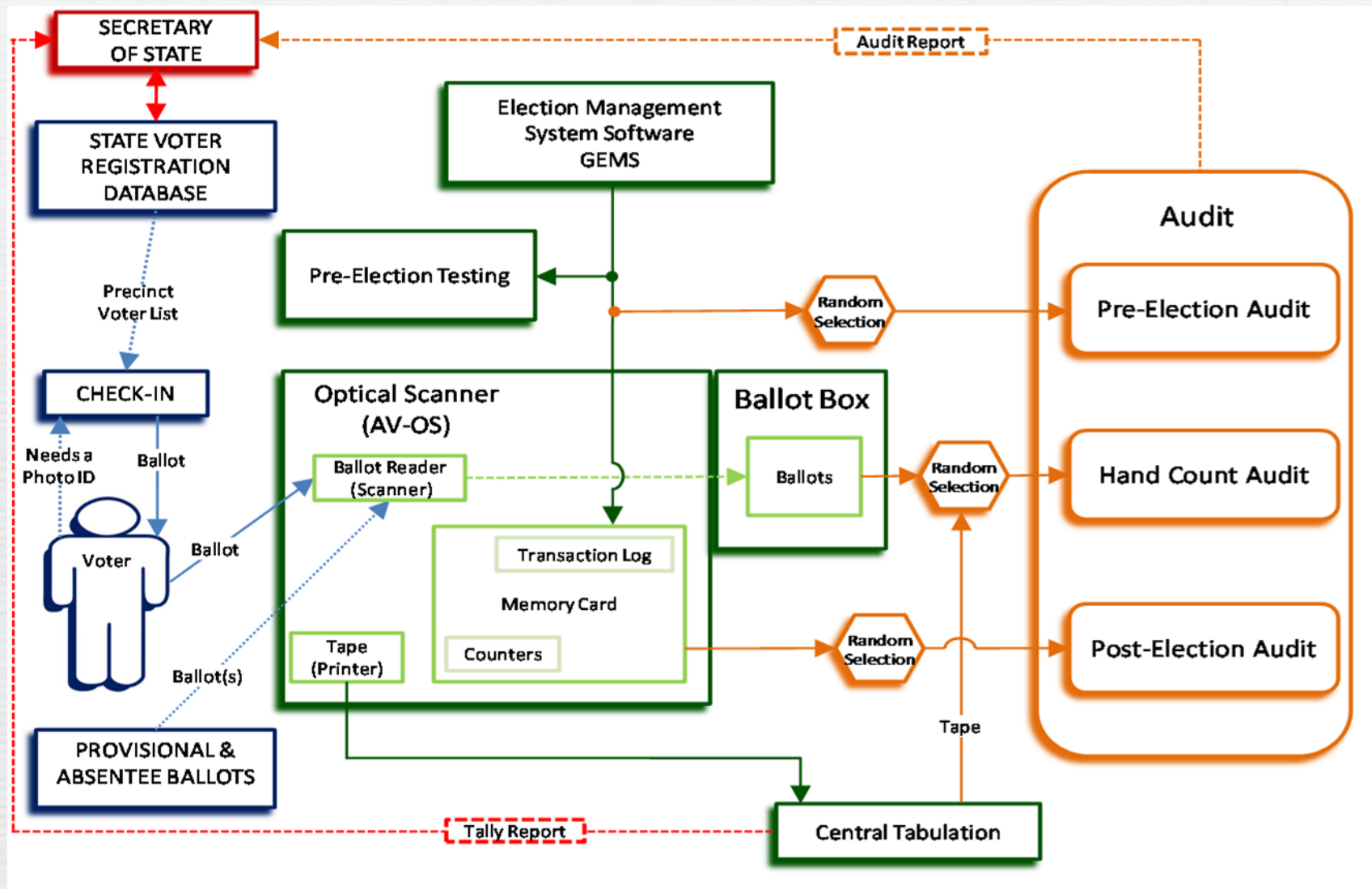
- States:
 - Preserved after a restart
 - ❖ Blank State
 - ❖ Loaded Election State
 - ❖ Set for Election with Zero Counters
 - ❖ Set for Election with Non-Zero Counters
 - ❖ Print Totals Report
 - ❖ Election Closed
 - Not preserved after restart
 - ❖ Voted Ballot Test
 - ❖ Unvoted Ballot Test
 - ❖ Test Election with Zero Counters
 - ❖ Test Election with Non-Zero Counters

- Transitions denoted by a triple $\langle U \parallel A \parallel L \rangle$
 - U: User action
 - A: Ensuing Sequence of Machine Actions
 - L: Sequence of Logged Events

Example – Set For Election State



Specify the Election Process



Time-Sensitivity of the Election Process

- ❑ Card Programming and Pre-Election testing **by Provider**
 - 3-4 weeks before the elections
- ❑ Pre-Election Testing and Setting for Election **in the Precincts**
 - 1-2 weeks before the elections
- ❑ Expected Sequence of timed events on Election Day:
 - **SESSION START-DATE, ZERO TOTALS REPORT**
 - ❖ Before the polls open
 - **BALLOT COUNT STARTS**
 - ❖ After the polls open
 - Any number of **OVERRIDE** events
 - ❖ While the polls are open
 - **ENDER CARD, BALLOT COUNT END, TOTALS REPORT**
 - ❖ When the polls close

Automating the Event Log Analysis

- Define a set of Time Sensitive Rules
 - Derived from FSM and Election Process
 - Rules defined in an XML file
 - ❖ Easily customizable

- Analysis Tool
 - Input: Set of Rules and AV-OS Event Log
 - Output: Return “Expected” or “Irregular”

Examples of Flagged Events

A. Expected Election Run

B. Restart During the Election Process

C. Power Failure and Restart During the Election Process

A. Expected Events	B. Flagged Events	C. Flagged Events
06:45 SESSION START 11-04-08 06:51 ZERO TOT REPORT 07:05 BAL COUNT START 21:07 ENDER CARD 21:07 BAL COUNT END 21:11 TOTALS REPORT	06:45 SESSION START 11-04-08 06:49 ZERO TOT REPORT 07:02 BAL COUNT START 11:20 SESSION START 11-04-08 11:20 COUNT RESTARTED 11:21 BAL COUNT START 21:03 ENDER CARD 21:03 BAL COUNT END 21:13 TOTALS REPORT	05:17 SESSION START 11-04-08 05:25 ZERO TOT REPORT 06:01 BAL COUNT START 08:10 POWER FAIL 10:47 POWER FAIL 13:17 SESSION START 11-04-08 13:17 COUNT RESTARTED 13:20 BAL COUNT START 14:44 POWER FAIL

AV-OS Event Log Defects/Deficiencies

- Printing an Overflowed Event Log

- “Totals Report” Recording Deficiency

- Date recording Deficiency

Printing Defect Demonstration

- Printing Enumerates Events
- Let an action event be denoted as $\langle s, n, t \rangle$
 - n : action name
 - t : time it occurred
- Let assume #entries=522
 - Date Entries = 11
 - Action Entries = 511
 - 10 first entries overwritten
 - ❖ Print starts from 11th entry $\langle n11, t11 \rangle$

Expected Behavior	Erroneous Behavior	Event Log Actions
Seq	Seq	Buffer
513	503	$\langle n513, t513 \rangle$
⋮	⋮	⋮
522	512	$\langle n522, t522 \rangle$
11	1 & 513	$\langle n11, t11 \rangle$
12	2 & 514	$\langle n12, t12 \rangle$
⋮	⋮	⋮
512	502	$\langle n512, t512 \rangle$

Beginning of buffer

First Not-Overwritten Entry

Expected Printout:

$\langle 11, n11, t11 \rangle, \langle 12, n12, t12 \rangle, \dots, \langle 512, n512, t512 \rangle, \dots, \langle 522, n522, t522 \rangle$

Erroneous Printout

$\langle 1, n11, t11 \rangle, \dots, \langle 502, n512, t512 \rangle, \dots, \langle 512, n522, t522 \rangle, \langle 513, n11, t11 \rangle, \dots, \langle 522, n22, t22 \rangle$

Duplicates

“Totals Report” Recording Deficiency

- Closing Election
 - Ender Card
 - Totals Report
 - Another Copy?

- Totals Report Event
 - **Not logged** unless “NO” is pressed
 - **Single** appearance in the log event

- Effects
 - Event is not logged
 - ❖ **Controversy** on the validity of printed totals report
 - Single appearance of the event affects
 - ❖ **Auditing Process**
 - ❖ **Electoral Process**

Date recording Deficiency

□ Deficiency

- Entries followed by date
 - ❖ INITIALIZE
 - ❖ SESSION START
- If >24 hours elapse from the date recording without any actions occurring
 - ❖ Cannot determine whether the next event occurred on the same date.

□ Effects

- Modification of the results
 - ❖ I.e., leave the terminal ON for a day, cast more votes and close it the next day at the expected time

```
06:45 SESSION START
11-04-08
06:51 ZERO TOT REPORT
07:05 BAL COUNT START
21:07 ENDER CARD
21:07 BAL COUNT END
21:11 TOTALS REPORT
```

Did these events
happen on
Nov 04, 2008?



Our Log Audit Procedure in Practice

- Connecticut Nov 2008 Presidential Elections
- We collected Event Logs from 421 AV-OS memory cards
 - 279 used in the elections
 - ❖ Corresponding to random selection of 30% of all precincts
 - 142 from back-up cards not used in the elections

Findings

- ❑ 314 out of 421 contain the **expected sequences**
- ❑ 15 (3.6%) had >10 SESSION START events
- ❑ 41 (9.7%) contained card duplication events
- ❑ 29 (6.9%) had a ZERO TOTALS REPORT printed before the date of the election.
- ❑ 24 (5.7%) were initialized between 10/27/2008 and 10/30/2008.
 - **Our pre-election audit included only cards programmed until 10/26/2008**
- ❑ 2 event logs had an additional ZERO TOTALS REPORT event during the election day.

Findings (Cont...)

- ❑ 1 event log had ELECTION CLOSE event at 22:08.
- ❑ 6 event logs had PREP ELECTION event the day of the election.
- ❑ 4 event logs had a MEMORY CARD RESET event.
- ❑ 1 event log had an UPLOAD STARTED event.
- ❑ 2 event logs had test elections on 10/31/08 and 1 event log showed a test election on 11/03/08.
- ❑ 1 event log had a test election on 11/26/08 and an election executed on 12/04/08.
- ❑ Findings Suggest
 - No serious security problem or malicious intent
 - Prescribed procedures are not followed uniformly

Summary

- Proposed and Developed an Automated Procedure for Event Log Analysis
 - Modeling AV-OS in terms of FSM
 - Time-Sensitive Action Rules
 - A tool to compare the actions in the logs over the defined rules
 - ❖ Our tool may be adjusted and used with other systems
- Discovered some defects and deficiencies in AV-OS logging procedures
 - Printing an Overflowed Event Log
 - “Totals Report” Recording Deficiency
 - Date recording Deficiency
- Used the automated tool in log analysis for CT Nov 2008 elections
 - Findings suggest no malicious intent but reveal non-uniformity in the electoral procedures

Conclusions

- Our Results Suggest
 - Full scale event log analysis is feasible
 - ❖ It provides information about
 - Usage of the machines
 - Deviation from procedures.
 - Should included in any procedural audit
 - ❖ Part of Post-Election Audit
 - Event Logs should be a part of any E-Voting Terminal



Thank You.

Questions?