



# Evaluating Electronic Poll Books: Challenges and Lessons

Matthew Desmarais and Alexander Schwarzmann

[desmarais@engr.uconn.edu](mailto:desmarais@engr.uconn.edu)

[aas@cse.uconn.edu](mailto:aas@cse.uconn.edu)

Work with

Laurent Michel and Alexander Russell

Center for Voting Technology Research

University of Connecticut

[voter.engr.uconn.edu](http://voter.engr.uconn.edu)

# Outline

- ❑ Introduction
- ❑ Electronic Poll Book Evaluation
- ❑ Evaluation Challenges
- ❑ Lessons Learned
- ❑ Conclusion and discussion

# VoTeR Center

voter.engr.uconn.edu

- ❑ UCONN Center for Voting Technology Research (VoTeR Center)
- ❑ Security and Integrity analysis of election systems
  - Voting Machines, EMS, E-PollBooks, etc.
  - Analysis of intrusion and tamper-resistance
  - Research and technology / Issue tracking
- ❑ Partnership with Connecticut Secretary of the State (SOTS) Office
  - Ongoing assessment of threat vectors
  - Technological audits: design, performance, and analysis
  - Semi-automation of hand-count audits
  - Analysis & development of firmware and protocols
  - Evaluation of electronic election systems

# Electronic Poll Book Systems (EPBS)

- ❑ Replace the paper list of registered voters
- ❑ Must
  - store the list of persons authorized to vote
  - allow voters to be checked in electronically
  - prevent voters from checking in more than once
  - produce a list of persons who voted
  - record voter information updates
- ❑ May
  - scan various forms of identification for search input
  - offer additional convenience features to election officials and candidates

# Connecticut EPBS Requirements

- ❑ Developed by VoTeR Center with SOTS, 3/6/2015\*
- ❑ Focus on functional requirements for an EPBS
- ❑ Emphasis on distributed nature of the EPBS
- ❑ Coverage of non-functional requirements
  - Fault-tolerance
  - Availability
  - Reliability
  - Consistency
  - Survivability
- ❑ Considerations of performance and scalability

\* [http://www.sots.ct.gov/sots/lib/sots/ElectionServices/Handbooks/e-poll-book-system-requirements-1\\_0c\\_\(2\).pdf](http://www.sots.ct.gov/sots/lib/sots/ElectionServices/Handbooks/e-poll-book-system-requirements-1_0c_(2).pdf)

# EPBS Evaluation Process

- ❑ Performed at VoTeR Center on behalf of CT SOTS
  - Law permits SOTS to recommend systems
- ❑ Evaluation, not certification
  - Assess usability of systems in light of requirements
  - Brisk schedule vs. the meaning of “certification”
- ❑ Vendors submit solutions to SOTS for evaluation
- ❑ Adherence to each requirement is assessed
- ❑ Result is an evaluation report for SOTS
  - Disposition with regard to each requirement
  - Interpretation of the raw results

# Challenges – System Complexity

- ❑ EPBS is more than just replacing a paper list
- ❑ Complex interactions
  - Components of the system and its peripherals
  - Remote systems, e.g., the Cloud
- ❑ Complex subject data
  - Registration records, signatures, photos
  - Data exchange standards
- ❑ Specialized customer needs
- ❑ Submitted solutions use a COTS platform
  - Size and complexity, e.g.,
    - AVOS tabulator executable is 128K vs. millions lines of code
    - iOS 9 update is 1.3GB
  - Impossible to fully assess platforms

# Challenges – Retail Platforms

- ❑ COTS (commercial off-the-shelf) hardware and OS
  - Desktop / Laptop OS: Windows, Mac, Linux
  - Mobile: Windows, iOS, Android
- ❑ Advantages
  - Cost
  - Availability
  - Familiarity
  - Support
  - Manufacturer upgrade (but must keep up)
- ❑ Disadvantages
  - Lower barrier to entry
    - Anyone can make an app
    - Building is easy, configuration is not
  - General purpose platforms
    - Must be molded to the purpose
    - Not designed with elections (or critical systems) in mind
  - Platforms are well-known
    - Security consequences



# Distributed Systems and Consistency

- ❑ EPBS is inherently a distributed system
  - Good news: multiplicity of devices enables fault-tolerance
  - Challenge: multiplicity of devices makes consistency hard
- ❑ Consistency – must ensure One Voter / One Vote
  - All devices must see the same state
  - Essential in preventing multiple voting
- ❑ Electronic voter lists
  - Devices may own some partition of the voter database
  - If this is the case, what happens if a device is lost?
  - If this is not the case, must ensure consistency

# Resiliency and Dynamicity

- ❑ System must survive loss of devices
  - Must not have single points of failure
- ❑ “Hot” introduction of check-in devices (21<sup>st</sup> Century!)
  - Replacement of failed devices
  - Dealing with high voter turnout
- ❑ Use of remote (vendor) systems is problematic
  - Require an Internet connection: Outage? Denial of service?
  - How to evaluate?
- ❑ Disaster recovery
  - Election must be able to continue despite system failure
  - Must be able to print up-to-date voter lists

# Challenges – Security

- ❑ EPB systems are election systems
  - Demand higher levels of scrutiny
  - Targets of opportunity for adversaries
- ❑ Complexity (again)
  - Large attack surface
- ❑ Securing data (at rest)
- ❑ Securing communications (in transit)
- ❑ COTS platforms
  - Platform may and do have inherent flaws

# Assessing Security

- ❑ Access to interfaces and data must be controlled
  - Unique account (username and password) per user
  - No shared passwords!
- ❑ Systems must be auditable
  - Is system activity traceable? (forensics)
  - Are significant events recorded?
- ❑ Integrity of data must be guaranteed
  - Can system inputs be tampered with?
  - Can the data and its source be authenticated?
  - Is the integrity of system outputs guaranteed?
- ❑ Data encryption
  - Definitely in transit
  - Sometimes at rest

# General Observations

- ❑ Expect the unexpected / take nothing for granted
  - EPBS is **not** a “solved problem”
  - Diverse solution approaches
- ❑ Documentation (or lack of it)
- ❑ Testing distributed systems
- ❑ Verifying security posture
- ❑ Overall robustness / completeness / “finish”
- ❑ Performance and scalability needs to be considered
  - Evaluation requires larger configurations (still to be done)
- ❑ Custom interaction with voter registration DB

# Common Problem Areas

- ❑ One Voter / One Vote
  - Still challenging for vendors
  - May be impossible to guarantee during communication outage or DOS attack
  - Upon restoration of order must identify double voting
- ❑ Preparation of electronic voter lists
  - Requires vendor involvement
  - May be prone to misconfiguration
- ❑ User roles and authentication
  - Need identifiable user roles
  - Individual users must be authenticated

# Common Problem Areas

- ❑ Fault-tolerance
  - Single points of failure
  - Reliance on vendor server
  - Implicit assumption that nothing will go wrong
  - Dynamic recovery considerations
- ❑ Auditability
  - Provision and adequacy of audit logs
  - Attribution: who (user/system) did what and why
- ❑ Data verification
  - Voter list input authentication & (un)signed outputs
  - Data tampering detection

# Must Have Documentation

- ❑ Documentation is a first-class feature
- ❑ Demand documentation in advance
  - Cannot evaluate if you don't know what to expect
- ❑ Connecticut requirements for documentation
  - System architecture
  - Functional Description
  - User manual
  - And more



# Discussion -- Questions?

- ❑ COTS platforms have advantages and disadvantages
  - Good for vendors
  - Tradeoffs for customers
- ❑ Require documentation
- ❑ EPB systems are distributed systems
  - Hard to build
  - Hard to evaluate (reliability, consistency, correctness)
- ❑ Security evaluation can be difficult
  - Get help and/or use the right tools
- ❑ Dependability / reliability
  - Must not be an afterthought
- ❑ Performance and scalability: needs and evaluation