Elections, Technology, and the Pursuit of Integrity

Alexander Schwarzmann
Center or Voting Technology Research (VoTeR Center)
University of Connecticut

Elections Used to be Easy

- Election of Pope St. Fabian
  Rome, 236 AD

"…all the brethren had assembled to select by vote him who should succeed to the episcopate of the church, … all the people… with all eagerness and unanimity cried out that he was worthy…"

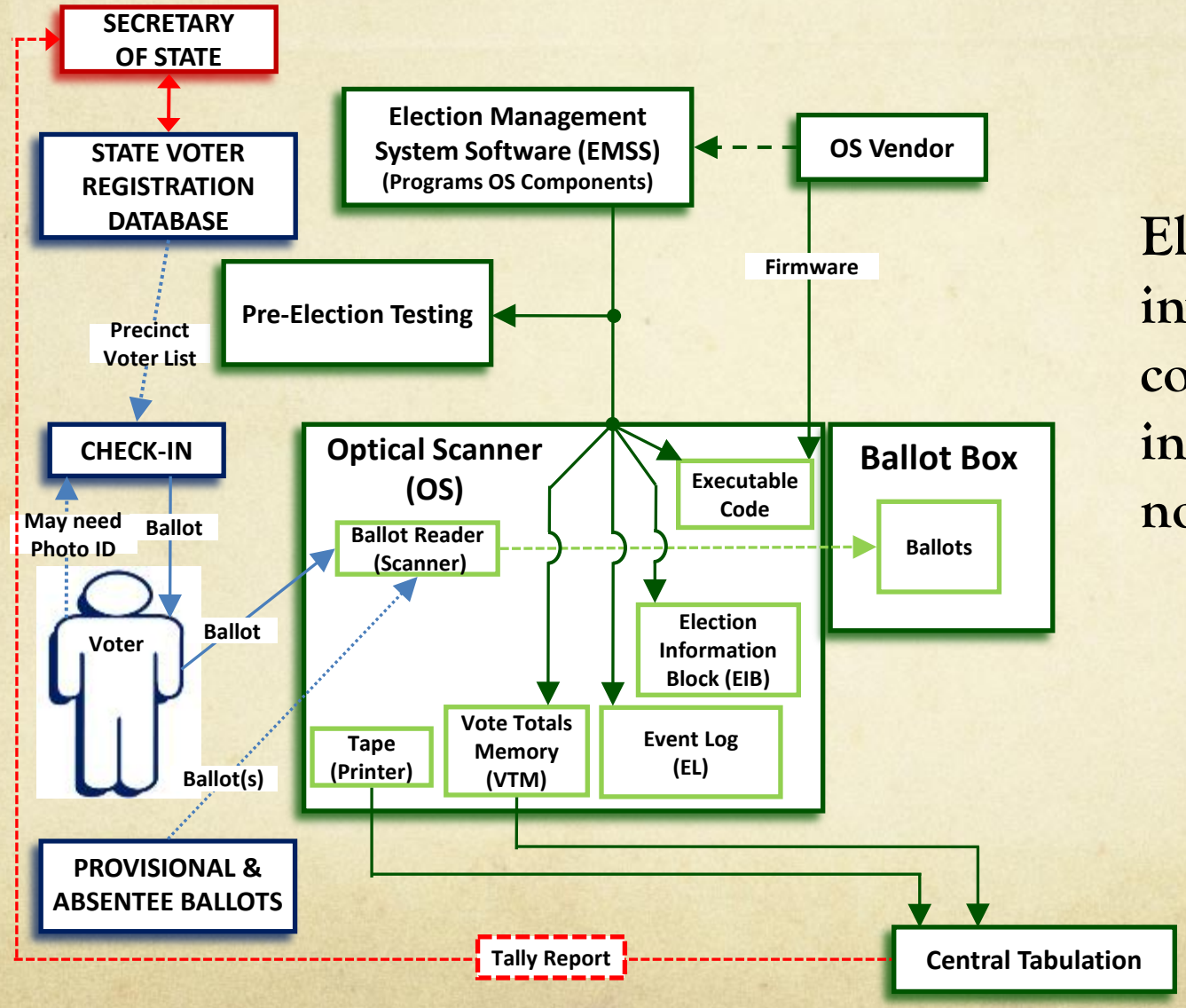
[Eusebius Pamphilius, ca. 300 AD]

Today: Massive Distributed Enterprise

- **Voter registration systems**
  - Database systems with remote access
  - Federated with other databases, e.g., DMV
- **Voter check-in systems, a.k.a. "poll books"**
  - Precinct-level manual or automated systems for voter check in
  - "One voter, one vote"
- **Voting terminals**
  - Optical scan tabulators – VG-VV-PAT
  - Touch screen, a.k.a. DRE, Direct Recording Electronic
- **Election management systems**
  - Individual programming for each voting terminal
- **Central tabulation**
  - Aggregation of tallies from voting terminals

The Voting Process

[IEEE Transactions on Information Forensics and Security 2009]



Elaborate process involving several complicated systems interacting in non-trivial ways

The Current Landscape

- Nationwide deployment of multi-billion dollar electronic election infrastructure following 2002 HAVA Act
- Unfortunately the election enterprise is impaired by ***premature deployment*** and ***immature technology***
  - Election management systems run on COTS
  - Poorly designed software for voting terminals
  - Insecure protocols allow a variety of attacks
  - Fallacious use of crypto gives false sense of security
  - Voting terminal hardware is not well thought out
  - Removable media is easily tampered
  - Viral propagation of malware is possible
  - Central tabulation errors can result in lost precinct results
  - ...

Dislocation of Theory and Practice

- Vendors rushed to market with immature and naively implemented products, and a number of states prematurely deployed these products without safeguards
- Security, integrity and reliability vulnerabilities found in all electronic voting terminals that were independently examined
- Electronic voting terminals can be tampered in a variety of ways resulting in arbitrary outcomes
- These problems can be traced back to the divergence from, and/or the obliviousness of, established results in algorithmics, verification, distributed computing, cryptography, and sound engineering practices

Who Would Interfere with Elections?

- Attacker objectives
  - Modify election results
  - Violate the privacy of the voter
  - Disrupt the election process
  - Extracting voting receipts (to sell or to coerce)
  - Inaccurate audit-trail
  - Bias results through interface manipulation
  - Denial of service
  - Skew/tamper aggregation of totals

…

- This is on top of issues of correctness and reliability …

Voting Equipment Vulnerability

- Critical areas that are vulnerable in a computer system
  - Bootstrapping
  - Authentication
  - Internal integrity
  - Data modification
  - Configuration
  - Shallow use of cryptography
  - Unprotected interfaces
  - Election management systems & central tabulation
  - Poor design choices

Voting Terminals: a Deeper Look

- Voting terminals are replete with vulnerabilities, e.g.,
  - Evidence of Internet ability or access despite prohibition
  - Insecure setup process permits tampered election data loading
  - Buffer overflow can lead to system takeover
  - Votes can be swapped despite encryption
  - Exposed USB ports allow rebooting
  - Arbitrary code can be injected
  - Terminals used for email
  - And for browsing erotic art

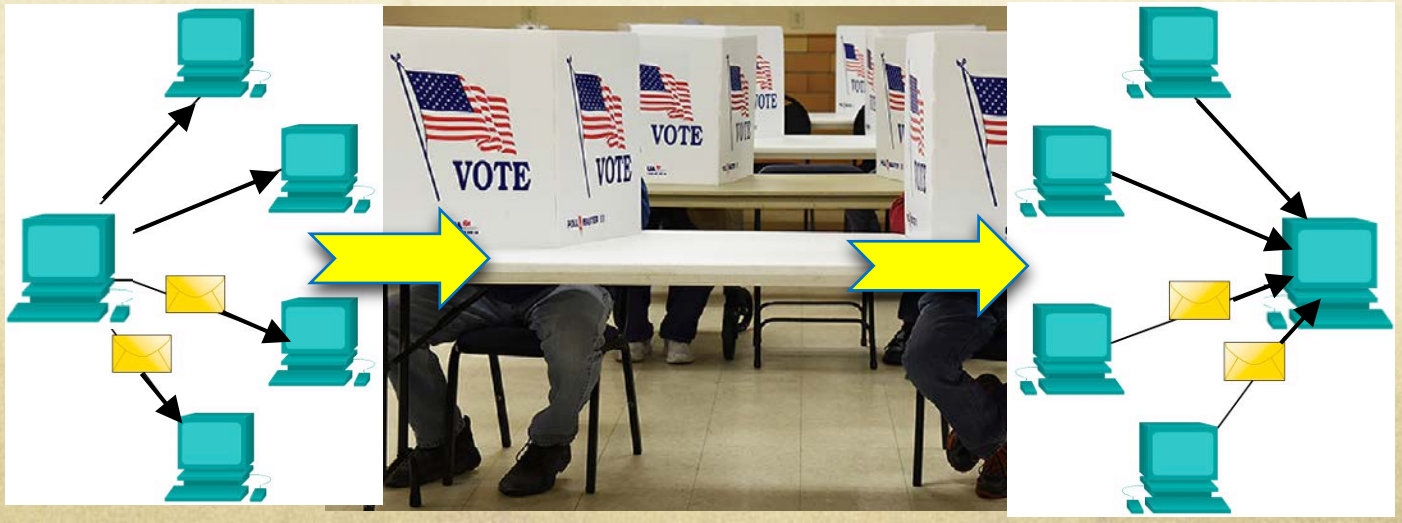
Full Takeover and Viral Propagation

- First indication that viral attacks are possible
  [Feldman Halderman Felten 2006]
- Complete takeover of an optical scan tabulator
  [Jancewicz Kiayias Michel Russell Shvartsman 2013]
- Some voting tabulators can be used to duplicate media
- Up to 6% of tabulators are programmed via card duplication
- Attacks can propagate themselves in a viral fashion
  - Attack from an infected memory cards is faithfully reproduced on clean cards

EMS / CTS Vulnerabilities

- Election Management System (EMS) vulnerabilities
  - Incorrect Voting Terminal programming/ballot layout
  - EMS impersonation during voting terminal programming
- Central Tabulation System (CTS) vulnerabilities
  - Voting Terminal impersonation during post-election transfer of results to CTS
  - Vulnerabilities during results aggregation stage

EMS Broad-cast



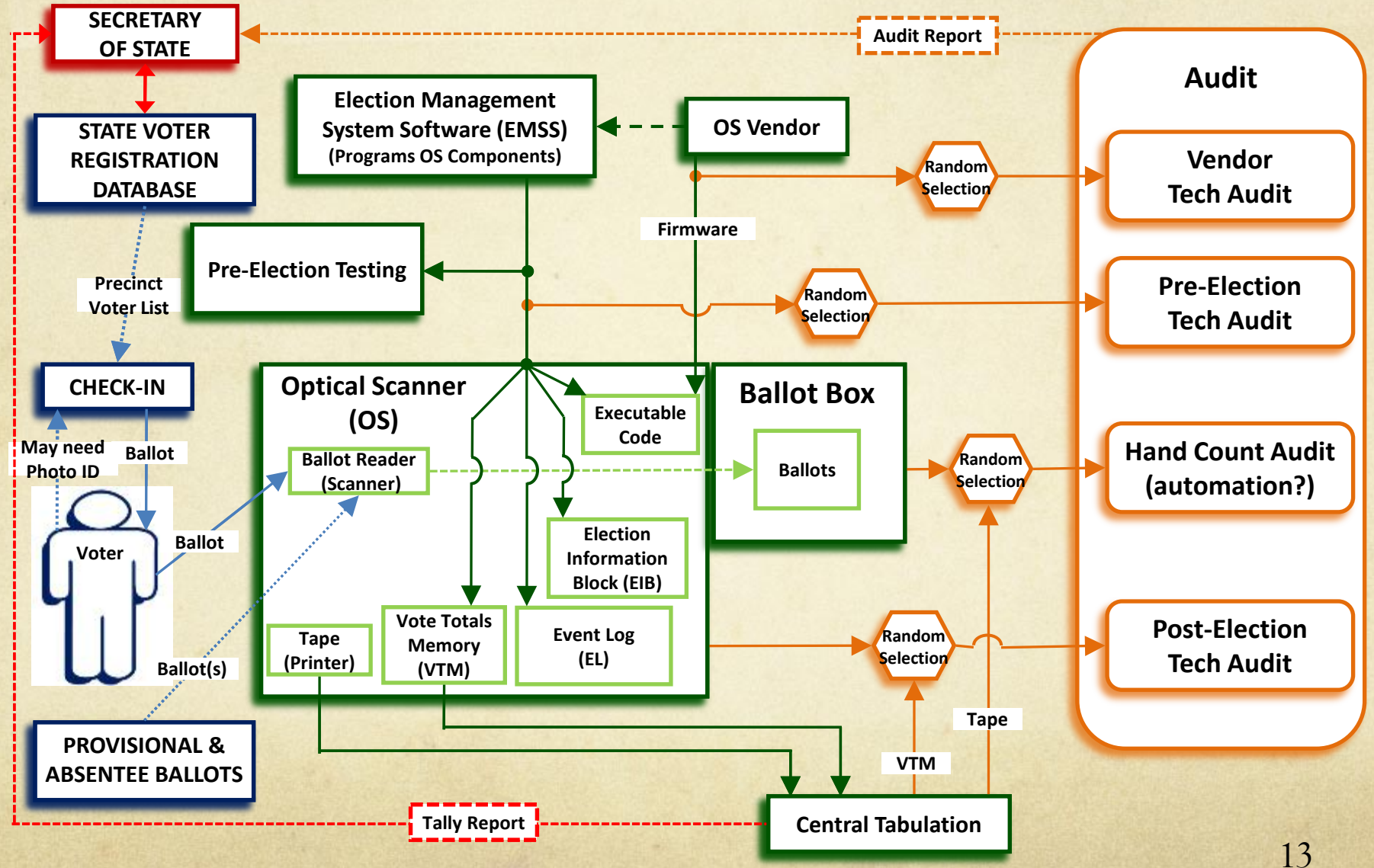
CTS Converge-cast

The Risks of Central Tabulation

- Central tabulation aggregates results
  - Uses general purpose computers with all associated risks
  - Prone to “routine” infestation with malware and viruses
- Security, integrity and reliability risks
  - Malicious tampering and attacks are possible
  - Even “good” central tabulation can accept tampered results
  - Software errors lead to lost votes (or entire precinct)
  - Network transmission of election results…
    let’s not even touch that!
  - (For these and other reasons automated central tabulation is not used in Connecticut)

The Voting Process & Audits

[IEEE Transactions on Information Forensics and Security 2009]



Audits

- Audits should include the following
  - (a) vendor tech audit: integrity and security of the electronic election systems
  - (b) pre-election tech audit: correctness and integrity of the programming of electronic election systems before the election
  - (c) post-election tech audit: proper settings, function, and use of the electronic systems
  - (c) post-election ballot audit – hand-counted (semi-automated)
- Conducted in Connecticut for each state-wide election
  - Pre-/post technological audits are substantially automated
  - State-mandated hand-counted audits in a percentage of randomly selected districts

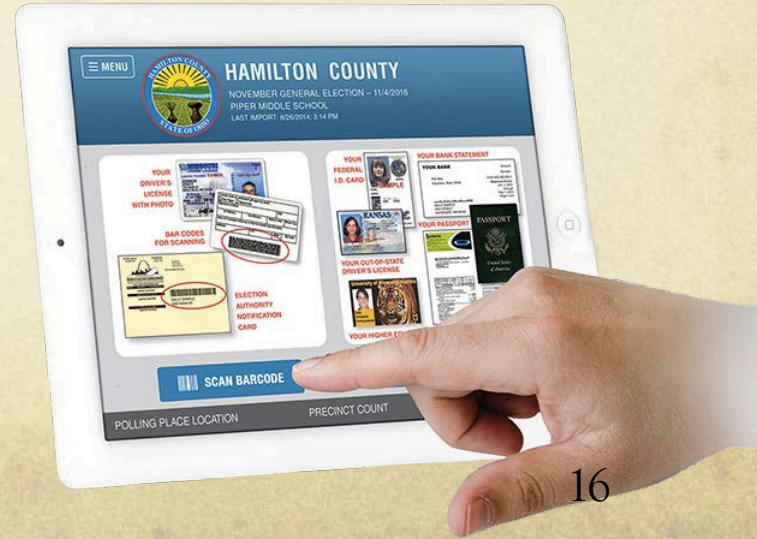
Onsite Voting vs. Online Voting

- This is considering just the **onsite voting**
  - Voting and tabulation is performed locally
- **Online voting** presents a plethora of new challenges
  - Voter registration, authentication, privacy, protection, lack of vgvpat, secure/private communication, aggregation, integrity, security, lack of recourse, fault-tolerance, denial-of-service …
- *"electronic voting from home should perhaps forever remain too risky a fantasy"*

Ron Rivest

Electronic Pollbooks

- Pollbooks have the purpose of ensuring “One voter, on vote”
- Provision and maintenance of registered voter lists during the election is commonly a manual process
  - Laborious and error-prone process to maintain the list and update registration database after the election
  - Documented cases where questionable processes caused poll opening delays, long lines, and errors, possibly disenfranchising numerous voters
- There is a growing demand for providing e-pollbooks to address these deficiencies and also to provide election day registration

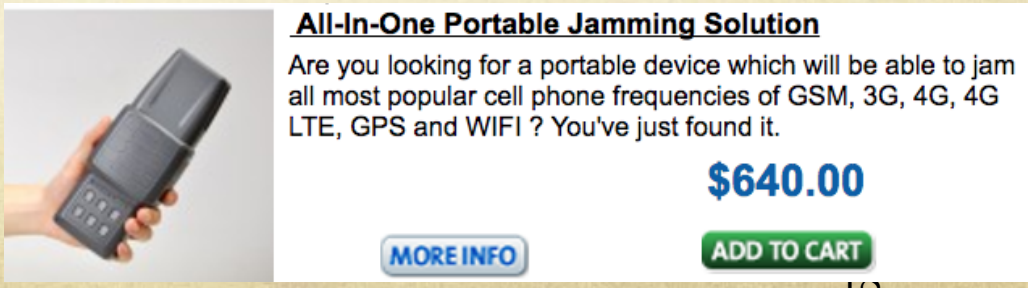


Electronic Pollbooks

- An inherently ***distributed*** and ***dynamic*** computer system
  - Multiple devices to check in voters to reduce lines
  - Dynamically add/remove devices – reconfiguration
  - Voter list storage must necessarily be replicated
  - Concurrent check in of voters – concurrent data updates
  - Consistency is mandatory
  - Must not contain single points of failure
  - Some level of service if/when communication is disrupted
  - Automatic restoration of consistency when disruption stops
  - Must be impervious to outside tampering/impersonation

Electronic Pollbooks

- Vendors are releasing immature and naïve solutions showing dislocation of theory and practice
  - "One voter / one vote" – not necessarily
  - Reliance on centralized servers and/or Internet
  - Use of unhardened COTS components
  - Unclear fault tolerance guarantees
  - Poor data integrity checks (e.g., scanning licenses)
  - Unknown or unexplored performance
  - Poor use of crypto to secure communication
  - Open to denial of service



Concluding Remarks

- Eschew premature use of immature technology
- Can less-than-perfect on-site election systems be used?
  - Evaluation of vulnerabilities (initial, then ongoing)
  - Harden systems (in particular VR)
  - Explicit safe-use and chain-of-custody procedures
  - Comprehensive audits
- Internet voting? No.
- Better cooperation and synergy
  - State Governments,
    Vendors & Integrators,
    Research Labs & Universities,
    Testing Labs