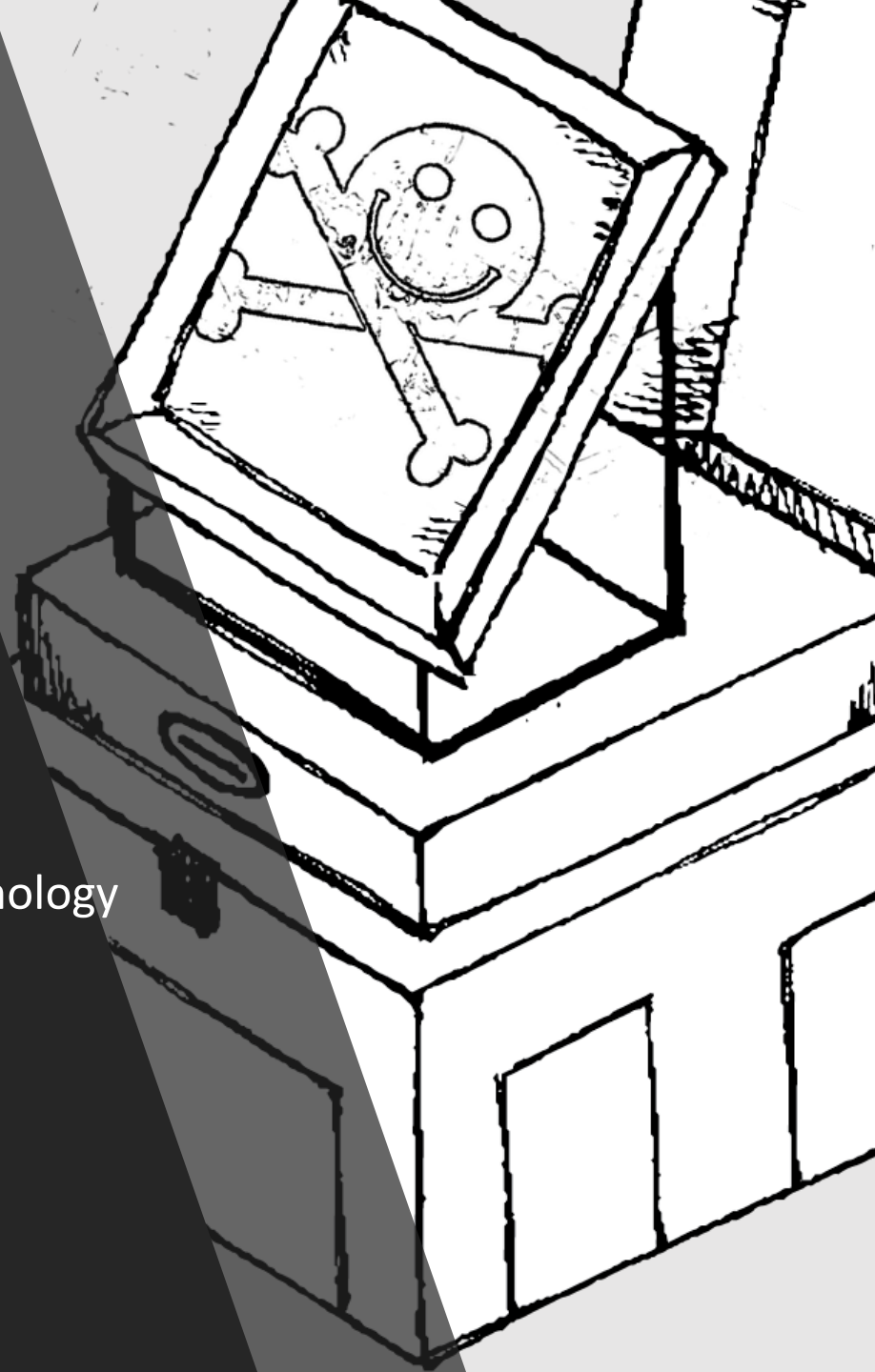
The State of US Voting System Security

DEFCON Voting Machine Hacking Village
July 2017

Joshua M Franklin
National Institute of Standards and Technology



VOTRON 5000

Election Fraud Types - 1934

- Registration fraud
- Repeating
- Ballot box stuffing
- Assistance to voters
- Intimidation & violence
- Altering ballots
- Ballot substitution
- False counts and returns
- Altering returns

[1] Joseph Harris, 1934

INSERT CARD HERE

VOTRON 5000

Bio

- IT Security Engineer, NIST
- Enterprise mobility, telecommunications, evoting
- 10+ years in the elections community
- Co-chair the Election Cybersecurity Working Group
- Masters in Information Security from George Mason

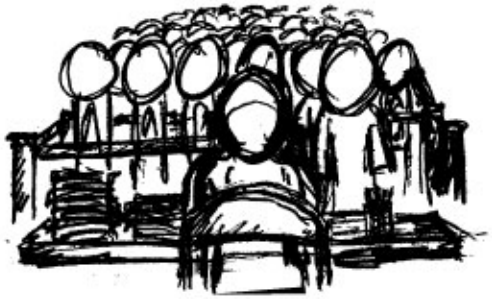
INSERT CARD HERE

VOTRON 5000

Get to Know an Agency

- Federal:
  - Election Assistance Commission (EAC)
  - NIST, DHS, and FBI
- State: Secretary of State's office
- Local: counties, cities, townships, parishes, hamlets

INSERT CARD HERE



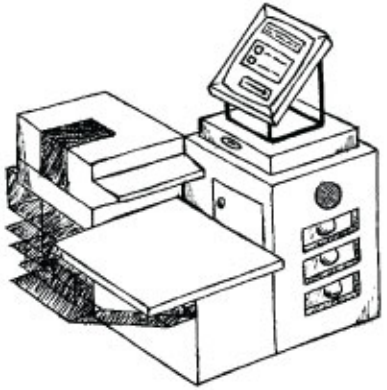
Local and Online Voter Registration

Electronic Pollbooks

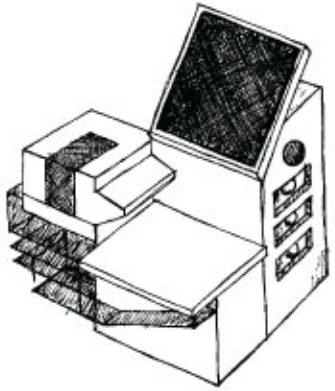
Candidate Filing Systems

Campaign Voter Info Databases

Direct Record Electronic



Optical Scan



Ballot Marking Device

VOTRON 5000

Types of Voting Systems

- Vote capture & tabulation
  - DREs, central & precinct optical scan, ballot marking device
  - Software associated with election administration
- Supporting election systems
  - Voter registration, epollbooks, election night reporting
  - Candidate filing, poll worker tracking, ballot tracking …

INSERT CARD HERE

VOTRON 5000

A Changing Threat Model

Old & Busted

- Physically proximate attackers
- Accidental events
- Natural disasters
- Events affecting public confidence and trust

New Hotness

- Nation state attackers
- Phishing
- Supporting election systems
- Everything in the old threat model, plus CYBER

INSERT CARD HERE

VOTRON 5000

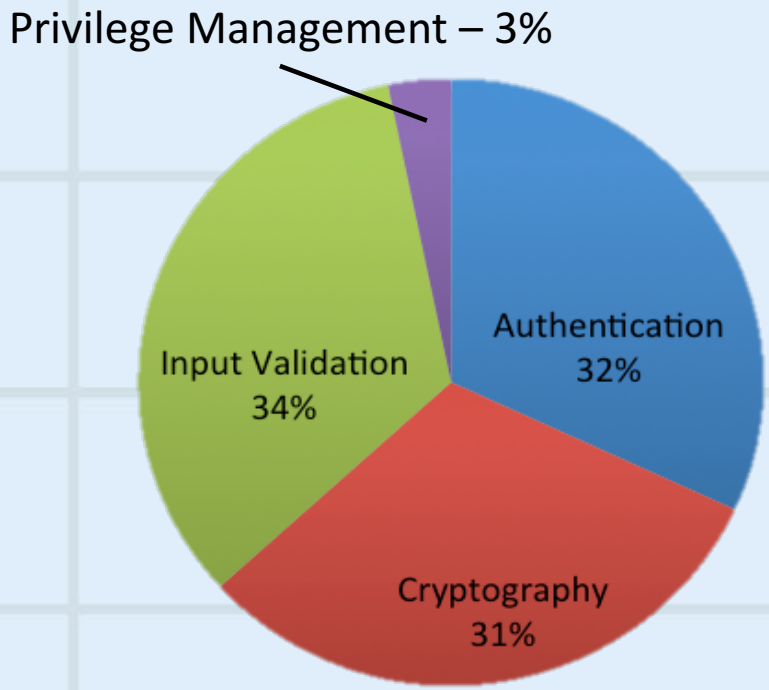
Security Architecture

- Embedded legacy system
  - Typically running *nix variant
- Older or proprietary physical media
- Working TCP/IP stack is common
- Wireless is possible
- Required to stand the test of time (10 - 15 years)
- Jurisdiction that can pay MAY receive 1 - 5 updates

INSERT CARD HERE

VOTRON 5000

Independent Reviews



Common CWEs

- CWE-306: Missing Authentication for Critical Function
- CWE-120: Classic buffer overflow
- CWE-522: Insufficiently Protected Credentials
- CWE-345: Insufficient Verification of Data Authenticity
- CWE-311: Missing encryption of sensitive data

[10] – [27]

INSERT CARD HERE

VOTRON 5000

Innovations in Voting Security

- Risk Limiting Audits [8]
- Software Independence [6]
- E2E verifiable cryptographic protocols [9]
- Recognition of usability as a security issue

INSERT CARD HERE

VOTRON 5000

Paper is not a Panacea

- Paper ballots provide tamper detection and enable auditability
- Paper can be modified
- Seals and chain of custody need verification
- Routine audits need to be performed
- Cyberhygiene

INSERT CARD HERE

VOTRON 5000

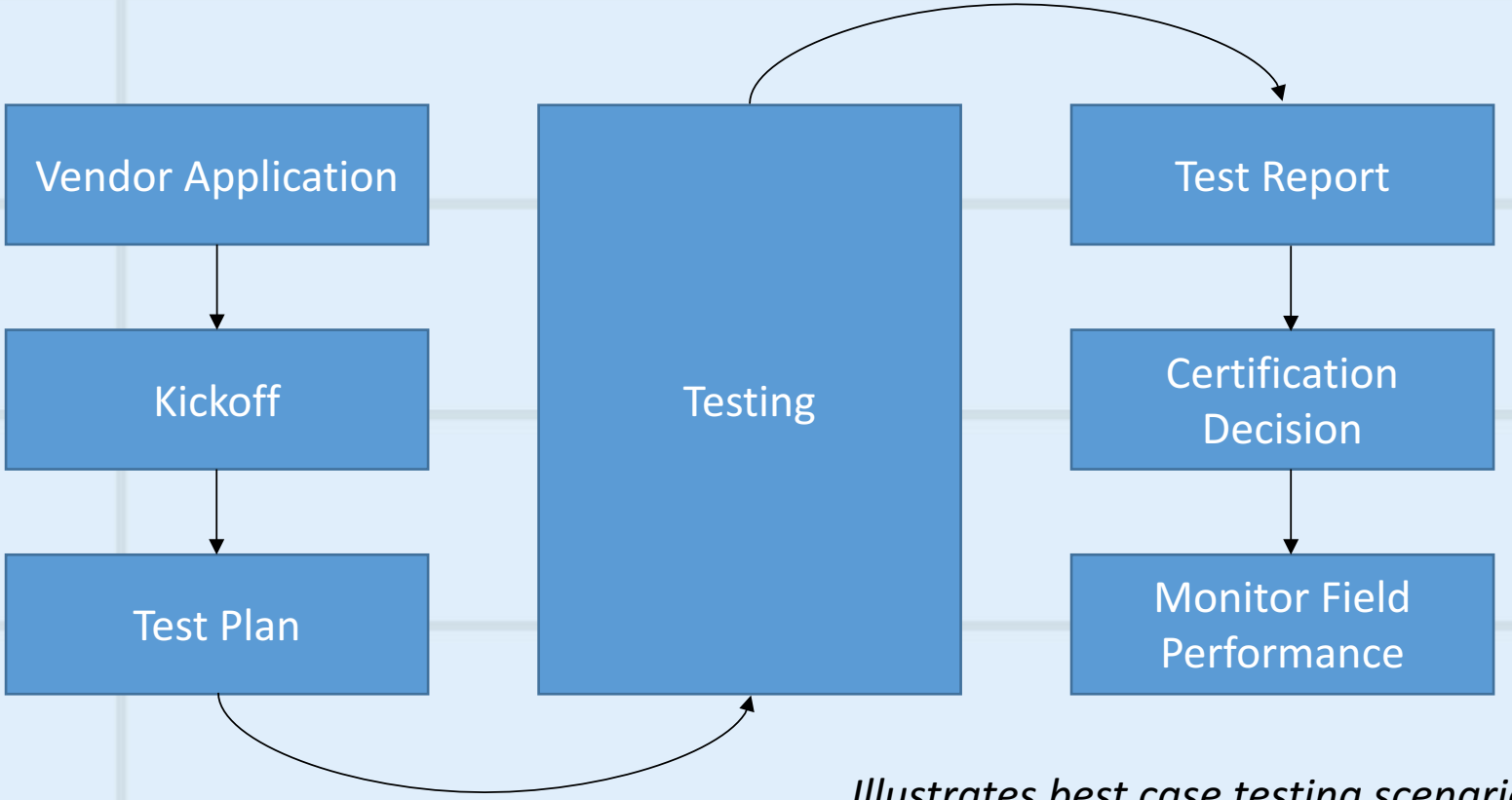
Testing & Certification

- EAC runs a testing and certification program
  - Most states do as well
- Voting system test labs (VSTLs) perform testing
- States are not required to use certified systems
- Testing validates voting machines *submitted for certification* meet the VVSG
- Freely available test reports!
  www.eac.gov

INSERT CARD HERE

VOTRON 5000

Certification Process



Illustrates best case testing scenario

INSERT CARD HERE

Voting Standards

- Voluntary Voting System Guidelines = VVSG [2]
- Scoped to vote capture and tabulation
- Not mandated for use
- Little security focus in initial drafts
  - Large overhaul in security requirements since 2005

VVSG Updates

1. 1990 VSS
2. 2002 VSS
3. 2005 VVSG
4. 2007 Recommendations
5. 2015 VVSG
6. Principles & Guidelines under development

VOTRON 5000

New Proposed Structure

- Principles
  - High level system design goals
- Guidelines
  - Broad system design details for election officials
- Requirements
  - Technical details for design and development by vendors
- Test Assertions
  - Technical specification for testing by labs

INSERT CARD HERE

Security Principles & Guidelines

- Auditability
- Ballot Secrecy
- Access Control
- Detection and Monitoring
- Data Protection
- Software Integrity
- Physical Security

[3] NIST & EAC Voting Twiki

apt-get upgrade

- Routine meaningful audits
- Responsible vulnerability disclosure
- Augment how we manage election security
  - Risk assessment, threat modeling, and contingency planning
- Regular, external scrutiny of systems is essential
- Voting systems need software updates
- Election officials need actionable guidance

VOTRON 5000

Help Make a Difference

- Register to vote
- Be a pollworker
- Work with your election official – not against
- Join the public working groups

INSERT CARD HERE

VOTRON 5000

References

1. Election Administration in the United States, 1934, by Joseph P. Harris
   https://www.nist.gov/itl/election-administration-united-states-1934-joseph-p-harris-phd
2. EAC, Voluntary Voting System Guidelines, 2017.
   https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines
3. NIST & EAC Security Principles & Guidelines, 2017.
   http://collaborate.nist.gov/voting/bin/view/Voting/SecurityObjectives
4. Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US elections*, ICA 2017-01D, 2017.
   https://www.dni.gov/files/documents/ICA_2017_01.pdf
5. ACM, *Statewide Databases of Registered Voters - Study Of Accuracy, Privacy, Usability, Security, and Reliability Issues*, 2006.
   http://usacm.acm.org/images/documents/vrd_report2.pdf
6. Rivest, Wack, *On the Notion of Software-Independence*, 2008.
   https://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf
7. Jones, Simons, *Broken Ballots*, 2012.
   http://brokenballots.com
8. Stark, *A Gentle Introduction to Risk Limiting Audits*, 2012.
   https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf
9. Benaloh et al, *End-to-end verifiability*, 2015.
   https://arxiv.org/pdf/1504.03778.pdf

INSERT CARD HERE

VOTRON 5000

References

10. SAIC - Risk Assessment Report Diebold AccuVote-TS Voting System and Processes, 2003
11. Analysis of an Electronic Voting System, 2004
12. RABA - Trusted Agent Report Diebold AccuVote-TS Voting System, 2004
13. Security Analysis of the Diebold AccuBasic Interpreter, 2006
14. Security Analysis of the Diebold AccuVote-TS Voting Machine, 2006
15. Diebold TSx Evaluation, 2006
16. Top to Bottom Review (TTBR), 2007
17. EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing, 2007
18. Software Review and Security Analysis of the Diebold Voting Machine Software, 2007
19. Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware, 2007
20. Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine, 2008
21. Software Review and Security Analysis of Scytl Remote Voting Software, 2008
22. Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage, 2009
23. Security Analysis of India's Electronic Voting Machines, 2010
24. Exploiting the Client Vulnerabilities in Internet E-voting Systems: Hacking Helios 2.0 as an Example, 2010
25. Maryland State Board of Elections Online Voter Services Penetration Testing Report, 2012
26. Attacking the Washington, D.C. Internet Voting System, 2012
27. Security Analysis of the Estonian Internet Voting System, 2014

INSERT CARD HERE