NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Marginal Remarks on Voting System Security

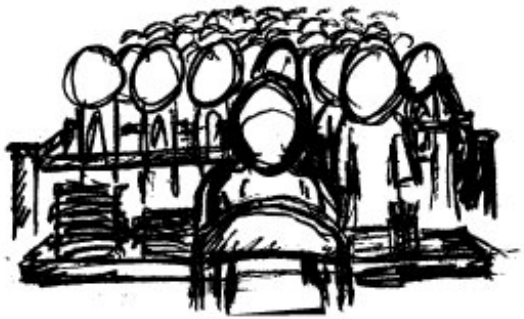
Joshua Franklin, NIST
Josh@nist.gov

Agenda

- Election infrastructure security
- Voting systems security
- Security priorities
- Identifying solutions

Election Fraud Types - 1934 [1]

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



Local and Online Voter Registration

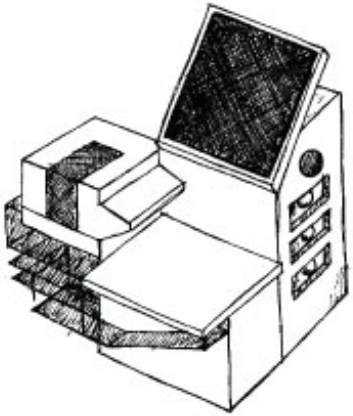
Electronic Pollbooks

Candidate Filing Systems

Campaign Voter Info Databases

Direct Record Electronic

Optical Scan



Ballot Marking Device

2016 General Election Attacks

- Data exfiltration from voter registration systems [3] [4]
- Phishing election officials & voting system vendors [2]
- Doxing of political campaigns [2]
- Attacks on backend, non-tabulation systems [2]

"We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US presidential election to future influence efforts worldwide, including against US allies and their election processes." – ODNI [2]

An Expanding Threat Model

Traditional Attacks

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

Recent Attacks

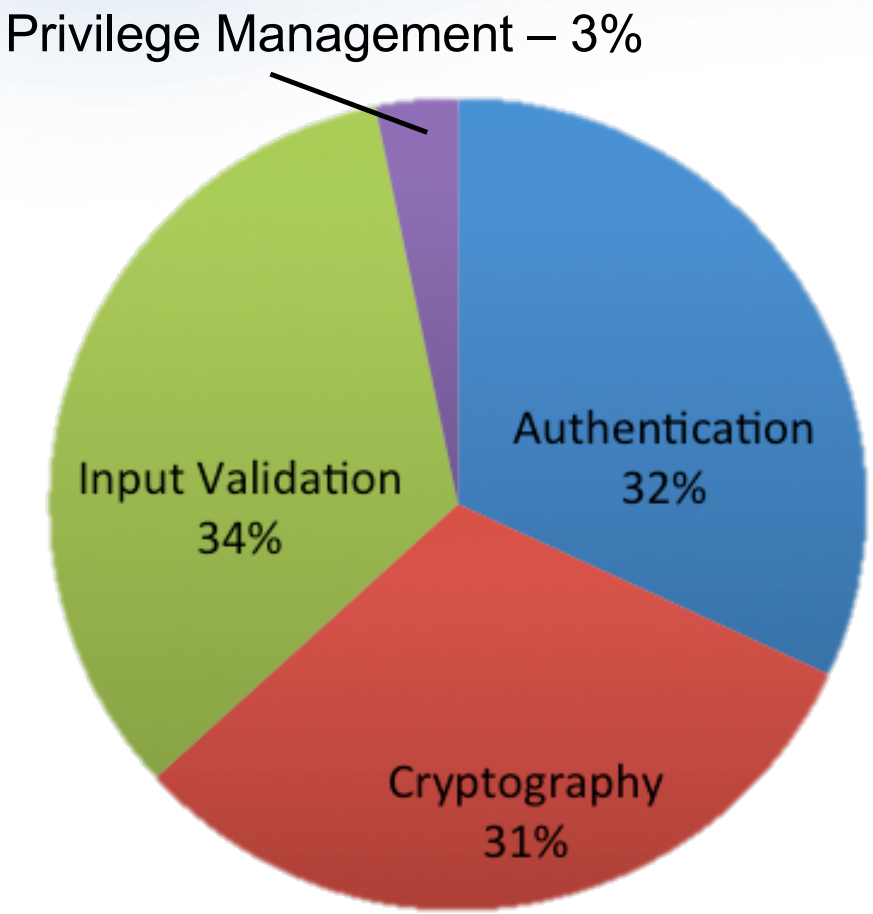
- Nation-state
- Phishing of work and personal accounts
- Supporting election systems

Voting System Security

- Embedded legacy Linux OS distro
- Older or proprietary physical media
- Working TCP/IP stack
- Wireless and public telecommunications
- Required to stand the test of time (10 - 15 years)
- Jurisdiction that can pay MAY receive 1 - 5 update

This is slowly changing as modern systems are introduced.

Independent Reviews



CWEs [8]-[25]

- 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

Security Innovations Since 2007

Industry

- Secure boot and strong process isolation
- Exploit mitigation technologies (e.g., ASLR, DEP)
- Stronger network protocols
- Security frameworks

Voting Systems

- Software Independence [5]
- Risk Limiting Audits [6]
- E2E verifiable cryptographic protocols [7]
- Recognition of usability as a security issue

Paper is not a Panacea

- Paper ballots provide tamper detection and enable auditability
- Paper can be modified or swapped
- Seals and chain of custody need verification
- Routine audits need to be performed
- Administrative controls are **very** important
- Cyber-hygiene

Standards vs. Best Practices

- Standards and best practices are different beasts
  - Standards are requirements, best practices often context dependent
- The VVSG is a voluntary voting system standard
- Examples of US election best practices:
  - EAC ENR Checklist
  - DHS VR guidance & EAC VR Checklist
  - EAC Incident Response Guidance
  - EAC EMGs
  - EVN's Top 10
  - NIST UOCAVA series

Voluntary Security Standards

Have

- DREs
- Optical scan
- Ballot marking devices
- Election management systems

Don't Have

- Electronic pollbooks
- Voting registration
- Campaign voter info systems
- Election night reporting
- Back-end office systems
- Supporting UOCAVA systems

Security Best Practices

Have

- Voter registration
- Election night reporting
- Supporting UOCAVA systems
- DREs
- Optical scan
- Ballot marking devices

Don't Have

- Electronic pollbooks
- Campaign voter info systems
- Back-end office systems
- Election management systems

Important Election Security Issues

- Technology
  - Need for accessible and auditable voting systems
  - External scrutiny of voting systems
  - Software updates for voting systems
  - Security posture of supporting infrastructure is an unknown
- Election Management
  - Meaningful post-election audits
  - Augment how we manage election security

Solving These Issues

- Threat modeling and risk assessments for all parts of the election process
  - Focusing first on known issues from 2016 General
- Best practices for procedural election security and audits
- Ensuring usable security controls for voting systems
- Changes to allow for regular, secure patching
- Information sharing between all levels of government, industry, and security community

Cybersecurity Awareness

- In most industries and sectors there is a need for enhanced cybersecurity awareness
  - Elections is no different
- Need to understand how modern computers are attacked
- DHS is already helping with online educational materials
- Election officials need information in their language
- Topics we may need election specific guidance for:
  - Incident response
  - Authentication issues and password management
  - Physical and operational security
  - Decommissioning of old systems and media sanitization

Some Coordination Required

- Many of these security issues are broader than our scope of voting system technology
  - Policy, procedures, and law
- Local and state officials can't defend themselves against state actors alone
- Coordination is needed between all levels of government, industry, academia, and the broader elections community

Questions?

Joshua Franklin, NIST
Josh@nist.gov

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. 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
3. VR systems, Media Statement, June 2017.
4. FBI, Targeting Activity Against State Board of Election Systems, August 2016.
5. Rivest, Wack, *On the Notion of Software-Independence*, 2008. https://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf
6. Stark, *A Gentle Introduction to Risk Limiting Audits*, 2012. https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf
7. Benaloh et al, *End-to-end verifiability*, 2015. https://arxiv.org/pdf/1504.03778.pdf

References

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