NCSL Summit

Security and Election Systems

Chicago, IL
August 2016
Merle S. King
In the News…

DHS examining cybersecurity threats in advance of 2016 election

By Eric DuVall | Aug. 4, 2016 at 3:32 PM
In the News…

- Hacking An Election: Why It’s Not As Easy As You Think
- 2016: The Year Americans Found out Our Elections Are Rigged
In the News…
Public Service or Panic?
Possibility vs. Probability

• Possibility is a boolean value … 1 or 0.
• There is Impossible = 0 and NOT(Impossible) = 1
• Probability is the likelihood of occurrence of an event \( >0 \) Event \(<1\).
• They are not synonyms
• Allocation of resources to mitigate threats must be done on the probability of the threat occurrence \( \times \) its potential consequence
SO YOU'RE TELLING ME

THERE'S A CHANCE
Issues

2. Undermining Confidence vs. Disrupting vs. Altering Outcomes
3. Layered Defense of Voting Systems
Systems

• Campaign Systems collect, store, transform, utilize, and share data related to a candidate, party, or ballot question.
• Campaign Systems are strategic.
• Campaign Systems may be short lived.
• Campaign Systems are not “owned” by governments – they are private systems.
• There are no standards for security. Their architecture and maintenance are at the discretion of their owner.
Systems

• Election Systems collect, store, utilize and share data related to the administration of elections.
• Election Systems are administered at the state and/or local level.
• Election Systems are characterized by their architecture, function(s), interfaces and data.
• Election Systems have no uniform standards and no testing protocols beyond those imposed by the purchaser and designer.
Attacking Elections

• Purpose of an election is to facilitate an acceptable transition or retention of political leadership or referendum.

• Confidence in the outcomes is built upon confidence in the personnel, processes and technologies.

• One of the easiest attacks on an election, is to undermine the confidence in the outcomes. Takes little investment of effort, can yield significant results.

• Speak in possibilities - make election officials prove the negative.
Attacking Elections

• Residual Votes in 2016 election
  – Adoption of VBM (Central Count) Systems
  – Intentional, advice of parties

"Residual votes represent the votes that do not properly record the voter's intent, or don't record any vote at all because of problems in voting mechanisms. This is an ongoing problem that regularly means that millions of votes are lost.” Kay Maxwell, LOWV 2005.
Disrupting Elections

• Elections are known, scheduled IT events
• Most of the technical details are known in advance, but not all
• Attacking an election system (like the VR system) could disrupt an election, but only for a short period of time
• Elections are not single-day events – time to recover
• Election planning is contingency planning
• Backups and rollbacks
Voting System

What voting systems do:
• Vote Capture
• Tabulation
• Ballot/Election Definition
• Reports
• Audits
Voting System

What voting systems do:
• Vote Capture
• Tabulation
• Ballot/Election Definition
• Reports
• Audits

Requirements:
• Security
• Accuracy
• Usability
• Functionality
• Robustness
• Auditability

*EAC Voluntary Voting System Guidelines
Voting System

What voting systems do:
• Vote Capture
• Tabulation
• Ballot/Election Definition
• Reports
• Audits

What it is legally required to do:
• Accessibility**

Requirements:
• Security
• Accuracy
• Usability
• Functionality
• Robustness
• Auditability

** Section 504, 1973 Rehabilitation Act
1990 Americans With Disabilities Act
Voting System

• Statute
• Rule
• Vetted Procedures
• Vendor-provided procedures
• IT Best practices
• Chain of custody
• Documentation
Voting System

- Statute
- Rule
- Vetted Procedures
- Vendor-provided procedures
- IT Best practices
- Chain of custody
- Documentation

Training is the essential control to ensure procedures are implemented
Voting System

• Election officials are trained to follow procedures
• Election officials have very small degrees of latitude in interpreting procedures
• Most election anomalies at the local level begin by an election official “winging it” or “using their judgment”.

“Upson County Georgia pollworker directs voter to wrong precinct, 227 miles away.”
Voting systems have specific storage requirements:
- Lock and key
- Seals
- Logs
- Video observation
- Chain of custody
- Preventative vs. Detective Controls
- Quarantine and removal
Voting System

- Authentication
- Encryption
- Hash Compares
- Audit Logs
- Air Gaps

Cyber Security

Procedures

Voting System

Physical
Voting System

- Voting System Test Labs
- State Certification
- Acceptance Testing
- Logic and Accuracy Testing
- Risk Limiting Audits
- Operational Audits
- Forensic Audits
Questions to Ask

• What security procedures are our election officials required to implement?
• How current is their training?
• How are voting system components physically secured?
• How are desktops and laptops used in election activities secured? By whom?
• Have all recent vendor service bulletins been reviewed and mitigations implemented?
Discussion

Merle S. King
Executive Director
Center for Elections Systems
mkings@kennesaw.edu