Ensuring Trust in Voting

Mark Skall

National Institute of Standards and Technology

www.vote.nist.gov

Background

- Help America Vote Act (HAVA) provides for the creation of the TGDC to recommend guidelines (standards)
- Assigns specific responsibilities to NIST
  - Chairing the TGDC
  - Providing technical support and research ot the TGDC
  - Methods to detect and prevent fraud

Status of Guidelines

- Voluntary Voting Systems Guidelines (VVSG) 2005 in place
  - Updated VSS 2002
  - Added new material on security and human factors
- VVSG 2007 due in July 2007
  - Complete rewrite
  - Much more comprehensive security requirements

Trust in Voting Systems

- Systems must be thoroughly tested to ensure all requirements are met, including reliability, security, usability and accessibility
- Must ensure that the tested and certified system is actually the system used on election day

Testing

- Key to ensuring trust
- Currently
  - Each testing lab develops their own tests
  - No uniformity in testing
  - No assurance of correctness or comprehensiveness
  - No transparency

Testing

- NIST will develop tests for VVSG 2007
  - Check that all requirements are implemented correctly
  - Open ended security testing
  - Human factors testing including usability and accessibility
- All test labs will use NIST tests
  - Ensure comprehensiveness
  - Uniformity
  - Transparency

Testing is Necessary but not Sufficient

- How do you know that the systems actually used on election day are the correct (certified) version of the hardware and software?
  - –i.e., What good is testing if we can't ensure that the tested version is the one being used

This is not Just Hypothetical

E-Voting Undermined by Sloppiness

SACRAMENTO, California -- An audit of Diebold Election Systems voting machines in California has revealed that the company installed uncertified software in all 17 counties that use its electronic voting equipment.

While 14 counties used software that had been qualified by federal authorities but not certified by state authorities, three counties, including Los Angeles, used software that had never been certified by the state or qualified by federal authorities for use in any election.

This Doesn't Only Affect Voting

The Bucklands Boys and Other Tales of the ATM

Crime came this spring to that secure oasis of familiarity, the anywhere and everywhere of a sky-lit mall court, surrounded by such recognized enterprises as The Gap, Haagen-Dazs, Victoria's Secret, The Sharper Image, Footlocker - and Babbage's Software.

In that software store hung a portrait of its namesake, Charles Babbage, the stern, bewhiskered creator of the first computer. Babbage seemed to be looking across the mall, past the perfume cart and the pretzel stand to the automated teller machine that for sixteen days sat innocently on wheels as dozens of patrons tried in vain to obtain cash from it.

It could have been anywhere in the country - which is why the unprecedented deployment of a bogus ATM at a mall in Manchester, Connecticut, east of Hartford, sent a jolt through the hearts of bank-machine users everywhere. The fake ATM, brought in by brazen con artists who convinced mall officials they were genuine, recorded the card numbers and personal id numbers of some 200 patrons, including a clerk at Kay's Jewelry, across from the ATM.

Why is this a Problem?

- Easier way to get malicious code into a voting system (for a software-based attack)
- Easy way to accidentally create problems (by loading uncertified version)
  - Software different from what poll workers were trained on
  - Software may not be sufficiently tested
  - Version incapability

How Can We Solve this Problem?

- Three Approaches:
  - –Chain of Custody
  - –Verify in Place
  - –Trusted Computing Base

How Can We Solve this Problem?
Chain of Custody (with seals, physical security)

- From the Test Lab
- To the State/County
- To the warehouse
- Through election definition and setup
- To the polling place
- And back again

How Can We Solve this Problem?
Chain of Custody

- Lots of places where a switch/unauthorized change could be made
- Does not address intentional update by well-meaning voting officials, vendors, or contractors

How Can We Solve this Problem?
Verify in place

- Read what is inside the machine
- Check it against the certified version
- Sounds straightforward

How Can We Solve this Problem?
Verify in place

- The magic of hashing
- Fingerprint Analogy
  - Smaller than you
  - Verifies it is you (more so than a real fingerprint)
  - Can't create a person from a fingerprint

How Can We Solve this Problem?
Verify in place

- Let's stretch the fingerprint analysis
- Need to know the questioned print is really attached to the person
- The person doesn't do the comparison. "Officer, I checked my fingerprints against the FBI fingerprint database and I am not the criminal you are looking for."

How Can We Solve this Problem?
Verify in place – For Voting Systems

- Need something besides the questioned computer to read what is inside the computer and do the comparison
  - Therefore, need "read access" to something "readable"
  - Need for this access to not create other security problems
- Need trusted source for the certified versions

How Can We Solve this Problem?
Verify in place – For Voting Systems

- Need something besides the questioned computer to read what is inside the computer and do the comparison
  - Therefore, need "read access" to something "readable."
  - Need for this access to not create other security problems.
- SOLUTION: trusted port or interface

How Can We Solve this Problem?
Verify in place – For Voting Systems

- Need trusted source for the certified versions.
- SOLUTION: Have test labs send certified versions of software to NSRL.

Current Status

- Polling stations may NOT have a trusted port. Therefore, they cannot be externally verified.
- Backend management (e.g., tabulation) systems are on PCs and therefore can be verified.

Current Status

- Not all voting systems store their software in a form that can be “read.”
- Some software files change as a normal part of operations (especially database files)

Limitation

- What if it isn't the same?
  - Hashes will be different for ANY change – even small ones that make no difference
  - Hashes don't help explain why a change occurred

How Can We Solve this Problem?
Trusted Path/Trusted Computing Base

- Use cryptography to augment seals and physical security to achieve a digital chain of custody
- Not currently available

Issues

- Trusted port/interface will be expensive
- May introduce security vulnerabilities
- Need software program to do the reading and comparison in a usable manner

Conclusion

- Trust in voting systems present a special challenge
- Trust at an all-time low
- Only through testing combined with integrity management can we begin to restore confidence

Other Issues

- This is NOT software escrow
  - This does not support reconstituting a system/environment in case of legal challenge or vendor failure.
  - Object/Executable code vs. source code. NSRL only collects executables.