Journal of Physical Security 6(1), 43-45 (2012)

Viewpoint Paper

Common Election Security Myths*

Roger G. Johnston, Ph.D., CPP
Vulnerability Assessment Team
Argonne National Laboratory

After talking with dozens of different election officials around the country, I've come to the conclusion that the following myths about election security are quite common.

Myth 1. Tamper-indicating seals will be blatantly damaged or missing if there has been an attack.

The reality: Stealing votes generally requires surreptitious attacks; tearing off seals is mere vandalism, not a credible attempt at vote stealing. Moreover, even amateurs can attack seals and leave little or no evidence.

Though they rarely get it, seal inspectors (and installers) need at least a few minutes of hands-on training, specific to the relevant seal(s) and application. (See paper #3 about seals in this issue of the *Journal of Physical Security*.)

Myth 2. Electronic voting machine security is the main issue.

The reality: The main issue, I believe, is having a healthy Security Culture. The fact that current electronic voting machines have little to no security built in is really part of a weak security culture, where manufacturers are not held accountable by their customers for making secure machines. Some of the other critical attributes of a healthy Security Culture include a strong focus on security, a willingness to think like the bad guys, openness to criticism and suggestions, and avoidance of denial.

Myth 3. "Certification" and "standards" are of great value for electronic voting machines.

The reality: Neither are likely to address major election security issues and attack scenarios. Certification and standards are often of minimal use in other security applications, and sometimes make things worse, e.g., ISO 17712 for cargo seals.

*Editor's Note: This viewpoint paper was not peer reviewed.

Myth 4. Checking that a voting machine seems to be operating properly is an effective security check.

The reality: In fact, you need to disassemble and reverse engineer the machine to look for signs of tampering and alien electronics. As we in the Vulnerability Assessment Team at Argonne National Laboratory have shown, turning cheating on and off (even remotely) is easy to do.

Myth 5. Cyber is the only important kind of attack.

The reality: Actually, other electronic and physical attacks are often easier, harder to detect, and harder to prevent, especially when executed by insiders.

Myth 6. An adversary has to be very sophisticated to steal votes.

The reality: Currently, this is clearly not the case in most election jurisdictions.

Myth 7. Manufacturers of voting machines do a good job with security, and know what they are doing when it comes to security.

The reality: All one has to do is look briefly at the designs of various electronic voting machines to see that this myth is not true.

Myth 8. There is little you can do about the insider threat.

The reality: The insider threat is always a challenge, but there are effective countermeasures that can be implemented.

Myth 9. Adversaries must tamper with hundreds or thousands of voting machines to succeed.

The reality: Due to improvements in gauging public sentiment, it is now possible to tell in advance when elections will be very close. In the 2008 Senate race in Minnesota, for example, pollsters predicted an extremely close contest. Indeed, Al Franken won by only 312 votes out of the 2.9 million cast. Tampering with 1-3 voting machines could have changed the outcome of that race. In contests in rural areas or small towns, tampering with a single voting machine might be sufficient.

It is also a fallacy to think that vote tamperers will be only interested in winning an election. Fringe candidates and parties may merely wish to gain credibility, attention, matching funds, or an invitation to future debates by securing, say, 5% of the vote. (The idea stated by some that this is ok as long as it does not affect who wins the election is, in my view, without merit. Even this kind of tampering is still undemocratic fraud that disenfranchises the voters.)

Myth 10. A Voter Verified Paper Record guarantees there will be no vote tampering.

The reality: While having a voter verified paper record is an excellent security measure, it does not guarantee election integrity. It just creates an extra step for an adversary. Given the poor protection typically provided for most paper records (including poor seal usage), tampering with paper records is not usually going to be very challenging, especially for an insider.

"Myth" 11. There has never been a successful cyber, electronic, or physical attack on voting in the United States in recent years.

The reality: We just don't know. Currently, a competent attack would be unlikely to be detected, especially for the 25% of voters who vote on electronic voting machines that lack a voter verified paper record.

Myth 12. If I as an election official can't conceive of how to defeat my election security, than nobody can.

The reality: Few election officials have much experience or expertise with security, and few seem to be highly imaginative. Few get good outside advice about security. (Often, security vendors are their only source of security information.) Few want there to be vulnerabilities—making it hard for them to see vulnerabilities.