Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Suggestions for Better Election Security

From the Vulnerability Assessment Team at Argonne National Laboratory

Summary of Common Security Mistakes

1. Electronic voting machines that fundamentally lack security thought and features, including an ability to detect tampering or intrusion, or to be reliably locked or sealed.

2. Failure to disassemble, examine, and thoroughly inspect (not just test) a sufficient number of voting machines before and after elections in order to detect hardware or software tampering.

3. Assuming that tamper-indicating seals will either be blatantly ripped/smashed open, or else there is no tampering. In reality, even amateurs can spoof most seals leaving (at most) subtle evidence.

4. Inadequate seal use protocols and training of seal installers and inspectors. Failure to show examples of blatantly and subtly attacked seals to seal inspectors.

5. Over confidence in use of a voter verified paper record (VVPR). A VVPR is an excellent security countermeasure, but it is not a silver bullet, especially for an election organization with poor overall security.

5. Little or no insider threat mitigation.

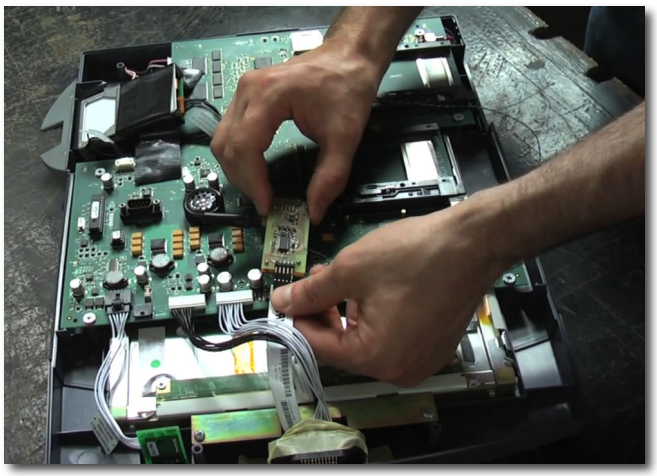
6. A poor security culture, including denial and no *a priori* procedures for dealing with security questions or concerns.

About These Suggestions

The following suggestions for better election security are from the Vulnerability Assessment Team (VAT) at Argonne National Laboratory (http://www.ne.anl.gov/capabilities/vat). The suggestions fall into two categories, "Minimum", which are security features that are essential in our view, and "Recommended", which are needed for the best security.

Hardware & Software Inspection

Recommended: Prior to the election, at least 1% of the voting machines—randomly chosen—should be removed from the polling places and tested, then disassembled, inspected, and the hardware examined for tampering and alien electronics. The software/firmware should also be examined, including for malware. It is not sufficient to merely test the machines in a mock election, or to focus only on cyber security issues! This analysis should be completed prior to the election.



Inserting alien electronics into an electronic voting machine in a classic (non-cyber) "man-in-the-middle" attack.

Minimum: It is completed less than 6 weeks after the election.

Minimum: Within 4 weeks after the election, at least 1% of the voting machines actually used in the election—randomly chosen—should be tested, then disassembled, inspected, and the hardware examined for tampering and alien electronics. The software/firmware should also be examined, including for malware. It is not sufficient to merely test the machines in a mock election, or to focus only on cyber security issues!

Recommended: The voting machines for the above inspection (or trial bribery discussed below) should be randomly chosen based on pseudo-random numbers generated by computer, or by hardware means such as pulling numbers or names from a hat. No individual should

make the random choices without the aid of hardware or software.

Insider Threat

Minimum: All election officials, technicians, contractors, or volunteers who prepare, maintain, repair, test, inspect, or transport voting machines, or compile "substantial" amounts of election results should have background checks, repeated every 3-5 years, that include a criminal background history, credit check, and (when practical) interviews with co-workers.

Minimum: Prior to each election, all poll workers, election judges, election officials, and relevant contractors and technicians should take an oath to protect election integrity. They should be warned of the legal penalties for vote tampering and fraud, and reminded of their patriotic and ethical responsibility to help guarantee fair elections. They should also be thanked for taking on this important responsibility, and being vigilant of election security.

Minimum: Before each election, the U.S. citizenship of every poll worker and election judge should be verified in a reliable manner.

Recommended: On a regular basis, try bribing a small subset of poll workers, election judges, election officials, technicians, clerks, and personnel who transport voting machines and other election materials. Let them keep the money and hail them publicly as honest heroes if they decline the bribe. (Allow at least 36 hours for the bribe to be reported or declined.) There are legal entrapment issues here, but the point isn't so much to identify and fire dishonest individuals as it is to make bribes untenable by creating publicity and uncertainty about whether an apparent bribe is some kind of test.

Recommended: A written policy should be in effect and periodically communicated to all employees and contractors that bribery attempts must be reported immediately, and where or to whom they should be reported.

Locks

Minimum: Locks on voting machines should not all open with the same key.

Minimum: Opening of a lock on a voting machine or container should be accompanied by a careful examination of the exterior of the voting machine or container in order to try to determine if the integrity of the voting machine or container has been compromised without disturbing the lock. This includes looking for evidence of cosmetic repair of the voting machine or container walls after they have been breached. Election officials, judges, and technicians should be trained on how to inspect the relevant voting machines or containers, including the underside.

Tamper-Indicating Seals

For information on tamper-indicating seals, see *American Scientist* **94**(6), 515-523 (2005); *ACM Transactions on Information and System Security*, 14, 1–29 (2011); http://www.cs.princeton.edu/~appel/voting/Johnston-AnalysisOfNJSeals.pdf and http://www.ne.anl.gov/capabilities/vat.

Minimum: Avoid the assumption that tamper-indicating seals will either be blatantly ripped/smashed open, or else there is no tampering. In reality, even amateurs can spoof most seals leaving (at most) subtle evidence.

Minimum: Prior to each election, all poll workers and election officials who inspect seals (including tamper-evident packaging) need to have a minimum of 10 minutes of training per kind of seal used. This training will include information as to how to install (if appropriate) and inspect the seal. This should include multiple samples, photos, or videos of that specific kind of seal that has been attacked subtly and samples, photos, or videos of that specific kind of seal that has been attacked blatantly, e.g., by being ripped open or smashed.

Minimum: Personnel who inspect seals that protect "large" numbers of election results should have an additional 10 minutes per kind of seal. This should include hands-on practice in spotting sample seals that have been opened subtly and those that have been opened blatantly.

Recommended: Only a small number of election officials should be authorized to order tamper-indicating seals, and the seal manufacturer or vendor should contractually agree to refuse orders not placed by those individuals or by anyone who does not know the secret password required for seal purchases for a given election district, and to report failed attempts to officials of that election district.

Recommended: The vendor or manufacturer of seals used for election purposes should contractually agree not to provide 2 or more seals with the same serial number (including at a later time) to anyone.

Recommended: A two-person rule should be in effect when a seal is applied to critical election assets. Each person should verify that the correct seal was correctly applied, and that its

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

serial number is correctly entered into the database of seal serial numbers.

Minimum: Only tamper-indicating seals with unique serial numbers should be used.

Recommended: Signing or initialing seals offers little effective security and should not be done.

Minimum: All seal inspections require checking the seal serial number against the secured data log of seal serial numbers. Each seal must also be carefully examined for evidence of both subtle and blatantly obvious opening, counterfeiting, damage, or removal.

Minimum: The list of seal serial numbers for seals applied to voting machines and containers or packages of sensitive election materials must be carefully protected from tampering, theft, or substitution.

Recommended: Seals should not be used in sequential order based on serial number (so that an adversary cannot predict a seal serial number in advance).

Minimum: Seal inspectors must not be fooled by a seal of the wrong kind or color that has the correct serial number—a common mistake.

Minimum: Seals must be inspected alongside an identical (except for serial number), well-protected unused seal of the same kind. There must be a comparison of size, morphology, color, surface finish, and serial number font, digit spacing, and digit alignment/orientation.

Recommended: Minimize the use of (pressure sensitive) adhesive label seals (because these tend to be easy to counterfeit or to remove, then replace without leaving easily detectable evidence, plus they require an inordinate amount of training and inspection time to be effective).

Minimum: With adhesive label seals, prior to installing the seal, the surface the seal is to be applied to must be cleaned and checked for evidence of oil or other substances that can reduce surface adhesion.

Minimum: With adhesive label seals, the way the seal behaves when it is removed is often a critical method for checking for tampering. To be effective, however, the seal inspector must know how the seal is supposed to behave when removed.

Minimum: Any checking of a seal for evidence of being broken or tampered should be accompanied by a careful examination of the container or package or voting machine the seal is attached to in order to try to determine if the integrity of the container or package or voting machine has been compromised without disturbing the seal. This includes looking for evidence of cosmetic repair of the container/package/voting machine walls after they have been breached. Seal inspectors should be trained on how to do this inspection for each kind of container, package, or voting machine.

Minimum: All used seals should be preserved until at least 3 months after the election for possible examination, then thoroughly destroyed (not just discarded in the trash) so that the parts cannot be used by adversaries to practice or execute seal attacks.

Minimum: All unused seals should be protected or guarded prior to use from theft or unauthorized access. Seal installers must be required to protect and turn in any unused seals.

Secure Transport

Recommended: Escort the voting machines to and from the polling place if at all possible. Use *pro bono* volunteers if necessary.

Recommended: Do not allow technicians to work on a specific voting machine without authorization and oversight.

Recommended: Personnel or contractors who transport voting machines to or from the polling places should be bonded.

Minimum: Some individual or group should be responsible for accepting voting machines and sensitive election materials delivered to the polling place before or on election day, sign for them, and be responsible for providing oversight to the extent practical. (This can include students at a school, for example.) It should be possible to determine if there was an unexpected delay in delivery of any such voting machines or election materials, and this delay must be investigated immediately. Similarly, any delay in receipt of the voting machines back at the storage warehouse after the election should be detectable and immediately investigated.

Chain of Custody

A chain of custody is a process that helps to secure voting machines, ballots, records, memory devices, seals, keys, seal databases with serial numbers, and other election materials. We henceforth refer to these items needing protection from theft, tampering , copying, or substitutions as “assets”. (Note:

A "chain of custody" is not a piece of paper that multiple people sign or initial.)

Recommended: An effective chain of custody starts by checking that everyone to be involved in handling the assets in question is trustworthy. This is best determined by periodic background checks.

Minimum: An effective chain of custody requires procedures to make sure that each person handing off the assets to another is sure of the identify of the person they are handing the material to, and that this person has been authorized to receive the assets.

Recommended: Each individual in the chain of custody must know the secret password of the day or the election before being allowed to take control of the assets.

Minimum: Each individual in the chain of custody must assume the individual responsibility of safeguarding the assets while in their custody, not letting the assets out of their sight to the extent possible, and securing the assets under lock or seal when not in sight.

Minimum except where noted: A chain of custody log should be kept with the assets. It must be signed by each recipient in the chain of custody when accepting the assets with a carefully signed signature (not initials) along with a printed, legible listing of their name, the date, location (Recommended), and time (Recommended). This log must also be protected from tampering, counterfeiting, or substitution.

Independent Security Review

Minimum: The majority of advice on election security should not come from vendors or manufacturers of voting machines or of tamper-indicating seals or other security products used in elections. It is necessary to seek out objective, independent security expertise and advice.

Minimum: Election officials will arrange for a local committee (*pro bono* if necessary) to serve as the Election Security Board. The Board should be made up primarily of security professionals, security experts, university professors, students, and registered voters not employees of the election process. The Board should meet regularly to analyze election security, observe elections, and make suggestions for improved election security and the storage and transport of voting machines and ballots. The Board needs considerable autonomy, being able to call press conferences or otherwise publicly discuss its findings and suggestions as appropriate.

Employees of companies that sell or manufacture seals, other security products often used in elections, or voting machines are not eligible to serve on the Board.

Minimum: At least once every 3 years, the Election Security Board should oversee or conduct a comprehensive vulnerability assessment of the local election process, involving external consultants, volunteers, and security experts (including *pro bono*) to the extent practical.

Minimum: A Chief Election Security Officer (paid or unpaid) should be appointed who may have other duties as well. He or she is responsible for analyzing and overseeing election security issues and security training. The Security Officer also deals with and investigates security questions, concerns, and incidents on election day. He/she serves on the Election Security Board (discussed above) as a voting member, but does not chair the Board or appoint its members.

Recommended: The Chief Election Security Officer should maintain a publicly posted, frequently updated list of what he/she judges as the ten best suggestions (from the Board, or other internal or external sources) for potentially improving election security, and the prospects for implementing them. Public comments on this list should be encouraged.

Creating & Nurturing an Effective Security Culture

The key to good security is to have a healthy security culture. This requires everyone to pay attention to security issues, be thinking critically and continuously about security, to ask good questions, avoid denial, and to be free to raise concerns and be listened to about security issues.

Minimum: When election security is questioned, the first response of election officials and the Chief Election Security Officer must not be to deny the possibility of security vulnerabilities, but rather to seek to learn more and solicit advice from the person(s) raising these questions (and others) as to possible countermeasures or security improvements.

Recommended: Before each election, discuss in some detail with poll workers, election judges, and election officials the numerous ways that the voting process can be tampered with, and what to watch out for. Have them individually, or in groups suggest other ways they would tamper with votes if they were so inclined, including fanciful ways, using insiders or outsiders or insiders collaborating with outsiders. (The merits of the attack scenarios they devise are less important that instilling a mindset of thinking like the bad guys).

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Recommended: Poll workers, election judges, election officials, and other personnel involved in running elections should be warned and educated about techniques for misdirection and sleight-of-hand, perhaps by having these techniques explained/demonstrated by a magician, live or on video. (The sense of alertness to malicious acts that this engenders is actually of greater benefit than awareness of misdirection and sleight-of-hand *per se*, though the latter is not negligible.)

Recommended: Before each election, discuss with poll workers, election judges, and election officials the importance of ballot secrecy, and the importance of watching for miniature wireless video cameras in the polling place, especially mounted to the ceiling or high up on walls to observe voters' choices. The polling place should be checked for surreptitious digital or video cameras at least once on election day.

Recommended: Poll workers, election judges, election officials, and other personnel involved in running elections should be told how to accurately verify the identify of authorized election and law enforcement officials, as well as election workers who may be present on election day.

Recommended: Security must not be based substantially on secrecy, i.e., Security by Obscurity is not a viable security strategy, nor is secrecy conducive to observers, critical review, process improvement, feedback, transparency, or accountability. Somewhat counter-intuitively, the best security is security that is transparent. (Note: Some short-term secrecy may be warranted, such as short-term passwords or secrecy about the details of voting machine transport.)

Minimum: Security is hard work so expect it to be hard work. Any security device, system, procedure, or strategy that sounds too good to be true almost certainly is.

Minimum: There must be a convenient way for poll workers, election judges, election workers and contractors, election officials, and the general public to report security concerns, including anonymously on election day. There must be mechanisms in place to respond in a timely manner to these concerns, perhaps through the Chief Election Security Officer discussed above.

Recommended: Welcome, acknowledge, recognize, praise, and reward good security practice, as well as reasonable security questions and suggestions from any quarter, including from employees, contractors, poll workers, election judges, journalists, bloggers, and the general public.

Recommended: Election officials are often elected or are political appointees. It is important for a good security culture to attempt to differentiate and separate concerns, questions, and criticisms about election security from political attacks on those election officials.

Recommended: Security is difficult and involves complicated, value-based tradeoffs. Thus, security policy and practice is intrinsically a controversial topic worthy of debate and analysis, and should be viewed and treated as such. The existence of disagreement and dissent in regards to security must not be taken as a sign of weakness, but rather welcomed as a sign of a healthy security culture.

Other Suggestions

Recommended: Election officials should pressure manufacturers of voting machines to design them with better physical security, cyber security, and tamper/intrusion detection. Insist that manufacturers of voting machines design them with secure hasps that allow the use of locks and seals other than pressure sensitive adhesive label seals.

Minimum: Poll workers, election judges, and election officials should be able and expected to determine if a voting machine has been replaced by an unauthorized voting machine or counterfeit voting machine.

Recommended: A hash should be printed on each paper ballot on election day after each voter has completed the ballot. This hash should be generated from a secret algorithm that is different for each election, and possibly each polling location.

Recommended: Consider using a virtual numeric token system. See, for example, http://www.scantegrity.org. These kinds of approaches have some strong disadvantages including increasing complexity, slowing down the voting process, centralizing the risk, and creating new privacy issues. They can, however, potentially improve election security and transparency to a considerable degree.

About the Vulnerability Assessment Team

The Vulnerability Assessment Team (VAT) at Argonne National Laboratory has conducted vulnerability assessments on over 1000 different physical security and nuclear safeguards devices, systems, and programs. This includes analyzing locks, anti-counterfeiting tags, tamper-indicating seals, RFIDs, GPS, microprocessor systems, contact memory buttons, electronic voting machines, medical electronics,

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

nuclear safeguards equipment, and biometrics and other access control devices. The VAT has demonstrated how all these technologies can be easily defeated using widely available tools, materials, and supplies, but has also devised and demonstrated simple and practical countermeasures.

In addition, the VAT has provided security consulting, training, R&D, specialty field tools, and novel security devices and approaches for more than 50 different companies, NGOs, and government organizations, including DoD, NNSA, DHS, U.S. Department of State, the International Atomic Energy Agency (IAEA), Euratom, and intelligence agencies.

VAT personnel have given over 90 invited talks (including 6 Keynote Addresses) at national and international conferences.

The VAT is frequently interviewed by journalists and security bloggers about its work and its views on security. See, for example:

"Diebold Voting Machines Can Be Hacked by Remote Control", http://www.salon.com/news/2012_elections/index.html?story=/politics/elections/2011/09/27/votinghack

Bradblog.com, http://www.bradblog.com/?p=8785, http://www.bradblog.com/?p=8790, http://www.bradblog.com/?p=8818

"Most Security Measures Easy to Breach", http://www.youtube.com/watch?v=frBBGJqkz9E

"Roger Johnston on Election Security", http://www.opednews.com/articles/Argonne-Lab-s-Head-of-Vuln-by-Joan-Brunwasser-110329-968.html

"Getting Paid to Break Into Things: How Vulnerability Assessors Work at Argonne National Lab", http://www.techrepublic.com/blog/security/getting-paid-to-break-into-things-how-vulnerability-assessors-work-at-argonne-national-lab/5072?tag=mantle_skin;content

"Closing the Curtains on 'Security Theater'", http://www.smartplanet.com/technology/blog/science-scope/at-argonne-national-lab-closing-the-curtains-on-security-theater/5167/

"Digital Privacy: Are You Ever Alone?", http://news.medill.northwestern.edu/chicago/news.aspx?id=187163

"Six Rising Threats from CyberCriminals", http://www.computerworld.com/s/article/9216603/Six_rising_threats_from_cybercriminals

"Roger Johnston on Security Vulnerabilities of Electronic Voting", http://blog.verifiedvoting.org/2010/10/15/1131

"Phishing Attacks: Training Tips To Keep Your Users Vigilant", http://www.techrepublic.com/blog/security/phishing-attacks-training-tips-to-keep-your-users-vigilant/5402

Roger Johnston interviewed live on WTTW Public Television's "Chicago Tonight" program about electronic voting machines, http://www.wttw.com/main.taf?p=42,8,80&pid=BMeOsuVOgSUbQammoGQxMIIX00avS55H

"IT Security: Maxims for the Ages", http://blogs.techrepublic.com.com/security/?p=2435

"Security Maxims", *Security Now!* Podcast #215, http://www.grc.com/sn/sn-215.htm

"Vulnerability Assessment's Big Picture", CSO Magazine, http://www.csoonline.com/read/060107/fea_qa.html

Argonne National Laboratory

About Argonne National Laboratory

Argonne National Laboratory, the nation's first national laboratory, is one of the U.S. Department of Energy's largest national laboratories for science and engineering research. It is located 25 miles from downtown Chicago. Argonne is managed by UChicago, LLC, for the United States Department of Energy.

Argonne has approximately 3,400 employees, including 1,100 scientists and engineers, three-quarters of whom hold doctoral degrees. Argonne's annual operating budget exceeds $738 million.

Argonne NATIONAL LABORATORY

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov