ACCURATE

A CENTER FOR CORRECT, USABLE, RELIABLE,
AUDITABLE, AND TRANSPARENT ELECTIONS

PUBLIC COMMENT ON: NIST-IR 7682: INFORMATION SYSTEM SECURITY BEST PRACTICES FOR UOCAVA-SUPPORTING SYSTEMS; NIST-IR 7711: SECURITY BEST PRACTICES FOR THE ELECTRONIC TRANSMISSION OF UOCAVA ELECTION MATERIALS[*]

Submitted to
U.S. Department Of Commerce,
National Institute of Standards and Technology

May 15, 2011

[*] This material is based upon work supported by the National Science Foundation under A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE), Grant Number CNS-0524745. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. This public comment was prepared by Joseph Lorenzo Hall in consultation with ACCURATE Principal Investigators.

ACCURATE Principal Investigators

Aviel D. Rubin
ACCURATE Director
Department of Computer Science
Johns Hopkins University
rubin@cs.jhu.edu
http://www.cs.jhu.edu/~rubin/

Dan S. Wallach
ACCURATE Associate Director
Department of Computer Science
Rice University
dwallach@cs.rice.edu
http://www.cs.rice.edu/~dwallach/

Dan Boneh
Department of Computer Science
Stanford University
dabo@cs.stanford.edu
http://crypto.stanford.edu/~dabo/

Michael D. Byrne
Department of Psychology
Rice University
byrne@rice.edu
http://chil.rice.edu/byrne/

David L. Dill
Department of Computer Science
Stanford University
dill@cs.stanford.edu
http://verify.stanford.edu/dill/

Jeremy Epstein
Computer Science Laboratory
SRI International
jepstein@csl.sri.com
http://www.csl.sri.com/people/epstein/

Douglas W. Jones
Department of Computer Science
University of Iowa
jones@cs.uiowa.edu
http://www.cs.uiowa.edu/~jones/

Deirdre K. Mulligan
School of Information
University of California, Berkeley
dkm@ischool.berkeley.edu
http://www.ischool.berkeley.edu/
people/faculty/deirdremulligan

Peter G. Neumann
Computer Science Laboratory
SRI International
neumann@csl.sri.com
http://www.csl.sri.com/users/neumann/

Natarajan Shankar
Computer Science Laboratory
SRI International
shankar@csl.sri.com
http://www.csl.sri.com/people/shankar/

David A. Wagner
Department of Computer Science
University of California, Berkeley
daw@cs.berkeley.edu
http://www.cs.berkeley.edu/~daw/

1 Introduction

1.1 ACCURATE Background

A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE),[1] a multi-institution, interdisciplinary, academic research center funded by the National Science Foundation, appreciates the opportunity to provide public comment on NIST-IR 7682: *Information System Security Best Practices for UOCAVA-Supporting Systems*[2] ("NIST-IR 7682") and NIST-IR 7711: *Security Best Practices for the Electronic Transmission of UOCAVA Election Materials* ("NIST-IR 7711").[3]

ACCURATE was established in 2005 to research methods for improving voting technology in government elections. ACCURATE's Principal Investigators direct research into software architecture, tamper-resistant hardware, cryptographic protocols and verification systems as applied to electronic voting systems. Additionally, ACCURATE evaluates voting system usability and how public policy, in combination with technology, can better support elections.

Since 2005, ACCURATE has made many important contributions to the science and policy of electronic voting.[4] With experts in computer science, systems, security, usability, and technology policy, and knowledge of election technology, procedure, law and practice, ACCURATE is uniquely positioned to provide helpful guidance to NIST as it seeks to improve the administration of remote voting election support.

1.2 Overview

The content of both draft documents are helpful and constructive contributions to how best serve the special class of overseas remote voters consisting of citizens in uniform stationed abroad or otherwise living overseas. We are especially heartened to see NIST set a bright line distinction between the security postures of expediting low-risk election operations, such as communicating election information and materials, and remote transmission of voted ballot data, possibly through unsupervised and uncontrolled computing platforms. In order to appropriately reduce the burden on this class of voters without exposing our elections to the full set of risks involved with arbitrary models for remote voting,[5] we must be able to accept the risks involved with expedited electronic transmission of materials and work to mitigate any opportunities for error and fraud.

We have comments in a few places that we felt the drafts could be improved. Our comments, below, will list each comment and provide a brief discussion where necessary. For each document, we will first list more substantive comments and then separately list more trivial comments having to do with formatting and language.[6]

[1] *See:* `http://www.accurate-voting.org/`.

[2] National Institute of Standards and Technology. *Draft NISTIR 7682: Information System Security Best Practices for UOCAVA-Supporting Systems*. NIST-IR 7682. 2010. URL: `http://www.nist.gov/itl/vote/upload/draft-nistir-7682.pdf`.

[3] National Institute of Standards and Technology. *Draft NISTIR 7711: Security Best Practices for the Electronic Transmission of UOCAVA Election Materials*. NIST-IR 7711. 2010. URL: `http://www.nist.gov/itl/vote/upload/draft-_nistir_7711_june2010.pdf`.

[4] See ACCURATE's list of publications (`http://accurate-voting.org/pubs/`), reports & commentary (`http://accurate-voting.org/pubs/reports/`) and testimony (`http://accurate-voting.org/pubs/testimony/`).

[5] Andrew Regenscheid and Nelson Hastings. *A Threat Analysis on UOCAVA Voting Systems*. NIST-IR 7551. National Institute of Standards and Technology, 2008. URL: `http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf`.

[6] In each case we refer to the PDF page number, section number and typically some surrounding text to aid NIST and other readers to locate the text to which our comment applies.

2 NIST-IR 7682

NIST IR 7682 is intended for a technical audience—IT staff working for election officials, and is entitled, “Information System Security Best Practices for UOCAVA-Supporting Systems”. In contrast to NIST-IR 7711, NIST-IR 7682 doesn’t break its organization down into the *ends* of a given task (e.g., “getting x to the remote voter electronically”) but instead discusses large classes of security concerns, regardless of the overarching function being performed: identification and authentication, host/server protection, network protection and ongoing system protection activities.

2.1 Substantive Comments

1. PDF p. 9, Section 1.1: This section comments that S/MIME and OpenPGP are out of scope but the document later talks substantially about S/MIME. It would be good if this document could point readers to resources for S/MIME and OpenPGP/GnuPG such that election officials that wish to accept S/MIME-encrypted email or receive OpenPGP signed and/or encrypted email will have guidance as to setting up and configuring their systems in this manner. Also, OpenPGP is an IETF standard[7] and the most widely used software implementing that standard is GnuPG (GPG). Adding a short discussion of PGP/GPG and a pointer to a discussion/tutorial for using PGP/GPG would be good in this document, especially in the section (§5.3.1, PDF pp. 32–33) that goes into further detail with respect to S/MIME.[8]

2. PDF p. 13, Section 3: In this section, the document distinguishes between electronic authentication and physical (real-world) authentication by assuming that someone looking at a and individual with a photo ID can tell if the ID is fake. Procedures for verifying identification documents, for example those employed by the Transportation Security Administration, require substantial training and involve the use of ultraviolet light (“black lights”) to detect laminate holograms and magnifying loops to examine ID documents for lack of microprinting features and the presence of inkjet dots (both of which can indicate a forged ID).[9] It seems important here to recognize the limitations of physical, interactive ID checking and the limited extent to which robust ID checking can be practically employed in election environments. Perhaps this section could be made more clear by simply pointing out the *greater opportunity* that real-world physical interaction can provide for rich authentication.

3. PDF p. 13, Section 3: The document here says that passwords are expected to be memorized. It seems important to recognize that password management tools are available to allow individuals to store large quantities of strong passwords securely. The tools are designed to create and store strong passwords for users in order to allow them to use more secure passwords without having to memorize them all. The document could be improved by adding here “…expected to memorize or store securely” and pointing to resources for information on password management and tools for managing passwords. Once complication here is that network-dependent or “cloud” password management tools that store an encrypted blob of passwords “in the cloud” have recently been

[7] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer. *RFC 4880: OpenPGP Message Format*. IETF, 2007. URL: `http://tools.ietf.org/html/rfc4880`.

[8] Of course, an alternative would be to strike this later section on S/MIME, but we would prefer brief remarks and citation to guidance rather than simply considering it out of scope.

[9] Transportation Security Administration. *Aviation Security Screening Management: Standard Operating Procedures (Revision 3)*. 2008. URL: `http://www.papersplease.org/wp/wp-content/uploads/2009/12/tsa_screening_mgmt_sop.pdf`, Appendix 2, at 80.

compromised.[10]

4. PDF p. 15, Section 3.1: This section first claims that bank checks have worked well for over a hundred years because wet-ink signature forgery is hard and then—in the table at the bottom of the page—says that signature verification is used in in-person voting so it must be strong enough for remote transactions. First, banks have slowly moved away from checking every check's signature to complex fraud detection mechanisms where the ultimate step is "check review", consisting of an examination of all the physical security properties a financial instrument.[11] It is important to note that financial institutions have very sophisticated methods of managing fraud risks and detecting anomalies that are impractical for elections. Further, modern signature verification techniques use complex machine learning algorithms[12] and such signature verification tools don't seem widely deployed in the elections context, where humans often employ manual signature comparison.[13] We would recommend that the casual enthusiasm for manual signature verification in this section be tempered somewhat and that the comparative angle be emphasized.

5. PDF p. 19, Section 3.4: This section should mention, in some manner, the Certificate Authority (CA) trust problem, as in the recent case where a CA, Comodo, was compromised such that an attacker was able to sign a number of certificates for popular web domains, including many relevant to remote voting (such as webmail services).[14] This issue brought CA trust chains to light such that if an attacker can convince a CA or subordinate issuer to sign certificates, they can make arbitrary web destinations appear to be "securely" coming from their own servers. (This is also relevant for the discussion on "Authentication of Endpoints" on PDF p. 34, starting "If and attacker…".) While we do not have any good advice here to include for election IT staff, readers should at least be aware that there is a significant limitation to the current CA model. When solutions like DNSSEC become closer to being a reality, the document should be updated to reflect relevant guidance.

6. PDF p. 27, Section 4.2.6: Here the document recommends "Constantly screen for cross-site scripting (XSS) vulnerabilities.", very good advice. However, the document does not give the reader any indication or guidance as to how one might "screen" for XSS and cross-site request forgeries (XSRF).

7. PDF p. 41, Section 6.4: This section on "Media Control" does not mention that keeping close watch on and control over election media is critical for thwarting viral propagation of malware

[10] Lance Whitney. "LastPass CEO reveals details on security breach". *CNET News* (May 2011). URL: `http://news.cnet.com/8301-1009_3-20060464-83.html`.

[11] E. J Potter. "Customer Authentication: The Evolution of Signature Verification in Financial Institutions". *Journal of Economic Crime Management* 1:1 (2002). URL: `https://utica.edu/academic/institutes/ecii/publications/articles/A026B1A2-B067-59DE-920C01AD24768FE3.pdf`.

[12] D. Bertolini, L. S. Oliveira, E. Justino, and R. Sabourin. "Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers". *Pattern Recognition* 43:1, 387–396 (2010). URL: `http://www.inf.ufpr.br/lesoliveira/download/PR2010.pdf`.

[13] From our own work with election officials in California, we have heard of a few anecdotal reports of automated signature verification being used for vote-by-mail (VBM) signature checking. Many election officials seem to err on the side of enfranchisement, and allow signature comparisons to "pass" signature verification that would otherwise fail in the financial application, where any significant deviation could be cause for further investigation (in elections, if a signature is deemed non-matching, that person's ballot is not counted). Election officials we have talked to, anecdotally again, find the high rate of false positives and negatives ($\approx 2-5\%$) for the election-oriented signature checking tools to be high.

[14] Peter Bright. "How the Comodo certificate fraud calls CA trust into question". *Ars Technica* (Mar. 2011). URL: `http://arstechnica.com/security/news/2011/03/how-the-comodo-certificate-fraud-calls-ca-trust-into-question.ars`.

through election media.[15] This section *must* recognize this type of vulnerability and recommend close physical control and chain-of-custody over election media, as many deployed voting system models seem to be susceptible to viral-media attacks.

2.2 Minor Comments

1. PDF p. 13: The first sentence of §3 could be reworded to emphasize that the goal of voting systems is to allow legitimate voters to cast a ballot: "One goal of voting system functionality is to ensure that every ballot be cast by a legitimate voter."
2. PDF p. 13: The following wording, "...because the system administrator can affect the validity of votes from many voters." could be more precise. Perhaps, "...because the system administrator has heightened privileges that allow them to affect the validity many votes."
3. PDF p. 14: The second bullet point from the bottom of the page is formatted incorrectly.
4. PDF p. 17: It would be good to quote some costs for multi-factor one-time password devices.
5. PDF p. 22: In, "...detected by even by an up-to-date scanner." replace "scanner" with "malware scanner".
6. PDF p. 23: "aegis" should probably be replaced with a plain language term such as "control", "responsibility", etc.
7. PDF p. 24: This simplistic-sounding sentence should be rephrased, or simply removed: "Servers and management stations have beginnings, middles, and ends."
8. PDF p. 35: The phrase "'...very large random number' methods..." should be replaced with "cryptographic methods".

3 NIST-IR 7711

NIST-IR 7711 is intended for an audience of election officials and is entitled, "Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters". It gives an overview of the types of materials that officials might want to transmit (information, registration materials, ballot materials) and then spends most of the paper talking about specifics of transmitting 1) voter registration materials and ballot requests and 2) blank ballots. The main distinction made throughout the paper is sensitive versus public information (e.g., voter personal information versus generic election information). The document has good high-level treatments of cryptography, web-based authentication (typically with a side channel) and best practices in secure web services.

3.1 Substantive Comments

1. There is a good deal of redundancy between the two major sections in this document with a lot of copied text between the two. We are hesitant to recommend anything specific here, as NIST might want each section to be stand-alone (e.g., a jurisdiction may not do electronic registration materials delivery but might have to do blank ballot delivery). If that's the case, the document should state that in Section 1 where scope, audience and organization is addressed.

[15] J. Alex Halderman, Eric Rescorla, Hovav Shacham, and David Wagner. "You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting Systems". *USENIX/ACCURATE Electronic Voting Technology Workshop* (Aug. 2008). URL: `http://www.usenix.org/event/evt08/tech/full_papers/halderman/halderman.pdf`.

2. PDF p. 16, Section 2.2.2.1: This section includes a phrase, "...while few postal workers may be in a position to intercept a large number of mailed election materials." It is hard to know to what extent this phrase is correct, in general. Some jurisdictions may have less risk in this respect than others; for example, large jurisdictions may have entire post office trucks tasked for delivery of voted VBM ballots and very small jurisdictions may have a single postal carrier, both of which would seem to contradict the phrase quoted above. Perhaps the NIST document could point out that email is *relatively* more susceptible to these transmission/receipt "choke point" types of vulnerabilities and that there are well-established legal penalties for tampering or intercepting postal mail.[16]

3. PDF p. 17, Section 2.2.2.3: This section lacks discussion of the degree to which common email attachment formats can contain security and privacy-implicating features/malware. This is especially true for DOC (which can contain macro viruses) and PDF (which can contain JavaScript exploits), and less so for HTML, RTF, JPG and TXT formats. In the future, NIST might consider developing a resource like an "attachment weather report" that discussed the relative malware susceptibility of various common email attachment file formats.

4. PDF p. 30, Section 3.2.4: Here the document mentions "signing" PDF files to allow voters to verify that the files came from the election official and have been unmodified. By context, we can guess that NIST is not talking about using PKI via PGP/GPG but using Adobe Certified Document services. It is important to note that Adobe Certified Documents are only verifiable in Adobe PDF reading products (Adobe Reader and Acrobat, for example), despite that the PDF standard allows any PDF reader to check these signatures.[17] This method of signing PDF documents can be expensive as the subscription services for getting and using a certificate require a hardware token and charge per-document signing fees (e.g., require the customer to buy a license for signing a certain volume of documents per year) or require a much more expensive "unlimited signing" subscription. NIST should make these limitations (only verifiable using Adobe products and not, e.g., Apple's `Preview.app`) and the required expense more explicit. We applaud NIST for recommending signing of transmitted materials outside of just the TLS/SSL session for a web connection (as PDFs can be delivered via email, of course). Note that similar text as this appears elsewhere: PDF p. 41.

5. PDF p. 30, Section 3.3: This sections needs to emphasize that if the jurisdiction uses an e-fax service on their side (such that any fax to the jurisdiction does not end on a telephonic fax machine), this creates a choke-point at the e-fax service by which an attacker can get personal information in quantity.

6. PDF p. 32, Section 3.4.2: This section advises removing sensitive email from servers after it is no longer needed. It should also discuss *secure deletion* of sensitive email. Granted, this is not a perfect solution for removing all traces of sensitive email given how many hops email goes through during transmission, but secure deletion is better advice than simply recommending they "remove" such material from the server at the destination as this does not technically delete that information unless it is over-written with a random bitstream.

[16] Statutes like the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §1030, and Electronic Communications Privacy Act (ECPA), 18 U.S.C. §2510, do deal with unauthorized access to computer systems, networks and communications, but aren't as well established as legal protections for mail theft and interception.

[17] *Document management – Portable document format – Part 1: PDF 1.7 (ISO 32000-1)*. Adobe Systems, Inc., 2008. URL: `http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/PDF32000_2008.pdf`, at 474, §12.8.3.

7. PDF p. 40, Section 4.2.4: In a section on ballot tracking, the document recommends encrypting any unique identifiers before printing them on ballots to remove any capability to link a ballot to a voter. We would recommend modifying this advice such that the encrypted identifier not be printed in a manner that someone could easily transcribe (e.g., it should be a barcode rather than alphanumeric text).

3.2 Minor Comments

1. PDF p. 5: The last sentence of the Abstract is incomplete; "Systems" should be added right before the period.

2. PDF p. 17: The second bullet from the top of the page should include spam. We recommend changing this to, "The outgoing e-mail server, or the recipient's e-mail server, detected a virus or classified the e-mail as spam."

3. PDF p. 21, Section 2.3.1: Typo; "beused" should be "be used".

4. PDF p. 22, Section 2.3.2: The usage of the word "tags" may be confusing; we suggest something like "fingerprint" or "protected fingerprint".

5. PDF p. 38: The reference at the bottom of the page to 4.3.4, should be to 4.2.4.

6. PDF p. 41: The paragraph right above §4.3 should point to §4.6 to cross-reference future discussion of online ballot markers.

4 Conclusion

ACCURATE appreciates the opportunity to comment on these important milestones in serving UOCAVA voters via electronic transmission of ballot materials and other UOCAVA-supporting information systems. We offer our analysis, experience and expertise in the hope it will help NIST develop practical, precise and constructive guidance to election jurisdictions as they increase their remote voting support. We would be happy to answer any questions NIST has about our comments and engage in further dialog with NIST.