Computer Technologists' Statement on Internet Voting

Election results must be verifiably accurate -- that is, auditable with a permanent, voter-verified record that is independent of hardware or software. Several serious, potentially insurmountable, technical challenges must be met if elections conducted by transmitting votes over the internet are to be verifiable. There are also many less technical questions about internet voting, including whether voters have equal access to internet technology and whether ballot secrecy can be adequately preserved.

Internet voting should only be adopted after these technical challenges have been overcome, and after extensive and fully informed public discussion of the technical and non-technical issues has established that the people of the U.S. are comfortable embracing this radically new form of voting.

A partial list of technical challenges includes:

- **The voting system as a whole must be verifiably accurate in spite of the fact that client systems can never be guaranteed** to be free of malicious logic. Malicious software, firmware, or hardware could change, fabricate, or delete votes, deceive the user in myriad ways including modifying the ballot presentation, leaking information about votes to enable voter coercion, preventing or discouraging voting, or performing online electioneering. Existing methods to "lock-down" systems have often been flawed; and even without that problem, there is no guaranteed method for preventing or detecting attacks by insiders such as the designers of the system.

- **There must be a satisfactory way to prevent large-scale or selective disruption** of vote transmission over the internet. Threats include "denial of service" attacks from networks of compromised computers (called "botnets"), causing messages to be mis-routed, and many other kinds of attacks, some of which are still being discovered. Such attacks could disrupt an entire election or selectively disenfranchise a segment of the voting population.

- **There must be strong mechanisms to prevent undetected changes to votes**, not only by outsiders but also by insiders such as equipment manufacturers, technicians, system administrators, and election officials who have legitimate access to election software and/or data.

- **There must be reliable, unforgeable, unchangeable voter-verified records** of votes that are at least as effective for auditing as paper ballots, without compromising ballot secrecy. Achieving such auditability with a secret ballot transmitted over the internet but without paper is an unsolved problem.

- **The entire system must be reliable and verifiable** even though internet-based attacks can be mounted by anyone, anywhere in the world. Potential attackers could include individual hackers, political parties, international criminal organizations, hostile foreign governments, or even terrorists. The current internet architecture makes such attacks difficult or impossible to trace back to their sources.

Given this list of problems, there is ample reason to be skeptical of internet voting proposals. Therefore, the principles of operation of any internet voting scheme should be publicly disclosed in sufficient detail so that anyone with the necessary qualifications and skills can verify that election results from that system can reasonably be trusted. Before these conditions are met, "pilot studies" of internet voting in government elections should be avoided, because the apparent "success" of such a study absolutely cannot show the absence of problems that, by their nature, may go undetected. Furthermore, potential attackers may choose only to attack full-scale elections, not pilot projects.

The internet has the potential to transform democracy in many ways, but permitting it to be used for public elections without assurance that the results are verifiably accurate is an extraordinary and unnecessary risk to democracy.

Endorsements

The computer technology experts below endorse this statement. Affiliations are for identification only, and do not imply that employers have a position on the statement.

Alex Aiken
Professor of Computer Science, Stanford University
http://cs.stanford.edu/~aiken

Andrew W. Appel
Professor of Computer Science, Princeton University
http://www.cs.princeton.edu/~appel/

Ben Bederson
Associate Professor, Computer Science Department, University of Maryland
http://www.cs.umd.edu/~bederson

L. Jean Camp
Associate Professor, School of Informatics, Indiana University
http://www.ljean.com/

David L. Dill
Professor of Computer Science, Stanford University and Founder of VerifiedVoting.org
http://verify.stanford.edu/dill

Jeremy Epstein
Software AG and Co-Founder, Verifiable Voting Coalition of Virginia
http://www.visualcv.com/jepstein

David J. Farber
Distinguished Career Professor of Computer Science and Public Policy, Carnegie Mellon University
http://www.epp.cmu.edu/httpdocs/people/bios/farber.html

Edward W. Felten
Professor of Computer Science and Public Affairs, Princeton University
http://www.cs.princeton.edu/~felten

Michael J. Fischer
Professor of Computer Science, Yale University, and President, TrueVoteCT.org
http://www.cs.yale.edu/people/fischer.html

Don Gotterbarn
Director, Software Engineering Ethics Research Institute, Computer and Information Sciences, East Tennessee State University
http://csciwww.etsu.edu/gotterbarn

Joseph Lorenzo Hall
UC Berkeley School of Information
http://josephhall.org/

Harry Hochheiser
Assistant Professor, Computer and Information Sciences, Towson University
http://triton.towson.edu/~hhochhei

Jim Horning
Chief Scientist, SPARTA, Inc., Information Systems Security Operation
http://www.horning.net/pro-home.html

David Jefferson
Lawrence Livermore National Laboratory
http://people.llnl.gov/jefferson6

Bo Lipari
Retired Software Engineer, Executive Director New Yorkers for Verified Voting
http://www.nyvv.org/bolipari.shtml

Douglas W. Jones
Professor of Computer Science, University of Iowa
http://www.cs.uiowa.edu/~jones/vita.html

Robert Kibrick
Director of Scientific Computing, University of California Observatories / Lick Observatory
http://www.ucolick.org/~kibrick

Scott Klemmer
Assistant Professor of Computer Science, Stanford University
http://hci.stanford.edu/srk/bio.html

Vincent J. Lipsio
http://www.lipsio.com/~vince/resume.pdf

Peter Neumann
Principal Scientist, SRI International
http://www.csl.sri.com/users/neumann

Eric S. Roberts
Professor of Computer Science, Stanford University
http://cs.stanford.edu/~eroberts/bio.html

Avi Rubin
Professor, Computer Science, Johns Hopkins University
http://avi-rubin.blogspot.com/

Bruce Schneier
Chief Security Technology Officer, BT Global Services
http://www.schneier.com/

John Sebes
Co-Director, Open Source Digital Voting Foundation
Chief Technology Officer, TrustTheVote Project
http://www.osdv.org/who

Yoav Shoham
Professor of Computer Science, Stanford University
http://cs.stanford.edu/~shoham

Barbara Simons
IBM Research (retired)
http://www.verifiedvoting.org/article.php?id=2074

Eugene H. Spafford
Professor and Executive Director of CERIAS, Purdue University
http://spaf.cerias.purdue.edu/narrate.html

Michael Walfish
Assistant Professor of Computer Science, University of Texas, Austin
http://nms.csail.mit.edu/~mwalfish

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

Luther Weeks
Retired Software Engineer and Computer Scientist
http://www.ctvoterscount.org/?page_id=2

Jennifer Widom
Professor of Computer Science, Stanford University
http://infolab.stanford.edu/~widom/

David S. Wise
Computer Science Dept., Indiana University
http://www.cs.indiana.edu/~dswise/

Questions and Answers on the "Computer Technologists' Statement on Internet Voting"

We hope these questions and answers clarify the intention of the statement.

Q: Who is behind this statement?

A: The primary author is David Dill, Professor of Computer Science at Stanford, with extensive input and editing from a number of others. This is also the position of VerifiedVoting.org on internet voting, and VerifiedVoting.org will help to publicize it.

Q: Why this statement at this time?

A: Serious proposals to use internet voting keep coming up. There have been several internet primaries in the last few years, including a primary conducted by Democrats Abroad in 2008. Furthermore, internet voting schemes are being promoted for the general election in 2008, including a proposal by Okaloosa County, Florida, and the State of Alabama.

In many cases, these schemes have been deployed without due consideration of the technical challenges, based on unsupported assertions by vendors that the systems are "secure". Independent experts need to speak out.

Q: Is this an anti-internet voting statement?

A: No. Some of the people who have endorsed it are working on internet voting methods. The statement is intended to be a warning: internet voting is not as easy to do safely as some people seem to think. Before we move to it, we need an informed public debate so the people know what they're getting into.

Q: What explains the enthusiasm for internet voting?

A: Currently, most of the momentum seems to be coming from the difficulties that Americans overseas, especially in the military, have voting. The mails are inefficient, so absentee ballots take a long time to reach the voter and a long time to return.

We understand this problem, but it seems clear that the situation can be made a lot better for overseas voters without internet voting. First, a system could be set up where any voter can print a ballot obtained over the internet (or obtain a remotely printed ballot at a military facility or embassy), which would eliminate half the mail problems, and difficulties with local elections offices that mail ballots late. Second, marked ballots could be returned by express mail or (better) by military transport or in diplomatic pouches, after being appropriately signed and sealed. This year, Federal Express is offering discounts to overseas voters for returning ballots. Finally, laws in some states could be modified to make the time constraints on ballot arrival less stringent, to reduce the risk that ballots will not be counted. In voting, there has been a tendency to look for technical solutions to problems that are mostly non-technical. We believe that is happening again with internet voting.

Alternatively, someone could come up with an internet voting scheme that is at least as safe as current overseas ballots, and convince the rest of us that it actually is secure and doesn’t have other harmful effects.

We do not feel that it is appropriate to “enfranchise” voters by providing them with a system that may allow their votes to be lost or stolen undetectably.

Q: The statement asks that the "principles of operation" of the system need to be disclosed. What does that mean? Does it require open source?

A: We're going by analogy with low-tech voting systems. For example, to understand why a fully manual paper ballot voting system can be trusted, people have to know how the ballots are handled, how polling places are run, etc. For example, if there are multiple poll workers present in each polling place at all times, it's harder for someone to "stuff" the ballot box. If hand counts are conducted in public view, it's less likely that the counts are erroneous.

We don't need to know everything about a system to know whether it is trustworthy. For example, most people would not feel that they need to know how computerized typesetting works before they marked a paper ballot. In fact, if you have to know a lot of complex details to understand whether a system can be trusted, that system probably can't be trusted.

The statement asks that the things we need to know to trust a proposed internet voting scheme be revealed. This is a problem because many schemes are being proposed where the details of operation are secret.

Some of us think "open source", or, more precisely, public disclosure of source code is a good idea. However, source code disclosure is neither necessary nor sufficient for trustworthy voting. Even when source code has been carefully inspected, it is very easy to overlook program bugs or malicious behavior in the system. It is also very difficult to make sure that the program running on a particular voting system matches the source code that was reviewed (vs. "acting the same" for certain test cases). Finally, errors and malicious changes can exist in parts of the system that are not in the source code, including low-level firmware and the hardware itself.

In a nutshell, if the security of a system depends on source code review, the system is not secure.

Q: Are you implying vendors or election officials are dishonest?

A: No, not any more than wanting bank statements implies that my bank is dishonest. Almost all trust in modern society is based on checks and balances (e.g., auditing requirements). Without the accountability that follows from checks and balances, systems become inaccurate and often dishonest. Classical election procedures are based on checks and balances, with the knowledge that elections are important and that unscrupulous people may seek to commit fraud. The same principles need to be maintained in new election systems.

Q: As someone without a strong technical background, why should I have to rely on a bunch of computer scientists to tell me whether I can trust my elections?

A: Maybe you shouldn't (however, the statement at least insists that there should be enough disclosure so that a technical person you trust can review the scheme and tell you what he or she thinks about it). If you have non-technical concerns about internet voting, this would be a good time to speak up. As the statement notes, we are NOT saying that the decision whether to use internet voting is a purely technical decision -- just that it needs to be a technically INFORMED decision. The technical challenges of internet voting are currently being minimized, often by people who simply don't understand them.

We're calling for an in-depth, public debate on the technical and NON-TECHNICAL issues in internet voting before adopting it. It's very possible that a technically sound internet voting scheme could be rejected for non-technical reasons, including other issues such as whether internet voting might disenfranchise legal voters who cannot easily access the internet.

Q: Isn't this statement at odds with the position of some of the people involved that only "voter verified paper ballots" should be used in elections?

A: The statement is a floor, not a ceiling. Endorsing it is definitely NOT an endorsement of internet voting or voting that uses electronic ballots. It says that internet voting should NOT be deployed unless certain minimum conditions -- with which we believe most technologists would agree -- are met. It does not imply the internet voting or electronic ballots can be used safely, or ever should be used.

Q: Why doesn't the statement demand (my favorite requirement)?

A: The statement is focused on the technical problems of internet voting, and sets out minimal conditions that represent a consensus of those endorsing it. The decision about whether or not internet voting should be used depends on many issues, including whether it has (your favorite requirement).

The main goal of the statement is to prevent deployment of internet voting without due consideration of the risks. It also calls for the ability of the general public to participate in the decision of whether or not to use internet voting -- including you, should you choose to argue for (your favorite requirement).

Q: Why “internet” and not “Internet”?

A: The early endorsers who objected to my earlier capitalization of “internet” were more passionate and spoke earlier than those who objected to spelling it in lower-case. Also, see http://www.wired.com/culture/lifestyle/news/2004/08/64596