DOI:10.1145/2347736.2347754

Internet voting is unachievable for the foreseeable future and therefore not inevitable.

BY BARBARA SIMONS AND DOUGLAS W. JONES

Internet Voting in the U.S.

THE ASSERTION THAT Internet voting is the wave of the future has become commonplace. We frequently are asked, "If I can bank online, why can't I vote online?" The question assumes that online banking is safe and secure. However, banks routinely and quietly replenish funds lost to online fraud in order to maintain public confidence.

We are told Internet voting would help citizens living abroad or in the military who currently have difficulty voting. Recent federal legislation to improve the voting process for overseas citizens is a response to that problem. The legislation, which has eliminated most delays, requires states to provide downloadable blank ballots but does not require the insecure return of voted ballots.

Yet another claim is that email voting is safer than Web-based voting, but no email program in widespread use today provides direct support for encrypted email. As a result, attachments are generally sent in the clear, and email ballots are easy to intercept and inspect, violating voters' right to a secret ballot. Intercepted ballots may be modified or discarded without forwarding. Moreover, the ease with which a `From` header can be forged means it is relatively simple to produce large numbers of forged ballots. These special risks faced by email ballots are in addition to the general risks posed by all Internet-based voting schemes.[17]

Many advocates also maintain that Internet voting will increase voter participation, save money, and is safe. We find the safety argument surprising in light of frequent government warnings of cybersecurity threats and news of powerful government-developed viruses. We see little benefit in measures that might improve voter turnout while casting doubt on the integrity of the results.[a]

Almost all the arguments on behalf of Internet voting ignore a critical risk Internet-based voting shares with all computerized voting—wholesale theft. In the days of hand-counted paper ballots, election theft was conducted at the retail level by operatives at polling places and local election offices. By contrast, introduction of computers into the voting process created the threat that elections can be stolen by inserting malware into code on large numbers of machines. The situation is even more dangerous with Internet voting, since both the central servers and the voters' computers are potentially under attack from everywhere.

a Portions of this article are taken from the book *Broken Ballots: Will Your Vote Count?* by Douglas W. Jones and Barbara Simons, CSLI Publications, Stanford, CA, 2012; http://brokenballots.com

» key insights

- **Internet voting is fundamentally insecure.**
- **Most people do not associate widely publicized computer viruses and worms with Internet voting.**
- **Internet voting is being pushed in many countries by vendors, election officials, and well-meaning people who do not understand the risks.**

ILLUSTRATION BY ALICIA KUBISTA/ANDRIJ BORYS ASSOCIATES

Despite the serious threats it poses to election integrity, Internet voting is being used in several countries and U.S. states, and there is increasing public pressure to adopt it elsewhere. We examine some of these threats, in the hope of encouraging the technical community to oppose Internet voting unless and until the threats are eliminated.

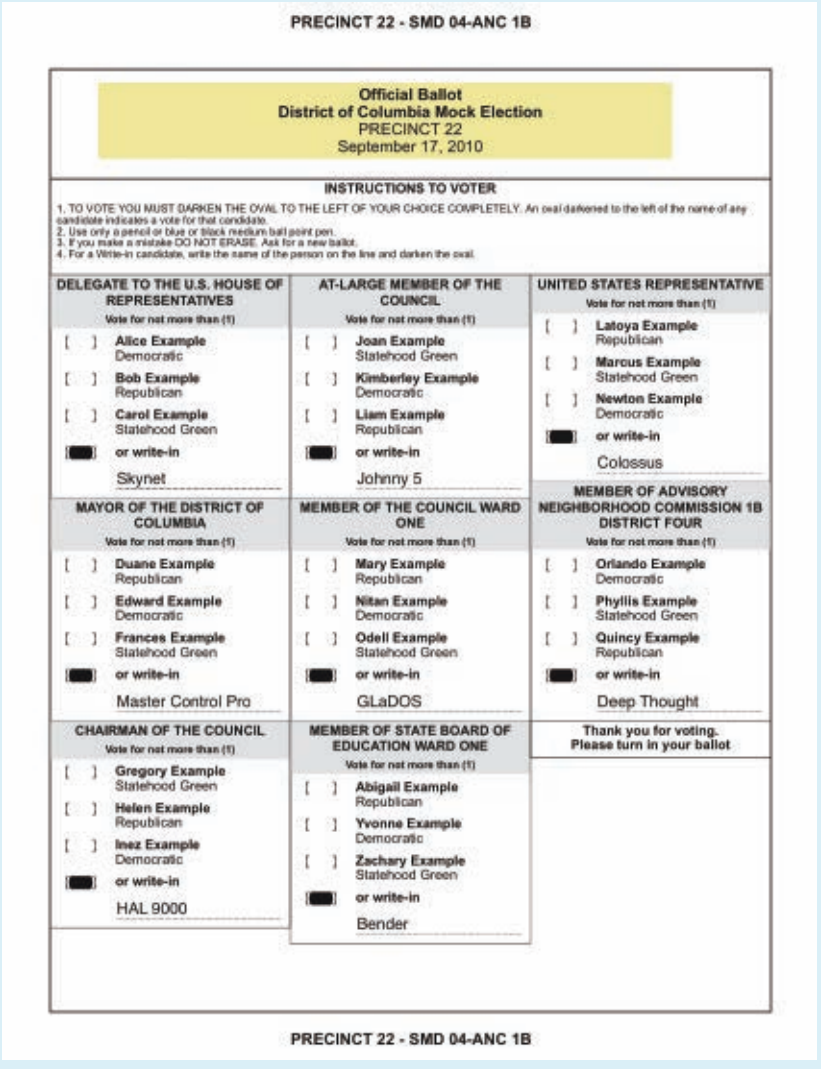
D.C. pilot test Internet voting has generally been deployed without being subjected to public testing prior to use. To the best of our knowledge, the only exception was a "digital vote by mail" pilot project in Washington, D.C. in 2010. In June of that year, the Open Source Digital Voting Foundation announced that it had been selected by the District of Columbia Board of Elections and Ethics (BOEE) to support a project to allow Internet voting for military and overseas voters, starting with the upcoming September primary. The BOEE had optimistically planned a "public review period" in advance of the primary in which everyone was invited to try to attack the system in a mock election. While the system was not ready for the primary, a public test was eventually scheduled to run from September 28 to October 6, with midterm election voting scheduled to begin October 11 or 12.

The break-in. By October 1 people testing the system reported hearing the University of Michigan fight song following a 15-second pause after they submitted their ballots.[6,44] A Michigan team had taken over the system within 36 hours of the start of the tests by exploiting a shell-injection vulnerability, thereby gaining almost total control over the BOEE server. The attackers remained in control for two business days, until the BOEE halted the test after noon on October 1. An attacker intent on subverting a real election would not leave such an obvious calling card. The delay between the break-in and the shutdown of the system reveals how difficult it is to determine that a break-in has occurred, even when the "culprits" announce themselves with music.

On October 5, Michigan professor Alex Halderman revealed that, in addition to installing the fight song, his team had changed ballots cast prior to their intrusion, had rigged the system to alter subsequently cast ballots, and could violate voters' secret ballot rights. That day the BOEE restarted the test with the song removed. Testers were told to print out and mail in their ballots, instead of returning them over the Internet. Figure 1 is the hacked ballot, with write-in candidates selected by the Michigan team.

Halderman was the star of an October 8 oversight hearing, where he dropped additional bombshells. From the start, his team had control of the network infrastructure for the pilot project. The team used the default master password from the owner's manuals, which had not been changed, for the routers and switches, thereby gaining control of the infrastructure and obtaining an alternative way to steal votes in a real election. Control of the network also enabled the team to watch network operators configure and test the equipment. When they discovered that a pair of security cameras in the BOEE data center was connected to the pilot system and unprotected, the team used the cameras to watch the system operators. As proof, Halderman brought some security-camera photos to the hearing. Halderman even discovered a file used to test the system that consisted of copies of all 937 letters sent to real voters. The letters included voter names, IDs, and 16-character PINs for authentication in the real Internet election. While the team could already change voter selections, inclusion of unencrypted PINs in a file used for testing demonstrates that the BOEE did not understand the fundamental principles of computer security. The PINs would have allowed the team or any other intruder to cast ballots for actual voters. Finally, Halderman found evidence of attempted break-ins that appeared to be from China and Iran. Since the attempts involved trying to guess the network logins, the Michigan team changed the previously unchanged defaults (user: *admin*, password: *admin*). Whether or not they were intentionally directed at the D.C. voting system, the attempts showed how dangerous the Internet can be, with sophisticated adversaries from around the world constantly trying to break in to systems.

Figure 1. The rigged District of Columbia ballot.



PRECINCT 22 - SMD 04-ANC 1B

Official Ballot
District of Columbia Mock Election
PRECINCT 22
September 17, 2010

INSTRUCTIONS TO VOTER

1. TO VOTE YOU MUST DARKEN THE OVAL TO THE LEFT OF YOUR CHOICE COMPLETELY. An oval darkened to the left of the name of any candidate indicates a vote for that candidate.
2. Use only a pencil or blue or black medium ball point pen.
3. If you make a mistake DO NOT ERASE. Ask for a new ballot.
4. For a Write-in candidate, write the name of the person on the line and darken the oval.

DELEGATE TO THE U.S. HOUSE OF REPRESENTATIVES
Vote for not more than (1)
[ ] Alice Example, Democratic
[ ] Bob Example, Republican
[ ] Carol Example, Statehood Green
[■] or write-in: Skynet

AT-LARGE MEMBER OF THE COUNCIL
Vote for not more than (1)
[ ] Joan Example, Statehood Green
[ ] Kimberley Example, Democratic
[ ] Liam Example, Republican
[■] or write-in: Johnny 5

UNITED STATES REPRESENTATIVE
Vote for not more than (1)
[ ] Latoya Example, Republican
[ ] Marcus Example, Statehood Green
[ ] Newton Example, Democratic
[■] or write-in: Colossus

MAYOR OF THE DISTRICT OF COLUMBIA
Vote for not more than (1)
[ ] Duane Example, Republican
[ ] Edward Example, Democratic
[ ] Frances Example, Statehood Green
[■] or write-in: Master Control Pro

MEMBER OF THE COUNCIL WARD ONE
Vote for not more than (1)
[ ] Mary Example, Republican
[ ] Nitan Example, Democratic
[ ] Odell Example, Statehood Green
[■] or write-in: GLaDOS

MEMBER OF ADVISORY NEIGHBORHOOD COMMISSION 1B DISTRICT FOUR
Vote for not more than (1)
[ ] Orlando Example, Democratic
[ ] Phyllis Example, Statehood Green
[ ] Quincy Example, Republican
[■] or write-in: Deep Thought

CHAIRMAN OF THE COUNCIL
Vote for not more than (1)
[ ] Gregory Example, Statehood Green
[ ] Helen Example, Republican
[ ] Inez Example, Democratic
[■] or write-in: HAL 9000

MEMBER OF STATE BOARD OF EDUCATION WARD ONE
Vote for not more than (1)
[ ] Abigail Example, Republican
[ ] Yvonne Example, Democratic
[ ] Zachary Example, Statehood Green
[■] or write-in: Bender

Thank you for voting.
Please turn in your ballot

PRECINCT 22 - SMD 04-ANC 1B

Implications of the attack. The D.C. incursion illustrates how Internet voting can be attacked from anywhere. Most complex software systems have an abundance of vulnerabilities, with attackers needing to exploit just one. Moreover, all attacks except those specifically targeting the designated BOEE election network were out of bounds in the pilot test. Examples of non-allowed attacks included client-side malware; denial-of-service attacks; attacks against ISPs; and DNS, routing, and other network attacks. Attackers in a real election would not have felt bound by such constraints. Once the Michigan team had changed all the votes, it was impossible for D.C. officials to reconstruct the original ballots. In a close race, attackers might control the outcome without risk of detection. It took more than a day for D.C. officials to realize their system had been successfully attacked, despite the musical calling card. By the time officials discovered the attack, it was too late to recover from it.

The BOEE had intended to accept voted ballots over the Internet. If there had been no pilot test or if the Michigan team had not participated, members of the military and civilians living abroad who vote in Washington, D.C. would have been voting over a highly vulnerable system. The BOEE did the right thing (for a municipality determined to deploy Internet voting) by setting up a public test. It also learned an important lesson from the test and ultimately canceled the Internet-ballot-return portion. Voters were instead allowed to download blank ballots from the Web and print and return them by postal mail. Unfortunately, other states have not been as responsible. In the upcoming 2012 U.S. election, 33 states will allow some kind of Internet voting, including at least one Web-based Internet pilot project, and the return of voted ballots over the Internet through email attachment or fax, without first

encouraging independent experts to test their systems.[42]

One of us (Jones) has consulted with several election offices, including the BOEE. He observed it to be above average, in terms of both physical and human resources, suggesting that the mistakes found by the Michigan team were not the result of isolated incompetence, but are typical of the best we can expect under current conditions. Likewise, Halderman has said that the quality of the D.C. source code seemed much better than the closed-source electronic voting systems he has examined. Security is difficult, and even organizations with security expertise have been successfully attacked. Given that elections offices are under-resourced, have many other problems to worry about, lack security expertise, and are highly decentralized, it is completely unrealistic to expect extraordinary security competence from them.

The Case for Internet Voting

Despite warnings from independent studies and commissions, as well as sensational news stories about hacking and viruses, some widely held misconceptions about Internet voting persist: It saves money and increases voter turnout; Web-based voting is more secure than postal voting or voting by email or fax; because banking and purchasing can be done over the Internet, voting can be done safely over the Internet; and Internet voting is inevitable—the wave of the future. We discuss the first three points in the following sections and the fourth in the sidebar "Internet Voting and E-Commerce Compared." Regarding the inevitability of Internet voting, some of the most outspoken Internet voting opponents are highly respected computer security experts. Our goal is to convince you that secure Internet voting is unachievable for the foreseeable future and therefore, we sincerely hope, not inevitable.

Saves money. The cost of Internet voting, especially up-front charges, can be steep. For example, 2009 cost estimates from Internet voting vendor Everyone Counts were so large that a legislative proposal in Washington state to allow Internet voting for military and civilian voters was killed in committee. The estimated costs, obtained by John Gideon of VotersUnite, included proposed up-front costs ranging from $2.5 million to $4.44 million. After that, each county would have been hit with an annual license fee of $20,000–$120,000, plus $2–$7 per overseas voter.[5]

In the March 2011 election in the state of New South Wales, Australia, 46,864 people voted on an Internet voting system called iVotes, also an Everyone Counts product.[33] The development and implementation costs for using iVotes in the election exceeded $3.5 million (Australian dollars), resulting in a cost of about $74 per vote cast. By contrast, the average cost for all forms of voting in the same election was $8 per vote, though the cost per Internet vote would have decreased if amortized over more voters.

Increases turnout. Internet voting does not necessarily increase turnout. Everyone Counts ran an Internet-based election in Swindon, U.K., in 2007 and a local election in Honolulu, HI, in 2009 where votes were cast only by Internet or telephone. The Electoral Commission, established by the U.K. Parliament, determined that Internet voting in Swindon had a negligible effect on turnout; meanwhile, in Honolulu there was an 83% drop in turnout compared to a similar election in 2007.[22,40] We know of no rigorous study of the impact of Internet voting on turnout; conducting such a study would be difficult, since turnout can vary enormously from election to election. But even if Internet voting could increase turnout, the increase would be irrelevant if the election results were at risk of corruption by insecure Internet use.

Web-based voting is more secure. Verifiability and transparency are critical aspects of any election, especially if it involves a secret ballot. It is fundamentally impossible for anyone, even election officials, to directly oversee or observe the tabulation of an Internet-based election, including one that is Web-based. A software bug or an attack could cause an election outcome to be wrong because either the tabulation is incorrect or the voters' selections were modified. To address such risks, we need to determine after an election that the technology operated correctly and the declared winner actually won.

We can verify the results of a paper-based election by auditing a sample of the cast ballots or, in the extreme, by recounting all of them. Such an audit or recount must involve a secure, observable chain of custody of the ballots, something impossible with current Internet voting technology. Allowing voters to print copies of their ballots for personal use is meaningless, because these copies may not match the electronic versions used in computing the results.

Military Voting

Members of uniformed services and their families and non-military citizens living overseas are called UOCAVA voters, after the U.S. Uniformed and Overseas Citizens Absentee Voting Act of 1986 (http://www.fvap.gov/reference/laws/uocava.html). They have long complained that absentee ballots are never delivered or their returned voted ballots arrive too late to be counted, concerns used to justify the push for Internet voting at both the state and federal levels. A widely discussed solution is to have the military run its own centralized Internet voting system over its high-security infrastructure. This is a bad idea for at least two reasons: First, it runs counter to the principle of civilian control over the military and creates the potential that the military might control the vote. Second, it is unrealistic and unwise to even consider connecting unsecure Web servers run by local election officials to a military network that is supposed to maintain a high level of security. Some supporters of Internet voting for the military have noted that postal mail ballots are also not secure. While it is true that all forms of remote voting pose security problems, Internet voting can be attacked by anyone from anywhere, something that is not the case for postal ballots. In addition, the Internet can be used for wholesale attacks on large numbers of voters, whereas attacks on postal ballots are inherently confined to a retail scale.

Two projects for UOCAVA voters are noteworthy: SERVE, killed in 2004, and Operation BRAVO, implemented in the 2008 U.S. presidential election:

SERVE. The Secure Electronic Registration and Voting Experiment, or SERVE (www.fvap.gov/resources/media/serve.pdf), was the most ambitious project to date intended for use

by UOCAVA voters. The goal of the $22 million project was to allow registration and voting over the Internet in the 2004 primaries and general election. Participation by states and counties within those states was voluntary. Voters could use any Windows computer, either their own or a public computer, like those found in libraries and cybercafés. Voters were responsible for the security of whatever computers they used. The vendor was Accenture.

In 2003, a group of experts called the Security Peer Review Group was assembled by the Federal Voting Assistance Program (FVAP) to evaluate SERVE; FVAP was charged with facilitating voting for all UOCAVA voters. Following two three-day meetings with FVAP and the lead technical staff of SERVE, the four computer scientists who attended both meetings, including one of us (Simons), released a report, the conclusion of which said: "Because the danger of successful, large-scale attacks is so great, we reluctantly recommend shutting down the development of SERVE immediately and not attempting anything like it in the future until both the Internet and the world's home computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear."[18]

When the report was issued in early 2004, 50 counties in seven states—Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah, and Washington—were planning to participate in SERVE. FVAP had estimated the maximum overall vote total would be approximately 100,000, including primaries and the general election. On January 30, 2004 Deputy Secretary of Defense Paul Wolfowitz said the Pentagon "...will not be using the SERVE Internet voting project in view of the inability to assure legitimacy of votes that would be cast using the system, which thereby brings into doubt the integrity of election results."[43] SERVE was subsequently terminated.

Operation BRAVO. In 2008, Operation BRAVO, or Bring Remote Access to Voters Overseas, provided Internet voting from secure kiosks for residents of Okaloosa County, FL. Unlike previous pilot projects, these kiosks were equipped with printers to create paper voter-choice records of voters' ballots. Voters could verify the records before leaving the kiosk, after which the records were flown back to Okaloosa County for manual reconciliation with the ballots sent over an Internet-based virtual private network. Small discrepancies in the ballot count were uncovered by law professor Martha Mahoney of the University of Miami, but, as of August 2012, BRAVO had yet to release a formal report explaining the discrepancies.[26] The vendor was Scytl.

The Okaloosa County experiment concerned only a single county. Expanding kiosk-based Internet voting for all service members would be very difficult, since the system would have to deal with tens of thousands of different ballot styles and conflicting state rules governing ballot presentation, requirements that would also add significantly to the cost.

The MOVE Act. Instead of Internet voting, why not allow remote voters to download a blank ballot from the Internet, print it, and return the voted ballots by mail? If the blank ballots are available early enough, most voted ballots should arrive in time to be counted. Such a system might not have the pizzazz of Internet voting but would have fewer security issues and almost certainly involve less cost. That is one of the reforms dictated by the 2009 Military and Overseas Voter Empowerment, or MOVE, Act. Written to address the problems of UOCAVA voters, MOVE requires states to make blank ballots available electronically at least 45 days prior to any federal election; UOCAVA voters may also request and receive voter-registration and absentee-ballot applications electronically.

The Military Postal Service Agency analyzed the handling of absentee ballots during the 2010 general election,[29] finding problems with getting postal ballots to members of the military, though paper ballots were generally returned quickly. Many had been electronically downloaded, filled out by service members, and returned by postal mail. The average postal delay for returned ballots was 5.2 days, well ahead of the seven-day limit set by the MOVE Act; 92% of absentee ballots were delivered within seven days of acceptance at overseas Military Post Offices (MPOs). Only 118 out of 23,900 voted ballots, most likely from Afghanistan or Iraq, took 20 or more days to be returned from an MPO. The time to get a voted ballot from a service member to an MPO ranged from two to 20 days. Therefore, if election officials provide downloadable blank ballots at least 45 days before an election, essentially all members of the military should be able to return their voted paper ballots in time to be counted.

Risks

Not satisfied with the significant speed-up provided by MOVE, Internet-voting advocates continue to call for the return of voted ballots through the Internet, either as email attachments or as some kind of Web form. Doing either securely would require solving some of the most intractable problems in cybersecurity:

The server. In the 2010 D.C. pilot project, University of Michigan graduate students attacked the election server over the Internet. Independent hackers, political operatives, foreign governments, and terrorists could also mount such attacks. Local election officials with little or no expertise in computer security have little hope of defending themselves.

Corporate and government vulnerability. Many corporations and government agencies store sensitive or classified information on their computers, sharing with election officials the goal of defending against attackers who might steal or alter such information. Despite large staffs of security professionals with significant resources, computers in major corporations and government agencies have been attacked successfully. For example, a 2008 survey of approximately 1,000 large organizations worldwide found the average loss per organization from intellectual property cybertheft was about $4.6 million.[19] A December 2009 report from the Computer Security Institute (http://gocsi.com) surveying 443 U.S. companies and government agencies found 64% had reported malware infections during the preceding year.[36]

A major China-based Internet attack on Google and many other companies in late 2009 showed that even major corporate sites are vulnerable. The attack targeted Gmail accounts of Chinese human-rights activists and Google's own intellectual property, including

software-development systems.[31] As many as 34 companies were targeted, including Adobe, Juniper Networks, defense contractor Northrop-Grumman, major security supplier Symantec, and Yahoo!.[41] The attacked companies have vastly more security expertise and resources than local election officials or today's relatively small Internet voting vendors. The attacks used email that appeared to come from trusted sources, so victims would be tricked into clicking on a link or opening an attachment. Then, using a vulnerability in Microsoft's Internet Explorer browser, the attacker would download and install malware that took complete control of the compromised systems.

George Kurtz, executive vice president and worldwide chief technology officer of McAfee, an Internet security company, expressed dismay at the implications: "All I can say is wow. The world has changed. Everyone's threat model now needs to be adapted to the new reality of these advanced persistent threats. In addition to worrying about Eastern European cybercriminals trying to siphon off credit card databases, you have to focus on protecting all of your core intellectual property, private nonfinancial customer information and anything else of intangible value."[23]

Government sites have also been vulnerable. In a March 2010 address to the RSA Security Conference, FBI director Robert S. Mueller said the FBI's computer network had been penetrated and the attackers had "corrupted data."[31] Later that year, General Michael Hayden, former director of both the CIA and the NSA, said: "The modern-day bank robber isn't speeding up to a suburban bank with weapons drawn and notes passed to the teller. He's on the Web taking things of value from you and me."[13]

Finally, malware that appears to be government-generated has been used to obtain critical intelligence, as in the case of the Flame virus, and, for targeted attacks, Stuxnet. Both were widely reported to have been developed by the governments of Israel and the U.S., with Stuxnet apparently created to attack Iran's nuclear facilities.[32,38] Similar tools could allow a foreign power to attack or subvert an Internet election anywhere.

Internet Voting and E-Commerce Compared

Internet voting involves complications not found in e-commerce:

Secret ballots. **Secret ballots are required by law to protect against vote buying and coercion. Ballot secrecy prohibits anyone from linking voted ballots to the voters casting them. This precludes the kind of transaction logging routinely used in e-commerce to allow reconstruction of who did what and when, should a question arise.**

Receipts. **Receipts, including unique transaction numbers and complete transaction descriptions, are routinely issued in e-commerce. These receipts confirm that the correct orders were placed and may be used as proof of purchase in the event of disputes. Ballot secrecy prevents issuing any documents to voters that voters could use to prove how they voted. Documents that do not provide such proof are of limited use in an audit or recount.**

Malfunction and fraud. **In the event of an e-commerce failure due to malfunction or fraud, there is a good chance the situation will be rectified or that the purchaser can stop a credit-card payment after noticing the discrepancy. However, if a ballot is not successfully cast on election day, the voter probably will not know and almost certainly will not be able to revote.**

Vote buying and selling. **Unlike commercial activities, vote buying and selling is illegal. In the 2000 U.S. presidential election between Republican George W. Bush and Democrat Al Gore, an online system designed to broker Green Party candidate Ralph Nader and Gore votes was created but forced to shut down by the California attorney general. There is no evidence that any votes were actually traded. With Internet voting, voters could sell their voting credentials, perhaps even online, using a Web site designed to automatically cast their ballots.[a]**

No proposed Internet voting system is able to overcome these hurdles.

a When family members vote on a home computer or citizens vote from a computer in a public library, multiple voters will share the same IP address; while it is possible to detect multiple votes from one IP address, it would be problematic to prohibit them.

Insider attacks. While many security discussions focus on outsider attacks, insider attacks might be even more dangerous. A risk of any computerized voting, including Internet voting, is that one or more insiders (programmers, election officials, volunteers, or vendors to whom the election is outsourced) could rig an election by manipulating election software. Since computerized voting is an opportunity for wholesale rigging through software used by large numbers of voters, the size of the conspiracy needed to win an election is greatly reduced, as is the risk of being caught.

An attacker could add a back door to the system, with or without the vendor's knowledge. In general, no amount of testing can be relied on to reveal the presence of a back door. A thorough code review (not required by current law) can sometimes do this, but code reviews cannot reliably distinguish between an innocent mistake and intentional malware. A trusted insider (such as former CIA agent Aldrich Ames[b]) can do tremendous damage, even if eventually caught.

The client. Since malware can infect public or privately owned machines linked to the Internet without the owner's knowledge or permission, client-side malware designed to steal an election poses significant risks for ballots cast from voters' computers. These risks include credential theft, copying of the ballot to a third party, and modification of the ballot before encryption, as well as outright prevention of voting. Machines can be infected in many ways, including downloading documents with malicious macros, browser plugins, or improper security settings.

Furthermore, millions of computers are already connected to botnets. In 2010, the FBI reported the Mariposa botnet may have infected eight million to 12 million computers worldwide.[9] The virus used to create the botnet could steal credit-card data and online-

b Ames gave the Soviet Union significant U.S. secrets resulting in the death of a number of "CIA assets."

banking passwords, as well as launch a denial-of-service attack; the creator of the virus also sold customized versions with augmented features. A Microsoft report estimated that in the first half of 2010 more that 2.2 million U.S. Windows PCs were in botnets.[4]

Those wishing to rig elections need not build new botnets. Many botnets used for financial fraud are available for rent. It would not take a large staff to alter existing malware to attack elections, and it would not be out of character for existing malware developers to offer ready-to-customize election-rigging malware as soon as Internet voting were to enter widespread use.

The sheer number of potential attacks and the difficulty of preventing any of them increase the vulnerability of Internet-based elections. In light of the many successful attacks against governments, major banks, and the world's technology leaders, it should be relatively easy to entrap large numbers of voters who are not technologists. Once a voter's computer is infected, all bets are off. Malware can make the computer display a ballot image that represents the voter's intent correctly, even as it sends something entirely different over the Internet. That is, it is the virus that votes, not the voter. The voter never knows, because it is impossible for the voter to see what is actually sent.

Since antivirus software works by checking for known viruses and worms, whenever a new virus appears, the antivirus software must be updated. There can be many days or even weeks between the time the virus is initially distributed and when it is recognized and analyzed. After that, the virus fix must be distributed, and victims must disinfect their machines. Because antivirus software has limited capability for recognizing unknown malware, a new virus or worm may well escape detection for a while. Even if detected, removal can be difficult, as most PC owners who have had to deal with adware and spyware are aware. A 2007 study found that antivirus software has become less effective over time, with recognition of malware by most commercial antivirus software falling from 40%–50% at the beginning of 2007 to 20%–30% by the end of that year.[12] Another set of experiments conducted at the University of Michigan showed the number of malware samples detected decreased significantly as the malware became more current; when the malware was only one week old, the detection rate was very low.[34] Given the limitations of antivirus software, an effective attack would be to distribute election-stealing malware far in advance of the election. If the malware were to spread silently, it could infect a large number of machines before being detected, if it is detected at all. Moreover, it might be impossible to determine which votes are modified or even which computers are infected.

The Conficker worm illustrates the risk malware poses to Internet elections. Having rapidly infected from nine million to 15 million machines in 2009, Conficker could "call home" for more instructions, so the unknown creator of Conficker could instruct infected machines to install additional malware remotely without the computer owner's knowledge.[2] The new instructions might target specific candidates and elections shortly before a vote.

While many viruses and worms are planted without the computer owner's knowledge, users can be duped into downloading highly questionable software. In August 2009 a spam message circulated, saying "If You dont [sic] like Obama come here, you can help to ddos [Distributed Denial of Service] his site with your installs." CNET News reported that people who clicked on the email link were offered money in exchange for downloading the software; they were even told to return to the Web site for updates if their virus-detection software deleted their first download.[30] While the source of the software is not known, the goal could have been to disrupt sites associated with President Barack Obama, to engage in identity theft, or even to infect machines of Obama opponents, something that could be especially useful if Internet voting were to become an option in the U.S.

Threat example: The Zeus virus. The Zeus virus illustrates how a virus can manipulate what a voter sees and change the voter's selection. While Zeus has been used mainly to steal money, it would not be difficult to reprogram it to steal votes.

In April 2009, malicious software was discovered in Paul McCartney's Web site that redirected visitors to an IP address in Amsterdam in order to exploit vulnerabilities on the victims' machines to install the Zeus virus.[16] The infection, planted shortly before McCartney's New York reunion concert with Ringo Starr, was timed to catch as many victims as possible before discovery.

The German edition of Wikipedia was another source of infection.[14] A bogus Wikipedia article about another dangerous piece of malware contained a link to software that would supposedly fix the problem. However, anyone who downloaded the "fix" was actually downloading a copy of Zeus. In 2009 it was estimated by security firm Damballa that Zeus had infected about 3.6 million PCs in the U.S. alone.[28]

Zeus was built to steal money from online financial accounts. When victims would visit their banks' Web sites, Zeus would copy their credentials and send them to a remote location where they would be used to steal from their accounts. Zeus could even forge financial statements so victims would see no evidence of the theft when checking their online statements.[39] Victims typically learned of the theft only when financial transactions failed to clear due to insufficient funds, at which point it was too late to retrieve the money.

The Zeus virus also spoofed verification systems used by Visa and MasterCard when enrolling new users[7] (see Figure 2), thereby obtaining sensitive information (such as Social Security numbers, card numbers, and PINs) from unknowing victims who would think they were providing the information to the real bank. This information, sent to the attacker's computers, would be used to defraud the victims.

Yet another attack was reported in August 2010 by Internet security firm M86 Security; the report said that about 3,000 bank customers in the U.K. were victimized by a form of the Zeus virus. The announcement accompanying the report's release, which did not provide the bank's name, said the following about the attack:[25] "Unprotected customers were infected by a Trojan—which managed to avoid detection by traditional anti-virus software—while browsing the Internet. The Trojan, a Zeus v3, steals the customer's online banking ID and hijacks

their online banking sessions. It then checks the account balance and, if the account balance is bigger than GBP 800 value, it issues a money transfer transaction... From July 5, the cyber criminals have successfully stolen GBP 675,000 (c. USD 1,077,000) and the attack is still progressing."

On September 29, 2010, the U.K. Police Central e-crime Unit announced the arrest of 19 individuals accused of using Zeus to steal $6 million from thousands of victims over a three-month period.[24] To this day, new Zeus attacks continue to be discovered; for example, in October 2010, *Computerworld* reported that Zeus was attacking Charles Schwab investment accounts,[20] with victims' machines infected by links to malicious sites hidden in bogus LinkedIn reminders. There is even a criminal service that will compile a Zeus binary for a fee.[10]

Impersonating the election server. Another Internet risk involves Website spoofing. Because counterfeit sites can be made to look like legitimate sites, spoofing can fool victims into revealing sensitive personal information. With Internet voting, spoofing can be used to trick voters into thinking they have actually voted when in fact they have not, while also collecting authentication codes and voters' intended ballots, a violation of the right to a secret ballot.

Phishing involves email messages that appear to be from a legitimate organization, such as a credit-card company. The phony message contains an authentic-looking link that appears to go to a legitimate site but actually goes to a spoofed site. When such email messages and Web sites are well designed, victims end up providing sensitive information, such as credit-card numbers. Phishing is usually used to steal personal information, but can also be used to trick voters into voting on a spoofed Web site. Phishing is a powerful tool for amplifying the power of spoofing, though its effectiveness can be reduced if voters are instructed to always type in the full URL of the voting Web site, instead of just clicking on links.

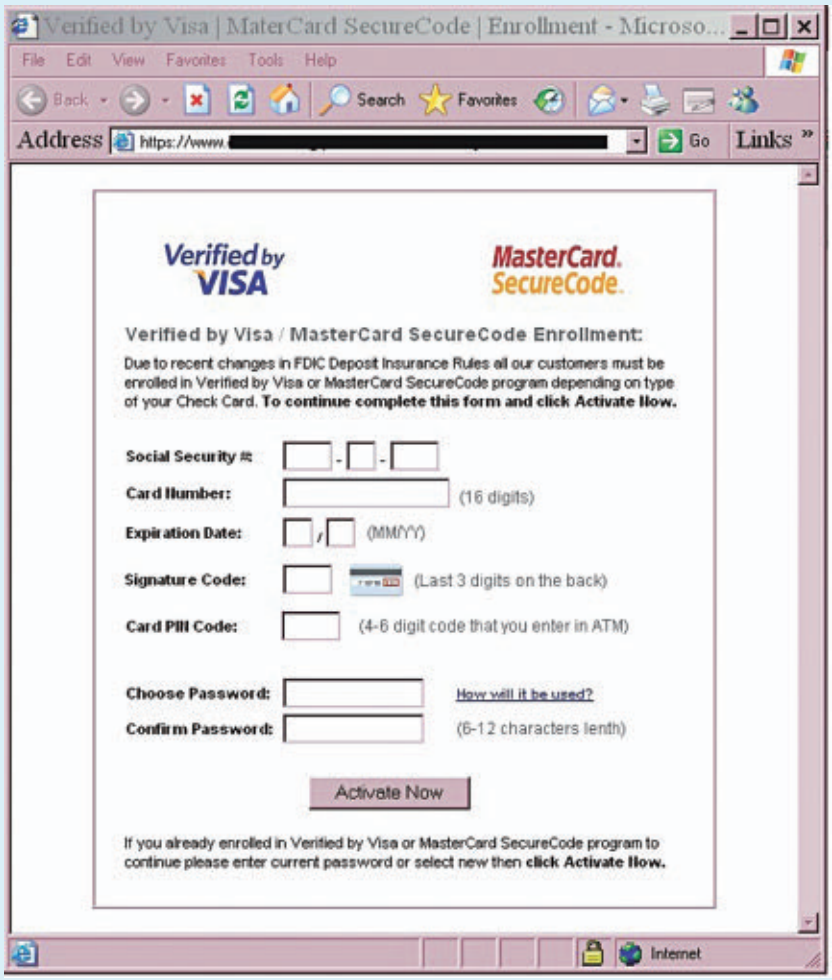
A counterfeit voting site can conduct a man-in-the-middle attack. In its simplest form, the counterfeit site relies entirely on the real site for content, monitoring and occasionally editing the information flow between the voter and the real election server. This allows the attacker to intercept information, such as passwords and votes, and potentially to alter votes. A more complex counterfeit could simulate a voting session, then use the credentials collected from the voter at a later time to cast a forged ballot. Monitoring the IP addresses from which ballots are cast is not a defense, since multiple voters might share the same IP address for legitimate reasons.

A common way to avoid counterfeit Web sites is to rely on a certificate authority (CA) to authenticate sites. If the browser does not recognize the issuer of a certificate, it will ask if the user still wants to access the site. A user who does not understand the significance of the browser's question may naïvely ignore it and access a counterfeit site.

Even when voters are careful to visit only sites they believe are legitimate, they could still be victimized. First, it is possible to trick many browsers into going to the attacker's, rather than to the legitimate, site.[45] Second, some CAs do not validate the identities of sites they vouch for.[35] Third, an attack on the CA can create fake SSL certificates, as happened to DigiNotar, a Dutch CA.[21] Finally, an attack on the routing infrastructure of the Internet could divert voters to a counterfeit voting site without their noticing the diversion.[27]

Denial-of-service attacks. There are many documented instances of Distributed Denial-of-Service (DDoS) attacks. For example, the massive 2007 DDoS attack on Estonia and the attacks on the Republic of Georgia during the 2008 Russo-Georgian war all originated in Russia. Other victims of DDoS attacks include Amazon, eBay, Facebook, Google, Twitter, and Yahoo!. Politically

Figure 2. Bogus enrollment screen displayed by Zeus; screenshot by Amit Klein of Trusteer.



motivated DDoS attacks, like the one on Wikileaks in 2010 and a reprisal by Anonymous against MasterCard, have become relatively common.

A DDoS attack could prevent certain groups from voting or even disrupt an entire election, as probably occurred in a 2003 leadership vote by the New Democratic Party (NDP) in Canada. Internet voting for the NDP election lasted from January 2 until the party convention January 25, 2003. Coincidentally, on January 25, the same day the Slammer worm was attacking large numbers of (unpatched) Windows 2000 servers on the Internet, the NDP voting site was reportedly down or effectively unusable for hours.[3]

Due to the secrecy surrounding the technical aspects of the NDP election, we do not know if the NDP voting site was brought down by a DDoS attack or by the Slammer worm. The vendor, election.com, claimed to have patched the servers against Slammer and maintained that it experienced a denial-of-service attack. Unfortunately, election.com provided neither logs nor other proof that its servers were patched, nor did it permit expert examination of its records. There was no transparency and hence no way for an independent outsider to determine what had happened.

Not having learned from the 2003 attack, the NDP suffered a massive DDoS attack during its March 2012 leadership election. The NDP was so ill prepared that people attending the party conference were unable to vote during the attack, as no back-up paper had been provided. Once again, there was no independent examination or report.

Loss of the secret ballot. All forms of remote voting diminish ballot secrecy and increase the risk of coercion and vote selling simply because they eliminate voting booths. Internet voting decreases secrecy still further. States that allow the return of voted ballots by fax or email attachments have been asking voters to sign statements relinquishing the right to a secret ballot. Mix nets and other cryptographic schemes can mimic the secrecy protections of the double envelopes traditionally used to partially preserve ballot secrecy in postal voting, but they do not protect against client-side attacks.

The threat to eliminate the secret ballot for a class of voters is disturbing for several reasons: First, it renders these voters second-class citizens, deprived of a right other citizens take for granted. Second, there is no need to eliminate the secret ballot for overseas voters, as we discussed earlier. Third, and most important, ballot-secrecy protection is more than an individual right; it is a systemic requirement, essential for fair, honest elections. Without ballot secrecy, voters, especially those in hierarchical organizations, such as the military, may be subject to coercion. An election where some voters can be pressured to vote a particular way is not a free and fair election.

Bribery. Finally, we cannot rule out the threat of old-fashioned bribery. National races in the U.S. cost vast sums—a small fraction of which would be an exceedingly large bribe and more than enough to cover the cost of attacks, such as the one on the 2010 pilot D.C. voting system, as well as others on voters' computers. Halderman said his team's attack would have cost less than $50,000 at generous consulting rates.

Other Countries

We have focused on Internet voting in the U.S., but Internet voting has been used in several other countries, including Estonia and Switzerland, neither of which protects against malware on voters' computers, and Norway in 2011.[c] The Netherlands provided an Internet voting option in its 2006 parliamentary elections, but Internet voting was subsequently banned, largely because of work by a group called "We Don't Trust Voting Computers." The U.K. tried Internet voting on a pilot basis in 2007, but the U.K. Electoral Commission recommended against further e-voting pilot projects until a range of issues had been addressed.[40]

Far Future

Systems like Helios[15] and Remotegrity[37] use encryption to allow voters to verify that their ballots were accurately received and counted. Unfortunately, cryptography does not protect Internet-based elections against DDoS attacks, spoofing, coercion, design flaws, and many kinds of ordinary software bugs.[8] Recounts on these cryptographic voting systems cannot recover from such threats. While these systems have been used for some small Internet elections, the consensus in the cryptographic community is that they are not ready for use in a major election. Ben Adida, creator of Helios, wrote in 2011: "The one problem I don't know how to address with Helios is client-side security...We now have documented evidence...that viruses like Stuxnet that corrupt nuclear power plants by spreading from one Windows machine to the other have been built...So if you run a very large-scale election for a president of a G8 country, why wouldn't we see a similar scenario? Certainly, it's worth just as much money; it's worth just as much strategically... All the ability doesn't change the fact that a client-side corruption in my browser can flip my vote even before it's encrypted, and if we... must have a lot of voters verify their process, I think we're going to lose, because most voters don't quite do that yet."[1] Note that while Helios can detect DDoS attacks, network attacks, and several other types of attacks mentioned here, it cannot prevent, diagnose, or fix them.

Perhaps eventually a paperless cryptographic Internet voting system will be developed that is sufficiently secure, accurate, usable, and transparent to be used in major elections. Until then, the conclusion of the National Commission on Federal Election Reform, co-chaired by Presidents Gerald R. Ford and Jimmy Carter in 2001, still stands, that Internet voting "is an idea whose time most certainly has not yet come."[11]

Conclusion

Proposals for conducting voting pilot projects using real elections continue to reappear in the U.S. and elsewhere, apparently independent of warnings from computer-security experts. While the appeal of Internet voting is obvious, the risks are not, at least to many decision makers. Computer profes-

c Norway uses encryption, but malware on a voter's computer is still able to change votes, so long as the change is consistent with the partial proof sent to the voter or the voter does not check the partial proof.

sionals have an obligation to explain these risks.

Pilot projects are routinely declared successes, regardless of any problems encountered. However, it is dangerous to draw conclusions from a "successful" Internet voting pilot project. There is little reason to attack a small pilot project, and a malicious player might refrain from attacking a major election until the new technology is entrenched. Having claimed success, independent of proof of the accuracy of the pilot project, Internet-voting vendors and enthusiasts routinely push to extend Internet voting to a broader group of voters, thereby seriously undermining election security. Computer professionals must object to pilot projects that do not plan for an assessment of the integrity of the election and a public reporting of any discrepancies encountered.

Unlike legitimate computer-security experts, malicious attackers are not likely to publicize their attacks, just as credit-card thieves do not openly advertise their thefts. When election officials and policymakers ask for proof that a voting system has been attacked, it is important to keep in mind that detecting well-devised attacks is inherently difficult. The burden of proof that a voting system has not been attacked should fall on those making the claim, not the other way around.

Ultimately, the balance between the integrity of election technology on the one hand and convenience on the other is both a public-policy and a technological issue. Decision makers must be warned of all the risks in order to craft wise policy.

Acknowledgment

We are grateful to the referees who provided us with excellent recommendations.

References

1. Adida, B. Panelist remarks at panel on Internet voting. *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections* (San Francisco, Aug. 9, 2011); http://www.usenix.org/events/evtwote11/stream/benaloh_panel/index.html
2. Bowden, M. The enemy within. *The Atlantic* (June 2010); http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098/
3. CBC News. Computer vandal delays leadership vote (Jan. 25, 2003); http://www.cbc.ca/news/story/2003/01/25/ndp_delay030125.html
4. Claburn, T. Microsoft Finds U.S. Leads In Botnets. *InformationWeek* (Oct. 14, 2010); http://www.informationweek.com/security/vulnerabilities/microsoft-finds-us-leads-in-botnets/227800051
5. DeGregorio, P. *UOCAVA Voting Scoping Strategy.* Washington Secretary of State Public Record, Jan. 18, 2009; http://www.votersunite.org/info/WA-PRR-ScopingStrategy.pdf
6. District of Columbia and Halderman, J.A. Thank you to voters (hacked ballot acknowledgment with Michigan fight song); https://jhalderm.com/pub/dc/thanks/
7. Dunn, J.E. Trojan attacks credit cards of 15 U.S. banks. *Techworld* (July 14, 2010).
8. Estehghari, S. and Desmedt, Y. Exploiting the client vulnerabilities in Internet e-voting systems: Hacking Helios 2.0 as an example. *2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections* (Washington D.C., Aug. 9, 2010); http://static.usenix.org/events/evtwote10/tech/full_papers/Estehghari.pdf
9. FBI. *FBI, Slovenian and Spanish Police Arrest Mariposo Botnet Creator, Operators.* Press Release, July 28, 2010; http://www.fbi.gov/news/pressrel/press-releases/fbi-slovenian-and-spanish-police-arrest-maripora-botnet-creator-operators/
10. Fisher, D. New Service helps attackers get Zeus botnet off the ground. *Threatpost* (Jan. 10, 2011); http://threatpost.com/en_us/blogs/new-service-helps-attackers-get-zeus-botnet-ground-011011
11. Ford, G.R. and Carter, J. *To Assure Pride and Confidence in the Electoral Process.* National Commission on Federal Election Reform, Aug. 2001; http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/election2000/electionreformrpt0801.pdf
12. The H Security. *Antivirus Protection Worse than a Year Ago.* Heise Media, U.K., Dec. 20, 2007; http://www.h-online.com/security/news/item/Antivirus-protection-worse-than-a-year-ago-735697.html
13. Hayden, M. Hackers force Internet users to learn self defense. *PBS NewsHour* (Aug. 11, 2010); http://www.pbs.org/newshour/bb/science/Jul.-dec10/cyber_08-11.html
14. Head, W. Hackers use Wikipedia to spread malware. *IT News for Australian Business* (Nov. 6, 2006); http://www.itnews.com.au/News/67796,hackers-use-wikipedia-to-spread-malware.aspx
15. Helios. http://heliosvoting.org/
16. InfoSecurity. McCartney site serves up Zeus malware. *InfoSecurity* (Apr. 8, 2009); http://www.infosecurity-us.com/view/1178/mccartney-site-serves-up-zeus-malware/
17. Jefferson D. Email voting: A national security threat in government elections. VerifiedVoting blog (June 2011); http:/blog.verifiedvoting.org/2011/06/20/1375
18. Jefferson, D., Rubin, A.B., Simons, B., and Wagner, D. A *Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*, Jan. 20, 2004; http://servesecurityreport.org/
19. Kanan, K., Rees, J., and Spafford, E. *Unsecured Economies: Protecting Vital Information.* Technical Report. McAfee, Inc., Santa Clara, CA, Feb. 2009; resources.mcafee.com/content/NAUnsecuredEconomiesReport
20. Keizer, G. Zeus botnet gang targets Charles Schwab accounts. *Computerworld* (Oct. 16, 2010); http://www.computerworld.com/s/article/9191479/Zeus_botnet_gang_targets_Charles_Schwab_accounts
21. Kirk, J. Comodo hacker claims credit for DigiNotar attack. *Computerworld* (Sept. 2011); http://www.computerworld.com/s/article/9219739/Comodo_hacker_claims_credit_for_DigiNotar_attack
22. KITV. Voting drops 83 percent in all-digital election. Honolulu, May 2009; http://www.kitv.com/politics/19573770/detail.html
23. Kurtz, G. Operation 'Aurora' hit Google, others. McAfee Security Insights blog, Jan. 10, 2010; http://blogs.mcafee.com/corporate/cto/operation-aurora-hit-google-others
24. Leyden, J. UK cybercops cuff 19 Zeus banking trojan suspects. *The Register* (Sept. 29, 2010); www.theregister.co.uk/2010/09/29/zeus_cybercrime_arrests/
25. M86 Security. *M86 Security Labs Discovers Customers of Global Financial Institution Hit by Cybercrime.* Press Release, London, U.K., Aug. 10, 2010; http://www.marketwire.com/press-release/m86-security-labs-discovers-customers-global-financial-institution-hit-cybercrime-1302266.htm
26. Mahoney, M.R. *Comment on Pilot Project Testing and Certification.* EAC, Washington, D.C., Apr. 2010; http://www.eac.gov/assets/1/AssetManager/Martha%20Mahoney%20-%20Comment%20on%20Pilot%20Project%20Testing%20and%20Certification.pdf
27. Marsan, C.D. Feds to shore up net security. *Network World* (Jan. 19, 2009); http://www.pcworld.com/businesscenter/article/157909/feds_to_shore_up_net_security.html
28. Messmer, E. America's 10 most wanted botnets. *Network World* (July 22, 2009); http://www.networkworld.com/news/2009/072209-botnets.html
29. Military Postal Service Agency. *2010 Analysis of the Military Postal System Compliance with the MOVE Act.* Washington, D.C., Aug. 2, 2011; www.fvap.gov/resources/media/2010_MPSA_after_action_report.pdf
30. Mills, E. Spam offers to let people use their PC to attack Obama site. *CNET* (Aug. 18, 2009); http://news.cnet.com/8301-1009_3-10312641-83.html?tag=nl.e757
31. Mueller III, R.S. *Prepared Remarks.* RSA Security Conference, San Francisco, Mar. 4, 2010; http://www.fbi.gov/news/speeches/tackling-the-cyber-threat
32. Nakashima, E., Miller, G., and Tate, J. U.S., Israel developed computer virus to slow Iranian nuclear efforts, officials say. *Washington Post* (June 19, 2012); http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officialssay/2012/06/19/gJQA6xBPoV_story.html?wpisrc=al_national
33. New South Wales Electoral Commission. *Report on the Conduct of the NSW State Election 2011;* http://www.parliament.nsw.gov.au/Prod/parlment/committee.nsf/0/67f2055c4d085409ca25795a0017cf2c/$FILE/NSW%20EC%27s%20Report%20on%20the%202011%20State%20Election.pdf
34. Oberheide, J., Cooke, E., and Jahanian, F. CloudAV: N-version antivirus in the network cloud. In *Proceedings of the 17th USENIX Security Symposium* (San Jose, CA, July 28–Aug. 1, 2008), 91–106.
35. Palmer, C. *Unqualified Names in SSL Observatory.* Electronic Frontier Foundation Deeplinks blog, Apr. 5, 2011; https://www.eff.org/deeplinks/2011/04/unqualified-names-ssl-observatory
36. Peters, S. *14th Annual CSI Computer Crime and Security Survey, Executive Summary.* Computer Security Institute, New York, Dec. 2009; http://www.docstoc.com/docs/40697141
37. Remotegrity. 2011; https://demo.remotegrity.org/http://www.scantegrity.org/wiki/index.php/Remotegrity_Frequently_Asked_Questions
38. Sanger, D.E. Obama order sped up wave of cyberattacks against Iran. *New York Times* (June 1, 2012); http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all
39. Trusteer Inc. *Measuring the In-the-Wild Effectiveness of Antivirus Against Zeus.* White Paper, Sept. 14, 2009; http://www.techrepublic.com/whitepapers/measuring-the-in-the-wild-effectiveness-of-antivirus-against-zeus/1686945/post
40. U.K. *Electoral Commission. Key Issues and Conclusions, May 2007 Electoral Pilot Schemes.* London, Aug. 2007; http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0009/16200/ICMElectoralPilotsresearchreport_27285-20161__E__N__S__W__.pdf
41. Vascellaro, J.E. and Solomon, J. Yahoo! was also targeted in hacker attack. *Wall Street Journal* (Jan. 14, 2010); http://online.wsj.com/article/SB10001424052748703657604575004421409691754.html
42. Verified Voting Foundation. *Internet Voting 2012*; http://www.verifiedvotingfoundation.org/article.php?list=type&type=27
43. Weiss, T.R. Pentagon drops online votes for armed forces. *Computer Weekly* (Feb. 6, 2004); http://www.computerweekly.com/news/2240054464/Pentagon-drops-online-votes-for-armed-forces
44. Wolchok, S., Wustrow, E. Isabel, D., and Halderman, J.A. Attacking the Washington, D.C. Internet voting system. In *Proceedings of the 16th Conference on Financial Cryptography and Data Security* (Bonaire, Feb. 28. 2012); http://fc12.ifca.ai/pre-proceedings/paper_79.pdf
45. Zetter, K. Vulnerabilities allow attacker to impersonate any website. *Wired.com* (July 29, 2009); http://www.wired.com/threatlevel/2009/07/kaminsky/

Barbara Simons (simons@acm.org) is a retired IBM Research staff member, Board Chair of Verified Voting, and former ACM President.

Douglas W. Jones (jones@cs.uiowa.edu) is an associate professor in the Department of Computer Science of the University of Iowa in Iowa City.