Internet Voting
An Idea Whose Time has NOT Come

Barbara Simons
What is Internet Voting?

- Safe (kind of)
  - Posting a blank ballot on a website
  - Downloading a blank ballot

- Unsafe
  - Sending a blank ballot over the Internet
    - Voting at a website
    - Sending a voted ballot as an email attachment
    - Phone voting that uses the Internet
    - Fax voting (of any kind)
Why is Internet Voting Unsafe?

- Malware: viruses, worms, etc. that attack the voter's computer
- Attacks on the computer managing the election (the server)
- Insider threats
- Fake websites: spoofing/phishing
- Impossible to audit or recount
- Denial of Service attacks
- “False flag” attacks
The DC Hack
Background

- DC Board of Elections and Ethics: Internet voting for military and civilians living abroad
  - Upcoming midterm (2010)
  - Open Source Digital Voting Foundation (OSDV) source code available for people to examine
  - Called “digital vote by mail,” not Internet voting
  - Agreed to first conduct a pilot test
  - Test announced, delayed, then re-announced only 1 days in advance – began Sept 28, 2010
    - Real voting scheduled to begin 2 weeks later
The First Problem

• David Jefferson test voted on an Apple Macintosh using common browser (Safari)
  • Voting system required voters to save voted ballots using SAVE AS command in PDF
    – SAVE AS saved unmodified \textit{blank} PDF of ballot, instead of the modified version containing his votes
  • No error message or warning
    – Unknowingly voted a completely blank ballot
    – When he realized later, it was too late.
The Attack

• Oct 1: U. of Mich Fight Song started playing 15 seconds after the test ballot was submitted
  • http://www.cse.umich.edu/~jhalderm/pub/dc/thanks/
• Later that day, test was suspended
  • Due to “usability issues” (the pdf bug?)
• 3 days later “digital vote by mail” cancelled
  • Voters could download blank ballot – but not return voted ballot over Internet
More news comes out

• Oct 5: Prof. Alex Halderman announced his team at U. Mich had penetrated the system
  • Within 36 hours of system going live, had found and exploited a vulnerability (“shell-injection”) that gave them complete control over system. Could:
    – Change already cast and future ballots
    – Reveal voters' secret ballots
    – Install “calling card” of U Mich fight song
    – [Website link]
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.

<table>
<thead>
<tr>
<th>DELEGATE TO THE U.S. HOUSE OF REPRESENTATIVES</th>
<th>AT-LARGE MEMBER OF THE COUNCIL</th>
<th>UNITED STATES REPRESENTATIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vote for not more than (1)</td>
<td>Vote for not more than (1)</td>
<td>Vote for not more than (1)</td>
</tr>
<tr>
<td>[ ] Alice Example</td>
<td>[ ] Joan Example</td>
<td>[ ] Latoya Example</td>
</tr>
<tr>
<td>Democratic</td>
<td>Statehood Green</td>
<td>Republican</td>
</tr>
<tr>
<td>[ ] Bob Example</td>
<td>[ ] Kimberley Example</td>
<td>[ ] Marcus Example</td>
</tr>
<tr>
<td>Republican</td>
<td>Democratic</td>
<td>Statehood Green</td>
</tr>
<tr>
<td>[ ] Carol Example</td>
<td>[ ] Liam Example</td>
<td>[ ] Newton Example</td>
</tr>
<tr>
<td>Statehood Green</td>
<td>Republican</td>
<td>Democratic</td>
</tr>
<tr>
<td>[ ] or write-in</td>
<td>[ ] or write-in</td>
<td>[ ] or write-in</td>
</tr>
<tr>
<td>Skynet</td>
<td>Johnny 5</td>
<td>Colossus</td>
</tr>
</tbody>
</table>

**MAYOR OF THE DISTRICT OF COLUMBIA**

<table>
<thead>
<tr>
<th>Vote for not more than (1)</th>
<th>MEMBER OF THE COUNCIL WARD ONE</th>
<th>MEMBER OF ADVISORY NEIGHBORHOOD COMMISSION 1B DISTRICT FOUR</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ] Duane Example</td>
<td>[ ] Mary Example</td>
<td>[ ] Orlando Example</td>
</tr>
<tr>
<td>Republican</td>
<td>Republican</td>
<td>Democratic</td>
</tr>
<tr>
<td>[ ] Edward Example</td>
<td>[ ] Nitam Example</td>
<td>[ ] Phyllis Example</td>
</tr>
<tr>
<td>Democratic</td>
<td>Statehood Green</td>
<td>Statehood Green</td>
</tr>
<tr>
<td>[ ] Frances Example</td>
<td>[ ] Odell Example</td>
<td>[ ] Quincy Example</td>
</tr>
<tr>
<td>Statehood Green</td>
<td>[ ] or write-in</td>
<td>Republican</td>
</tr>
<tr>
<td>[ ] or write-in</td>
<td>GLaDOS</td>
<td>[ ] or write-in</td>
</tr>
<tr>
<td>Master Control Pro</td>
<td></td>
<td>Deep Thought</td>
</tr>
</tbody>
</table>

**CHAIRMAN OF THE COUNCIL**

<table>
<thead>
<tr>
<th>Vote for not more than (1)</th>
<th>MEMBER OF STATE BOARD OF EDUCATION WARD ONE</th>
<th>Thank you for voting. Please turn in your ballot</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ] Gregory Example</td>
<td>[ ] Abigail Example</td>
<td></td>
</tr>
<tr>
<td>Statehood Green</td>
<td>Republican</td>
<td></td>
</tr>
<tr>
<td>[ ] Helen Example</td>
<td>[ ] Yvonne Example</td>
<td></td>
</tr>
<tr>
<td>Republican</td>
<td>Democratic</td>
<td></td>
</tr>
<tr>
<td>[ ] Inez Example</td>
<td>[ ] Zachary Example</td>
<td></td>
</tr>
<tr>
<td>Democratic</td>
<td>Statehood Green</td>
<td></td>
</tr>
<tr>
<td>[ ] or write-in</td>
<td>[ ] or write-in</td>
<td></td>
</tr>
<tr>
<td>HAL 9000</td>
<td>Bender</td>
<td></td>
</tr>
</tbody>
</table>
A bombshell at Oct 8 DC Hearing

- Halderman: since beginning of test his team had control of network
  - Default master password unchanged
    - A common security vulnerability
    - Found default password in manual
  - Could watch network operators configure and test equipment – brought pictures from video feed to hearing
  - Since security cameras didn't have passwords, could watch what operators were typing, including passwords
  - Could have reprogrammed switches to steal votes in a real election
Still more from Hearing

- Halderman: while in control of network, saw other attacks coming from China and Iran
  - Defended network by changing password and adding other security measures
  - Probably not aimed directly at test – always floating around Internet
- A file used to test system appears to have been 937 invitation letters sent to registered voters
  - Contained voters' PINs
    - U Mich team could have subverted real election
What has been the impact?

- DC not using web based system for return of voted ballot
  - Still allows voted ballots to be returned as email attachments or via fax
- Other states not learning from DC hack
How an election could be rigged by malware
Malicious viruses: Zeus

- Primary goal is to steal money from on-line bank accounts
  - So clever that can mimic financial statement so that victim is unaware of theft – until a check bounces
  - Over GPB 675,000 stolen from about 3000 customers of unnamed UK bank
  - As of 2009 about 3.6 million PCs infected in US
  - New credit card verification system scam being used to steal personal info
    - I received copy from Commerce Bank on 9/13
Verified by Visa / MasterCard SecureCode Enrollment:

Due to recent changes in FDIC Deposit Insurance Rules all our customers must be enrolled in Verified by Visa or MasterCard SecureCode program depending on type of your Check Card. To continue complete this form and click Activate Now.

Social Security #: __-__-____
Card Number: ___________ (16 digits)
Expiration Date: __/____ (MM/YY)
Signature Code: ___________ (Last 3 digits on the back)
Card PIN Code: ___________ (4-6 digit code that you enter in ATM)

Choose Password: _________ How will it be used?
Confirm Password: _________ (6-12 characters length)

Activate Now

If you already enrolled in Verified by Visa or MasterCard SecureCode program to continue please enter current password or select new then click Activate Now.
Zeus attacking Charles Schwab

- Computerworld (Oct 16): Zeus attacking Schwab investment accounts
- Fake LinkedIn reminders with disguised links to malicious sites
  - Sites hit Windows PCs looking for exploit that works
  - Once get onto PC, silently captures log-in credentials for online banks + Schwab usernames and passwords
  - Can get additional info via a bogus form
    - Mother's maiden name, driver's license number, employer
More about Zeus

- Zeus being marketed
  - Upgrades available for purchase
- Spread via legitimate websites
  - Paul McCartney's website, German Wikipedia, etc.
- Avoids detection by using SSL (encryption) to communicate with “handler"
- Vote rigging on voters' computers a relatively easy problem
Conficker Worm

- “Calls home” for more instructions
  - Infected machine can remotely install malicious software without computer owner's knowledge
- In 2008 had infected 9 – 15 million machines
- In 2009 discovered in >300 imaging machines in hospitals – could have send patient info
  - Devices not supposed to have been connected to Internet, but were
- Could install election rigging software/names
If the voter's computer is infected with an election-rigging virus or worm, the virus will be voting, not the voter.

The voter will never know.
How an Election could be Rigged by an Attack on the Server
Recent attacks on Google, etc.

- China-based: Google, Yahoo, Adobe, Juniper Networks, Northrop-Grumman, Symantec, etc.
- Attacks appeared to be from trusted sources
  - Victims tricked into clicking on link or file
- Malware downloaded by exploiting vulnerability in Microsoft Explorer
- Attacker gained complete control over compromised system
  - Systems used by software developers to build code
  - Gmail accounts of Chinese human rights workers
Government Sites Vulnerable

- FBI Dir. Robert Mueller: FBI's computer network penetrated; attackers “corrupted data”
- Gen. Michael Hayden, former Dir. CIA and National Security Agency:

  - “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.”
Internet voting organizations do not have the resources of Google or many of the other companies that were successfully attacked.

How do they expect to defend themselves against attacks?
Insider Threat

- With computers a single insider (programmer) could possibly rig an election
  - Jerome Kerviel: convicted of losing about $7 billion in unauthorized transactions at Société Générale by exploiting insider status
  - CIA agent Aldrich Ames
- Money loss eventually discovered – secrets passed to the USSR eventually uncovered
- How can you PROVE an election was stolen?
Distributed Denial of Service Attacks

• Prevents people from accessing website by overwhelming website with requests
  • Typically done with “botnets”: large number of infected computers (zombies) controlled by creators
  • FBI: Mariposa Botnet may have infected 8,000,000 to 12,000,000 computers internationally
  • Virus used to create Mariposa can steal credit card data and online banking passwords
  • Customized versions sold
• Could disenfranchise voters on Election Day
Examples: Estonia

- April – May, 2007 massive attack against Estonian websites
  - Speculation originated in Russia because of Estonian decision to move a Soviet war memorial
- Earlier in 2007 national parliamentary elections
  - Estonian could vote over Internet or at polls
  - If DDoS attacks held during vote, could have disenfranchised many voters
Canada

- Political party (New Democratic Party) held leadership vote over Internet Jan 2 - 25, 2003
- Jan 25 NDP voting site down for several hours
  - Because of secrecy, we don't know exact reason
  - Either Denial of Service attack or Slammer Worm
  - Vendor claims to have patched for Slammer, but no independent examination ever conducted and no logs or other proof released
It can be very very hard to find cleverly concealed malware

- Similar to the problem of finding software bugs
  - If finding all bugs (and risks) were easy, major software vendors would not need to send out periodic security updates
- The US tax code
  - No one claims to completely understand it, even though it is written in English
  - Provisions benefitting a single company have been inserted and not found until after passage
Concealed Malware

• In addition to hiding election rigging code, an insider can insert a “backdoor”
  • Allows someone later to insert code and information, e.g. candidate names

• Sometimes intentional
  • SonyBMG rootkit had been distributed on millions of music CDs in 2005 to gather information about users surreptitiously
    • Was discontinued when exposed
    • Lawsuits against Sony – affected CDs recalled
Internet Voting may Not save Money

• Swindon, UK; the Electoral Commission:
  – “The pilot scheme led to an overall increase in expenditure by the Council. . . . The average cost of the 2007 pilot scheme per elector was £8.33, compared with £2.30 for a conventional election, while the cost per electronic vote cast was £102.50.”
  – Each internet vote over 44 times more costly than conventional vote

• No way to check if reported results were correct
Need Accountability

- Computer software can be buggy or might contain malicious code
  - Open source not an adequate defense, though better than proprietary software
    - Open source used in DC system that was hacked
- Votes are secret
  - Current voting systems do not allow me to verify that my vote was accurately received and counted
  - Even if were possible (via use of crypto), what happens if discrepancy is uncovered?
Must be able to Audit/Recount

- Ballots sent over Internet unreliable
  - Therefore, recount is meaningless
- Require paper ballots and mandatory audits
  - Randomly select ballots to be recounted AFTER close of election
    - Closeness of election a factor
    - **Risk limiting audit**: statistics can reduce amount of work
    - If discrepancies that could change election outcome discovered, expand audit size or move to total recount