Internet Voting: What Could Go Wrong?

J. Alex Halderman
University of Michigan
Voting as a Security Problem?

Integrity ↔ Ballot Secrecy

No Trusted Parties
Electronic Voting in Practice?
Diebold AccuVote-TS
President of the United States
RACE # 0
# Running  2
# To Vote For  1

# Times Counted  5
# Times Blank Voted  0
# Times Over Voted  0
# Number Undervotes  0

George Washington  2
Benedict Arnold  3

WE, THE Undersigned, DO HEREBY CERTIFY THE ELECTION WAS CONDUCTED IN ACCORDANCE WITH THE
Today, >70% of American voters get to see a physical record of their vote.
Internet Voting?
Server-side Threats

Results
A: 1000
B: 999

- Denial of Service
- Remote Intrusion
- Insider Attacks
- State-Sponsored Attacks
Client-side Threats

- Credential Theft
- Imposter Sites
- Malware
MEDIA RELEASE

D.C. BOARD OF ELECTIONS AND ETHICS
September 21, 2010

Contact: Alysoun McLaughlin, amclaughlin@dcboee.org
202-727-2511 (direct)/202-441-1121 (cell)

Board Announces Public Test of
Digital Vote by Mail Service

Open Source Solution Provides Secure Alternative for Overseas Voters
Who Are Underserved by Traditional Vote by Mail

WASHINGTON, D.C. — The Board of Elections and Ethics today announced that the public examination phase of the Digital Vote by Mail pilot project for overseas voters will begin on Friday, September 24.

Digital Vote by Mail is a first-in-the-nation use of open source technology to provide a secure means for overseas voters to obtain, print and mail their ballot — and, if the voter so chooses, have it verified for accuracy. This pilot project is a joint effort between the Board of Elections and Ethics and the Department of Foreign Affairs and International Trade Canada; the project will test the security and accuracy of the system and provide a model for future use.
DC General Election
November 2, 2010

The service offers two options:

1. Physical Ballot Return
   Complete your ballot and return materials by mail or express delivery service.
   - Obtain your blank ballot and other vote-by-mail materials
   - Complete them online and print them
   - Return materials by mail or express delivery service
   See more information about this option.

2. Digital Ballot Return
   Complete your ballot and return it electronically.
   This pilot project allows you to return your ballot through the internet.
   - Obtain your blank ballot and other vote-by-mail materials
   - Complete them online
   - Return completed ballot electronically
   See more information about this option.

Start Mail-in Ballot
Start Digital Ballot
Check In

Your name, zip code, and voter ID number must match the information we have in your current voter record. The PIN number must exactly match the number that was provided to you by mail, by the Board of Elections and Ethics. All fields are required.

Name: Iva Pfannerstill
Zip Code: 20018
Voter ID Number: 27218848

PIN: 1DC56A2A9DD9B94

Enter 10-digit Number Provided by BOEE

Continue
Complete Ballot
Digital ballot return lets you return your ballot electronically. You will need to save your marked ballot, locate it on your computer, and upload it to the BOEE. Keep this page open until you have saved your completed ballot.

1. Check In
2. Confirm Identity
3. Complete Ballot
4. Send Ballot

Download
Download and View Your Ballot
Click the PDF icon at the right to download your ballot. The ballot PDF will open in your default PDF viewing application, on top of your web browser.

Mark
Mark Your Ballot
To complete the ballot online, click on the circles next to your candidates to select them. You can also type in candidates where indicated.

Save
Save Your Ballot
You must save your ballot when you have marked it. Save the PDF on your computer by selecting File/Save As in your default PDF viewing application. Save the ballot to a place where you can easily find it again (for example, your desktop). Do NOT rename the ballot.

Key Dates
October 1
Vote-by-Mail service begins

October 22
Last day to apply for a Vote-by-Mail Ballot

November 2
Last day to return your ballot (by mail, must be postmarked by 5:00 pm)
Please fill out the following form. If you are a form author, choose Distribute Form in the Forms menu to send it to your recipients.

PRECINCT 69 - SMD 11-ANC 5A

Official Ballot
District of Columbia Mock Election
PRECINCT 69
September 17, 2010

DELEGATE TO MAYOR MAYORAL REPRESENTATIVE

1. TO VOTE, carefully read each candidate's position and then fill in the appropriate circles in the boxes below.
2. Use only a black or dark blue ink.
3. If you make a mistake, you may erase it with a pencil. Marking more than one circle in any box indicates your intention to vote for all candidates listed.
4. For a Write-In, write the name of the person you wish to vote for in the Write-In box.

COLUMBIA FIVE DISTRICT ELEVEN
Send Your Ballot

To send your ballot electronically, you must find the ballot file and upload it.

1. Check In
   Locate Ballot PDF and Send
   On the web page that is open, select the Choose File button to browse for your ballot file. In the dialog box that comes up, navigate to the PDF file that you saved in the previous step, and select that file. Press Send.

   A confirmation message will appear on the next web page to let you know your ballot has been delivered.

2. Confirm Identity

3. Submit Ballot

4. Review
Your marked ballot has been sent. Thank you for your participation in this election.

Thank You!

Ballot Received
7:37 PM, March 25, 2011

Check the status of your ballot at any time at the Board of Elections and Ethics website.
Recruit
module Paperclip

class Encrypt < Processor
  def initialize(file, options = {}, attachment = nil)
    super

    @file = file
    @recipient = options[:geometry]
    @attachment = attachment
    @current_format = File.extname(@file.path)
    @basename = File.basename(@file.path, @current_format)
  end

  def make
    src = @file
    dst = Tempfile.new([@basename, 'gpg'].compact.join("."))
    dst.binmode

    raise PaperclipError, "GPG recipient wasn't set" if @recipient.blank?

    begin
      run("rm", "-f \"#{File.expand_path(dst.path)}\"")
      run("gpg", "--trust-model always -o \"#{File.expand_path(dst.path)}\" -e -r \"#{@recipient}\" \"#{File.expand_path(dst.path)}\"")
    rescue PaperclipCommandLineError
      raise PaperclipError, "couldn't be decrypted. Please try again later" end
  end

end
ballot.xyz → /tmp/49d5.xyz
ballot.$(sleep 5) \rightarrow \text{"/tmp/49d5.$(sleep 5)\"}
Board of Election Ethics Network

Port Assignment, same ports for both Switches:
- Management vlan 102: Port 0/3 – 10
- Data Vlan trunk: Port 0/11 – 15 (trunk allow vlan 101,103)
- Data vlan 103: port 0/16
- DMZ vlan 101: Port 0/17 - 20

Symbol means Cisco network IDS

Surveil
Steal database passwords, keys, etc.
Replace all existing votes with ours
<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>Johnny 5</td>
<td>or write-in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Colossus</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAYOR OF THE DISTRICT OF COLUMBIA</td>
<td>MEMBER OF THE COUNCIL WARD ONE</td>
<td>MEMBER OF ADVISORY</td>
</tr>
<tr>
<td>Vote for not more than (1)</td>
<td>Vote for not more than (1)</td>
<td>Neighborhood Commission 1B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DISTRICT FOUR</td>
</tr>
<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>[ ] Nitan Example</td>
<td>[ ] Phyllis Example</td>
</tr>
<tr>
<td>Democratic</td>
<td>Democratic</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>Republican</td>
<td>Republican</td>
</tr>
<tr>
<td>( ] or write-in</td>
<td>GLaDOS</td>
<td>or write-in</td>
</tr>
<tr>
<td>Master Control Program</td>
<td></td>
<td>Deep Thought</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHAIRMAN OF THE COUNCIL</td>
<td>MEMBER OF STATE BOARD OF EDUCATION WARD ONE</td>
<td></td>
</tr>
<tr>
<td>Vote for not more than (1)</td>
<td>Vote for not more than (1)</td>
<td></td>
</tr>
<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></td>
<td>Thank you for voting,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Please turn in your ballot.</td>
</tr>
</tbody>
</table>
Attack!

- Steal database passwords, keys, etc.
- Replace all existing votes with ours
- Replace any new votes
- Back door to reveal new votes
- Clear logs
- “Calling card”
<section id='main'>
  <section class='instruction'>
    <header>
      <h1>Thank You!</h1>
    </header>
    <div id='owned'>
      <embed autostart='true' hidden='true' loop='true' src='/victors.mp3' volume='100'/>
    </div>
  </section>
  <section class='instruction'>
    <header>
      <h2>Ballot Received</h2>
      <h2>12:18 PM, October 01, 2010</h2>
    </header>
  </section>
  <footer>
    <p>Check the status of your ballot at any time at the Board of Elections and Ethics website</a>.</p>
  </footer>
</section>
Case Study
New South Wales, Australia  (March 2015)
New South Wales
Most populous Australian state

New South Wales: Internet voting

Vic: polling-place e2e

2011  System by Everyone Counts
2015  iVote system by Scytl

“People’s vote is completely secret. It’s fully encrypted and safeguarded, it can’t be tampered with …”
LOGIN TO iVote®

Please enter your iVote® number and PIN.
Your 8 digit iVote® Number was provided to you by the New South Wales Electoral Commission after you registered to use iVote®. At the time of registration you selected your own 6 digit PIN.
Both iVote® number and PIN are required to proceed.

Enter your 8 digit iVote® number here

Enter your 6 digit PIN here
VOTE RECEIPT

Thank you for using the iVote® for Web demonstration system. Your practise vote is complete and the demonstration Receipt Number is:

3111 6228 8894

When voting in a real election you would need your Receipt Number to use the services described below.

Print this page

When you have finished please select the Exit button to be redirected to the iVote® home page.
Internet Voting Hackers (IVH)

**Access:** External

**Intention:** Embarrassment

**Boundary:** None

**Organisation:** Individual

**Proficiency:** Advanced

**Purpose:** Indifferent

**Attribution:** Overt

**Affiliations:** Other hacktivist groups including Anonymous

**Date revised:** 10 Jan 14

**Summary:** IVH individuals have a broad range of capabilities depending on individual skill level which varies significantly. They target Internet voting applications to demonstrate the lack of security, show their lack of trust in governments generally and to demonstrate their skill level to the rest of the hacker community. Their actions are very public and may be more about causing embarrassment than actually impacting Internet voting applications or the results of elections.

After officials reported the system was secure following remediation, Abhaxas again gained access to private file directories publicising the subsequent insecurity. IVH may be motivated by a wish to emulate the lawful work of Internet voting security researchers such as Scott Wolchok from the University of Michigan, who breached the **Washington DC election system** in a test in 2010. Wolchok and his colleagues have received significant media attention for their exploits and IVH might choose replicate these activities in an illegal manner to gain notoriety and promote their cause.

**Target:** IVH specifically target Internet voting applications but may also be involved in other hacktivist activity.
March 2015

<table>
<thead>
<tr>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>Alex Arrives in Melbourne</td>
<td>iVote Opens</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
</tr>
</tbody>
</table>

29  | 30  | 31  | Apr 1 | 2   | 3   | 4   |

Election Day
iVote Closes
LOGIN TO iVoté®

Please enter your iVoté® number and PIN.

Your 8 digit iVoté® Number was provided to you by the New South Wales Electoral Commission after you registered to use iVoté®. At the time of registration you selected your own 6 digit PIN.

Both iVoté® number and PIN are required to proceed.

Enter your 8 digit iVoté® number here

Enter your 6 digit PIN here
SSL Report: ivote.piwikpro.com (91.109.21.165)

Overall Rating

Certificate: 100
Protocol Support: 70
Key Exchange: 0
Cipher Strength: 60

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports insecure Diffie-Hellman (DH) key exchange parameters. Grade set to F.

This server supports 512-bit export suites and might be vulnerable to the FREAK attack. Grade set to F. MORE INFO

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO
FREAK and Logjam Attacks

Man-in-the-middle attacks that downgrade TLS to export-grade RSA or Diffie-Hellman, Impersonate the server and arbitrarily read or change connection data.
FREAK affected most major browsers, patched one week before the election.

Logjam discovered by team including AH in early March. Not public until May 20 (responsible disclosure).

We had a TLS 0-day affecting every browser!
Attacking iVote

Malicious Network

ivote.piwikpro.com

Malware runs in iVote app’s origin

ivote.nsw.gov.au

Load iVote site

Load piwik.js

Vote Stealing Malware

Malicious Network
Defeating Verification?

Apart from telephone-based cast-as-intended verification, no meaningful verifiability.

Verification is easily sidestepped.

Verification is a critical **fail-safe mechanism**. If you need to rely on it, your security has already failed.
<table>
<thead>
<tr>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 1</td>
<td></td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Logjam Discovered (Not Public)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**March 2015**

3-4 June: First patches available. iVote gets offline as a patch is applied to correct the vulnerability. 66,000 votes cast while vulnerable, closest margin was only 3177 votes.

5 June: Logjam patches available.

6 June: First Logjam patches available.

7-8 June: First Logjam patches are available.

9-10 June: First Logjam patches are available.

11 June: First Logjam patches are available.

12 June: First Logjam patches are available.

13 June: First Logjam patches are available.

14 June: First Logjam patches are available.

15-16 June: First Logjam patches are available.

17-18 June: First Logjam patches are available.

19 June: First Logjam patches are available.

20 June: First Logjam patches are available.

21 June: First Logjam patches are available.

22 June: First Logjam patches are available.

23 June: First Logjam patches are available.

24 June: First Logjam patches are available.

25 June: First Logjam patches are available.

26 June: First Logjam patches are available.

27 June: First Logjam patches are available.

28 June: First Logjam patches are available.

29 June: First Logjam patches are available.

30 June: First Logjam patches are available.

31 June: First Logjam patches are available.

1 July: First Logjam patches are available.

2 July: First Logjam patches are available.

3 July: First Logjam patches are available.

4 July: First Logjam patches are available.

››› May 20 First Logjam patches Available
The Future?
California Online Voting Ballot Initiates (2016)
Securing online elections requires solving some of the most challenging open problems in computer security.

Commodity tools and frameworks are too fragile and complex. Small mistakes are inevitable and have dire consequences.

History gives voters good reason to be skeptical. Even a perfectly engineered system needs to earn their trust.

My take: Decades, if ever, until Internet voting can be adequately secured, and not without fundamental advances.
Internet Voting: What Could Go Wrong?

J. Alex Halderman
University of Michigan

https://jhalderm.com