ATTACKING THE
WASHINGTON, D.C.
INTERNET VOTING SYSTEM

J. Alex Halderman
The University of Michigan
Who am I?
J. Alex Halderman

CS Prof.
University of Michigan
Security and Privacy
Tech Policy
Technology for Democracy

Selected Projects
2012  Widespread Weak Keys in Network Devices
2011  Telex: Anticensorship in the network infrastructure
2010  Hacking Washington D.C.’s Internet voting
2010  Vulnerabilities in India’s e-voting machines
2010  Reshaping developers’ security incentives
2009  Analysis of China’s Green Dam censorware
2009  Fingerprinting paper with desktop scanners
2008  Cold-boot attacks on encryption keys
2007  California’s “Top-to-Bottom” e-voting review
2007  Machine-assisted election auditing
2006  The Sony rootkit: DRM’s harmful side-effects
MEDIA RELEASE

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

Contact: Alyson 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 chooses, also digitally mark and return their ballot. After testing is completed, the service will be made available to overseas voters, who often do not have enough time to receive and return their ballot by mail in the few weeks between the September primary and the November general election. Prior to Digital Vote by Mail, the only option for these voters was to sacrifice the secrecy of their ballot by using e-mail or fax.

During the test period, which will continue through Thursday, September 30, individuals who wish test and comment on the technology and usability of the application will be granted access to the application, a complete system architectural diagram, and access to the underlying source code.

A limited number of test credentials will be available on a first-come, first-served basis beginning on Friday morning. Using these test credentials, a tester may log in as a fictitious District voter and request, complete and submit an absentee ballot. The Board will compile all test ballots and test the decoding software and back office processes needed to accept and process digitally transmitted ballots. The Board asks testers to thoroughly test the system and disclose any security, programmatic, usability or other functional or design issues they discover in the testing process. All data, hardware and software are logically and physically segregated from all other Board systems. Users will not be held liable for damage resulting from good faith efforts at testing system integrity.
The diagram illustrates a network architecture involving several components:

1. **Public Network**
2. **Firewall and Intrusion Detection**
3. **Web Server**
4. **Firewall**
5. **Application Server**
6. **Database Server**

The allowed TCP ports are specified as follows:

- **Public Network** allows TCP ports 80 and 443.
- **Web Server** allows TCP port 80.

The domain name mentioned is `digital-vbm.dc.gov`.
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.

D.C. Digital Vote-by-Mail is a new service to the overseas and military voters of the District of Columbia. We’ve designed this service to make it easier for you to receive your voting materials and help you return your completed ballot more quickly.

Thank you for your participation in this election.

District of Columbia Board of Election and Ethics

Start Mail-in Ballot
Start Digital Ballot
1. **Check In**
   - Enter name, ZIP code, voter ID number, and PIN.

2. **Confirm Identity**
   - Confirm your identity.
   - Affirm voting eligibility.
   - Review attestation document (optional).

3. **Complete Ballot**
   - Download your ballot.
   - View your ballot.
   - Mark your ballot.
   - Save your ballot (Do NOT rename the file).

4. **Send Ballot**
   - Locate your ballot on your computer.
   - Upload your ballot.
   - Receive notice of ballot receipt.

---

**Key Dates**

- **October 1**: Vote-by-Mail service begins.
- **October 22**: Last day to apply for a Vote-by-Mail Ballot.

---

[Complete instructions for the Digital Vote-by-Mail Service.]

[Find out more about D.C. Digital Vote-by-mail, and the digital ballot return pilot project.]

District of Columbia Digital Vote-by-Mail Service | About | Help | Security | Contact
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.

1 Check In

Please enter your name, address, and PIN.

Name: Iva Farmerstill

Zip Code: 20018

Voter ID Number: 272188488

PIN: 1DC58A2A9DD9B94

Enter 16-digit Number Provided by BOEE

2 Confirm Identity

3 Complete Ballot

4 Send 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 EST)

Last day to return your ballot (in person or drop box)

---

District of Columbia Digital Vote-by-Mail Service | About | Help | Security | Contact

Find out more about D.C. Digital Vote-by-mail and the digital ballot return pilot project.

Complete instructions for the Digital Vote-by-Mail Service.
Confirm Your Identity
To vote through the Digital Vote-by-Mail Service, you must confirm your identity and your eligibility to vote. Select the checkboxes to confirm. You can also review the attestation document that confirms your voting eligibility by clicking on the PDF. (This step is optional.) Keep this page open until you have finished viewing your attestation document.

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

Confirm
Confirm Your Identity
Please confirm your identity and voter registration address. If the address shown is incorrect, you will need to contact the BOEE to have it updated before you can mark your ballot. If the information is correct, check the box.

If this isn’t you, press the Back button and re-enter your information.

Iva Pfannerstill
Addison Ave, Unit 261
WASHINGTON DC 20018

Affirm
Affirm Your Eligibility
Review the text inline. Check the box to confirm statements are correct.

I swear or affirm, under penalty of perjury, that:
1. I am a U.S. citizen, at least 18 years of age, and I am eligible to vote in the District of Columbia; and

Review
Review Your Attestation Document (Optional Step)
If you would like to review your attestation document, click the PDF icon at the bottom of the page.
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 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 Your Ballot

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)
Send Your Ballot
To send your ballot electronically, you must find the ballot file and upload it.

Send
Locate Ballot PDF and Send
On the web page that is open, select the Choose File button to browse for your

Save As
Save in: My Documents

No items match your search.

File name: PDFSignature Arg
Save as type: Adobe PDF Files (*.pdf)

Save
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.

Tell everyone you voted! Facebook Twitter
1. Collect info (remember to log)
2. Establish local control
3. Clear track
4. Install attacks

- Replace old ballots
- Steal new ballots
- Rig to replace new ballots
- Rig to steal new ballots
- Rig at root
- Ficus men.

SSL cert?
SSL backed?
DC Digital VBM

Requirements

- Ruby 1.8+ (tested on Ruby 1.8.7)
- RubyGems 1.3.6+ (tested on RubyGems 1.3.6)
- Bundler 0.9.26
- GnuPG (gnupg.org) with the public key for ballots signing

Installation (locally)

Get the Bundler:

```
$ sudo gem install bundler --version=0.9.26
```

Get the sources:

```
$ git clone git://github.com/trustthevote/DCdigitalVBM.git
```

Install gem requirements:

```
$ cd DCdigitalVBM
$ bundle install
```
module Paperclip

class Encrypt < Processor

  def initialize(file, options = {}, attachment = nil)
    super

    @file = file
    @recipient = options[:geometry]
    @attachment = attachment
    @current_format = File.basename(@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}" "")
    rescue PaperclipCommandLineError
      raise PaperclipError, "couldn't be encrypted. Please try again later!"
    end
  end
end
ballot.pdf  → /tmp/49d5.pdf
ballot.xyz → /tmp/49d5.xyz
ballot.$(sleep 5) → /tmp/49d5.$(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

Management Vlan102: 10.83.2.128/25
DATA Vlan103: 10.83.3.24/24

EMC AX100 Storage Array
Digi Passport™ 8 Configuration and Management

User administration
/admin/user_admin

Current local users

<table>
<thead>
<tr>
<th>#</th>
<th>User name</th>
<th>User group</th>
<th>Shell</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Hoang</td>
<td>System admin</td>
<td>Configuration menu</td>
</tr>
<tr>
<td>2</td>
<td>admin</td>
<td>System admin</td>
<td>Configuration menu</td>
</tr>
<tr>
<td>3</td>
<td>ilie</td>
<td>System admin</td>
<td>Configuration menu</td>
</tr>
<tr>
<td>4</td>
<td>ocee</td>
<td>System admin</td>
<td>Configuration menu</td>
</tr>
<tr>
<td>5</td>
<td>root</td>
<td>Root</td>
<td>CLI</td>
</tr>
</tbody>
</table>

Add | Remove | Unlock
ATTACK!
Steal database credentials, keys, logs, etc.
Replace all existing votes with our choices
### 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 pen or black or blue 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

<table>
<thead>
<tr>
<th>Vote for not more than 1</th>
<th>Vote for not more than 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice Example</td>
<td>Joan Example</td>
</tr>
<tr>
<td>Democratic</td>
<td>Statehood Green</td>
</tr>
<tr>
<td>Bob Example</td>
<td>Kimberly Example</td>
</tr>
<tr>
<td>Republican</td>
<td>Democratic</td>
</tr>
<tr>
<td>Carol Example</td>
<td>Liam Example</td>
</tr>
<tr>
<td>Republican</td>
<td>Republican</td>
</tr>
<tr>
<td>or write-in</td>
<td>or write-in</td>
</tr>
<tr>
<td>Skynet</td>
<td>Johnny 5</td>
</tr>
</tbody>
</table>

#### MAYOR OF THE DISTRICT OF COLUMBIA

<table>
<thead>
<tr>
<th>Vote for not more than 1</th>
<th>Vote for not more than 1</th>
<th>Vote for not more than 1</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>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>Odeli Example</td>
<td>Quincy Example</td>
</tr>
<tr>
<td>Republican</td>
<td>Republican</td>
<td>Republican</td>
</tr>
<tr>
<td>or write-in</td>
<td>or write-in</td>
<td>or write-in</td>
</tr>
</tbody>
</table>

#### CHAIRMAN OF THE COUNCIL

<table>
<thead>
<tr>
<th>Vote for not more than 1</th>
<th>Vote for not more than 1</th>
<th>Vote for not more than 1</th>
<th>Vote for not more than 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gregory Example</td>
<td>Abigail Example</td>
<td>Thank you for voting.</td>
<td></td>
</tr>
<tr>
<td>Statehood Green</td>
<td>Republican</td>
<td>Please turn in your</td>
<td></td>
</tr>
<tr>
<td>Helen Example</td>
<td>Yvonne Example</td>
<td>ballot</td>
<td></td>
</tr>
<tr>
<td>Republican</td>
<td>Democratic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inez Example</td>
<td>Zachary Example</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Democratic</td>
<td>Statehood Green</td>
<td></td>
<td></td>
</tr>
<tr>
<td>or write-in</td>
<td>or write-in</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HAL 9000</td>
<td>Bender</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Steal database credentials, keys, logs, etc.
Replace all existing votes with our choices
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>
<footer>
<p>Check the status of your ballot at any time at the Board of Elections and Ethics <a href='http://www.dcboee.us' target='_blank'>website</a>.</p>
</footer>
</section>

</section>
One more thing...
D.C. Overseas Digital Vote by Mail Service

Dear HARRIET DANIEL:

You have been selected to participate in the Digital Vote by Mail initiative. As part of its implementation of the MOVE Act, the District of Columbia Board of Elections and Ethics (BOEE) will offer overseas voters an option to receive and, optionally, send their absentee ballots digitally. While you may choose to return your absentee ballot by mail or fax, the BOEE’s Digital Vote by Mail process provides you a rapid return option that will maintain ballot secrecy and integrity.

The Way it Works

Approved overseas and military voters with internet access, such as you, may log on to our special digital delivery website. In your internet browser type in: http://www.dcbboee.us/dvm in the address field. You will then be prompted to provide your name, address and personal identification number. For security purposes, please enter the information EXACTLY as listed below.

Voter ID Number: [Redacted]
Your name as listed with BOEE: HARRIET SANDRA DANIEL
Residence Zip Code: 20007
Personal Identification Number: BD15B35F1E3C41B6

If your information needs to be updated, please contact our office separately by calling (202) 727-2525 or by visiting our website http://www.dcbboee.org. DO NOT enter updated information in the Digital Vote by Mail website.
CONCLUSIONS
Web applications tend to be *brittle*

Small mistakes can have huge consequences

Voting is harder to secure than e-commerce

Deep security challenges left to solve

Decades, *if ever*,

before we can vote online securely.
ATTACKING THE WASHINGTON, D.C. INTERNET VOTING SYSTEM

Full paper available at https://jhalderm.com

J. ALEX HALDERMAN
THE UNIVERSITY OF MICHIGAN