Internet Voting:
What Could Go Wrong?

J. Alex Halderman
University of Michigan

Voting as a Security Problem?

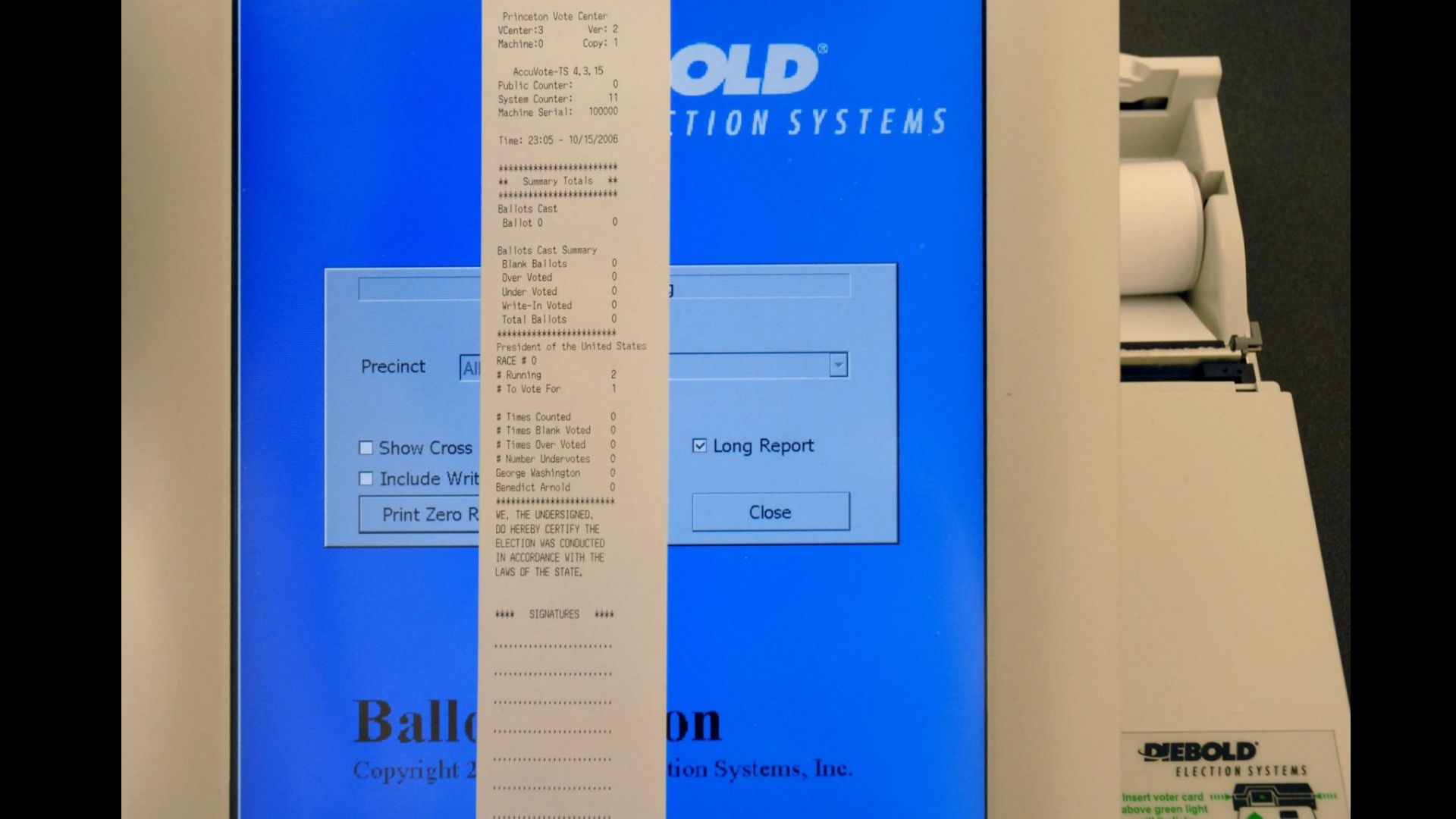
Integrity  Ballot Secrecy

No Trusted Parties

Electronic Voting in Practice?


PHOENIX CONTACT

Diebold AccuVote-TS


Princeton Vote Center
VCenter:3 Ver: 2
Machine:0 Copy: 1
AccuVote-TS 4.3.15
Public Counter: 0
System Counter: 11
Machine Serial: 100000
Time: 23:05 - 10/15/2006
** Summary Totals **
Ballots Cast
Ballot 0 0
Ballots Cast Summary
Blank Ballots 0
Over Voted 0
Under Voted 0
Write-In Voted 0
Total Ballots 0
President of the United States
RACE # 0
Running 2
To Vote For 1
Times Counted 0
Times Blank Voted 0
Times Over Voted 0
Number Undervotes 0
George Washington 0
Benedict Arnold 0
WE, THE UNDERSIGNED,
DO HEREBY CERTIFY THE
ELECTION WAS CONDUCTED
IN ACCORDANCE WITH THE
LAWS OF THE STATE.
**** SIGNATURES ****
Precinct
Show Cross
Include Writ
Print Zero R
Long Report
Close
Copyright 2
tion Systems, Inc.
DIEBOLD
ELECTION SYSTEMS
Insert voter card
above green light

****
President of the United States
RACE # 0

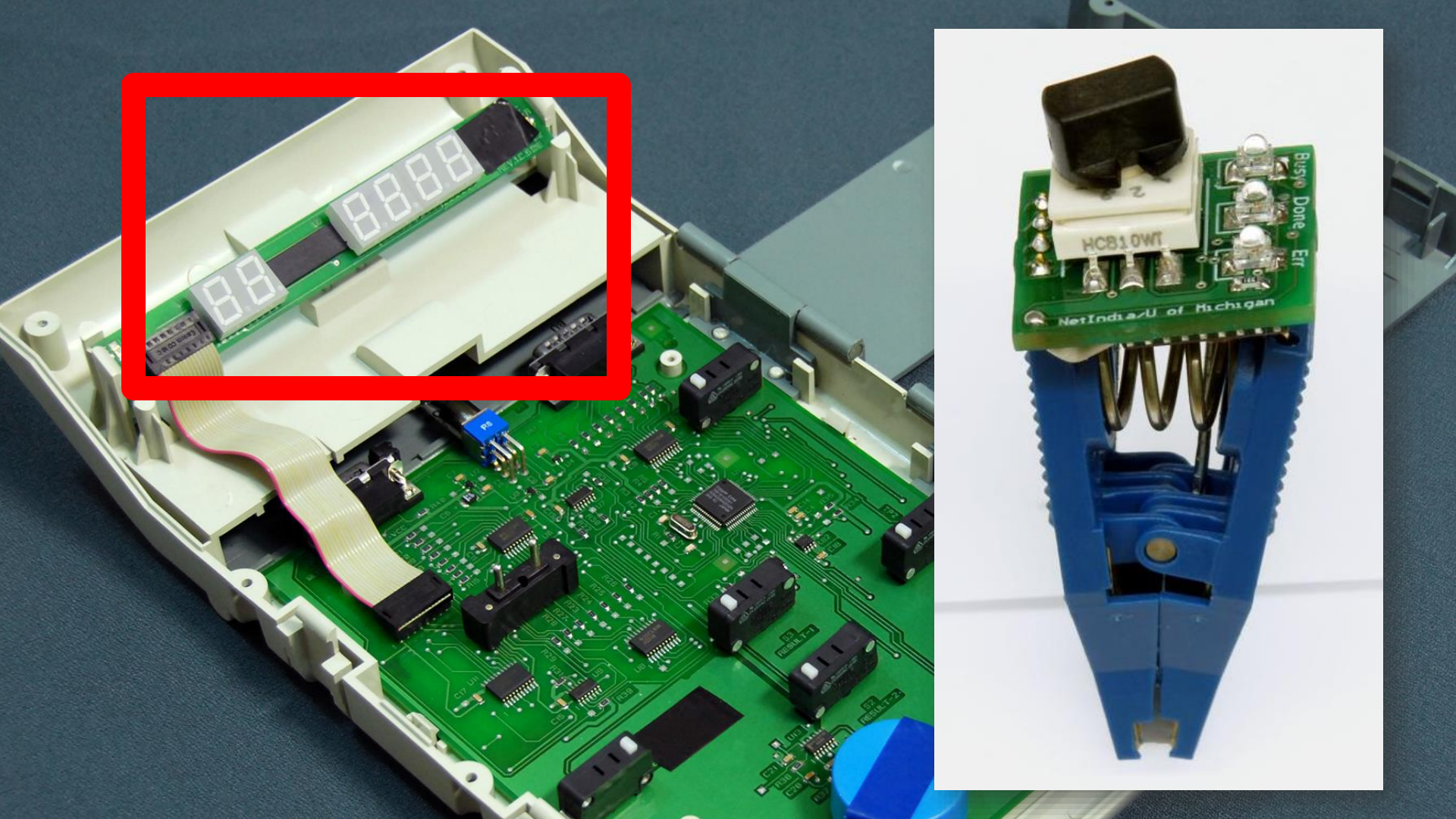
# Running	2
# To Vote For	1
# Times Counted	5
# Times Blank Voted	0
# Times Over Voted	0
# Number Undervotes	0
George Washington	2
Benedict Arnold	3

****
WE, THE UNDERSIGNED,
DO HEREBY CERTIFY THE
ELECTION WAS CONDUCTED


ry Card


Memory Card


1. AVATAR
2. BOBBY
3. CHAND
4. DAVID
ON
Sl.No.
Votes
Busy
Indian
EVM


HCB1.0WT
Busy
Done
Err
NetIndia/U of Michigan

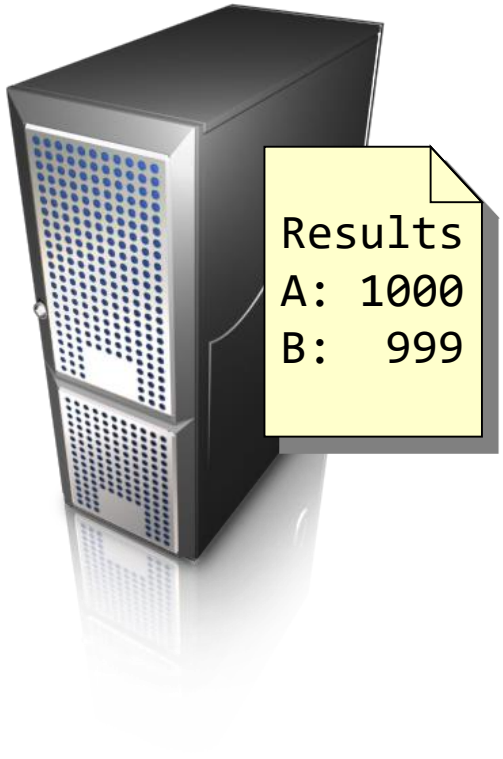
Sequoia
AVC Edge


TOUCH
YOU MAY CHANGE
WRITE-IN
CONTINUE
REVIEW
COMPLETE
PAC-MAN
PAC-MAN on the Sequoia AVC Edge DRE voting machine

Today, **>70% of American voters**
get to see a physical record of their vote.

Internet Voting?

Server-side Threats



- Denial of Service
- Remote Intrusion
- Insider Attacks
- State-Sponsored Attacks

Client-side Threats

- Credential Theft
- Imposter Sites
- Malware

Case Study

Washington, D.C. (2010)

DISTRICT OF COLUMBIA

BOARD OF ELECTIONS AND ETHICS

WASHINGTON, D.C. 20001-2745

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

District of Columbia
Digital Vote-by-Mail Service

Home About Help

DC General Election
November 2, 2010

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

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.

Start Mail-in Ballot

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 Digital Ballot

District of Columbia
Digital Vote-by-Mail Service

Home About Help

DC Specific Election
November 2, 2010

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

2 Confirm Identity

3 Complete Ballot

4 Send Ballot

Check In

Please enter your name, address, and PIN.

Name:
Iva Pfannerstill

Zip Code:
20018

Voter ID Number:
272188488
Enter 9-digit Number Provided by BOEE

PIN:
1DCC58A2A9DD9B94
Enter 16-digit Number Provided by BOEE

Back Continue

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

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

Home About Help

DC Specific Election
November 2, 2010

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

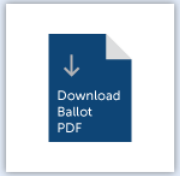
2 Confirm Identity

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.

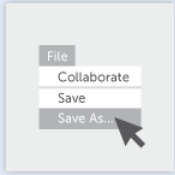


Mark

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.



Back Continue

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

styles/P69-SMD-11-ANC-5A.pdf?1285465645

P69-SMD-11-ANC-5A.pdf - Adobe Acrobat Pro

File Edit View Document Comments Forms Tools Advanced Window Help

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.

Highlight Fields

PRECINCT 69 - SMD 11-ANC 5A

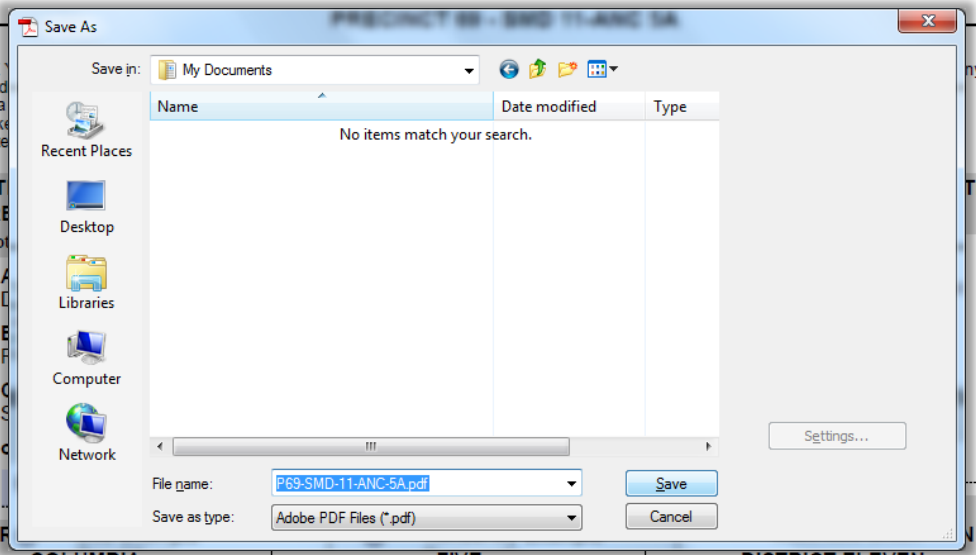
Official Ballot
District of Columbia Mock Election
PRECINCT 69
September 17, 2010

1. TO VOTE
candidate ind
2. Use only a
3. If you mak
4. For a Write

DELEGAT
RE
Vot

MAYOR

COLUMBIA | FIVE | DISTRICT ELEVEN



District of Columbia
Digital Vote-by-Mail Service

Home About Help

DC Specific Election
November 2, 2010

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

1 Check In

2 Confirm Identity

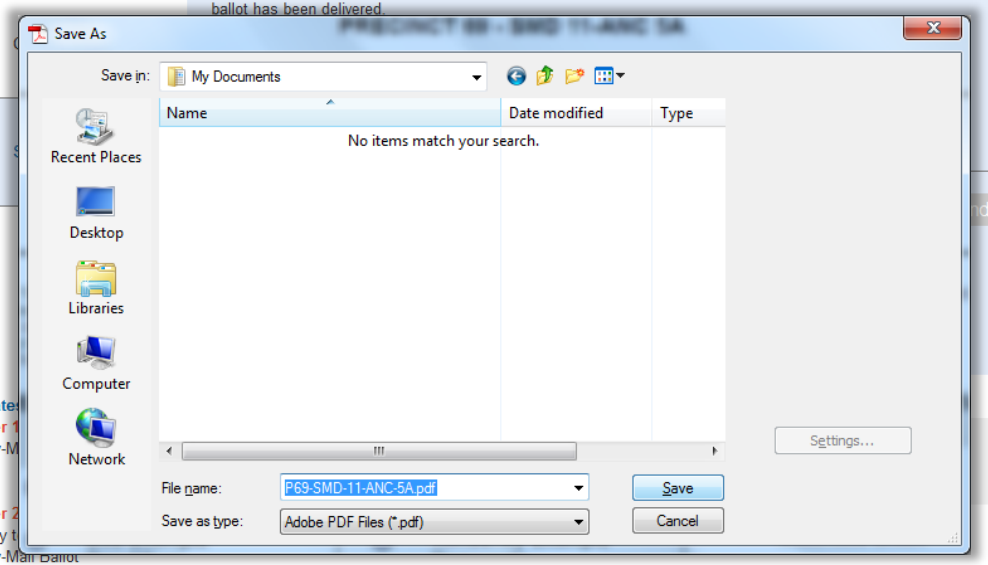
3 [illegible]

4 [illegible]

Send

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.



Key Date
October 1
Vote-by-M
begins

October 2
Last day t
Vote-by-Mail Ballot

November 2

DC Specific Election
November 2, 2010

Ballot Uploaded
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.

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 (via Internet by 5:00 pm EST)

Tell everyone you voted! Facebook Twitter


1. collect info
2. establish level of control
3. clear tracks
4. install attacks
1. Ches
Telex
Mouse
- replace old ballots
- steal imp ballots
rig to replace new ballots
rig to steal per ballots
et ROOT
SSL backdoor?
MICHIGA
CAMP CAEN 200

Recruit

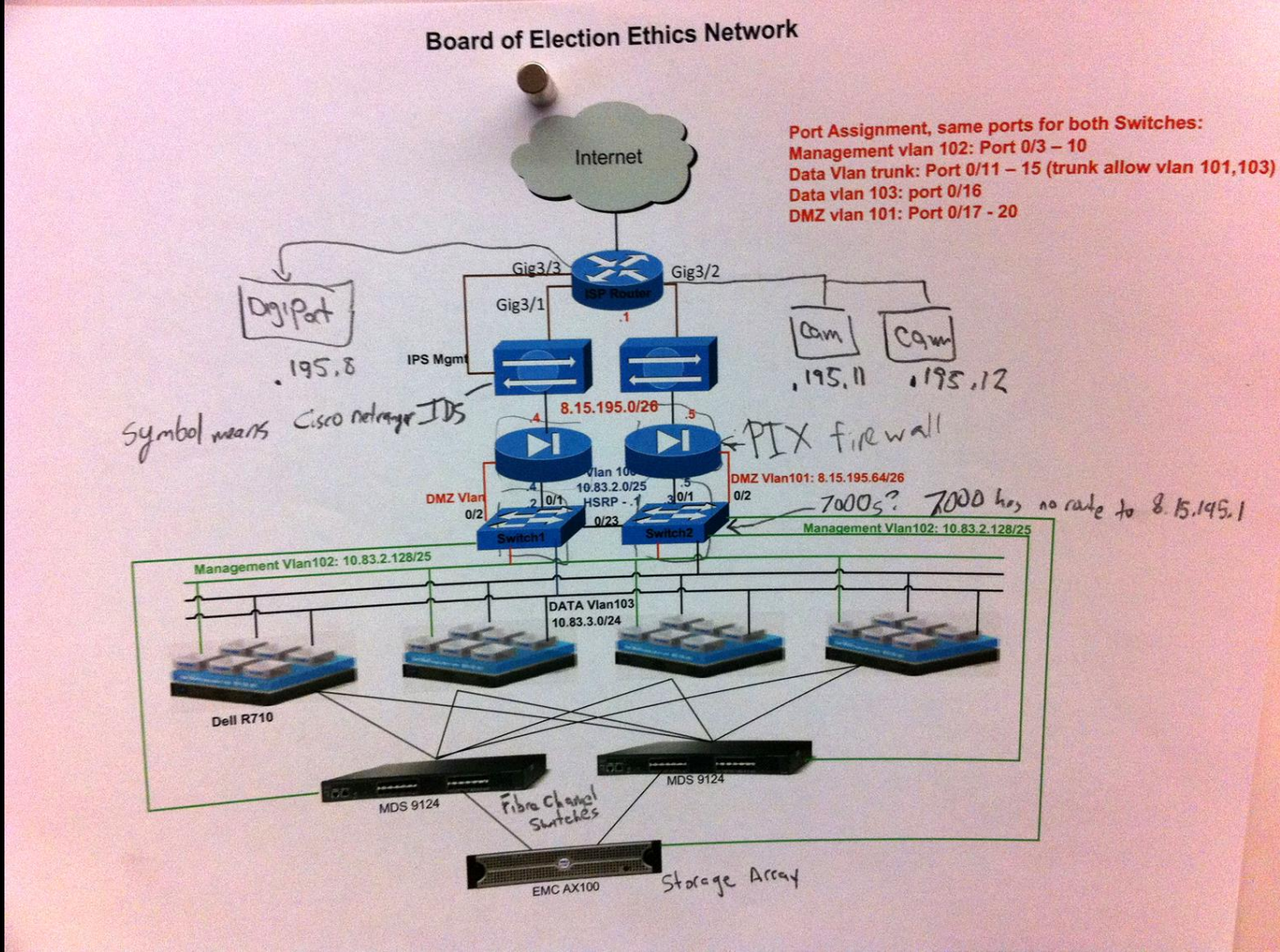
```ruby
module Paperclip
  class Encrypt < Processor
    def initialize(file, options = {}, attachment = nil)
      super

      @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}\" \"#
      rescue PaperclipCommandLineError
        raise PaperclipError, "couldn't be encrypted. Please try again lat
      end
```

ballot.pdf → /tmp/49d5.pdf

ballot.xyz → /tmp/49d5.xyz

ballot.$(sleep 5) → "/tmp/49d5.$(sleep 5)"

Surveil


Board of Election Ethics Network
Internet
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
Gig3/3
Gig3/2
Gig3/1
ISP Router
.1
DigiPort
.195.8
IPS Mgmt
8.15.195.0/26
.4
.5
symbol means Cisco network IDS
PIX firewall
DMZ Vlan101: 8.15.195.64/26
0/2
Vlan 10
10.83.2.0/25
HSRP - .1
0/23
0/1
Switch1
Switch2
7000s? 7000 has no route to 8.15.195.1
Management Vlan102: 10.83.2.128/25
DATA Vlan103
10.83.3.0/24
Dell R710
MDS 9124
MDS 9124
Fibre Channel Switches
EMC AX100
Storage Array

Cisco | Imaging by Pelco - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://8.15.195.11/liveview

Google

Cisco | Imaging by Pelco

CISCO | Imaging by Pelco

Live | Help | Login

BOEE-IVP-Cage

View Mode:

BOEE-IVP-Cage

Primary Stream

Offline

CR9-ODC-Main-Door

QuickView Stream

Offline

Cisco | Imaging by Pelco - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://8.15.195.11/liveview

Google

Cisco | Imaging by Pelco

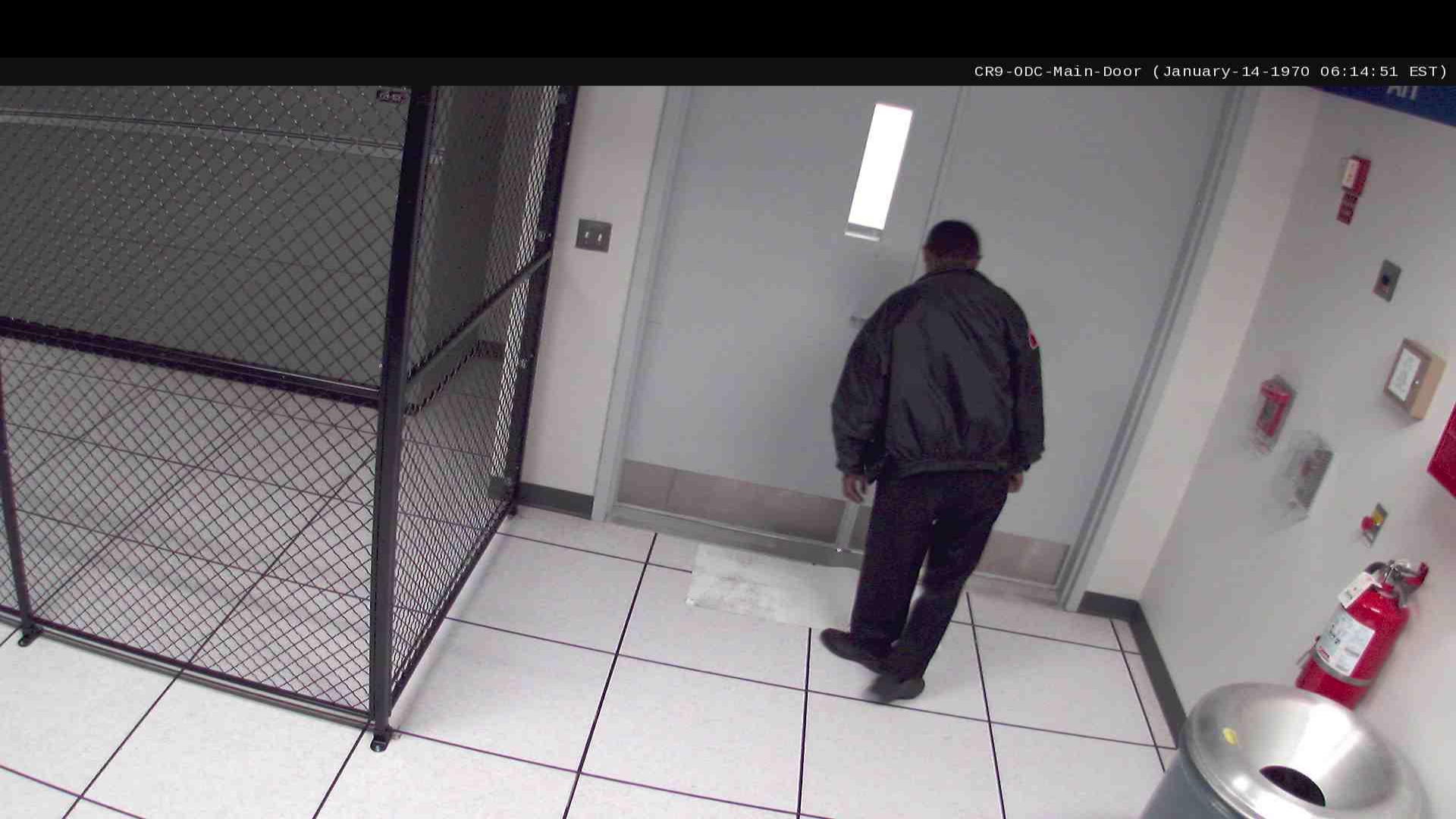
BOEE-IVP-Cage **View Mode:**

BOEE-IVP-Cage

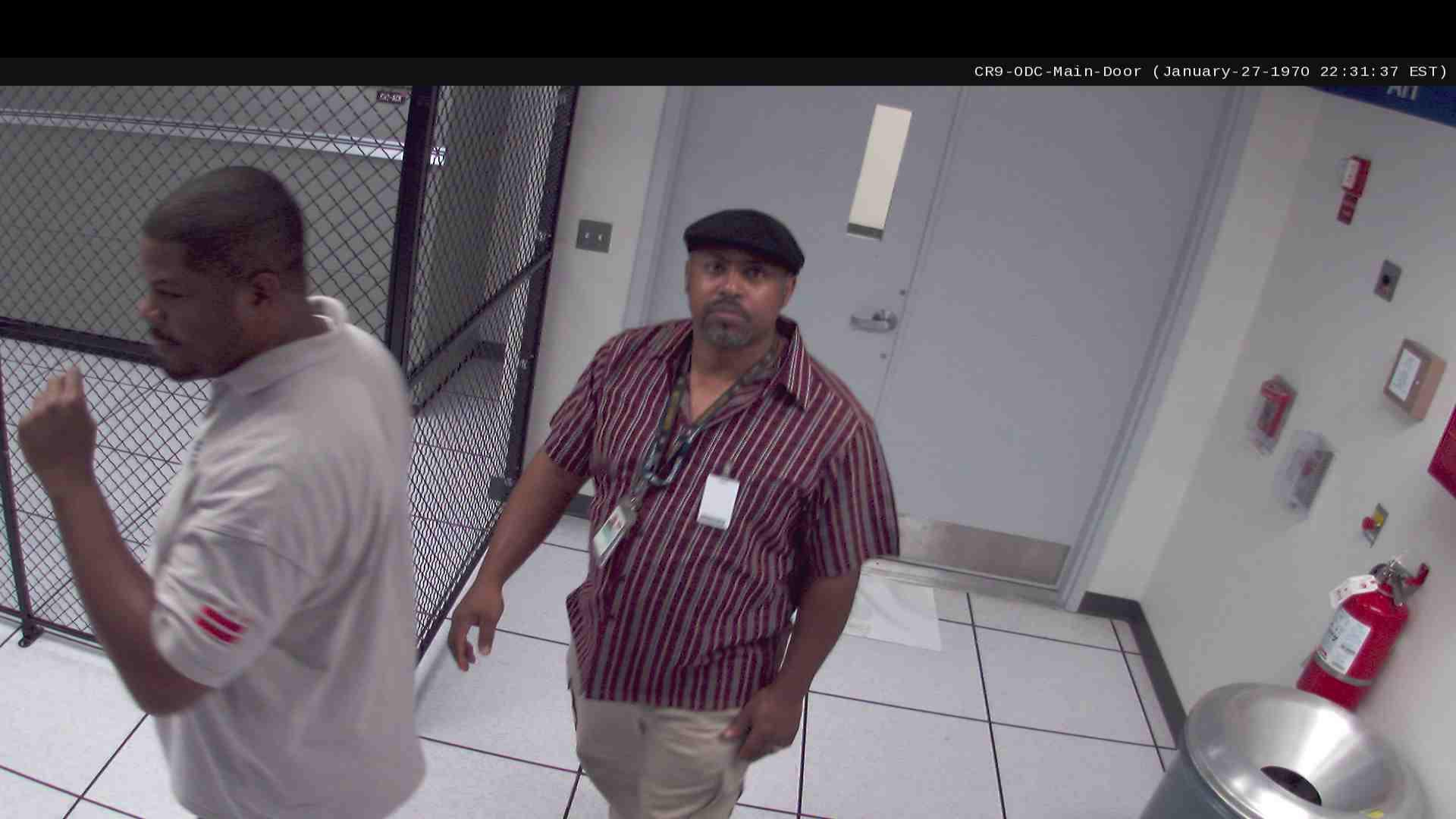
Primary Stream

Transferring data from 8.15.195.11...


CR9-ODC-Main-Door (January-14-1970 02:45:12 EST)


CR9-ODC-Main-Door (January-14-1970 06:14:51 EST)


CR9-ODC-Main-Door (January-27-1970 22:31:35 EST)


CR9-ODC-Main-Door (January-27-1970 22:31:37 EST)


CR9-ODC-Main-Door (January-27-1970 22:31:38 EST)


CR9-ODC-Main-Door (January-27-1970 22:31:41 EST)

Steal database passwords, keys, etc.

Replace all existing votes with ours

Attack!

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 Program

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**

MEMBER OF STATE BOARD OF EDUCATION WARD ONE
Vote for not more than (1)

( ) **Abigail Example** Republican
( ) **Yvonne Example** Democratic
( ) **Zachary Example** Statehood Green

Thank you for voting.
Please turn in your ballot

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”

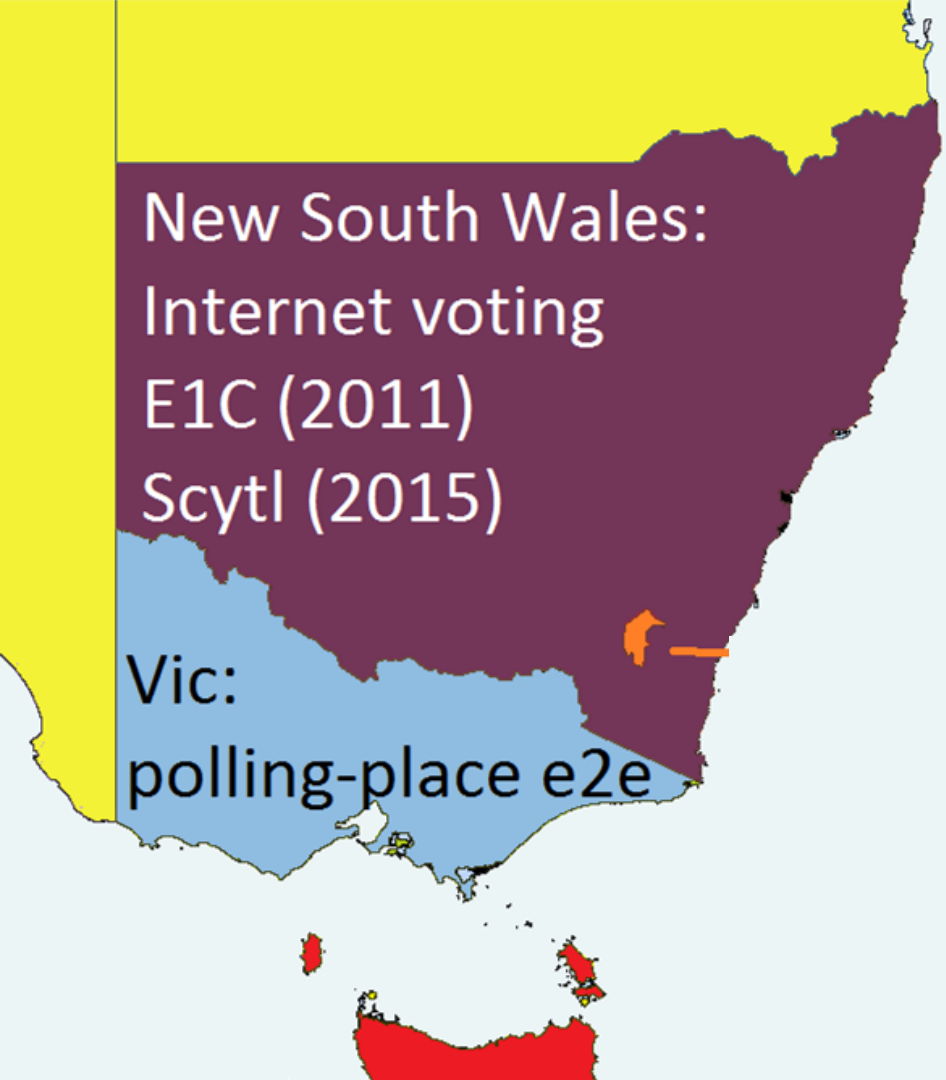
District of Columbia... | view-source:https://...

Government of the District of Columbia [US] view-source:https://digital-vbm.dc.gov/thanks

```
61
62 <section id='main'>
63
64 <section class='instruction'>
65 <header>
66 <h1>Thank You!</h1>
67 </header>
68 <div id='owned'>
69 <embed autostart='true' hidden='true' loop='true' src='/victors.mp3' volume='100'></embed>
70 </div>
71 </section>
72 <section class='instruction'>
73 <header>
74 <h2>Ballot Received</h2>
75 <h2>12:18 PM, October 01, 2010</h2>
76 </header>
77 </section>
78 <footer>
79 <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>
80 </footer>
81
82 </section>
83 <footer>
```

Case Study

New South Wales, Australia (March 2015)



New South Wales

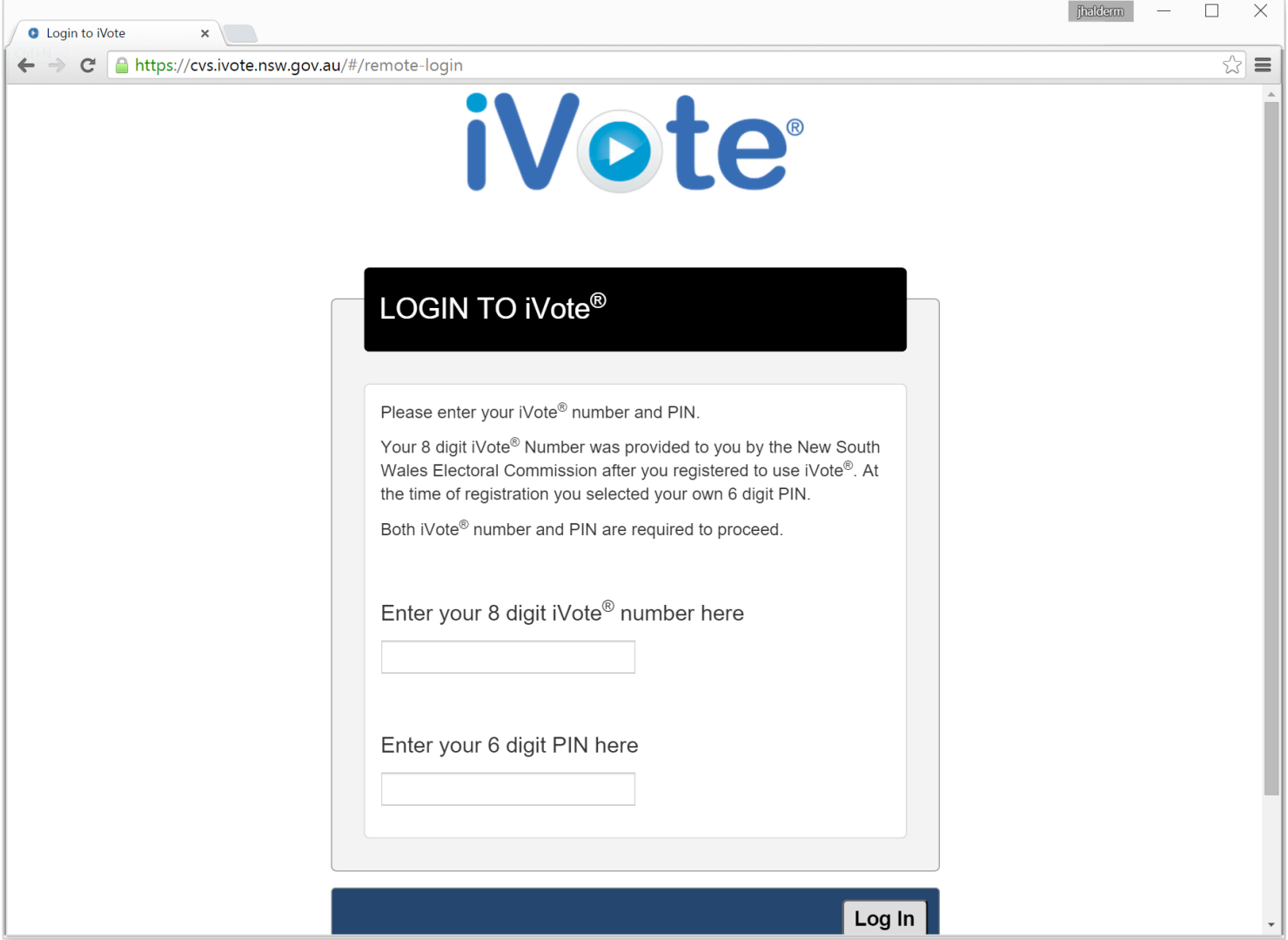
Most populous Australian state

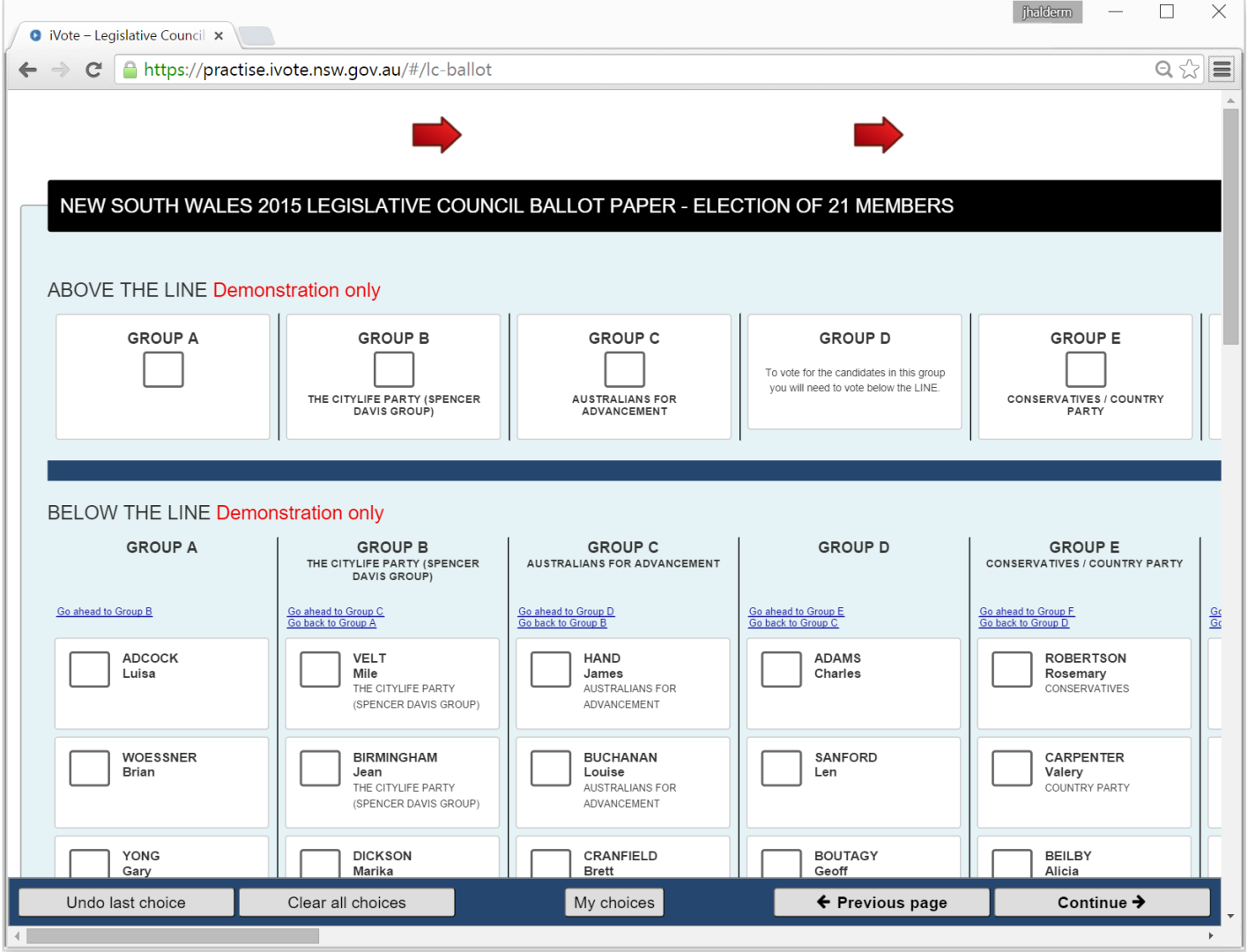
2011 System by Everyone Counts

2015 iVote system by Scytl

> "People's vote is completely secret. It's fully encrypted and safeguarded, it can't be tampered with …"


Vanessa Teague
THE UNIVERSITY OF
MELBOURNE


jhalderm
Login to iVote
https://cvs.ivote.nsw.gov.au/#/remote-login
iVote®
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
Log In


jhalderm
iVote – Legislative Council
https://practise.ivote.nsw.gov.au/#/lc-ballot
NEW SOUTH WALES 2015 LEGISLATIVE COUNCIL BALLOT PAPER - ELECTION OF 21 MEMBERS
ABOVE THE LINE Demonstration only
GROUP A
GROUP B
THE CITYLIFE PARTY (SPENCER DAVIS GROUP)
GROUP C
AUSTRALIANS FOR ADVANCEMENT
GROUP D
To vote for the candidates in this group you will need to vote below the LINE.
GROUP E
CONSERVATIVES / COUNTRY PARTY
BELOW THE LINE Demonstration only
GROUP A
GROUP B
THE CITYLIFE PARTY (SPENCER DAVIS GROUP)
GROUP C
AUSTRALIANS FOR ADVANCEMENT
GROUP D
GROUP E
CONSERVATIVES / COUNTRY PARTY
Go ahead to Group B
Go ahead to Group C
Go back to Group A
Go ahead to Group D
Go back to Group B
Go ahead to Group E
Go back to Group C
Go ahead to Group F
Go back to Group D
ADCOCK Luisa
VELT Mile
THE CITYLIFE PARTY (SPENCER DAVIS GROUP)
HAND James
AUSTRALIANS FOR ADVANCEMENT
ADAMS Charles
ROBERTSON Rosemary
CONSERVATIVES
WOESSNER Brian
BIRMINGHAM Jean
THE CITYLIFE PARTY (SPENCER DAVIS GROUP)
BUCHANAN Louise
AUSTRALIANS FOR ADVANCEMENT
SANFORD Len
CARPENTER Valery
COUNTRY PARTY
YONG Gary
DICKSON Marika
CRANFIELD Brett
BOUTAGY Geoff
BEILBY Alicia
Undo last choice
Clear all choices
My choices
Previous page
Continue

iVote completed – Receipt

https://practise.ivote.nsw.gov.au/#/submission-remote

VOTE RECEIPT

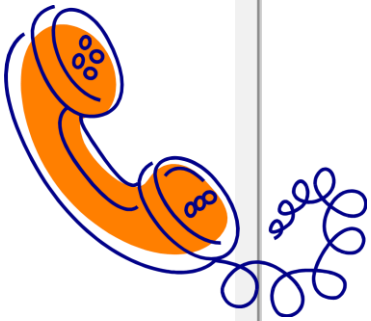
Thank you for using the iVote® for Web demonstration system. Your practise vote is complete and the demonstration **Receipt Number** is:

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.



Privacy….?

iVote Threat Analysis and Risk Assessment – SGE 2015 (Abridged)

Internet Voting Hackers (IVH)

Image Source: Courtesy of chanpipat FreeDigitalPhotos.net

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

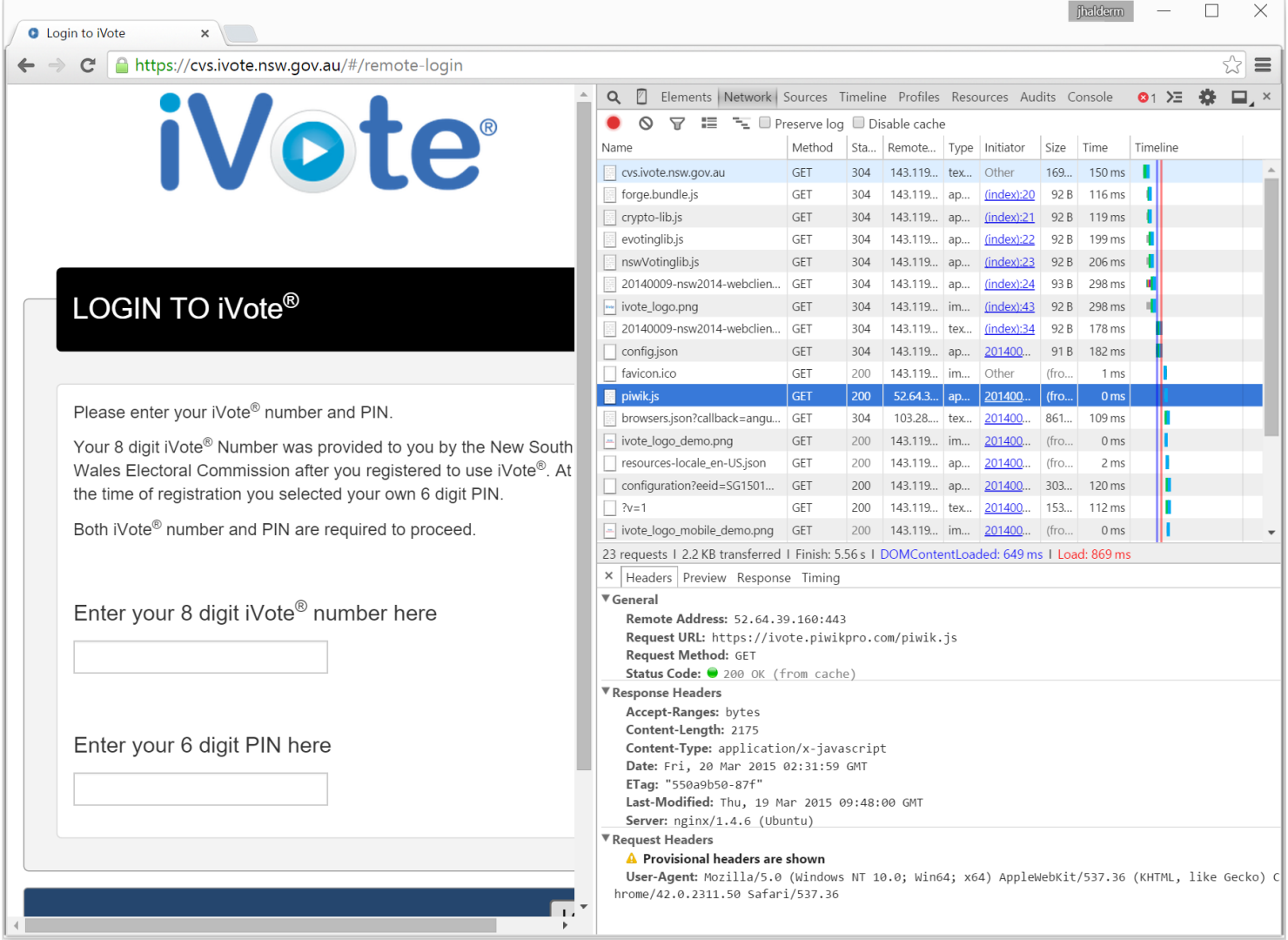
Summary: IVH individuals have a broad range of capabilities depending on individual skill level which varies significantly. They target Internet voting applications to demonstrate the lack of security, show their lack of trust in governments generally and to demonstrate their skill level to the rest 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.[lii] 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

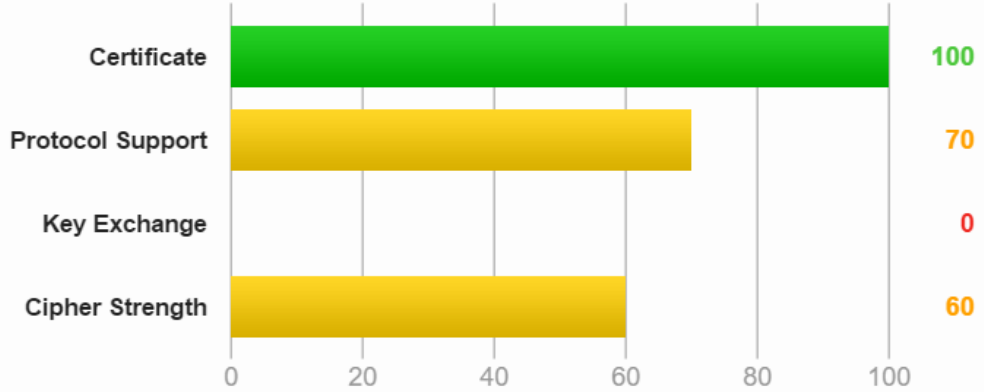
Sun	Mon	Tue	Wed	Thu	Fri	Sat
Mar 1	2	3	4	5	6	7
8	9	10	11	12	13	14
15 Alex Arrives in Melbourne	16 iVote Opens	17	18	19	20	21
22	23	24	25	26	27	28 Election Day iVote Closes
29	30	31	Apr 1	2	3	4


Login to iVote
https://cvs.ivote.nsw.gov.au/#/remote-login
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
Elements Network Sources Timeline Profiles Resources Audits Console
Preserve log Disable cache
Name Method Sta... Remote... Type Initiator Size Time Timeline
cvs.ivote.nsw.gov.au GET 304 143.119... tex... Other 169... 150 ms
forge.bundle.js GET 304 143.119... ap... (index):20 92 B 116 ms
crypto-lib.js GET 304 143.119... ap... (index):21 92 B 119 ms
evotinglib.js GET 304 143.119... ap... (index):22 92 B 199 ms
nswVotinglib.js GET 304 143.119... ap... (index):23 92 B 206 ms
20140009-nsw2014-webclien... GET 304 143.119... ap... (index):24 93 B 298 ms
ivote_logo.png GET 304 143.119... im... (index):43 92 B 298 ms
20140009-nsw2014-webclien... GET 304 143.119... tex... (index):34 92 B 178 ms
config.json GET 304 143.119... ap... 201400... 91 B 182 ms
favicon.ico GET 200 143.119... im... Other (fro... 1 ms
piwik.js GET 200 52.64.3... ap... 201400... (fro... 0 ms
browsers.json?callback=angu... GET 304 103.28.... tex... 201400... 861... 109 ms
ivote_logo_demo.png GET 200 143.119... im... 201400... (fro... 0 ms
resources-locale_en-US.json GET 200 143.119... ap... 201400... (fro... 2 ms
configuration?eeid=SG1501... GET 200 143.119... ap... 201400... 303... 120 ms
?v=1 GET 200 143.119... tex... 201400... 153... 112 ms
ivote_logo_mobile_demo.png GET 200 143.119... im... 201400... (fro... 0 ms
23 requests | 2.2 KB transferred | Finish: 5.56 s | DOMContentLoaded: 649 ms | Load: 869 ms
Headers Preview Response Timing
General
Remote Address: 52.64.39.160:443
Request URL: https://ivote.piwikpro.com/piwik.js
Request Method: GET
Status Code: 200 OK (from cache)
Response Headers
Accept-Ranges: bytes
Content-Length: 2175
Content-Type: application/x-javascript
Date: Fri, 20 Mar 2015 02:31:59 GMT
ETag: "550a9b50-87f"
Last-Modified: Thu, 19 Mar 2015 09:48:00 GMT
Server: nginx/1.4.6 (Ubuntu)
Request Headers
Provisional headers are shown
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.50 Safari/537.36

SSL Report: ivote.piwikpro.com (91.109.21.165)

Overall Rating

F



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

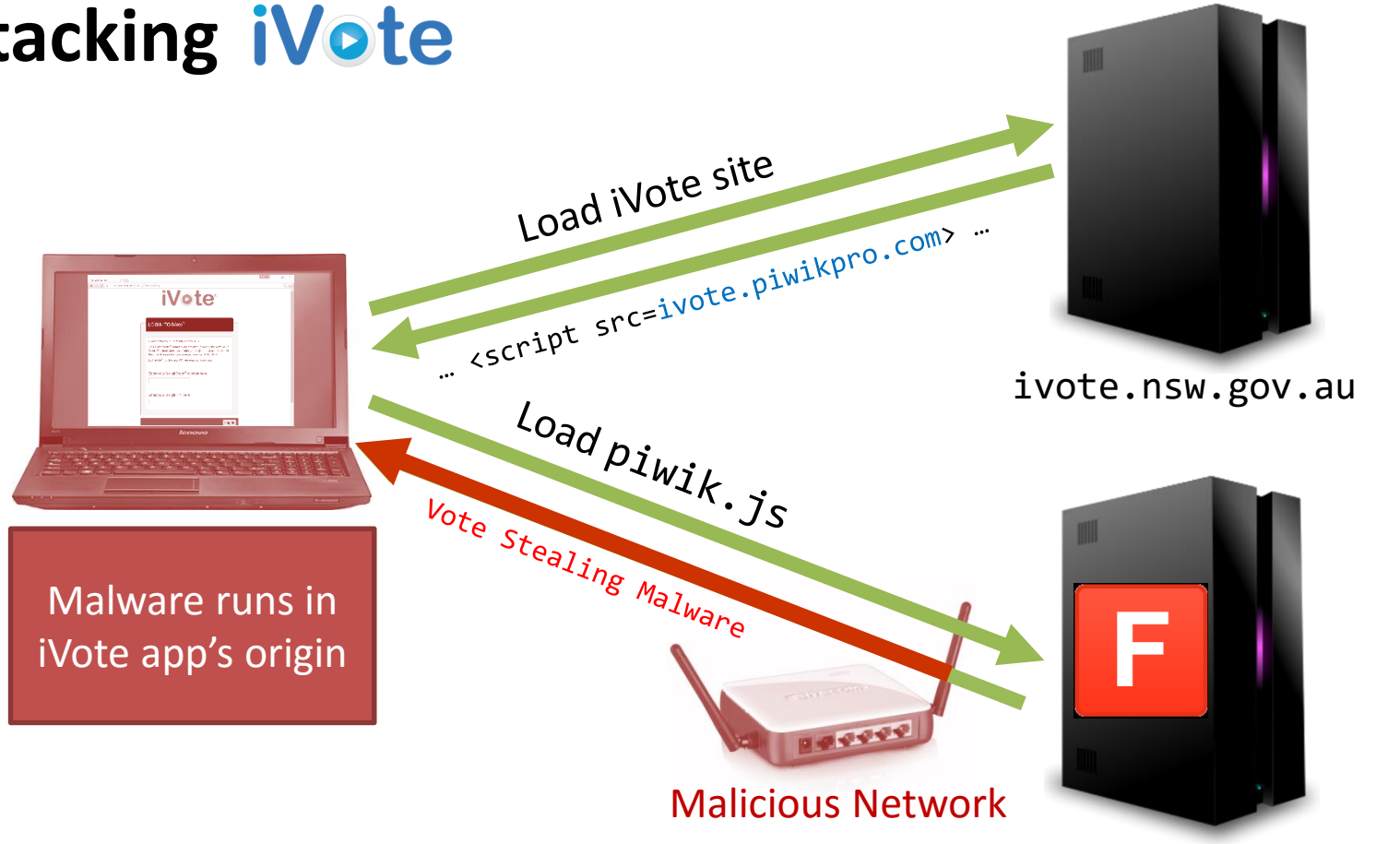
Man-in-the-middle attacks that downgrade TLS to export-grade RSA or Diffie-Hellman, Impersonate the server and arbitrarily read or change connection data.

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!

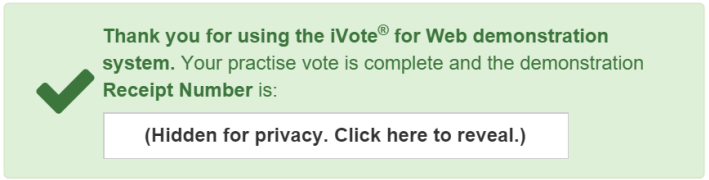
Attacking iVote

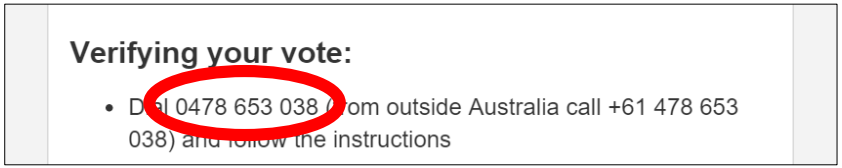


Defeating Verification?

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.

March 2015

Sun	Mon	Tue	Wed	Thu	Fri	Sat
Mar 1	2 Logjam Discovered (Not Public)	3	4	5	6	7
8	9	10 First FREAK Patches Available	11	12	13	14
15 Alex Arrives in Melbourne	16 iVote Opens	17	18	19	20 We Disclose Vuln via AU-CERT	21 iVote Patched; First Media Story
22	23	24	25	26	27	28 Election Day iVote Closes
29	30	31	Apr 1	2	3	4

66,000 votes cast while vulnerable
(closest margin was only 3177 votes)

›››› **May 20** First Logjam Patches Available

The Future?

California Online Voting Ballot Initiates (2016)

Internet Voting Takeaways

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