

Security Analysis of the
Estonian Internet Voting System



J. Alex Halderman
University of Michigan

Based on joint work with:

Drew Springall

Travis Finkenauer

Zakir Durumeric

Jason Kitcat

Harri Hursti

Margaret MacAlpine

Security Analysis of the Estonian Internet Voting System.
*Proc. 21st ACM Conference on Computer and Communications
Security (CCS '14)*, Scottsdale, AZ, November 2014.

E-Voting?

Integrity

The outcome matches voter intent.

Votes are cast as intended.

Votes are counted as cast.

Security Requirements

Integrity

Ballot Secrecy

Weak form:

Nobody can figure out how you voted...

Strong form:

...even if you try to prove it to them.

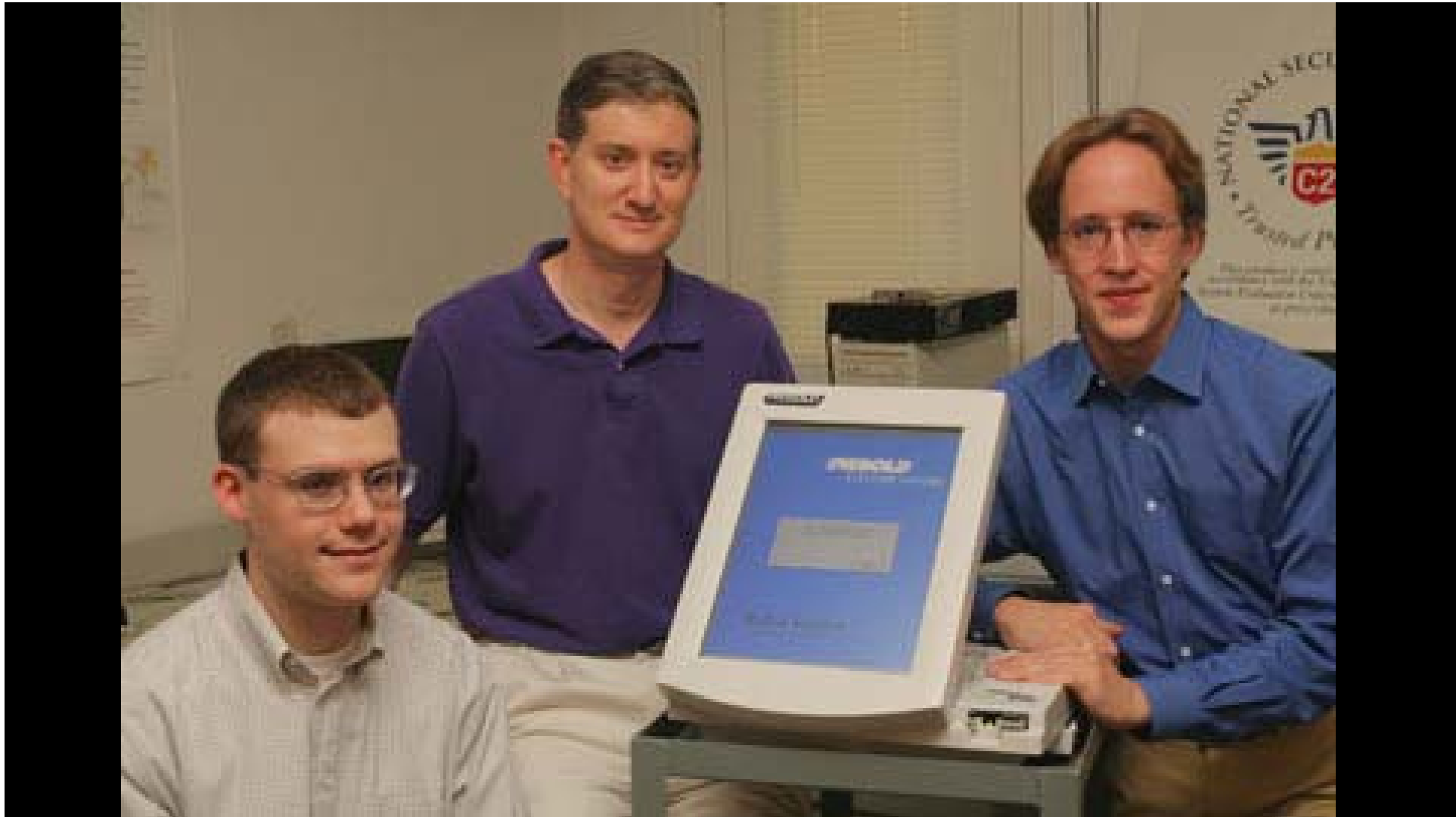
Security Requirements

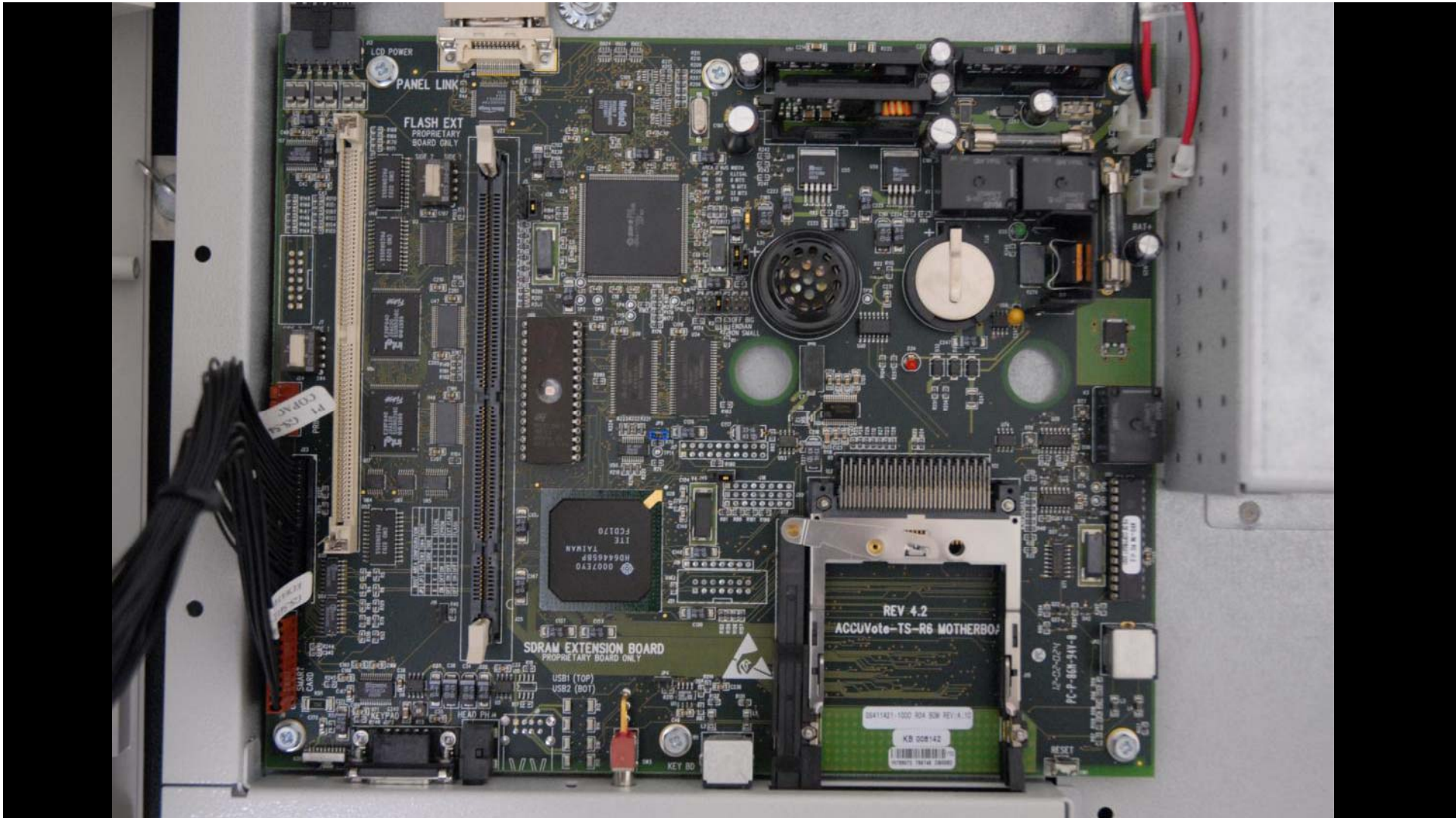
- Integrity
- Ballot Secrecy

Integrity  **Ballot Secrecy**

**Diebold
AccuVote-TS**









Primary Vote Record

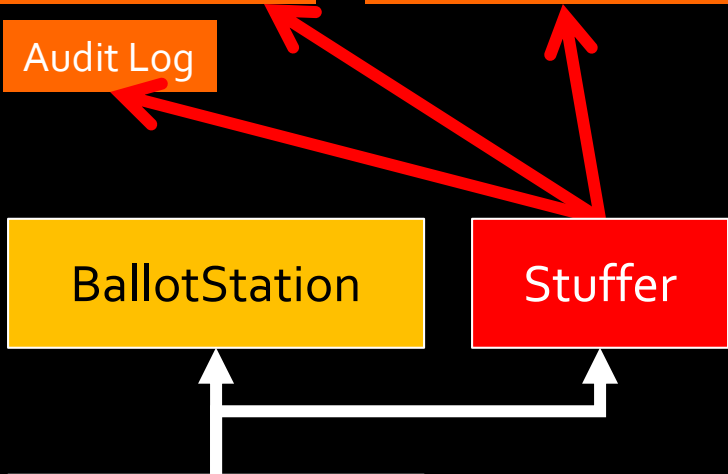
Backup Vote Record

Audit Log

BallotStation

Stuffer

WinCE Kernel



PRINCETON BALLOT STUFFER DEMO

Select the race and candidate to fix:

President of the United States

Candidate Name	Votes So Far
George Washington	0 (0%)
Benedict Arnold	0 (0%)

Set the final outcome: Percent for "Benedict Arnold"



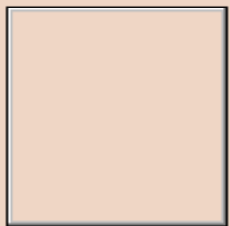
OK

Cancel

President of the United States



George Washington
Framers Party



Benedict Arnold
Redcoat Party

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

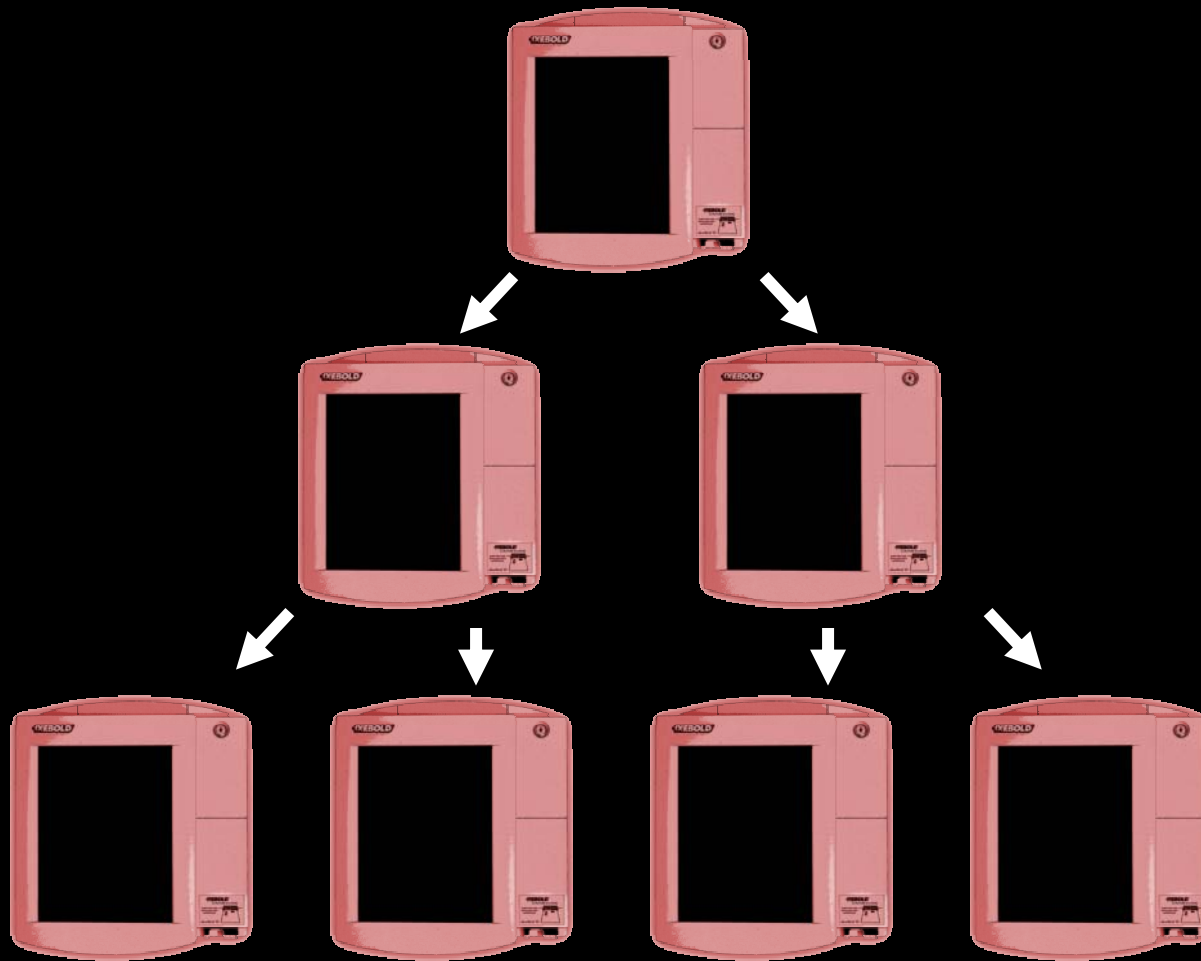
Benedict Arnold 3

WE, THE UNDERSIGNED,

DO HEREBY CERTIFY THE

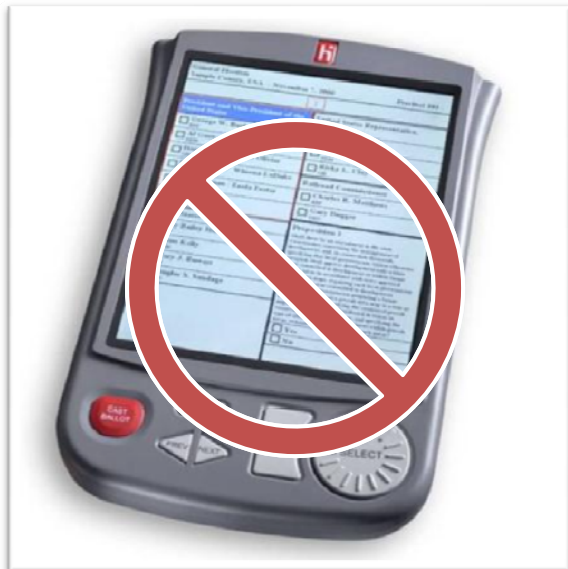
ELECTION WAS CONDUCTED

IN ACCORDANCE WITH THE





Hart



Sequoia



Diebold





NEDAP ES3B



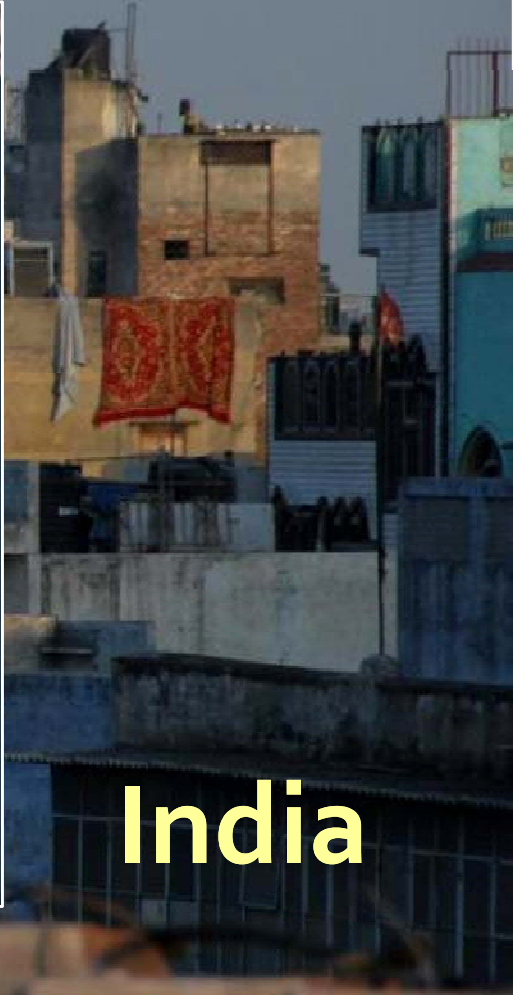
NEDAP ES3B

**Sequoia
AVC Edge**



Sequoia AVC Edge





India









Internet Voting?

Client-side Threats



Coercion

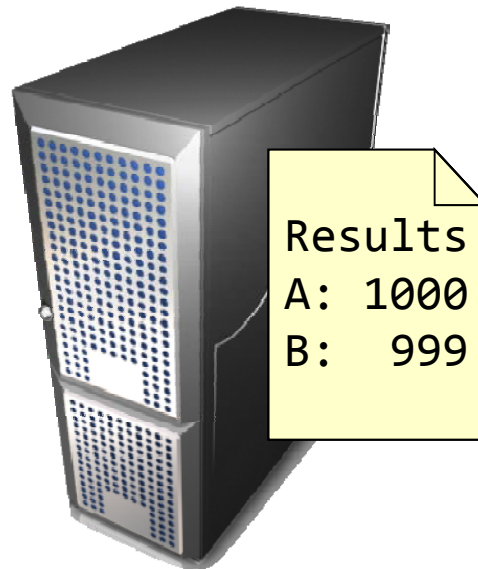
Credential Theft

Imposter Sites

Malware

Botnets

Server-side Threats



Denial of Service

Insider Attacks

Remote Intrusion

State-Sponsored Attacks



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@dcoee.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



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.

[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](#)

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



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.



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

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)

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

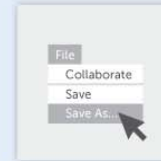
To complete the ballot online, click on the circles next to your candidates to select them. You can also type in candidates where indicated.



Save

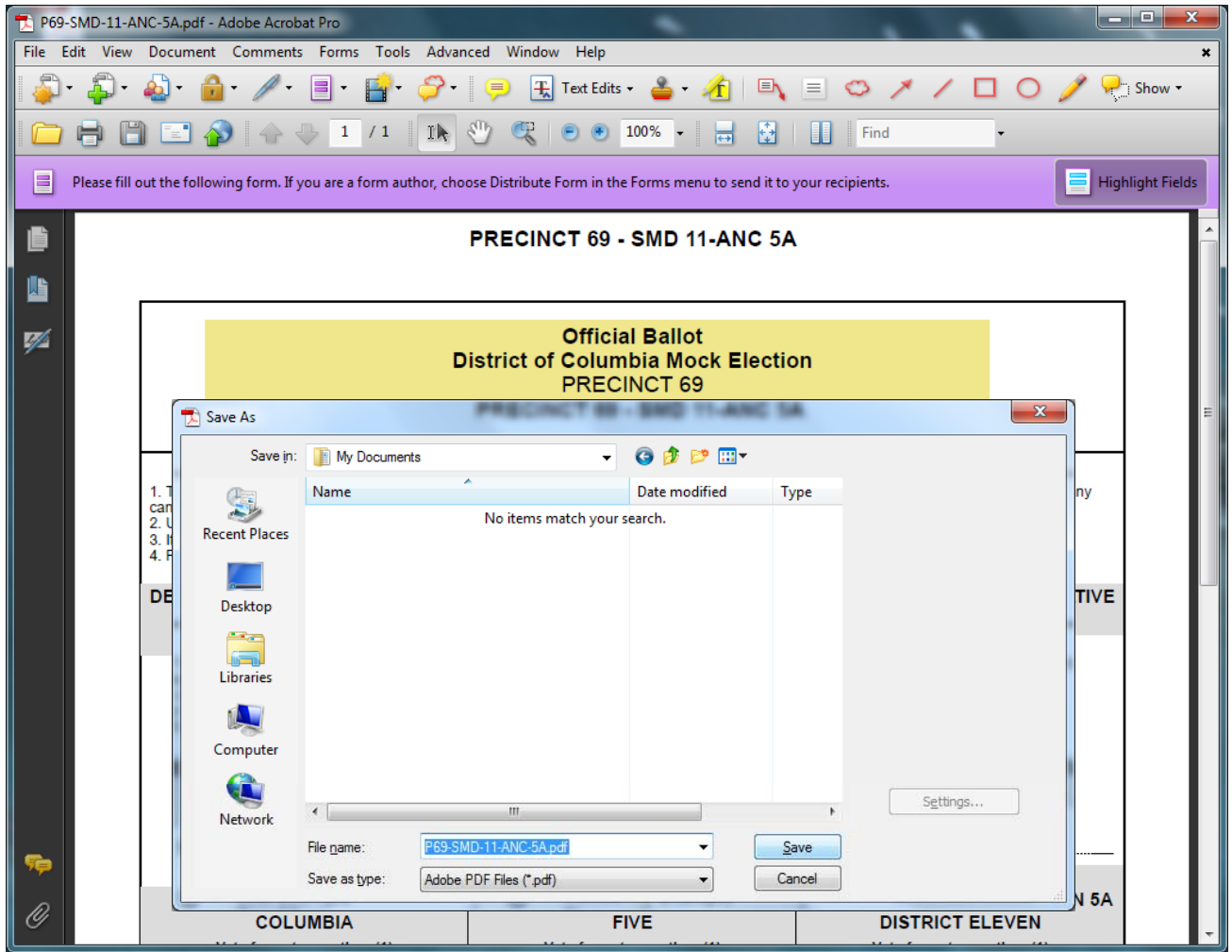
Save Your Ballot

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



DC Specific Election
November 2, 2010

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

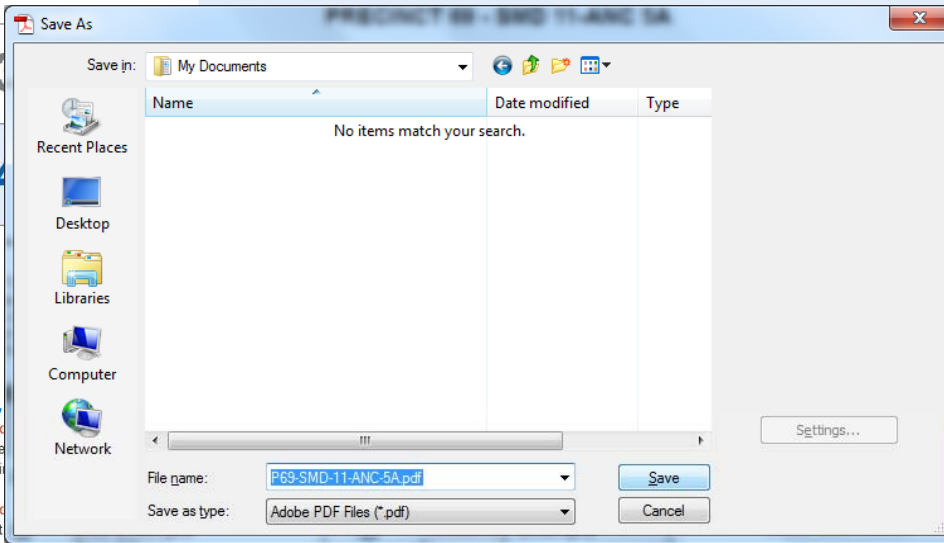
1 Check In

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.

2 Confirm Identity



Key
Oct
Vote
begi
Oct
Last
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 mto (removal)
- ✓ 2. establish level of control
- ✓ 3. clear tracks
- ✓ 4. install attacks

↓

~~replace old ballots~~

~~steal trap ballots~~

~~rig to replace new ballots~~

~~rig to steal new ballots~~

at ROOT?

refactor

~~SSL cert?~~

SSL backend?

1. Ches
Telex
Mouse

fr
d

MICHIGAN
CAMP CAEN 200

```

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 later"
      end
    end
  end

```

ballot.pdf → /tmp/49d5.pdf

ballot.xyz → /tmp/49d5.xyz

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

Surveil

Memo!
Part 1 of
Alas

Georgia

Switch TODO

1. get Port ↔ Computer map (arp?) main? 172.16.1.4
2. Find VFN
3. Tunnel 172.16.1.5

Port 3

5010-01

Eth 1/5
Eth 1/6
Eth 1/2
Eth 1/1

Port 4

5010-02

Eth 1/5
Eth 1/6
Eth 1/1
Eth 1/2

Vlan 2
172.16.1.6
/24

Port 1

7010-01

Eth 2/2
Eth 2/4
Eth 2/1
Eth 9/1
Eth 2/6

Port 2

7010-02

Eth 2/2
Eth 2/1
Eth 9/1
Eth 2/6

Alex is crazy:
HIT 1

A: Contacts
S: SU
M: HW?
A: what w/ lan
E: Look into Infest.

1. Find collision - in loop
2. Find size of loop (L)
3. Find collision: $L-1=5$

Cisco | Imaging by Pelco - Mozilla Firefox


File Edit View History Bookmarks Tools Help

http://8.15.195.11/liveview

Cisco | Imaging by Pelco


BOEE-IVP-Cage Live Help Login View Mode:

BOEE-IVP-Cage



Primary Stream Offline

CR9-ODC-Main-Door



QuickView Stream Offline

The image shows a web browser window displaying a live video monitoring interface. The browser title is "Cisco | Imaging by Pelco - Mozilla Firefox" and the address bar shows "http://8.15.195.11/liveview". The page header includes the Cisco and Pelco logos, the text "BOEE-IVP-Cage", and navigation links for "Live", "Help", and "Login". There are also "View Mode" controls with three icons. The main content area is divided into two panels. The left panel, titled "BOEE-IVP-Cage", shows a "Primary Stream" of a server room with a metal cage. Below the video is an "Offline" status indicator. The right panel, titled "CR9-ODC-Main-Door", shows a "QuickView Stream" of a hallway with two people walking. Below this video is also an "Offline" status indicator. Both video players have a small icon with a red 'X' at the bottom center, indicating a connection issue.

Cisco | Imaging by Pelco - Mozilla Firefox

File Edit View History Bookmarks Tools Help

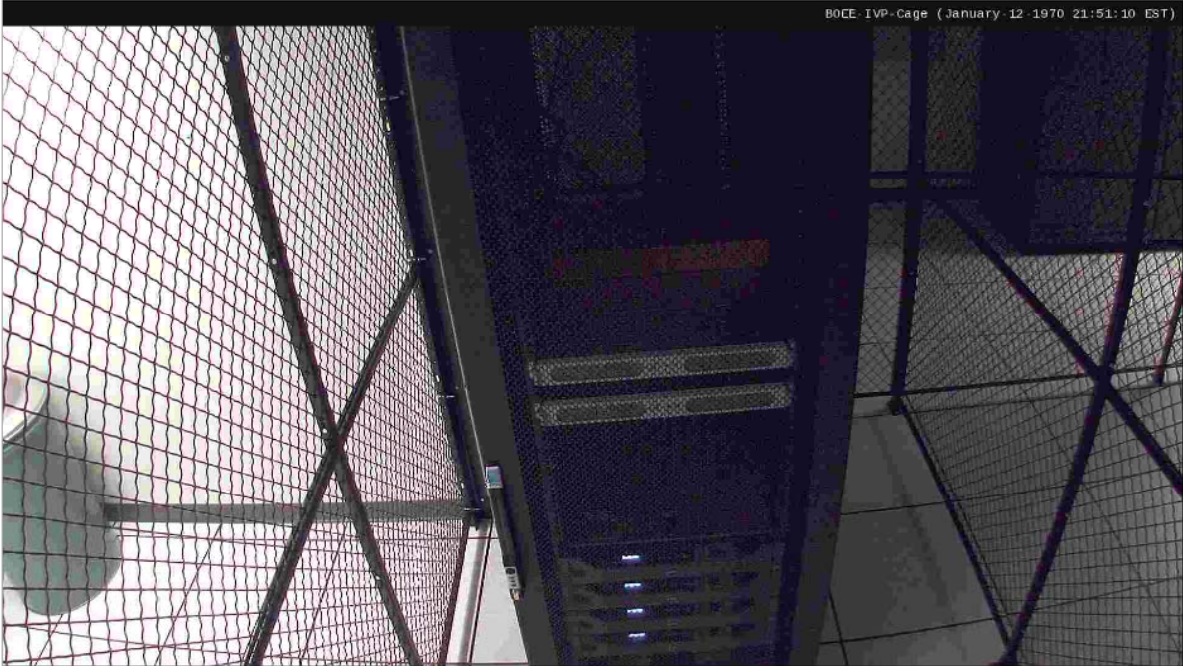
http://8.15.195.11/liveview

Cisco | Imaging by Pelco

BOEE-IVP-Cage

View Mode: [Icons]

BOEE-IVP-Cage (January 12 1970 21:51:10 EST)



Primary Stream [Icons]

Transferring data from 8.15.195.11...

The image shows a live video stream from a server room. The view is through a chain-link fence, looking into a dark aisle where server racks are visible. The racks have some blue indicator lights. The video player interface includes a title bar, menu, address bar, and a status bar at the bottom.

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!

Steal database passwords, keys, etc.

Replace all existing votes with ours

Replace any new votes

Back door to reveal new votes

Attack!

Clear logs

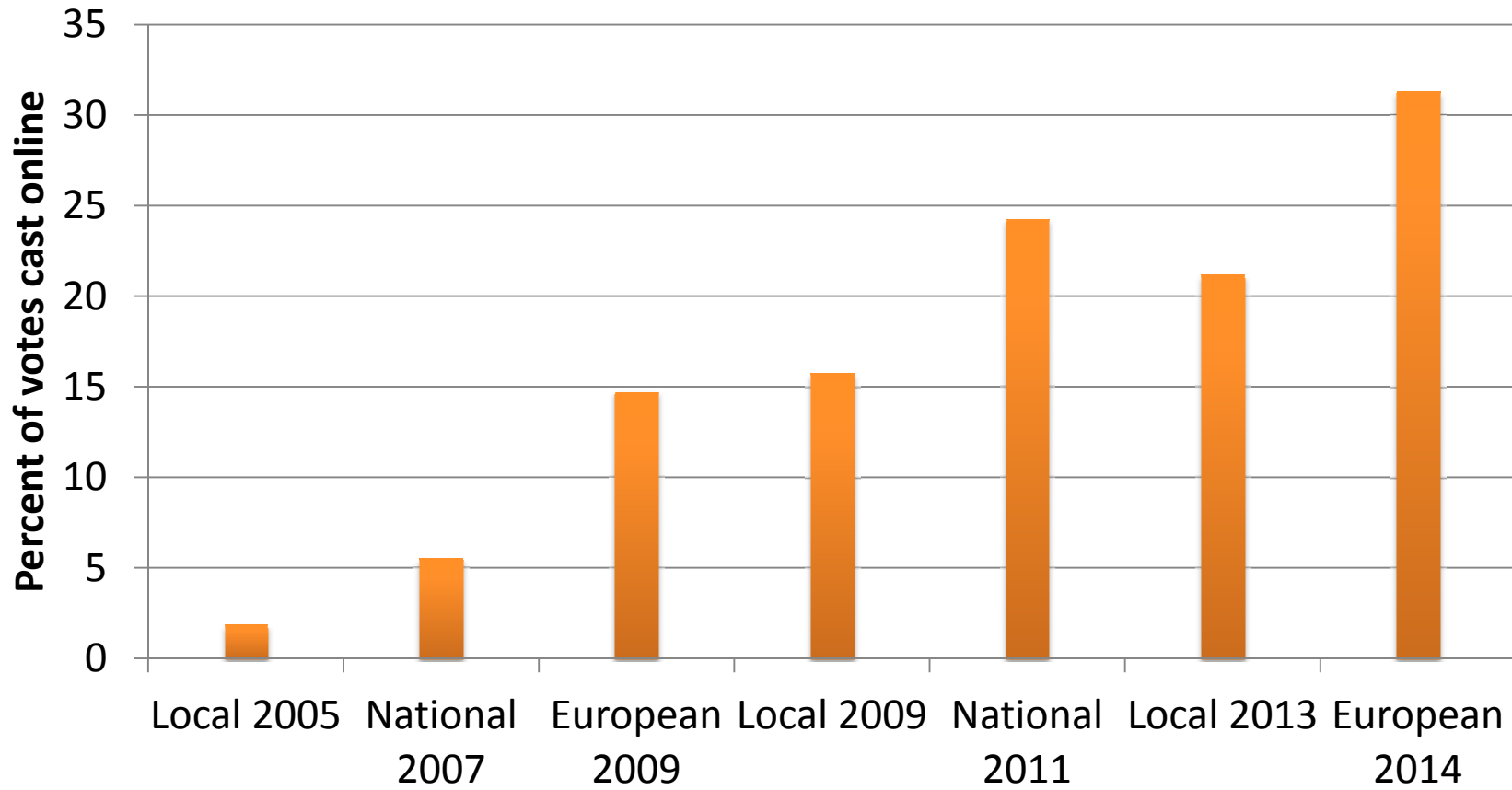
“Calling card”

```
District of Columbia... x view-source:https://... x +
Government of the District of Columbia [US] view-source:https://digital-vbm.dc.gov/thanks ☆ 🔍
81
82 <section id='main'>
83
84 <section class='instruction'>
85 <header>
86 <h1>Thank You!</h1>
87 </header>
88 <div id='owned'>
89 <embed autostart='true' hidden='true' loop='true' src='/victors.mp3' volume='100'></embed>
90 </div>
91 </section>
92 <section class='instruction'>
93 <header>
94 <h2>Ballot Received</h2>
95 <h2>12:18 PM, October 01, 2010</h2>
96 </header>
97 </section>
98 <footer>
99 <p>Check the status of your ballot at any time at the Board of Elections and Ethics <a
100 href='http://www.dcboee.us/' target='_blank'>website</a>.</p>
101 </footer>
102 </section>
103 <footer>
```

Internet Voting in Estonia



Internet Voting in Estonia



Estonia gets to vote online. Why can't America?

BY BRAD PLUMER November 6, 2012 at 3:26 pm



More ▾

Comments

If anecdotal reports are anything to go by, millions of Americans on Tuesday [are standing in the cold for hours](#) to vote at their local polling places. But why should they have to? Many Americans can already pay their utilities online and bank online. Why can't we vote over the Internet as well?

That's the question raised by Thad Hall, a political scientist and author of [Electronic Elections](#). In theory, he says, allowing Americans to vote online could have all sorts of benefits. We wouldn't



Has Estonia solved the hard security problems of Internet voting?

What is a realistic threat model for a national Internet voting system?

What can other countries learn from Estonia's experience?



VAATLEJATUNNISTUS

Kohaliku omavalitsuse volikogu valimised

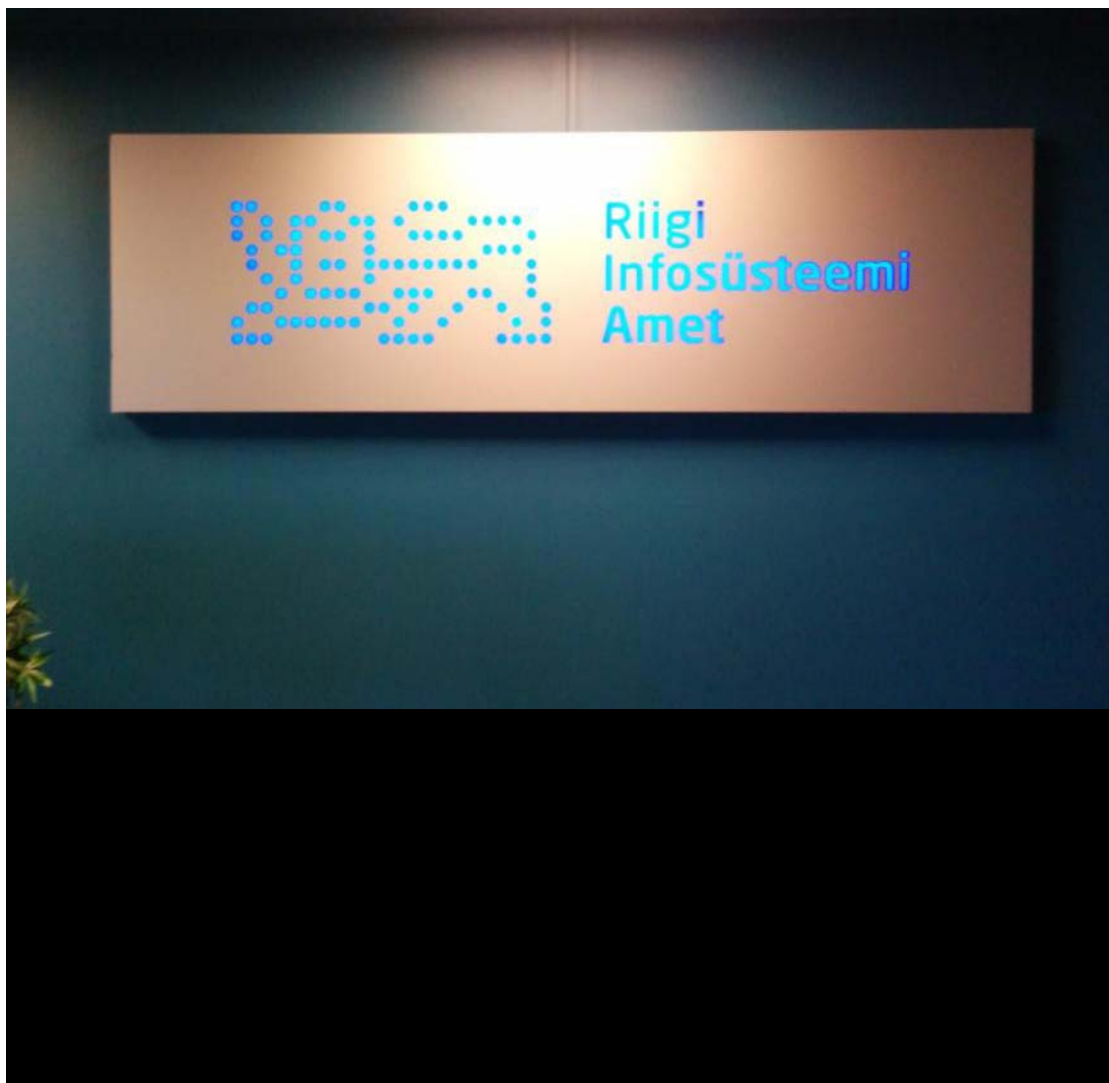
JASON KEITCAT

vaatleja ees- ja perekonnanimi

9.10.2013

väljaandmise kuupäev







Tarvi Martens



This repository ▾

Search or type a command



Explore Gist Blog Help

PUBLIC



vk-ehk / evalimine

Watch ▾

107



e-hääletamise tarkvara

8 commits

1 branch

0 releases

1 contributor



branch: master ▾

evalimine / +

Source-code changes for EP2014 ...



svenheiberg authored May 02, 2014

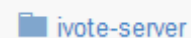
latest commit d1473a512c



docs

presentation from 11.07.2013

11 months ago



ivote-server

Source-code changes for EP2014

a month ago



LICENSE

license

11 months ago



README.md

README

10 months ago

README.md

Ehk Videod

Subscribe 6

Home Videos Playlists Channels Discussion About

Uploads

Date added (newest - oldest)



26:51

E-hääle hävitamine 1/2
118 views 4 months ago



23:15

E-hääle hävitamine 1/1
58 views 4 months ago



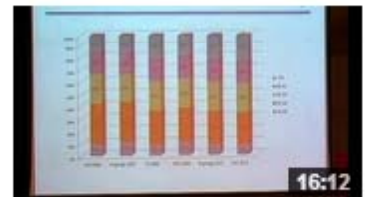
12:52

20.10.2013 seadmete kokkupanek
41 views 7 months ago



48:28

20.10.2013 e-hääle tühistamine ja lugemisek...
54 views 7 months ago



16:12

20.10.2013 hääle üleslaadimine infosüsteemi
29 views 7 months ago



18:54

20.10.2013 hääle kokkulugemine...
76 views 7 months ago



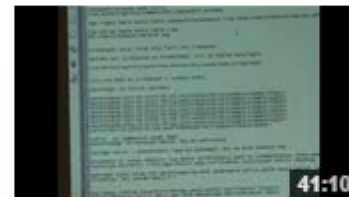
11:18

20.10.2013 ettevalmistus hääle lugemiseks
36 views 7 months ago



12:48

16 10 2013 e hääletamise lõpetamine 3/3
39 views 7 months ago



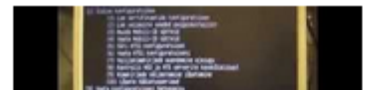
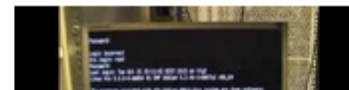
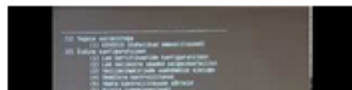
41:10

17.10.2013 E-hääletanute nimekirjade valmendus 4/4
54 views 7 months ago

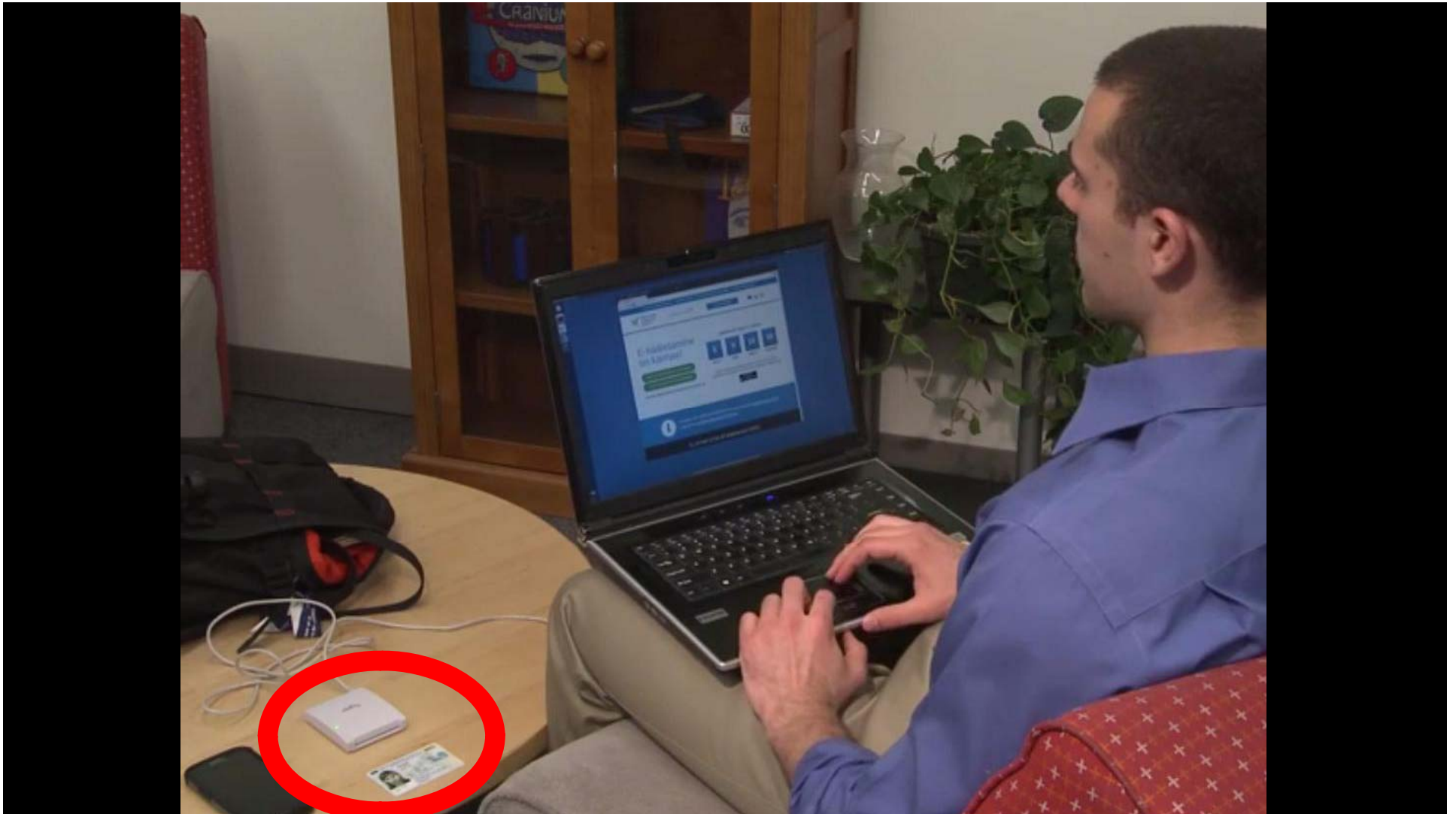


30:31

17.10.2013 E-hääletanute nimekirjade valmendus 2/4
23 views 7 months ago



The Voter's Experience





Text size: A A A

OPEN CONTENT

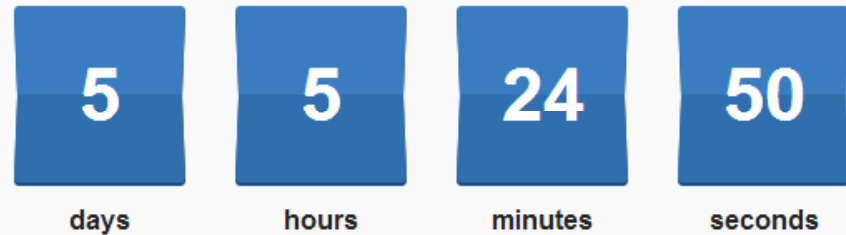


You can vote now in Internet!

From 10 to 16 October, it is possible to vote [at this web page](#).

[Read more](#) how to vote.

Voting ends in



Voting

Election
Servers

Signed
Encrypted
Ballot

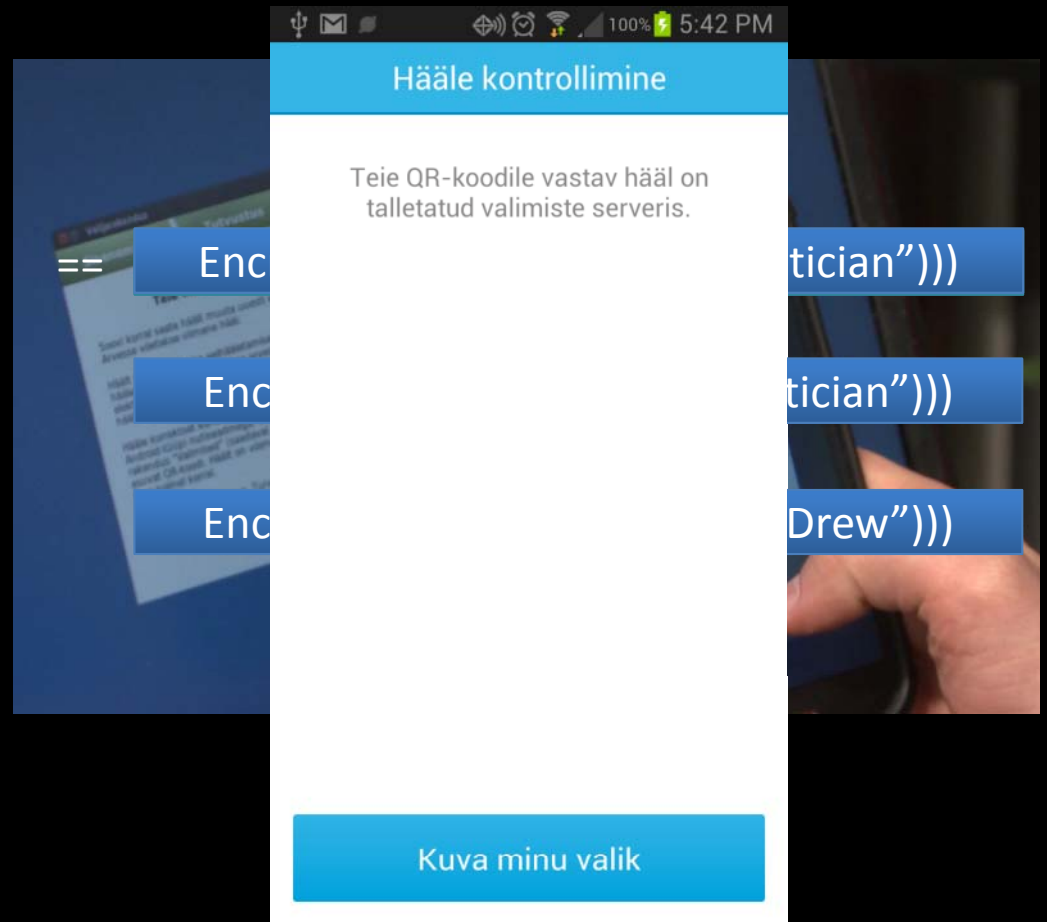
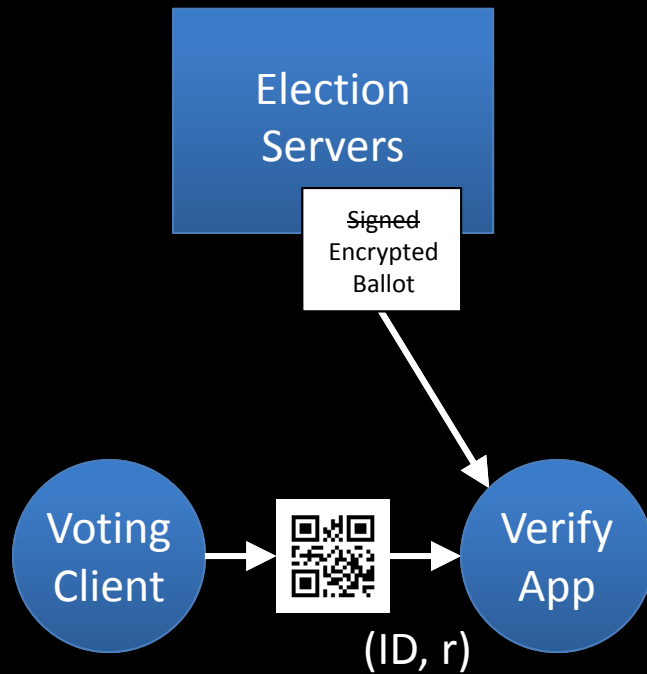


1. Encrypted Ballot = $\text{Encrypt-RSA}(PK_{\text{election}}, \text{Pad}_r(\text{Ballot}))$

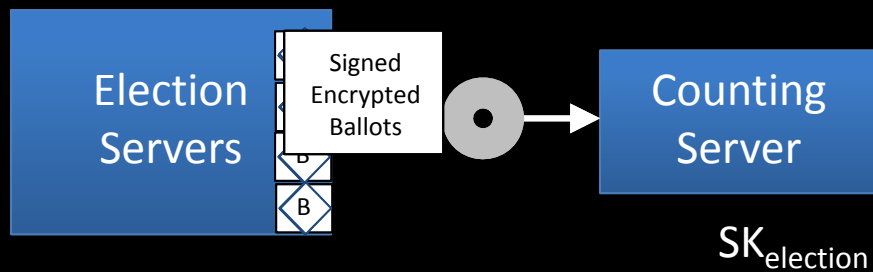
2. Signed Ballot = $\text{Sign}(SK_{\text{voter}}, \text{Encrypted Ballot})$



Verification



Counting



$\text{Decrypt}(SK_{\text{election}}, \text{Encrypted Ballot})$

Political party or independent candidate	VOTES	% Of votes
Estonian Reform	79,849	24.3%
Estonian Centre Party	73,419	22.4%
Pro Patria and Res Publica Union	45765	13.9%



Inner Envelope: $\text{Encrypt}(PK_{\text{elect}}, \text{Pad}_r(\text{Ballot}))$
 Outer Envelope: $\text{Sign}(SK_{\text{voter}}, \text{Inner Envelope})$

Threats?

BBC NEWS [Watch One-Minute World News](#)

Last Updated: Thursday, 17 May 2007, 15:21 GMT 16:21 UK

[E-mail this to a friend](#) [Printable version](#)

Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.



Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Estonia says many state websites have been affected Moscow denies any involvement.

Estonia says the attacks began after it moved a Soviet war memorial in Tallinn. The move was condemned by the Kremlin.

A Nato spokesman said the organisation was giving Estonia technical help.

"It's the 21st century. It's not just about tanks and artillery."

News Front Page

- Africa
- Americas
- Asia-Pacific
- Europe**
- Middle East
- South Asia
- UK
- Business
- Health
- Science & Environment
- Technology
- Entertainment

Also in the news

Video and Audio

Programmes

Have Your Say

RT QUESTION MORE. [LIVE](#)

News USA Russian politics Business Op-Edge In vision In motion

UKRAINE TIMELINE

BREAKING NEWS OSCE CONFIRMS UKRAINE BOMBED LUGANSK ADMIN HQ FROM

Home / News /

'Cyber-attack' cripples Ukraine's electronic election system ahead of presidential vote

Published time: May 24, 2014 23:02
 Edited time: May 26, 2014 01:16 [Get short URL](#)



Implicitly Trusted Components:
Voter's Client
Counting Server

Client-side Attack



1. How to infect clients?

2. How to defeat verification?

Client-side Malware

1. Steals PINs
2. Casts Replacement Vote

Server-side Attack

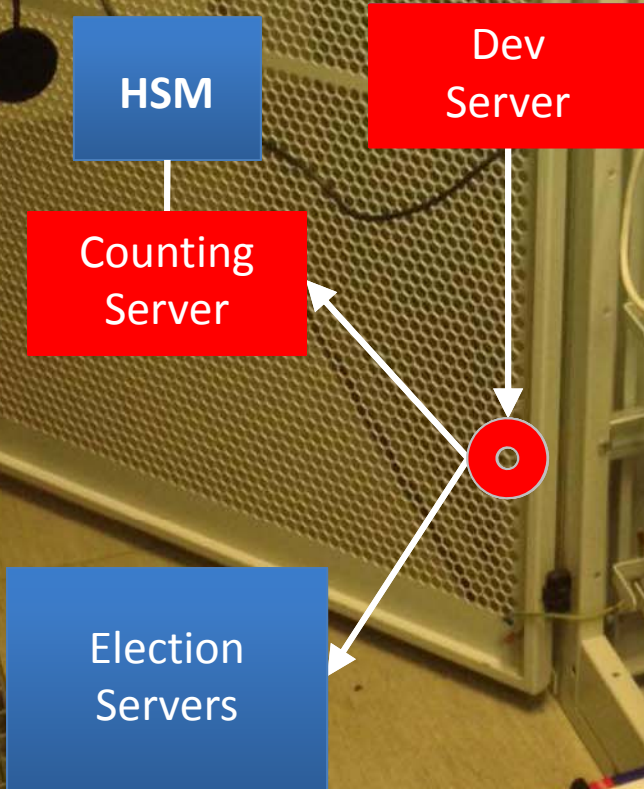
HSM

Counting
Server

Election
Servers



Server-side Attack



1. How to infect counting server?

Server-side Attack

HSM

Counting
Server

Election
Servers

```
try:  
    exit_code = subprocess.call([self.decrypt_prog] + args)  
except OSError, oserr:
```

1. How to infect counting server?
2. How to change votes?

Operational Security?

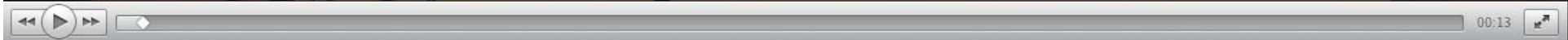
Our security is better than Google's.

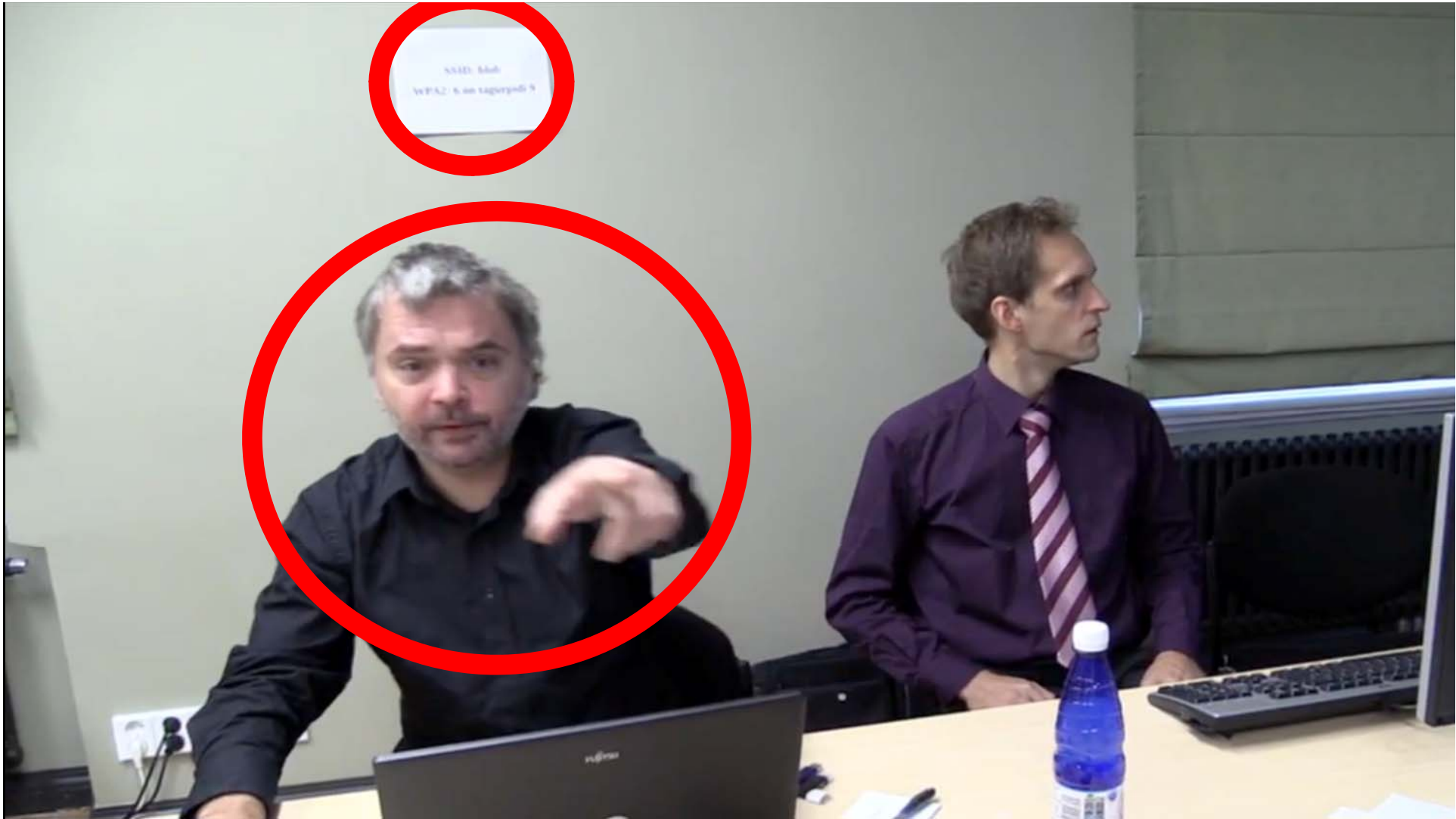
— Toomas Hendrik Ilves
President of Estonia



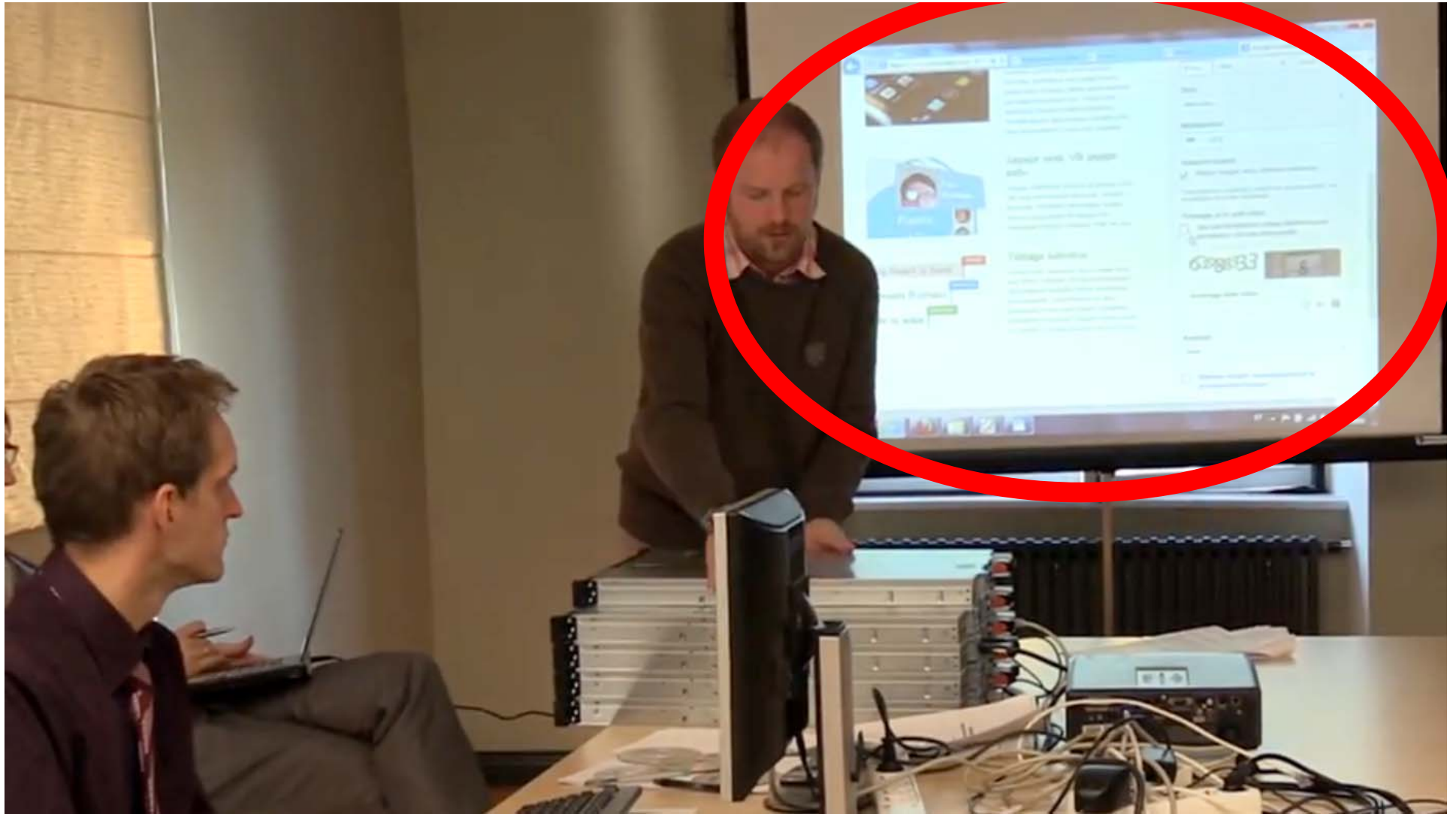


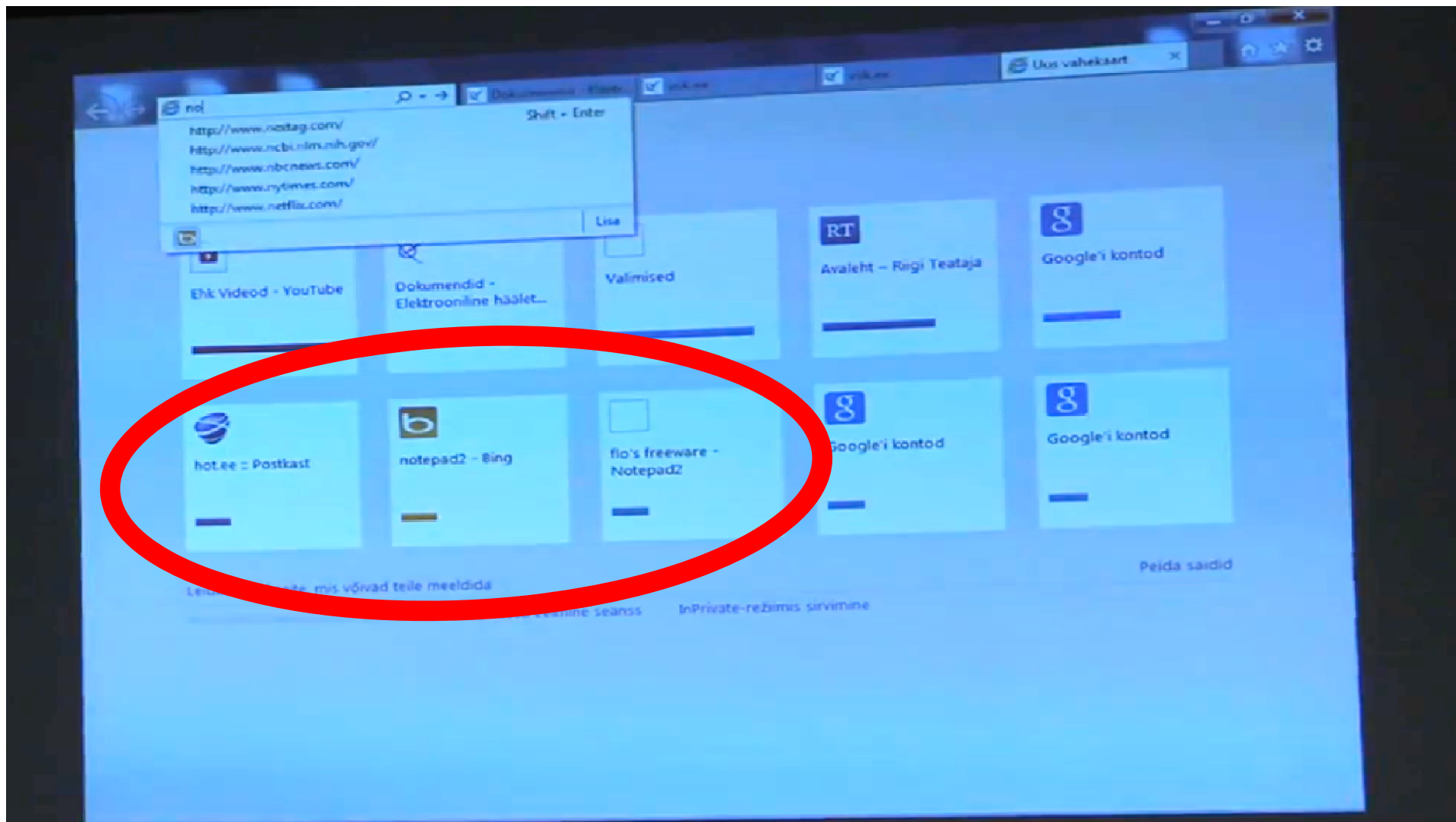
Official YouTube Videos

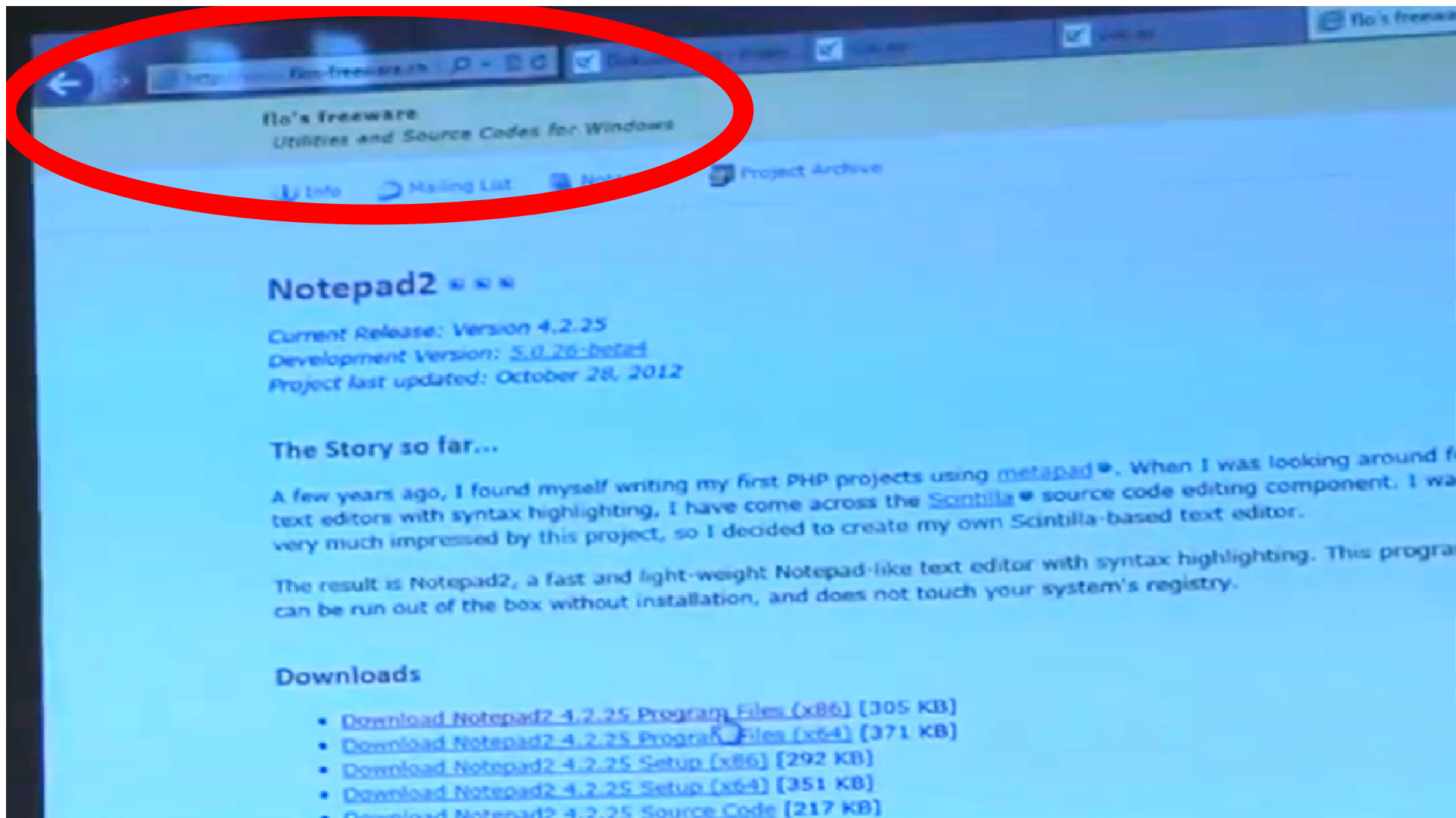




SMID: Bob
WPA2: 6. an tagirpodi 9







Notepad2

Current Release: Version 4.2.25
Development Version: [5.0.26-beta2](#)
Project last updated: October 28, 2012

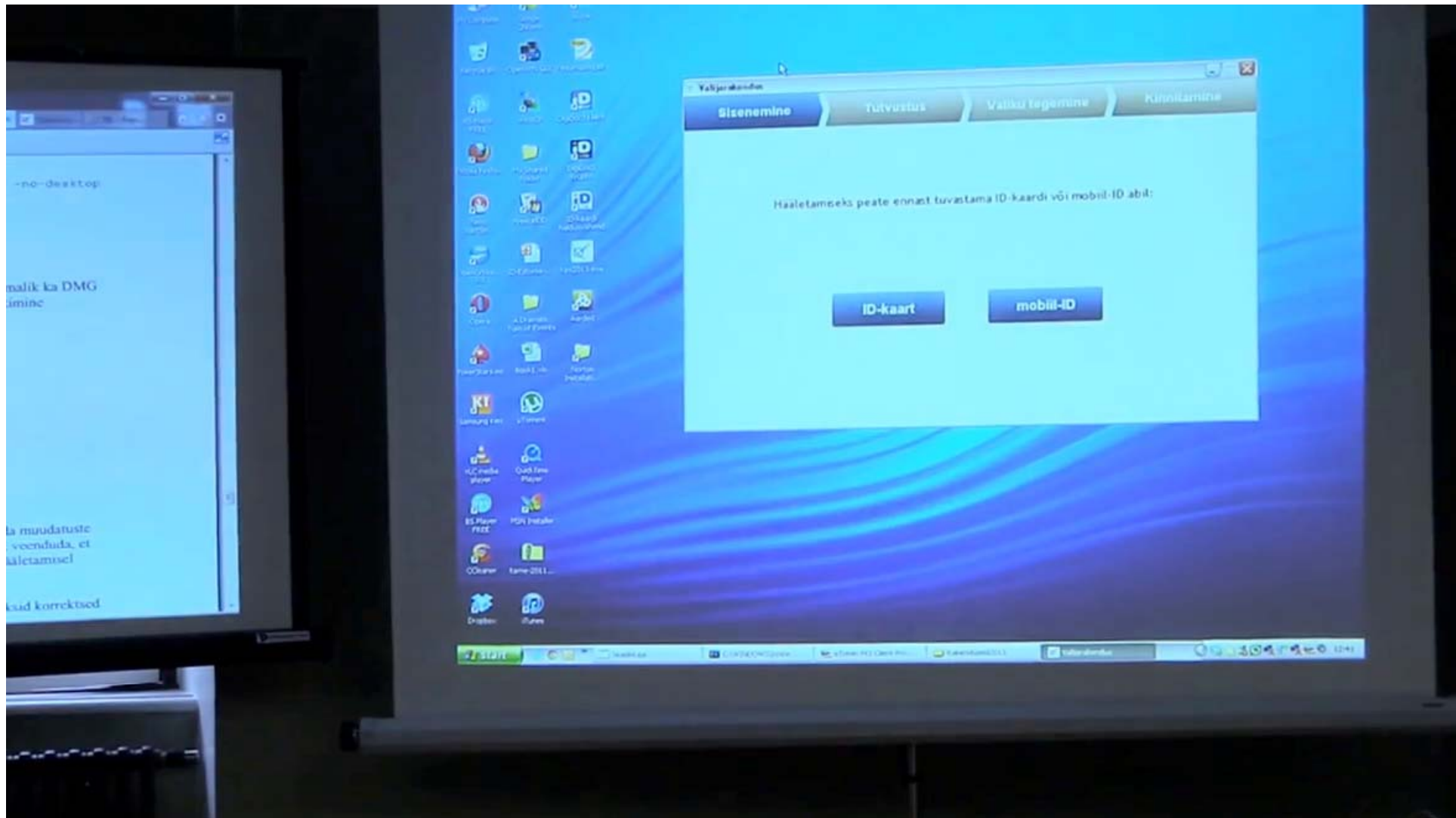
The Story so far...

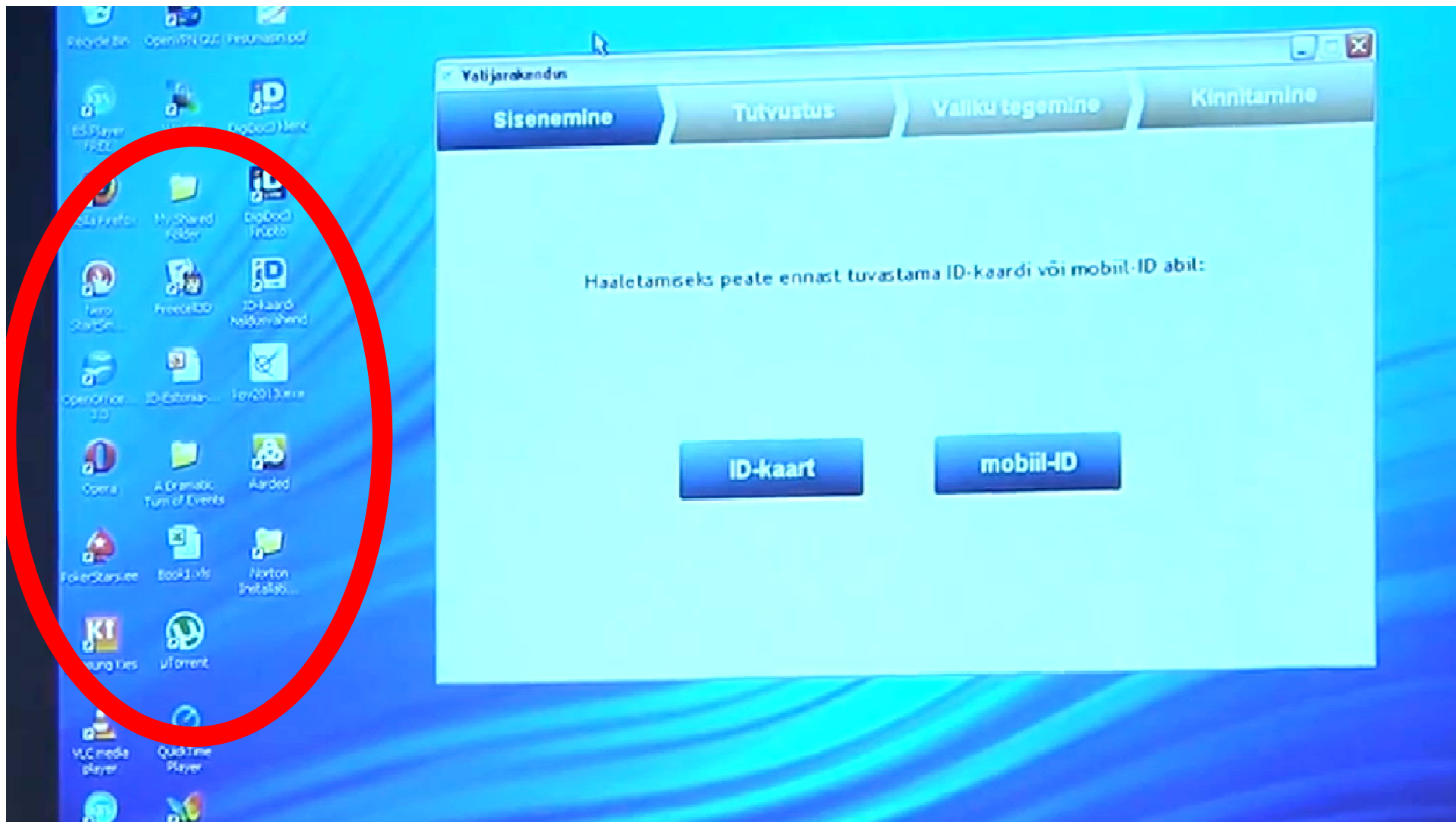
A few years ago, I found myself writing my first PHP projects using [metapad](#). When I was looking around for text editors with syntax highlighting, I have come across the [Scintilla](#) source code editing component. I was very much impressed by this project, so I decided to create my own Scintilla-based text editor.

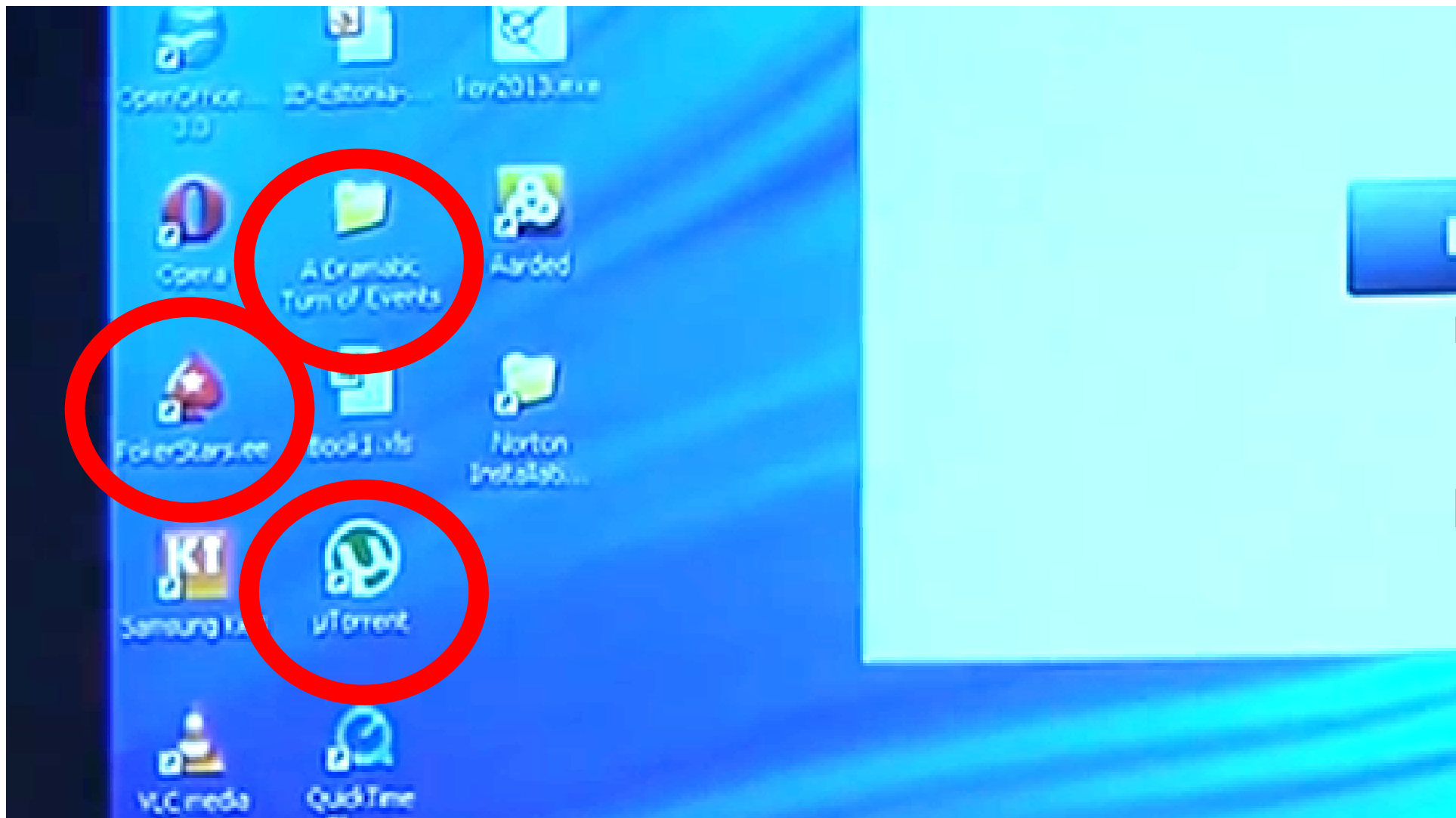
The result is Notepad2, a fast and light-weight Notepad-like text editor with syntax highlighting. This program can be run out of the box without installation, and does not touch your system's registry.

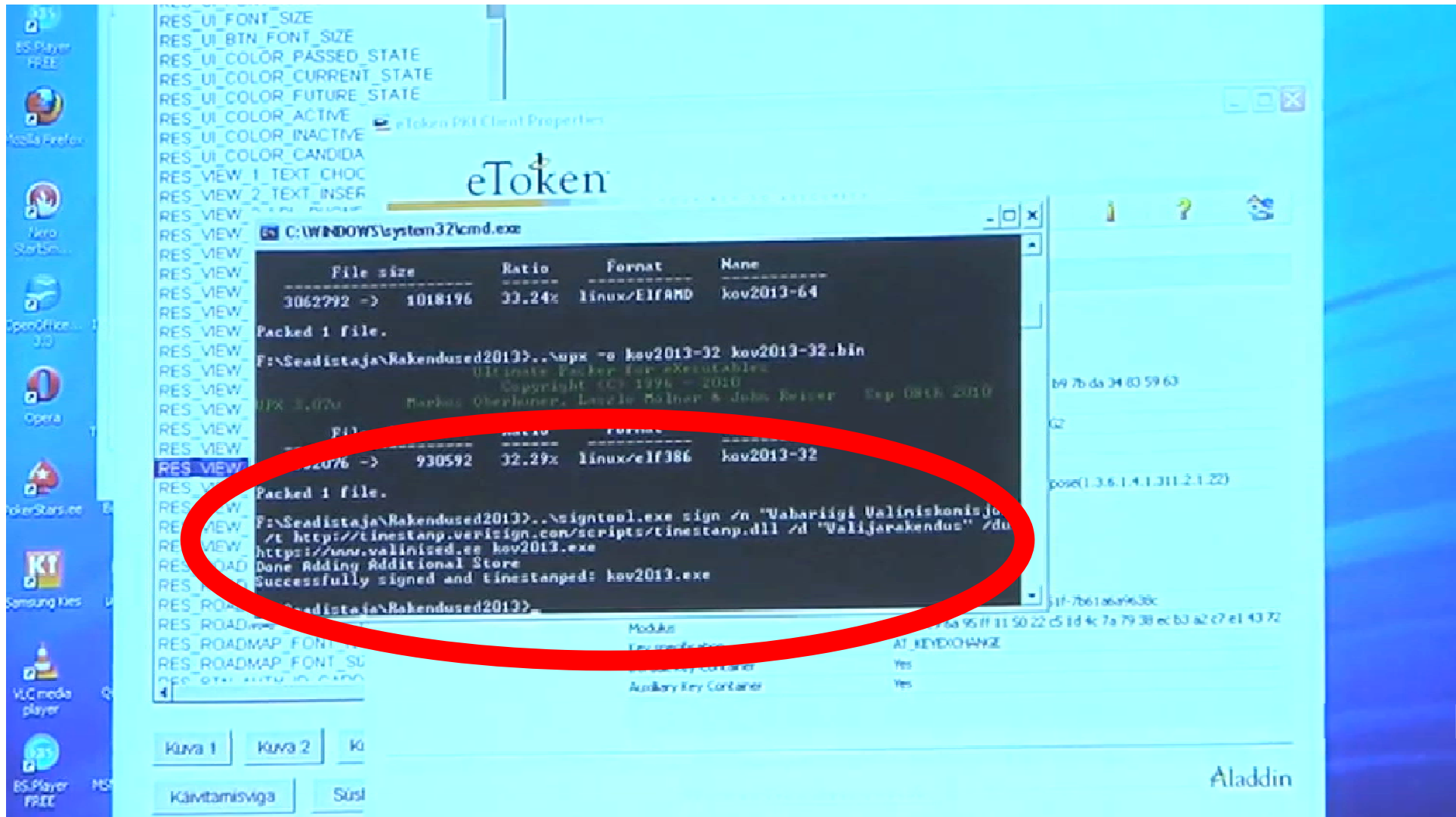
Downloads

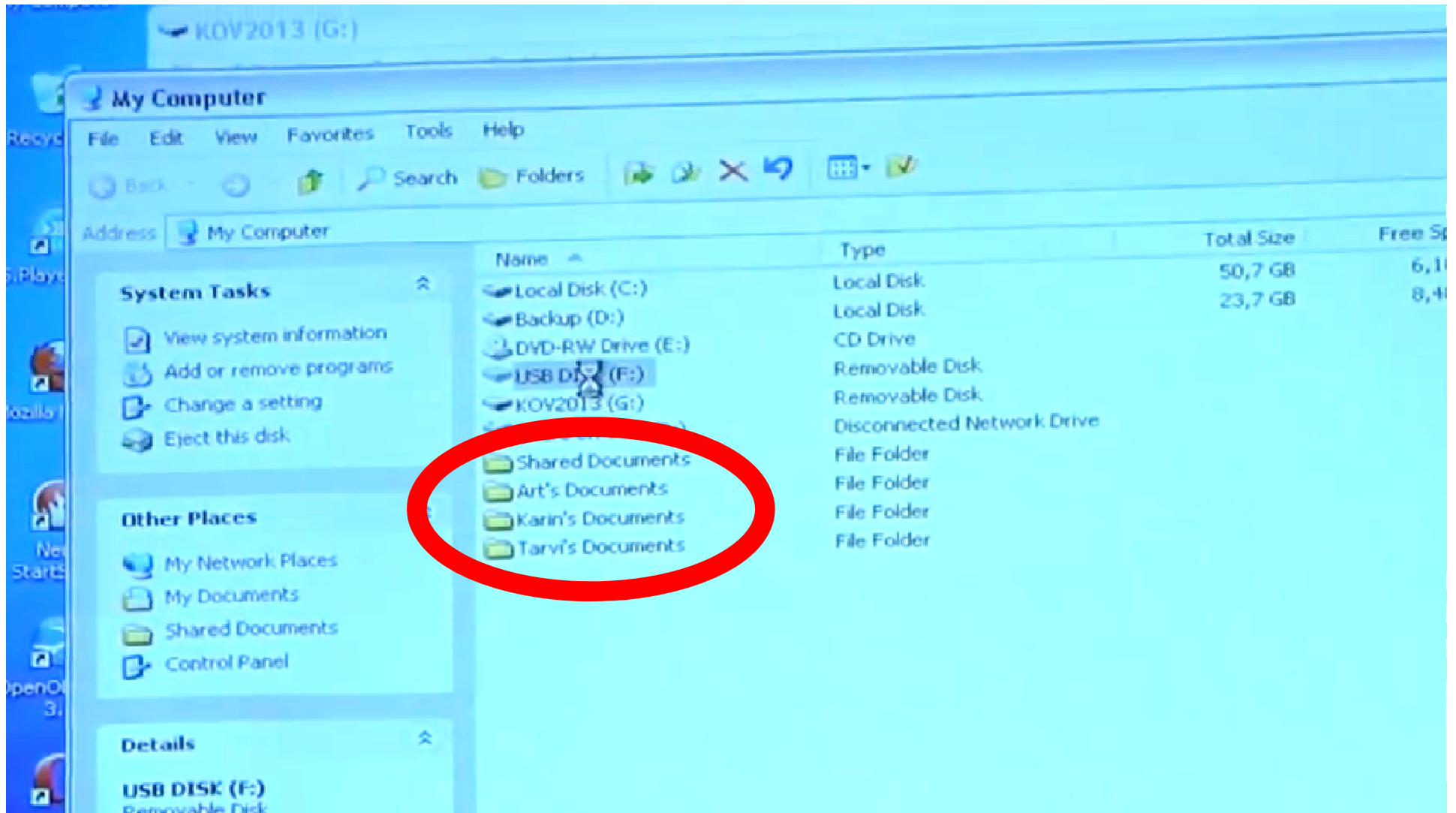
- [Download Notepad2 4.2.25 Program Files \(x86\)](#) [305 KB]
- [Download Notepad2 4.2.25 Program Files \(x64\)](#) [371 KB]
- [Download Notepad2 4.2.25 Setup \(x86\)](#) [292 KB]
- [Download Notepad2 4.2.25 Setup \(x64\)](#) [351 KB]
- [Download Notepad2 4.2.25 Source Code](#) [217 KB]

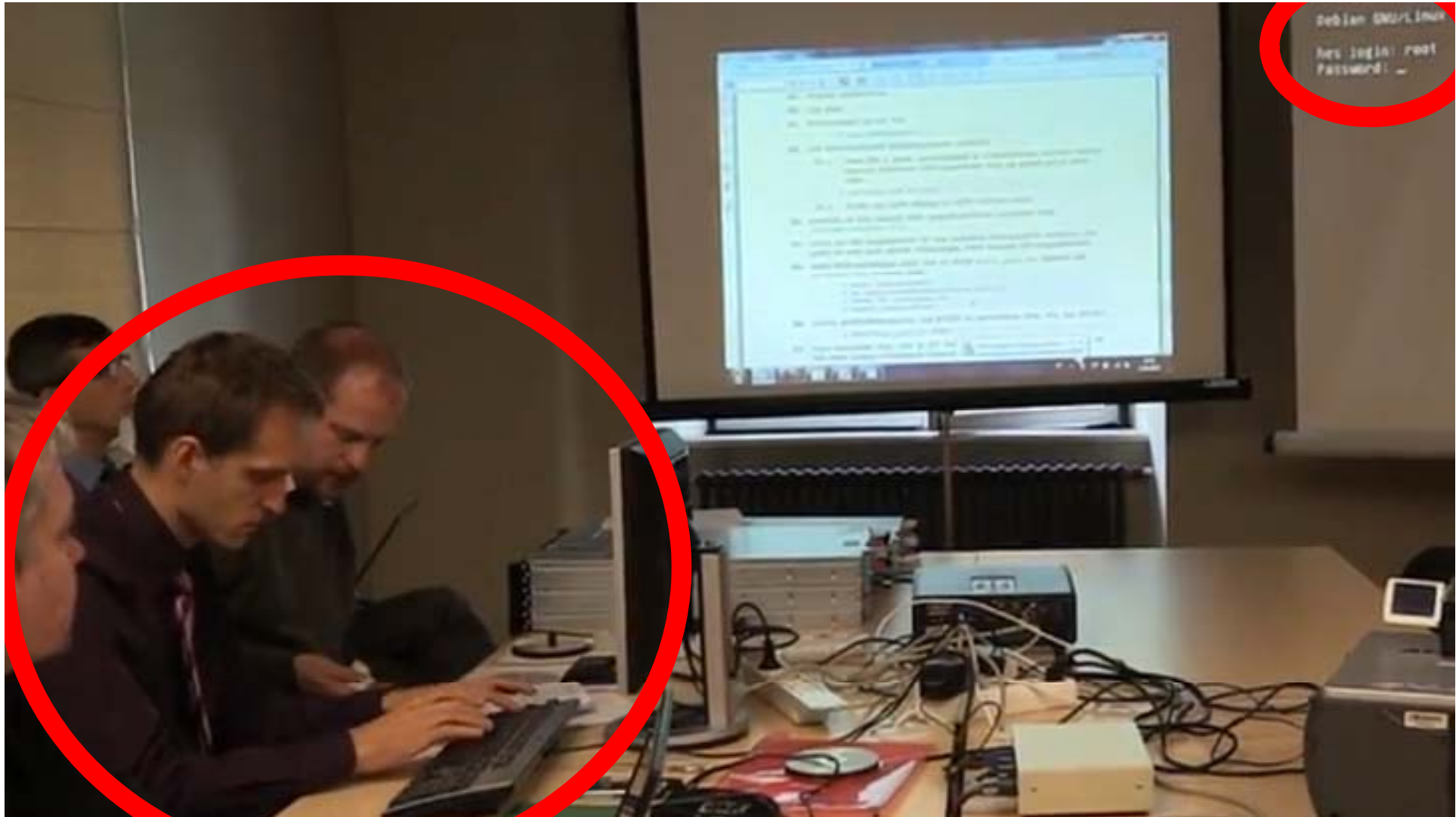




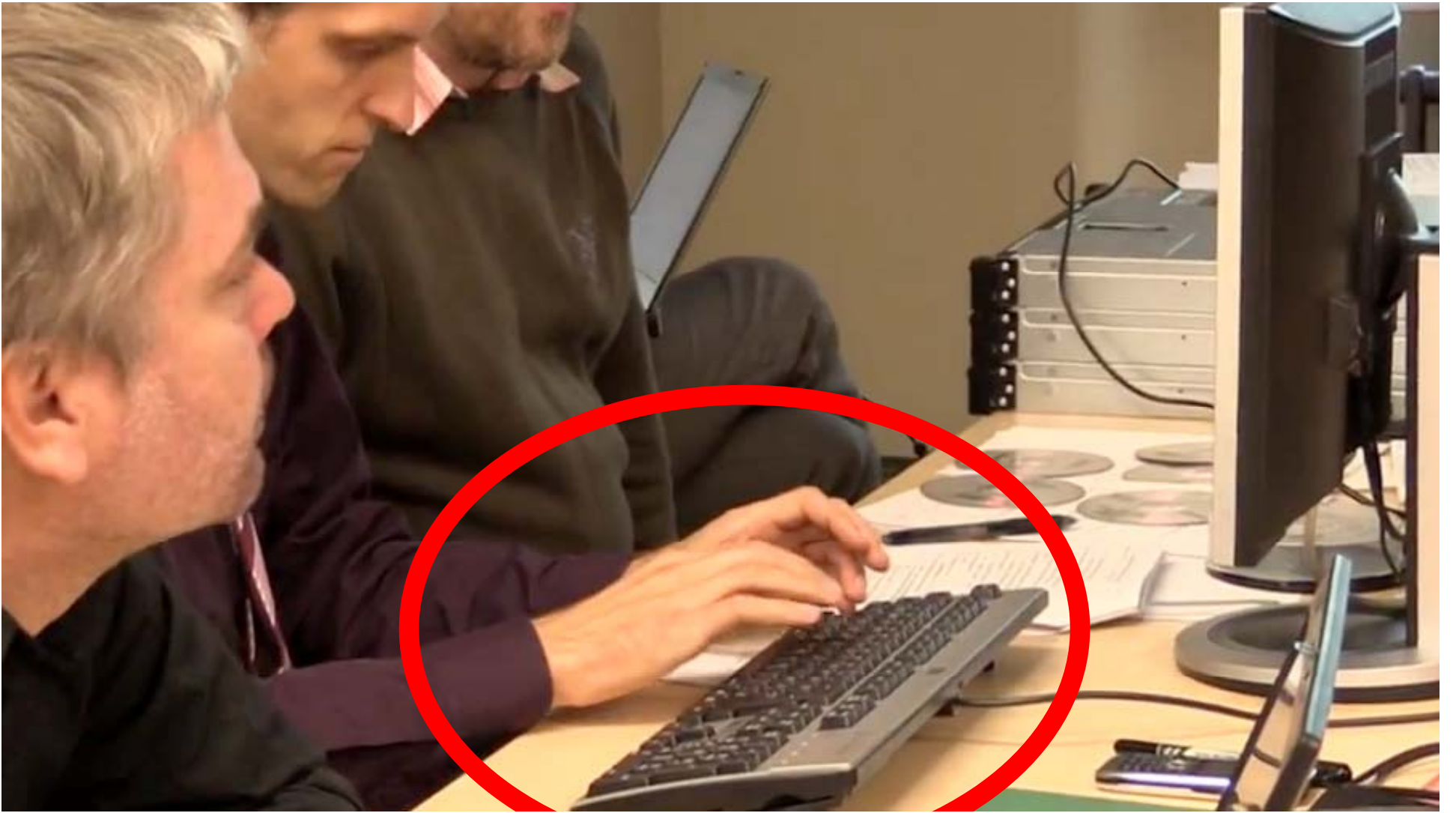


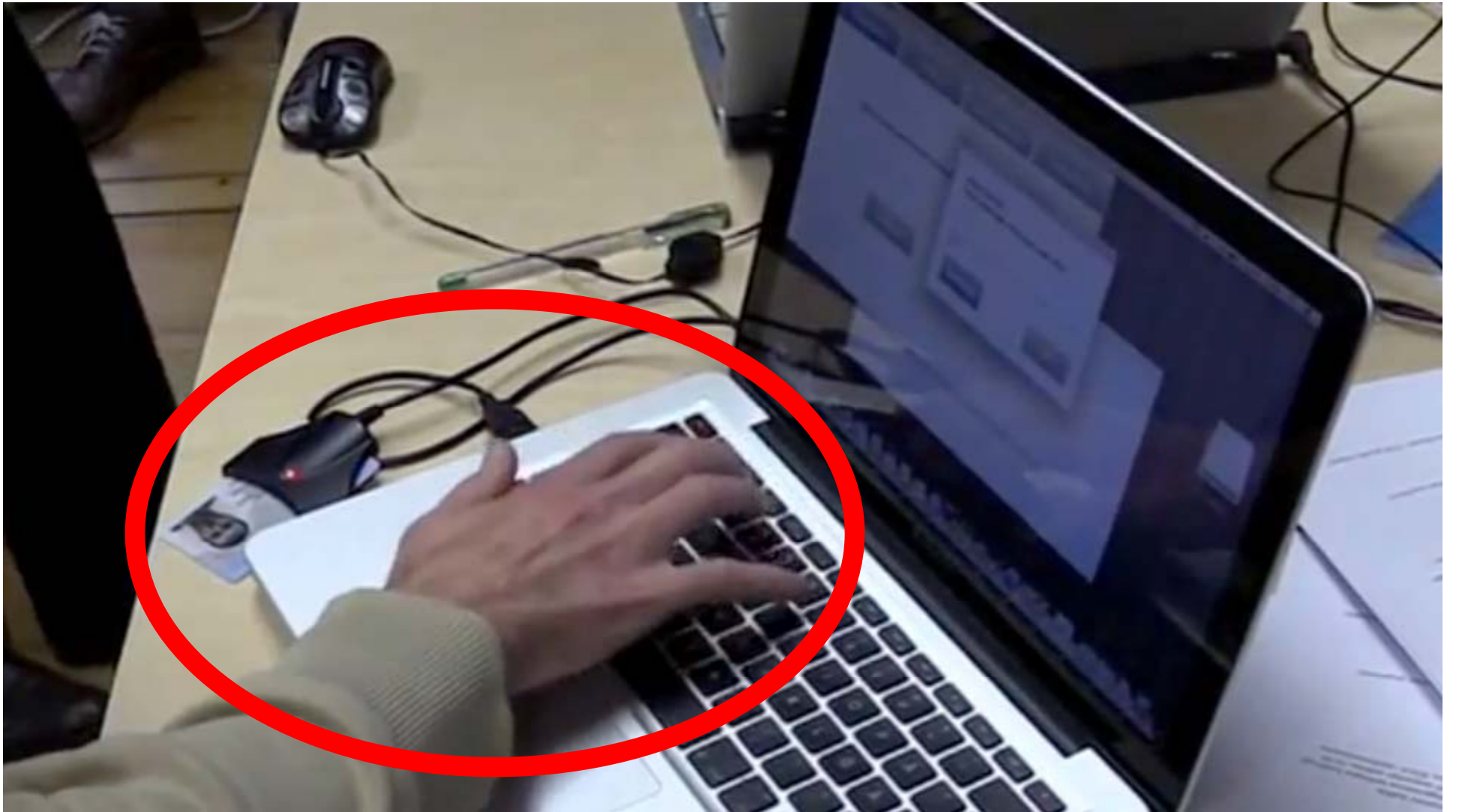






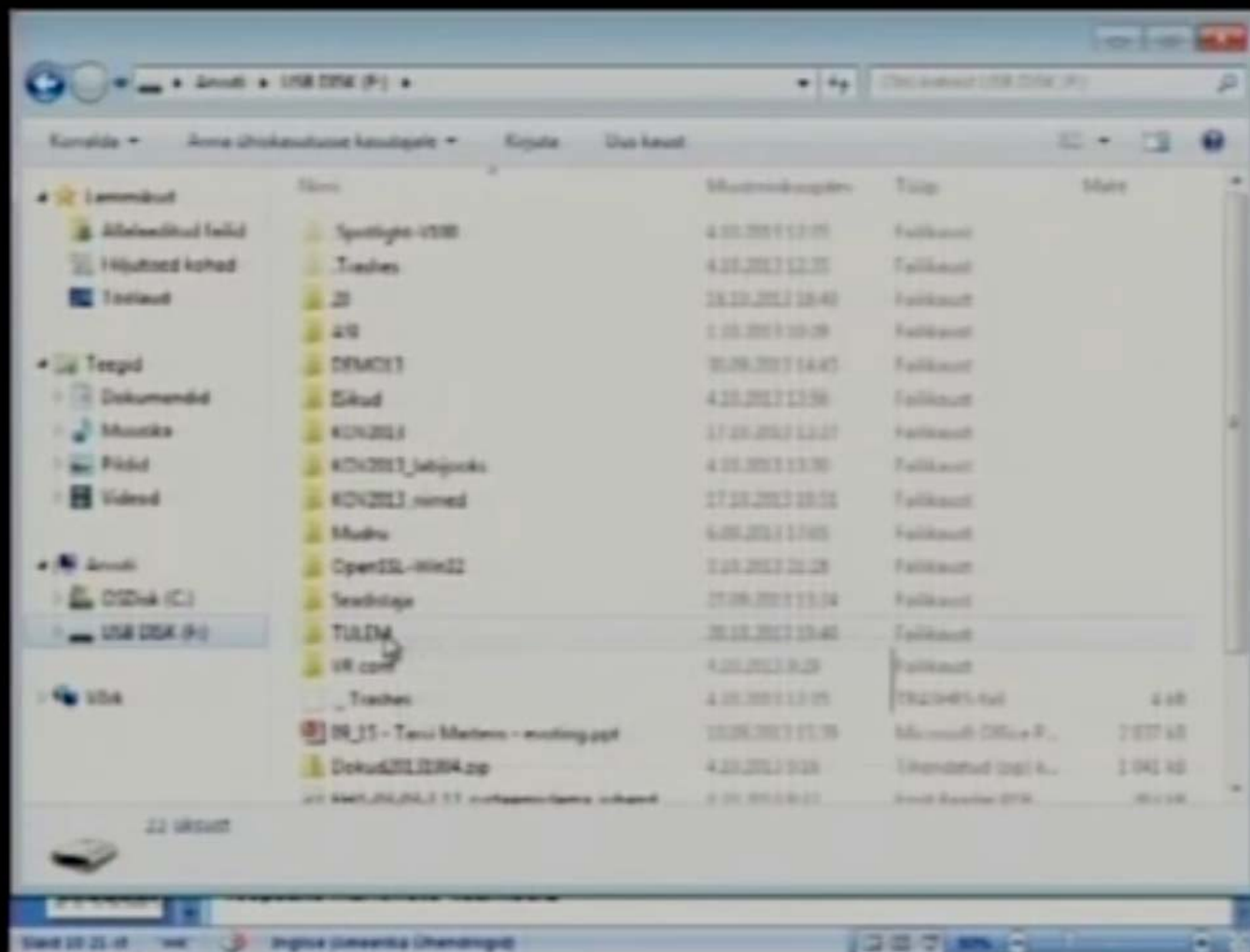
```
Debian GNU/Linux  
hes login: root  
Password: _
```











Going Public















Our Findings | Independen x

← → ↻ <https://estoniaevoting.org/findings/>   



Independent Report on E-voting in Estonia HOME OUR FINDINGS PRESS RELEASE ▾ FAQ PHOTOS VIDEOS THE TEAM DOWNLOADS 


voting system by
international e-voting
experts.




OUR FINDINGS

Overview

The researchers describe their findings in this [video overview](#).

Security Analysis of the Estonian E-Voting System  



0:00 / 7:30   YouTube 

Security Analysis of the Estonian Internet Voting System

J. Alex Halderman¹ Harri Hursti Jason Kitcat² Margaret MacAlpine
Travis Finkenauer¹ Drew Springall¹

¹ University of Michigan, Ann Arbor, MI, U.S.A.

² Open Rights Group, U.K.

Technical report – May 2014

For additional materials and contact information, visit estoniaevoting.org.

1. INTRODUCTION

Several countries have experimented with casting votes over the Internet, but today, no nation uses Internet voting for binding political elections to a larger degree than Estonia [38]. When Estonia introduced its online voting system in 2005, it became the first country to offer Internet voting nationally. Since then, it has used the system in local or national elections five times, and during recent elections 20–25% of participating voters cast their ballots online [24].

Rather than proving integrity through technical means, Estonia relies on a complicated set of procedural controls, but these procedures are inadequate to achieve security or transparency. During our in-person observations and in reviewing official videos of the 2013 process, we noted deviations from procedure and serious lapses in operational security, which leave the system open to the possibility of attacks, fraud, and errors. Transparency measures, such as video recordings and published source code, were incomplete and insufficient to allow outsider observers to establish the integrity of results.



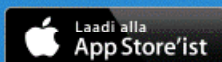
Estonian Reform Party
National Government
30% of Parliament
Wealthy, ethnic Estonians



Estonian Centre Party
Tallinn City State
20% of Parliament
75% of non-ethnic Estonians

Kõige mugavam on uudiseid lugeda **mobiiList!**

Tiri Delfi rakendus oma telefoni!



E-pood • Vaata.ee • E-post • Kaart • Raamat • Töö • Raha • Müü • Kataloog • Mängud • Igav.ee • Filmid • Mis toimub • Kasulik • Date • Piit E, 12. mai **SISUKAART**

Delfi Delfi 2 Rus Ilm Eesti Elu Ärileht Sport Publik Forte Naistekas Rahva hääl Noorte hääl EPL Ekspress Maaleht Reisijuhut Moodne Kodu TV Täheke

Kõik uudised Eesti Arvamus Maailm Krimi EP valimised Delfi TV saated Laulu- ja tantsupidu Uut Delfis Teemalehed Suures pildis Arhiv



Ekspertid: Eesti e-valimised on nii ebaturvalised, et tuleks kohe ära lõpetada (73)



"Donetski Rahvavabariik" palub Vladimir Putinil end Venemaaga ühendada Täiendatud: 19.00! (173)

ANTON TŠEHOVI KOMÖÖDIA
KAJAKAS

www.smsraha.ee

Tähelepanu! Iga laen on finantskohustus. Mõtle oma otsus hoolikalt läbi, tutvu laenulepingu tingimustega smsraha.ee ja vajadusel pea nõu meie asjatundjatega. Näiteks 300 eur 30 päevaks tagasimaksega 315 eur - krediidikulukuse määr 79,59%

VAATA JA KLIKI

EESTI LOTO

peatoovaja MERKO Ehitus.
Kõrval töötsoonis keevitustöö-
dega tegelenud tööline sisenes

penud viis toonnetust, neist
kolme asjaolusid alles selgita-
takse. ● Delfi

Soojaga on oodata nii äike-
sevihma kui ka tavalist vih-
ma. ● Delfi

Eesti eksperdid: e-valimised pole manipuleeritavad

E-valimiste turvalisuse eest vastutavad eksperdid ei pea tõestatuks end rahvusvahelisteks ekspertideks nimetava seltskonna väiteid, nagu nad suudaks valmisolukorras e-hääletamist Eestis manipuleerida. Tallinna linnavalitsuse initsiatiivil Eestisse kutsu-

tud eksperdid selgitasid, et e-valimiste tulemusi on võimalik lihtsasti ja mitmest kohast pahatahtlikult muuta.

Cybernetica AS tarkvaraarendaja ja e-valimiste üks turvaekspert Sven Heiberg ütles aga, et manipuleeritavusest rääkivad eksperdid

on loonud liiga palju eeldusi, mida päriselus on keeruline saavutada.

Elektroonilise hääletamise komisjoni esimees Tarvi Martens kinnitas pärast kriitiseerijatega kohtumist, et nende etteheidetes pole midagi uut ja e-hääletamine on turvaline. „Komisjon on esitletud riskidega alati arvestanud ja riskide maandamiseks kasutatakse konkreetseid meetodeid,” lausus ta. ● ERR

BLRT Grupp Aktsiaselts
Erakorralise üldkoosoleku teade

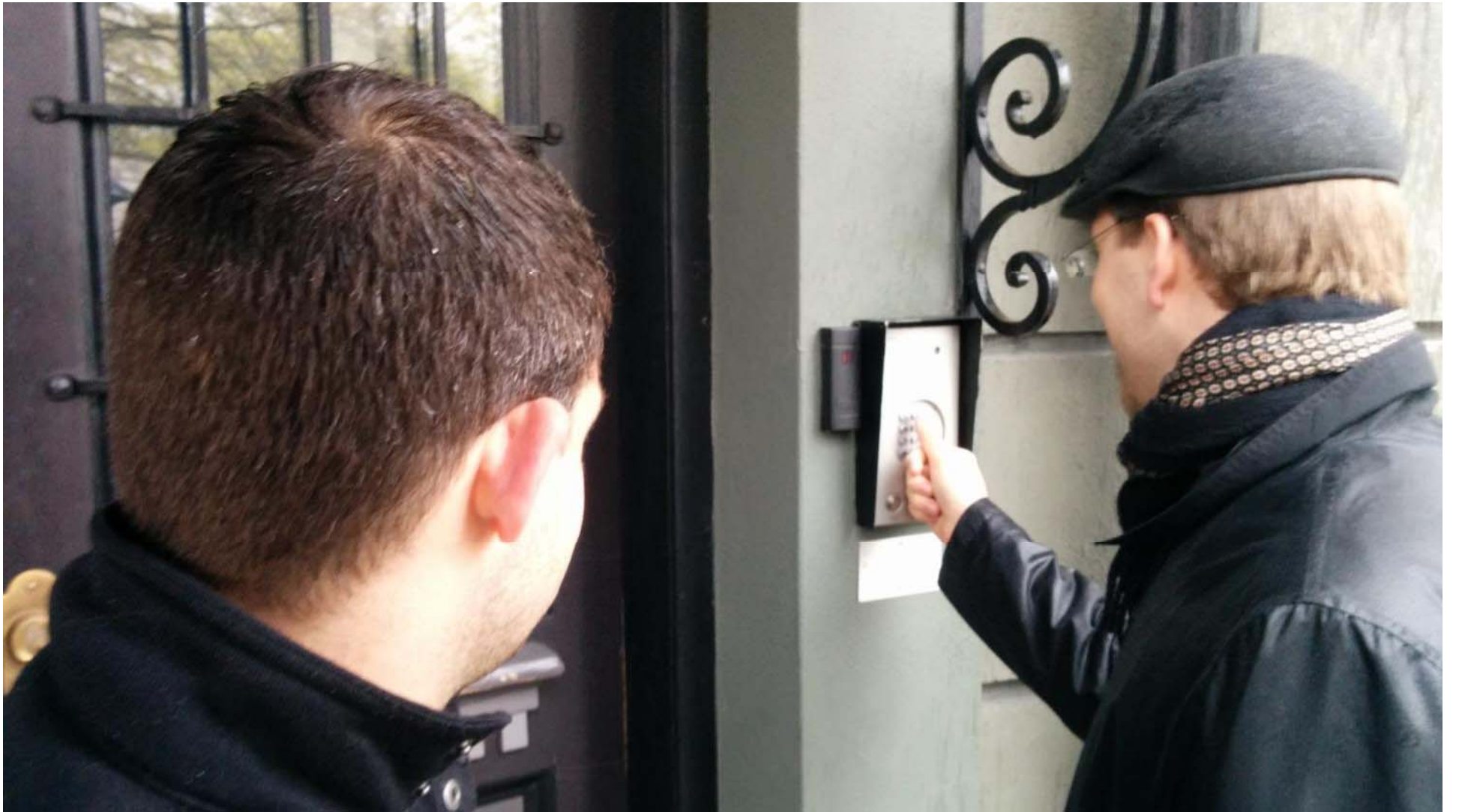
22. mai 2014

CORY DOCTOROW



Estonia's online system is horribly insecure and can't be trusted - Jason Kitcat writes, "I'm currently in Tallinn, Estonia as part of a team of independent security and elections researchers sharing our findings that [the Estonian online e-voting system has serious flaws](#). • [Play video](#)











I Facebooked those guys.
And they're working
for my opponents.

— Taavi Rõivas
Prime Minister of Estonia

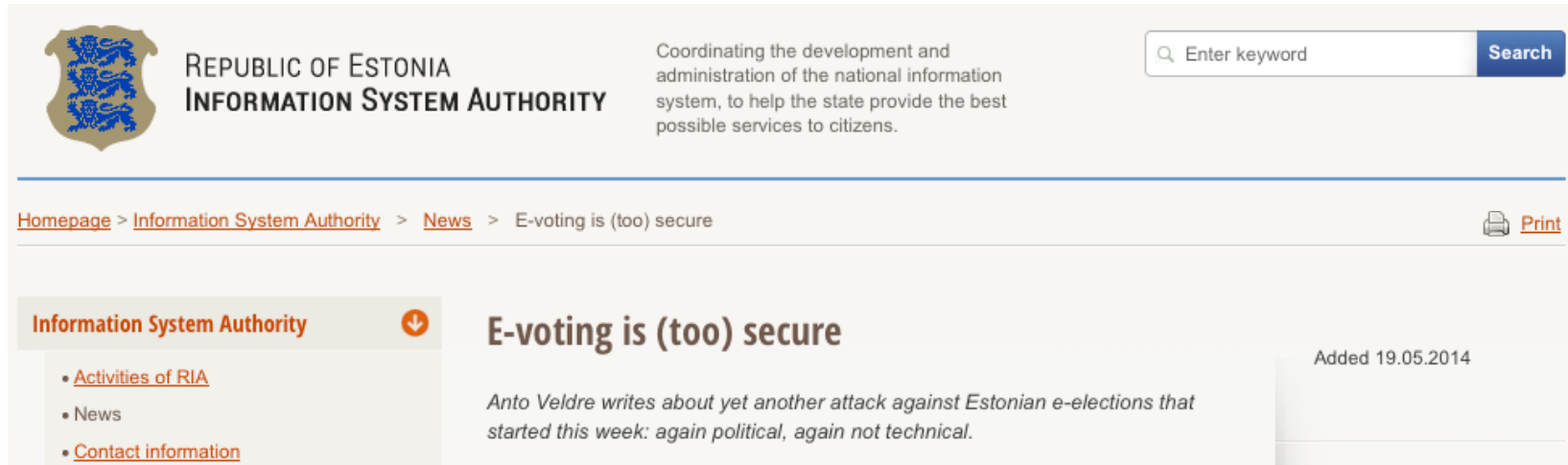




Verification app detects all bad behavior.

Why steal votes when you can steal money?

CERT Estonia



The screenshot shows the website of the Republic of Estonia Information System Authority. The header includes the national coat of arms, the organization's name, and a search bar. The main content area features a news article titled "E-voting is (too) secure" with a sub-headline: "Anto Veldre writes about yet another attack against Estonian e-elections that started this week: again political, again not technical." The article is dated 19.05.2014. A sidebar on the left lists navigation options: "Activities of RIA", "News", and "Contact information".

“nice people who care about computer hygiene have no viruses”

“In practice, computer risks have been eliminated”

“they’re here not because of their technical savvy, but their politically suitable (although technically incompetent) message”



Lessons

Estonia's I-voting approach is not secure.

State-level attacks are a rising threat to I-voting.

– National security issue; not a gov't IT problem!

Politics can obscure major technical problems.

Recommendation: Estonia should discontinue Internet voting until fundamental security advances.

The Internet Voting Problem

Want a voting system where you, or I, or our friends, or Tarvi Martens, or the NSA, or Vladimir Putin can't hack in and dictate the election result.

That's called a democracy!

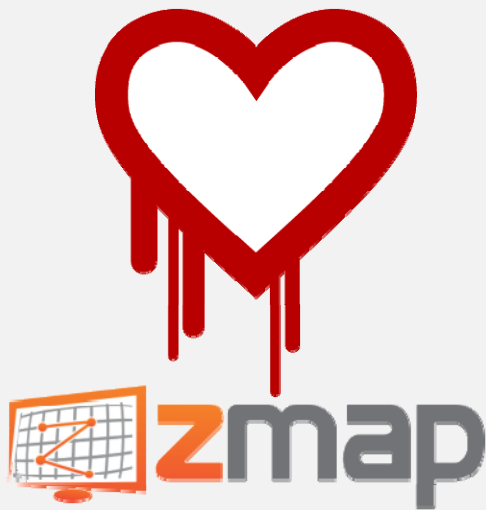
Major fraud should be at least as hard as with paper.

My take: *Decades, if ever*, until Internet voting can be secured, and not without fundamental advances.

Security Analysis of the
Estonian Internet Voting System
EstoniaEVoting.org

J. Alex Halderman
University of Michigan
jhalderm.com

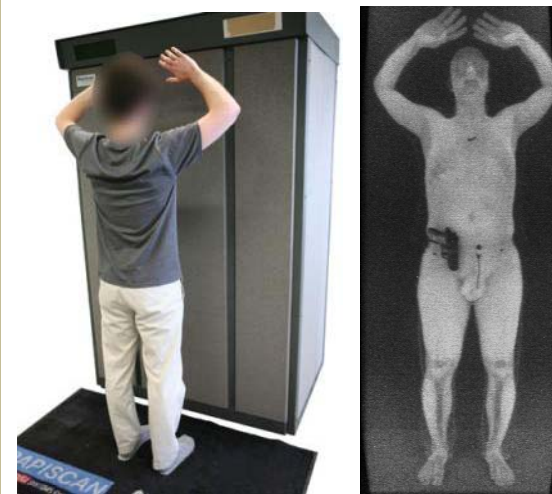
More Talks About My Lab's Research



Day 2 22:00 Saal 1

**Understanding Heartbleed
with the ZMap Scanner**

Zakir Durumeric



Day 3 11:30 Saal G

**Security Analysis of a
TSA Naked Scanner**

Hovav Shacham/Eric Wustrow



Day 4 14:00 Saal 6

**Building a Free HTTPS CA
to Encrypt the Entire Web**

Seth Schoen

End-to-End (E2E) Voter-Verifiability

As a voter, I can be sure that:

- My vote is cast as I intended.
- My vote is counted as cast.
- All votes are counted as cast.

Not a secret ballot!



Alice Johnson, 123 Main . . YES
Bob Ramirez, 79 Oak NO
Carol Wilson, 821 Market . NO

End-to-End Voter-Verifiability

As a voter, I can be sure that:

- My vote is cast as I intended.
- My vote is counted as cast.
- All votes are counted as cast.
- No voter can demonstrate how he or she voted to a third party.

