QAWARE
SOFTWARE ENGINEERING

Tag der Informatik-Lehrerinnen und -Lehrer 2015

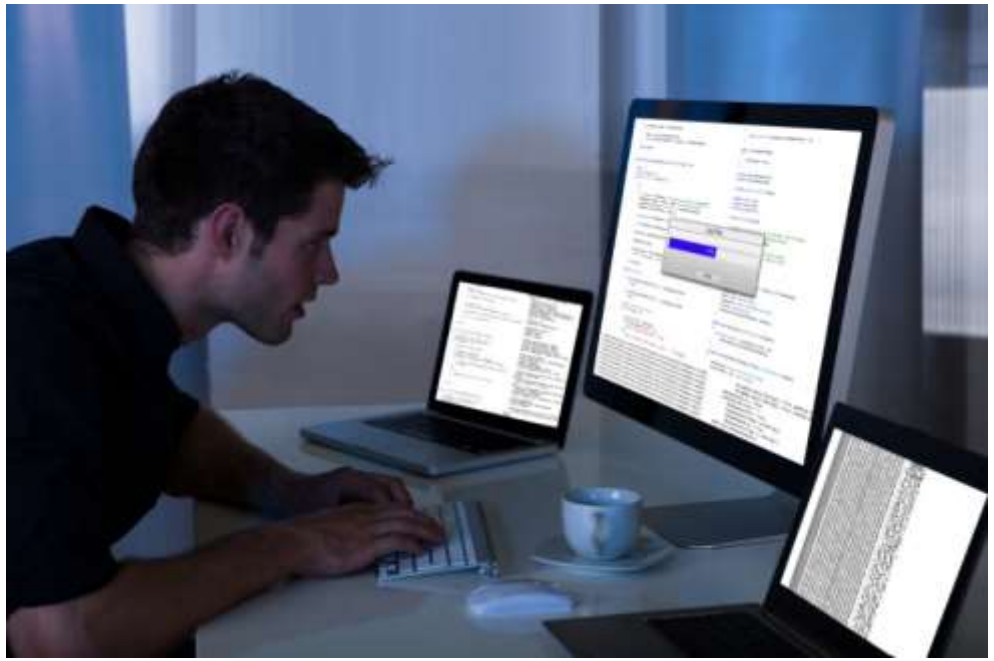
Operations Security - Sicherheit zwischen Script Kiddies und Geheimdiensten

München, 03. Juli 2015

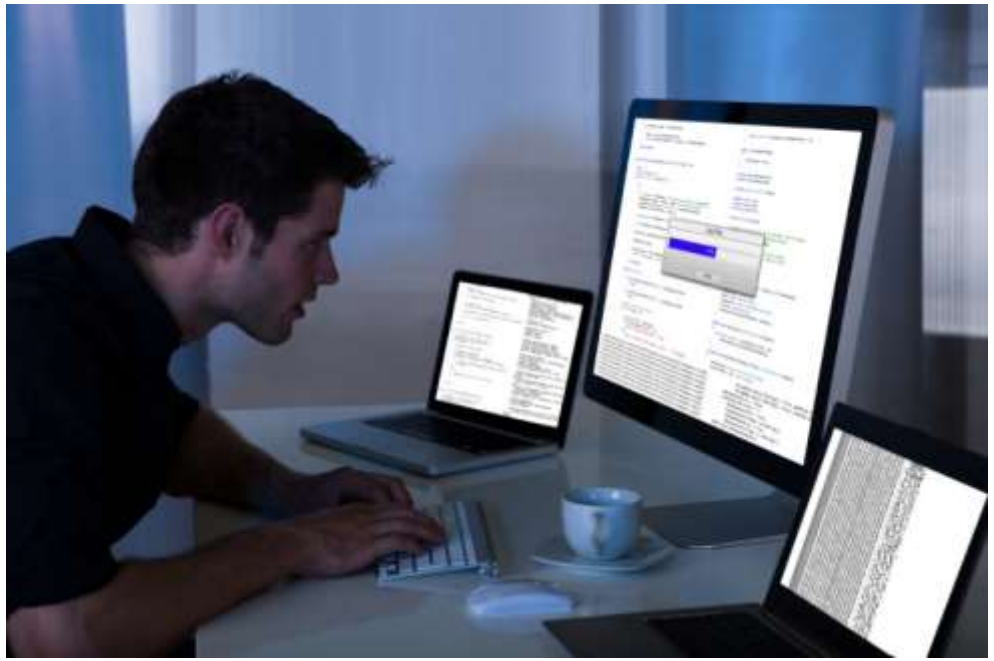
Andreas Janning


QAWARE
SOFTWARE ENGINEERING

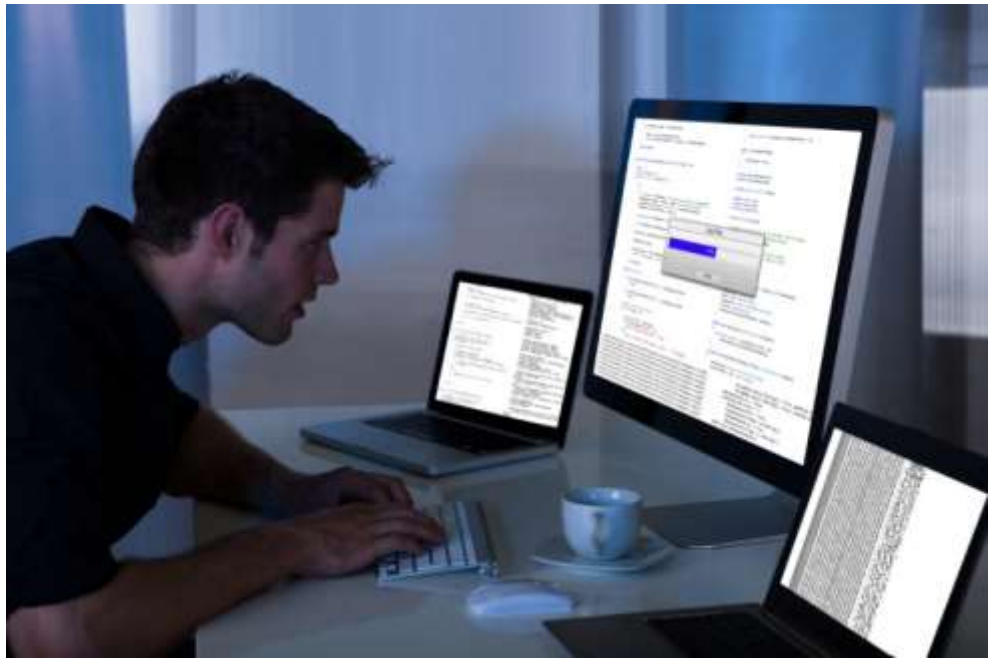
QAWARE
SOFTWARE ENGINEERING

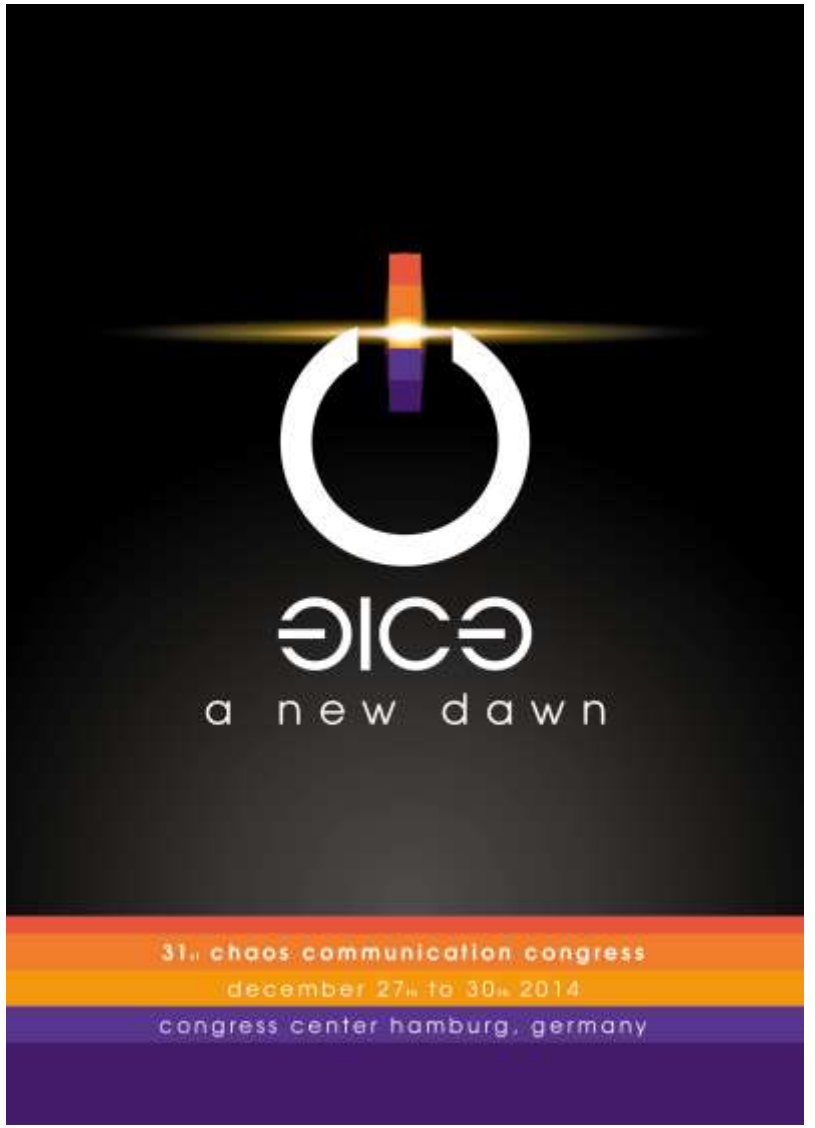


QAWARE
SOFTWARE ENGINEERING



QAWARE
SOFTWARE ENGINEERING






12:23:55
DAY 0


room information

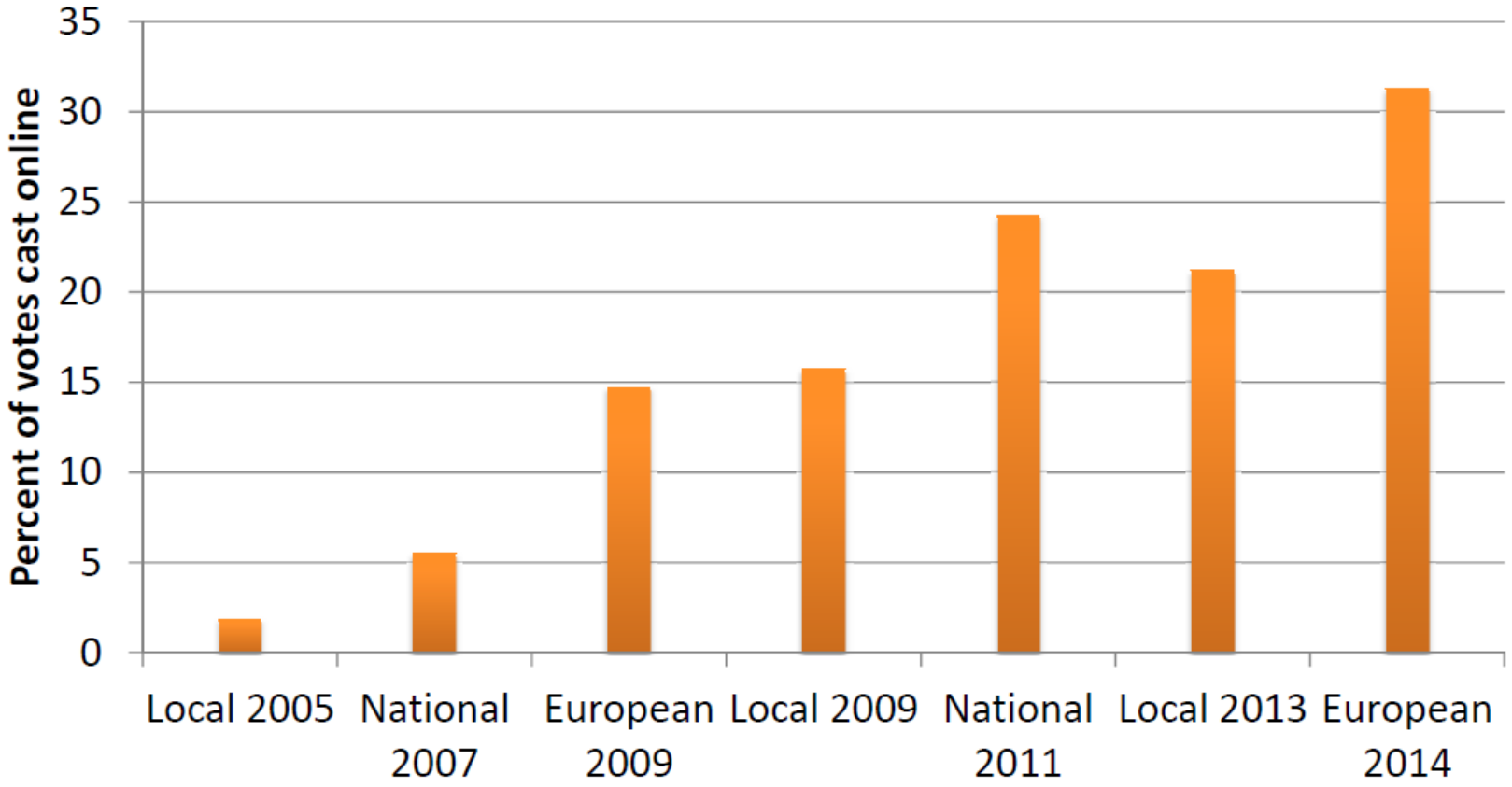
https://www.openrightsgroup.org/

https://www.cse.umich.edu/


DÄNEMARK
(Grönland)
Grönland-
see
Irminger-
see
Barentsee
Europäisches
Nordmeer
ISLAND
DÄNEMARK
(Färöer)
ATLANTISCHER
OZEAN
NOR-
WEGEN
FINNLAND
RUSSLAND
SCHWEDEN
EST-
LAND
Ostsee
LETTLAND
Nordsee
LITAUEN
KASACHSTAN
DÄNE-
MARK
RUSS-
LAND
WEISS-
RUSSLAND
IRLAND
MAN
VEREINIGTES
KÖNIGREICH
POLEN
NIEDER-
LANDE
DEUTSCH-
LAND
UKRAINE
Kaspisches
Meer
BELGIEN
GUERNSEY,
JERSEY
TSCHECHIEN
SLOWAKEI
MOLDA-
WIEN
ATLANTISCHER
OZEAN
LUXEM-
BURG
(SÜD-
OSSETIEN)
(ABCHASIEN)
ÖSTER-
REICH
UNGARN
GEORGIEN
ASER-
BAID-
SCHAN
FRANKREICH
SCHWEIZ
RUMÄNIEN
Schwarzes
Meer
ARME-
NIEN
SLO-
WENIEN
KROATIEN
IRAN
BOSNIEN
UND
HERZE-
GOWINA
SERBIEN
BULGARIEN
*SAN
MARINO
MONACO
TÜRKEI
ANDORRA
MONTE-
NEGRO
MAZE-
DONIEN
PORTU-
GAL
VATIKAN
ITALIEN
ALBA-
NIEN
SPANIEN
GRIECHEN-
LAND
SYRIEN
Mittelmeer
(NORDZ.)
IRAK
ATLAN-
TISCHER
OZEAN
LIBA-
NON
ZYPERN
JORDA-
NIEN
MAROKKO
ALGERIEN
TUNESIEN
MALTA
Mittelmeer
ISRAEL
SAUDI-ARABIEN


DÄNEMARK
(Grönland)
Grönland-
see
Irminger-
see
Barentsee
Europäisches
Nordmeer
ISLAND
DÄNEMARK
(Färöer)
ATLANTISCHER
OZEAN
NOR-
WEGEN
FINNLAND
RUSSLAND
SCHWEDEN
EST-
LAND
Ostsee
Nordsee
LETTLAND
LITAUEN
KASACHSTAN
DÄNE-
MARK
RUSS-
LAND
WEISS-
RUSSLAND
IRLAND
MAN
VEREINIGTES
KÖNIGREICH
POLEN
NIEDER-
LANDE
BELGIEN
DEUTSCH-
LAND
UKRAINE
Kaspisches
Meer
GUERNSEY,
JERSEY
ATLANTISCHER
OZEAN
LUXEM-
BURG
TSCHECHIEN
SLOWAKEI
MOLDA-
WIEN
(SÜD-
OSSETIEN)
(ABCHASIEN)
ÖSTER-
REICH
UNGARN
GEORGIEN
ASER-
BAID-
SCHAN
FRANKREICH
SCHWEIZ
RUMÄNIEN
ARME-
NIEN
Schwarzes
Meer
SLO-
WENIEN
KROATIEN
BOSNIEN
UND
HERZE-
GOWINA
SERBIEN
IRAN
*SAN
MARINO
MONACO
BULGARIEN
ANDORRA
TÜRKEI
PORTU-
GAL
VATIKAN
ITALIEN
MONTE-
NEGRO
MAZE-
DONIEN
SPANIEN
ALBA-
NIEN
GRIECHEN-
LAND
SYRIEN
Mittelmeer
(NORDZ.)
IRAK
ATLAN-
TISCHER
OZEAN
ZYPERN
LIBA-
NON
JORDA-
NIEN
MAROKKO
ALGERIEN
TUNESIEN
MALTA
Mittelmeer
ISRAEL
SAUDI-ARABIEN

Internet Voting in Estonia



Was sind die Anforderungen an ein E-Voting System?

- Integrität – Das Ergebnis entspricht dem Willen der Wähler
  - Die Stimmen werden so abgegeben wie es der Wähler wollte
  - Die Stimmen werden so gezählt wie sie abgegeben wurden
  - Jeder Wähler hat nur eine Stimme
- Geheimhaltung – Das Wahlgeheimnis ist gewahrt
  - Niemand kann herausfinden für wen ich gestimmt hat
  - Selbst wenn ich versuche es jemandem zu beweisen

BBC NEWS

Watch One-Minute World News

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

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.

Estonia says many state websites have been affected

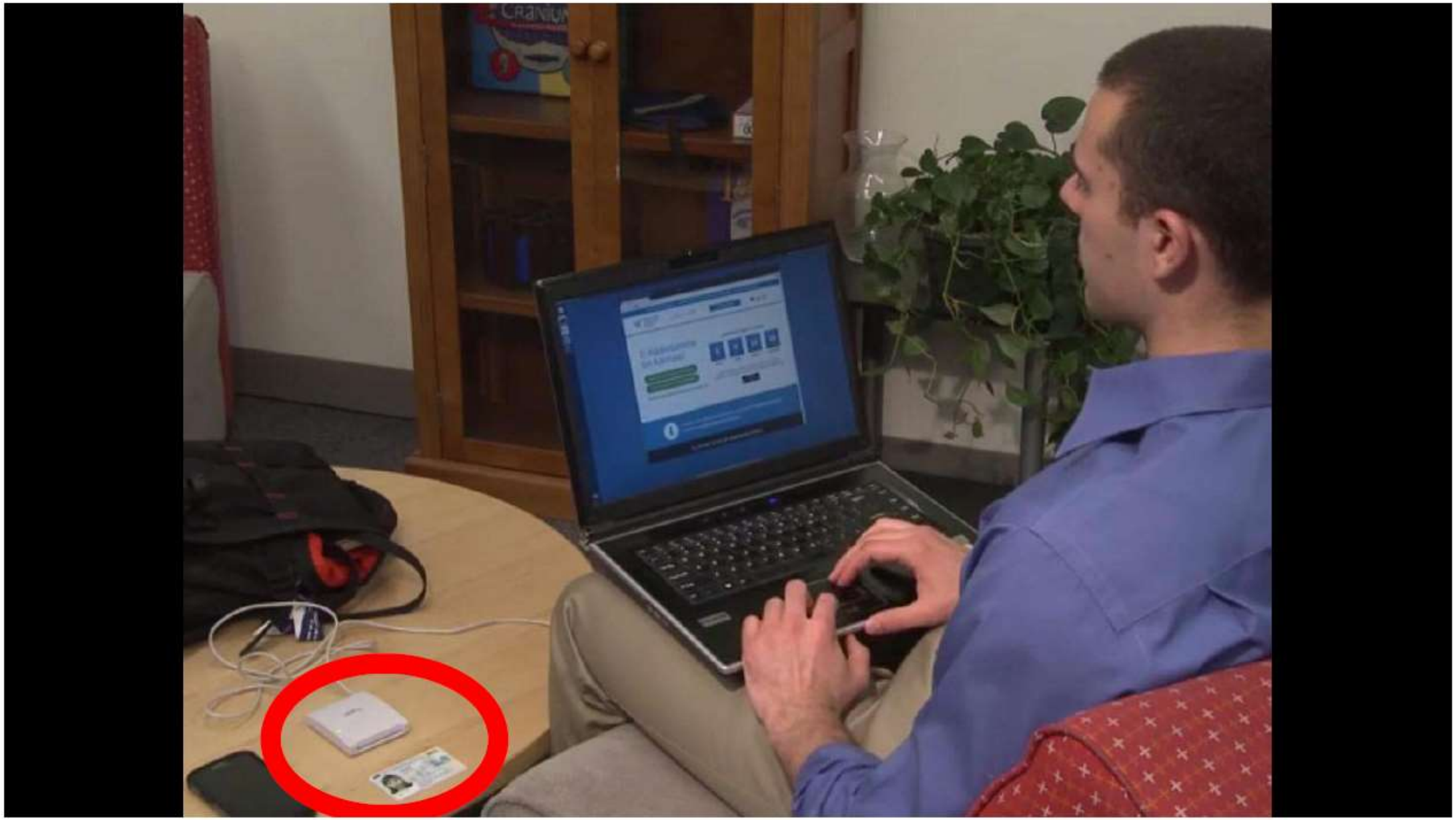
Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.

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

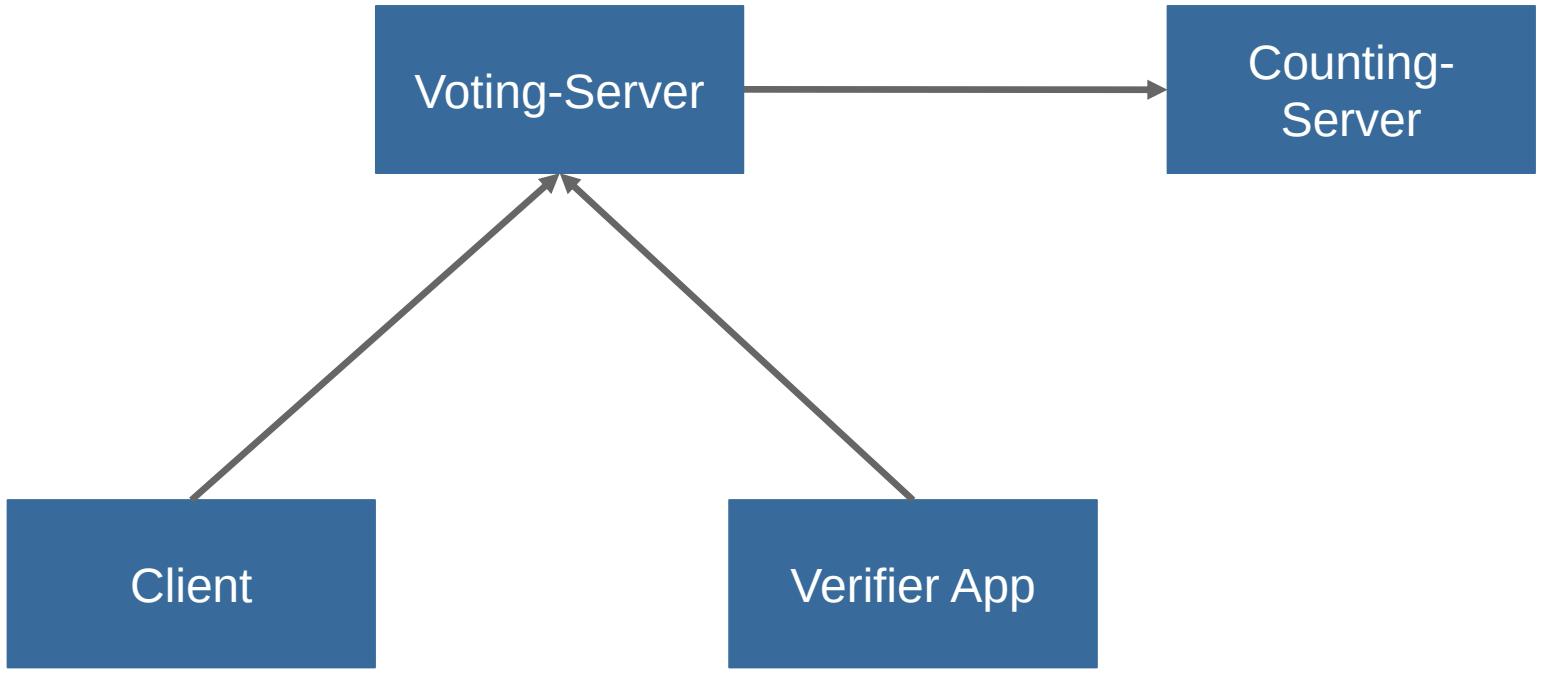
A Nato spokesman said the organisation was giving Estonia technical help.

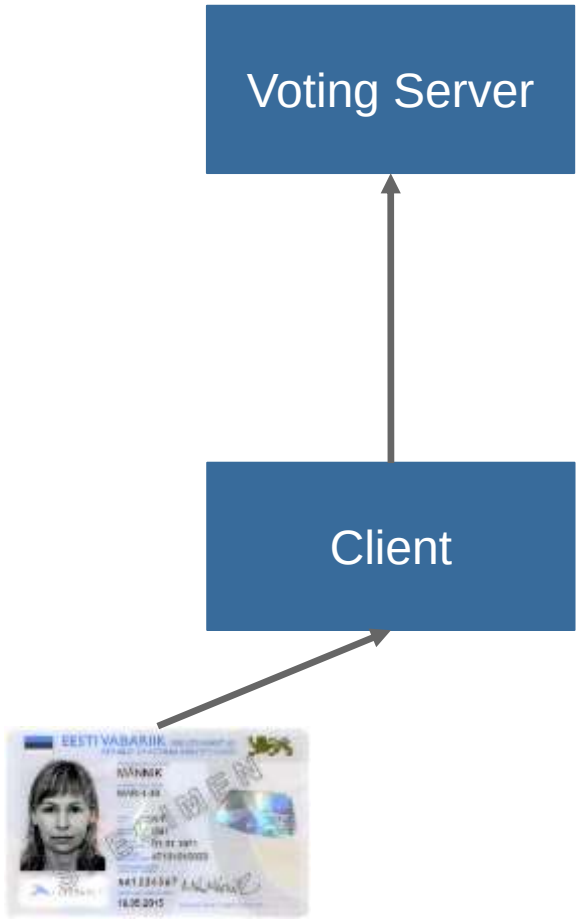

EESTI VABARIIK ISIKUTUNNISTUS
REPUBLIC OF ESTONIA IDENTITY CARD
MÄNNIK
MARI-LIIS
N/F
EST
01.01.1971
47101010033
AA1234567
19.05.2015
SPECIMEN


EESTI / EST
19.05.2010
IDESTAA12345678<<<<<<<<<<<<<<<
7101010F1505199EST<<<<<<<<<<<0
MAENNIK<<MARI<LIIS<<<<<<<<<<<



Architecture Time!

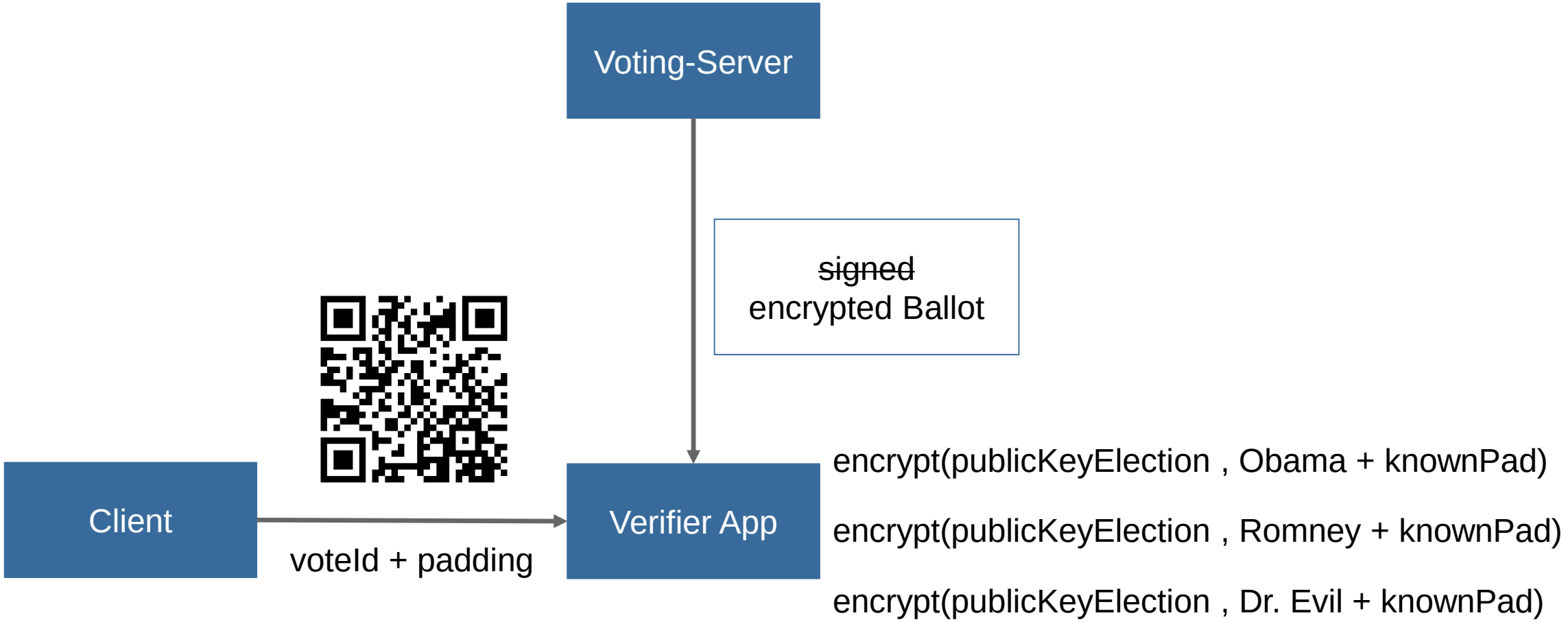


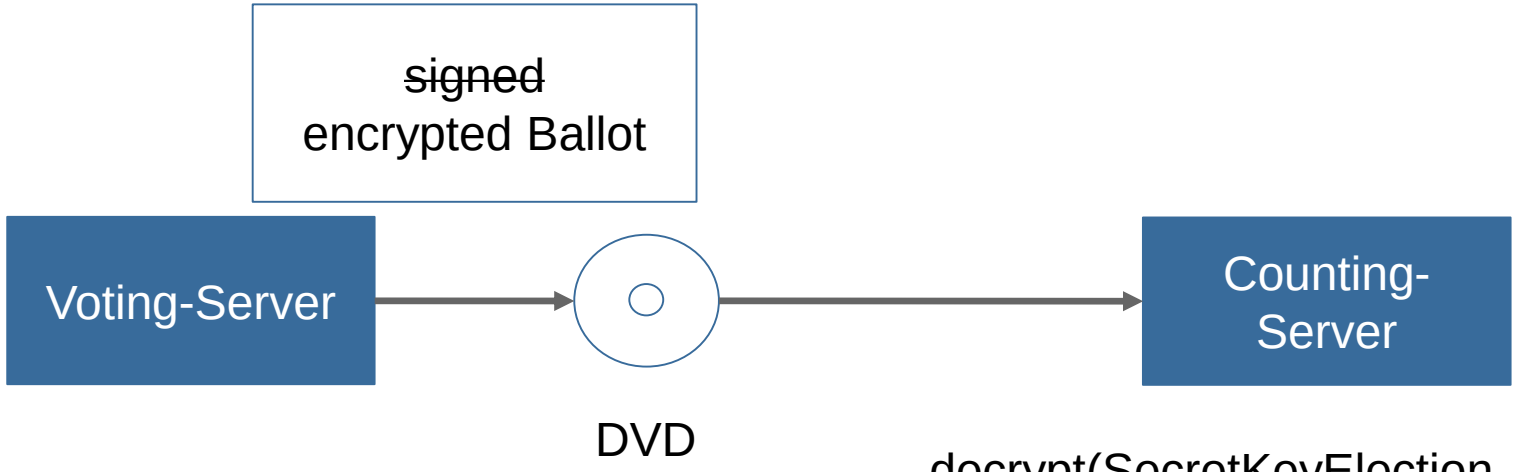


encryptedBallot = encryptRSA(publicKeyElection , vote + randomPad)

signedBallot = sign(secretKeyVoter, encryptedBallot)

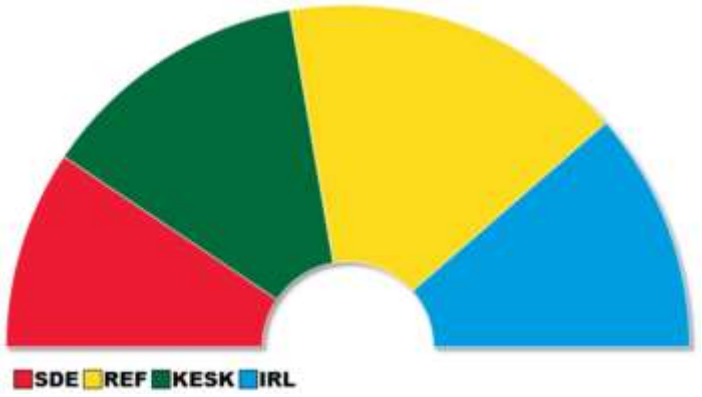
send(TLSClientAuth, signedBallot)


Voting-Server
~~signed~~
encrypted Ballot
Client
voteId + padding
Verifier App
encrypt(publicKeyElection , Obama + knownPad)
encrypt(publicKeyElection , Romney + knownPad)
encrypt(publicKeyElection , Dr. Evil + knownPad)



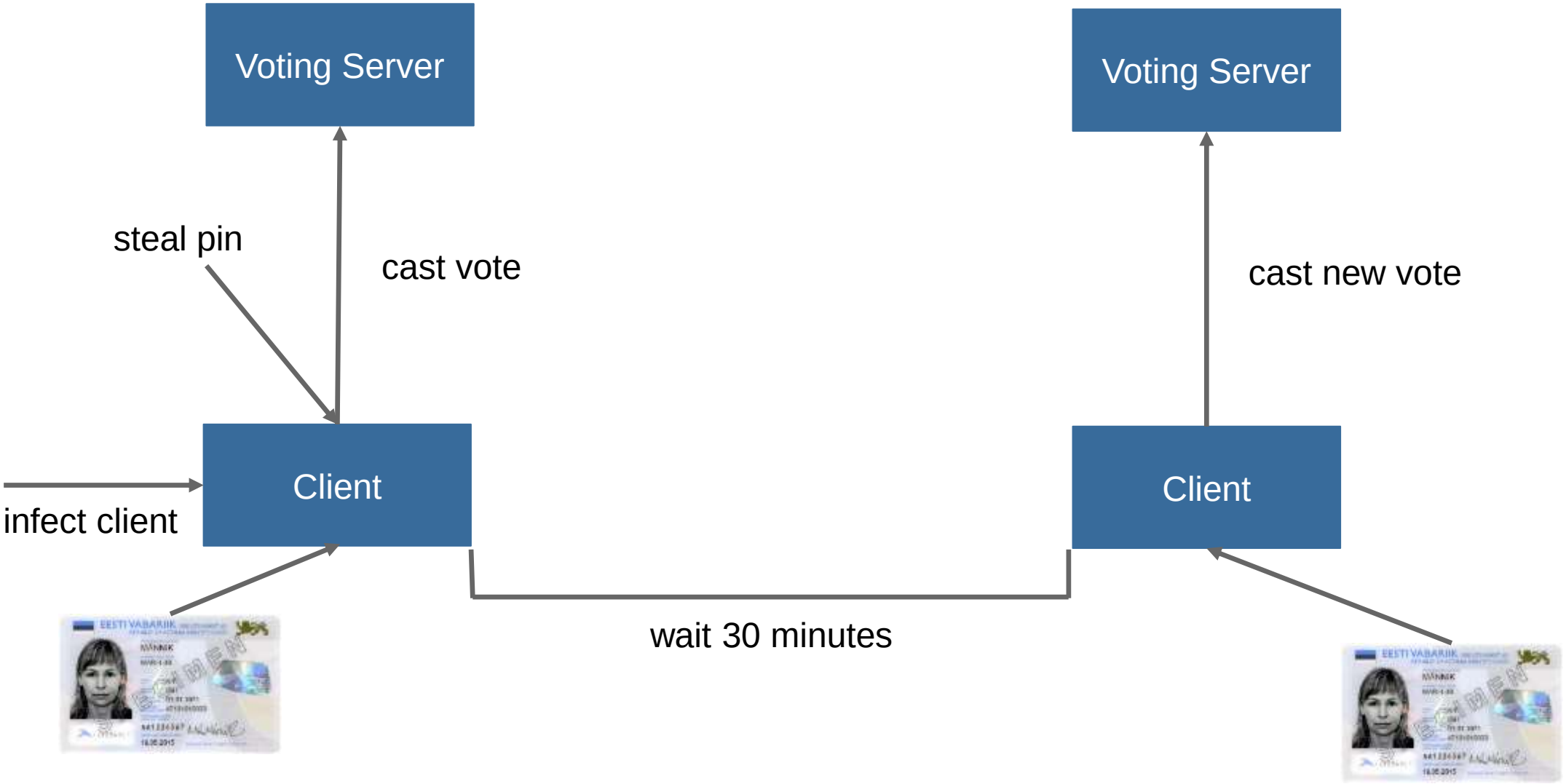
decrypt(SecretKeyElection, encryptedBallot)

count(ballots)

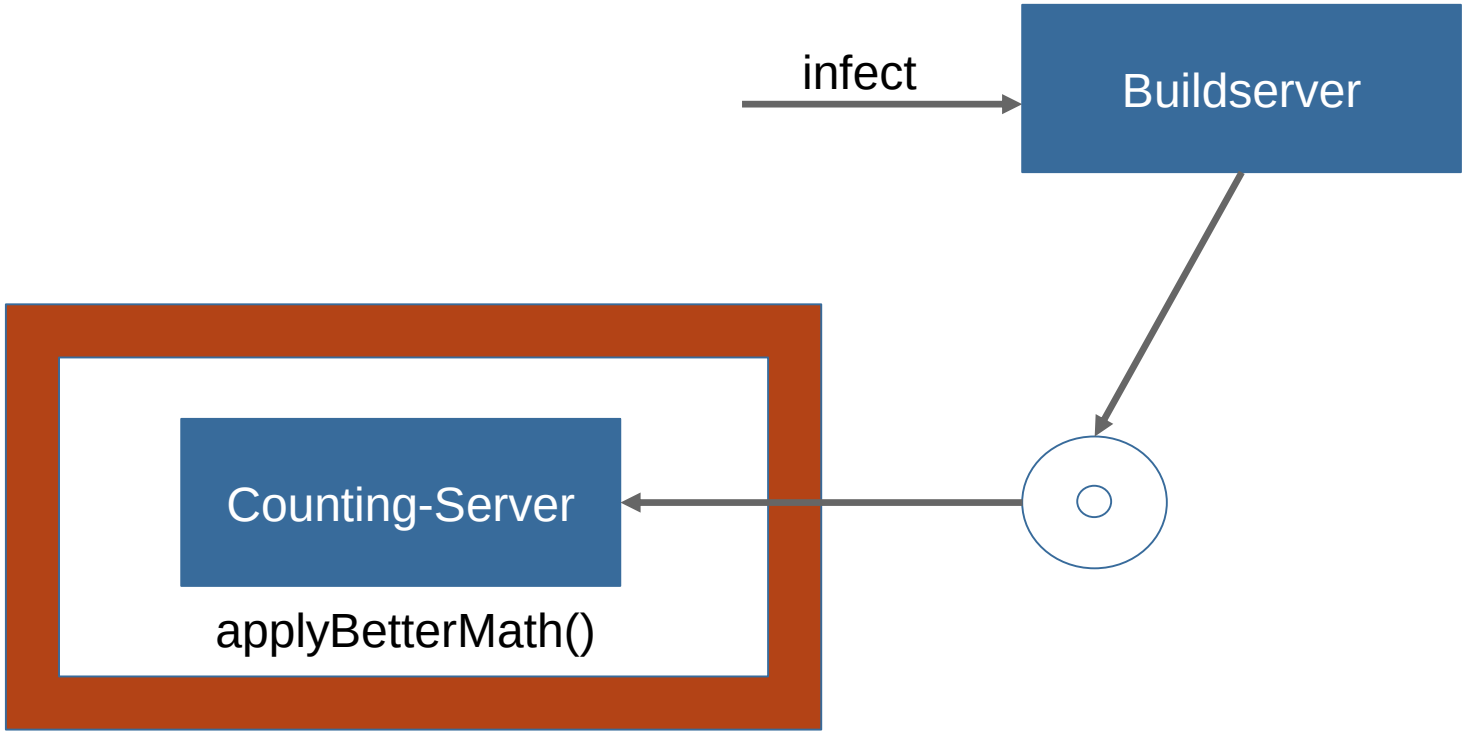


Ist das System angreifbar?

Client Side


Voting Server
Voting Server
steal pin
cast vote
cast new vote
Client
Client
infect client
wait 30 minutes

Server-Side

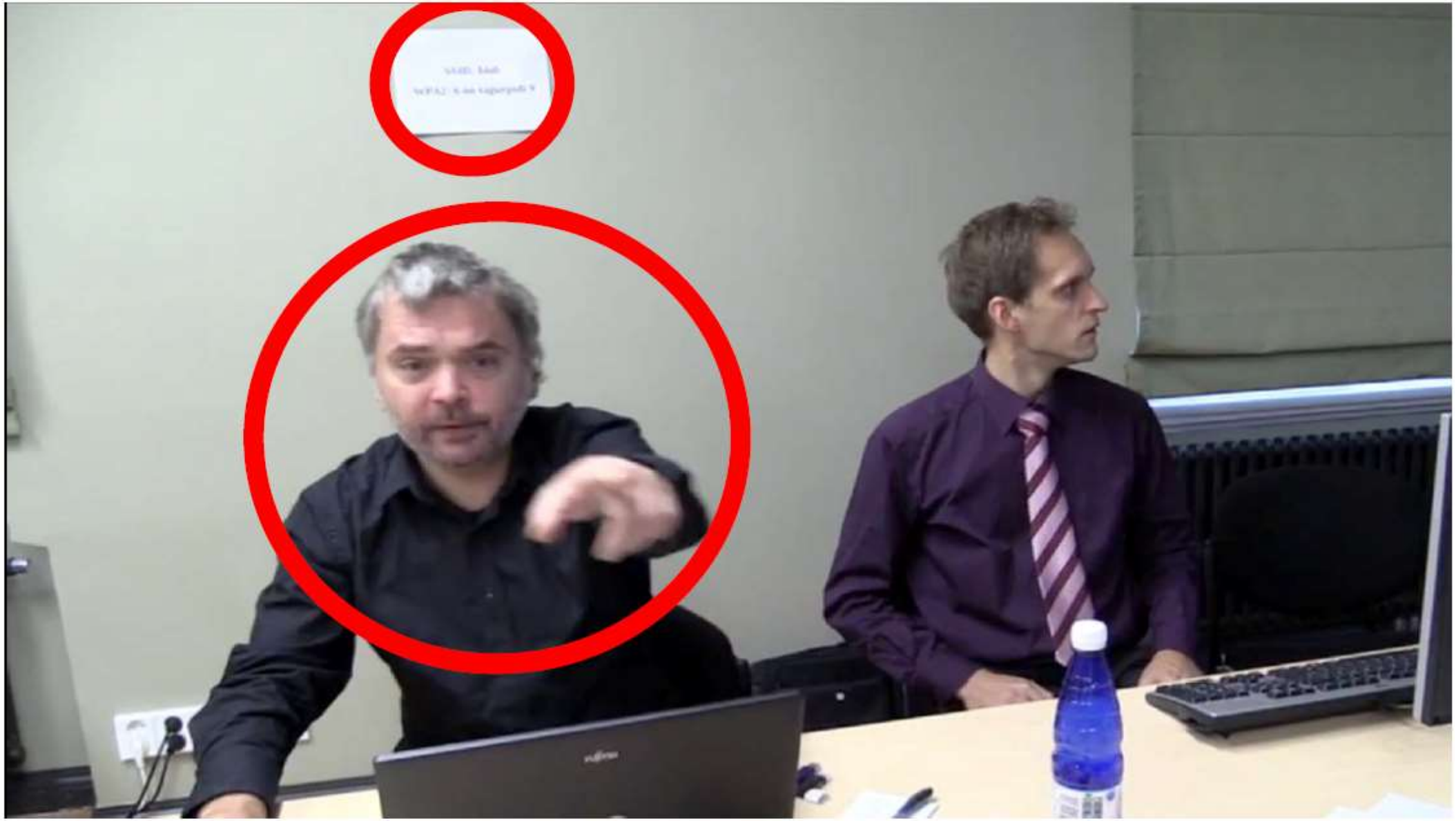


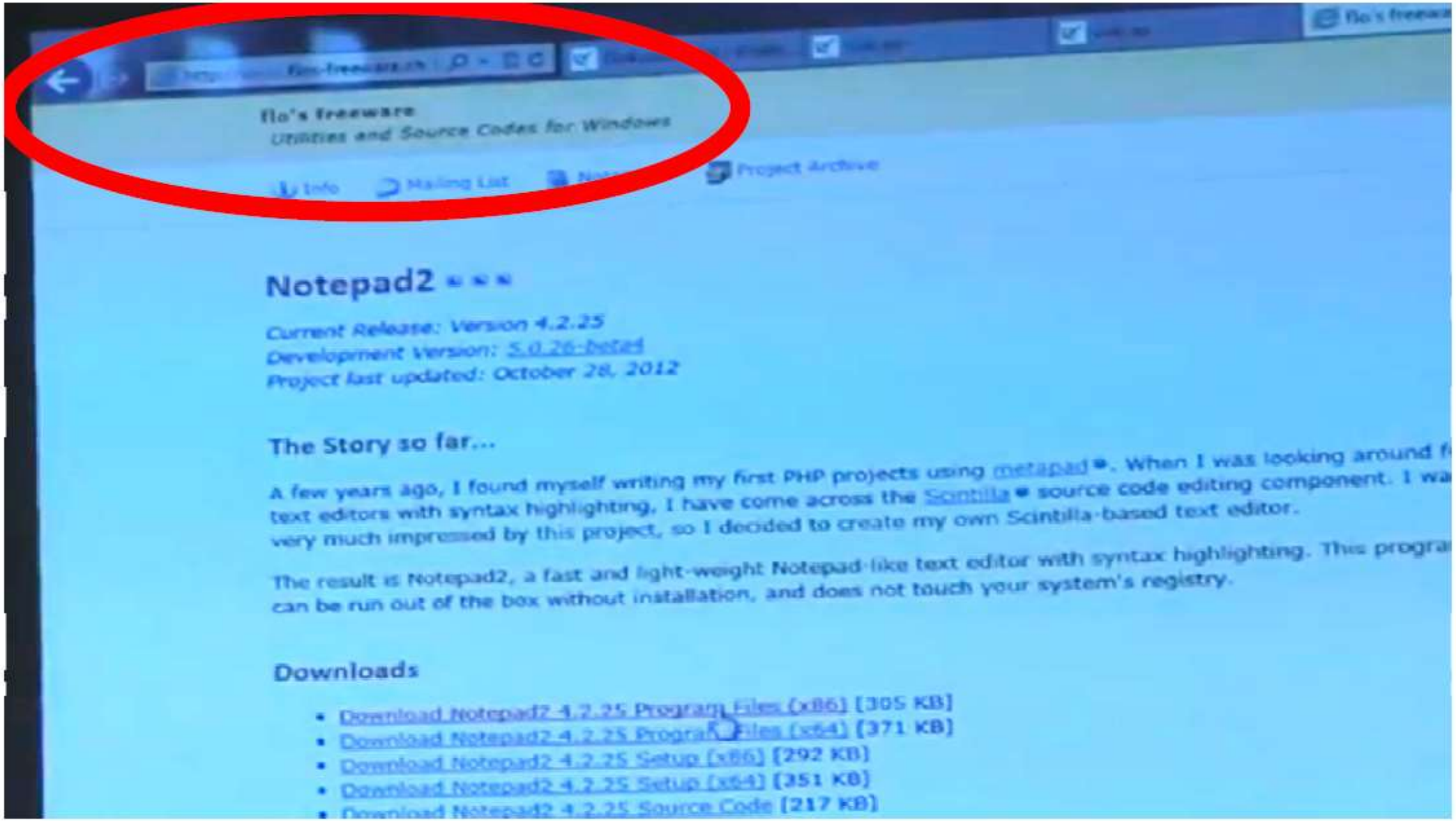
Operational Security

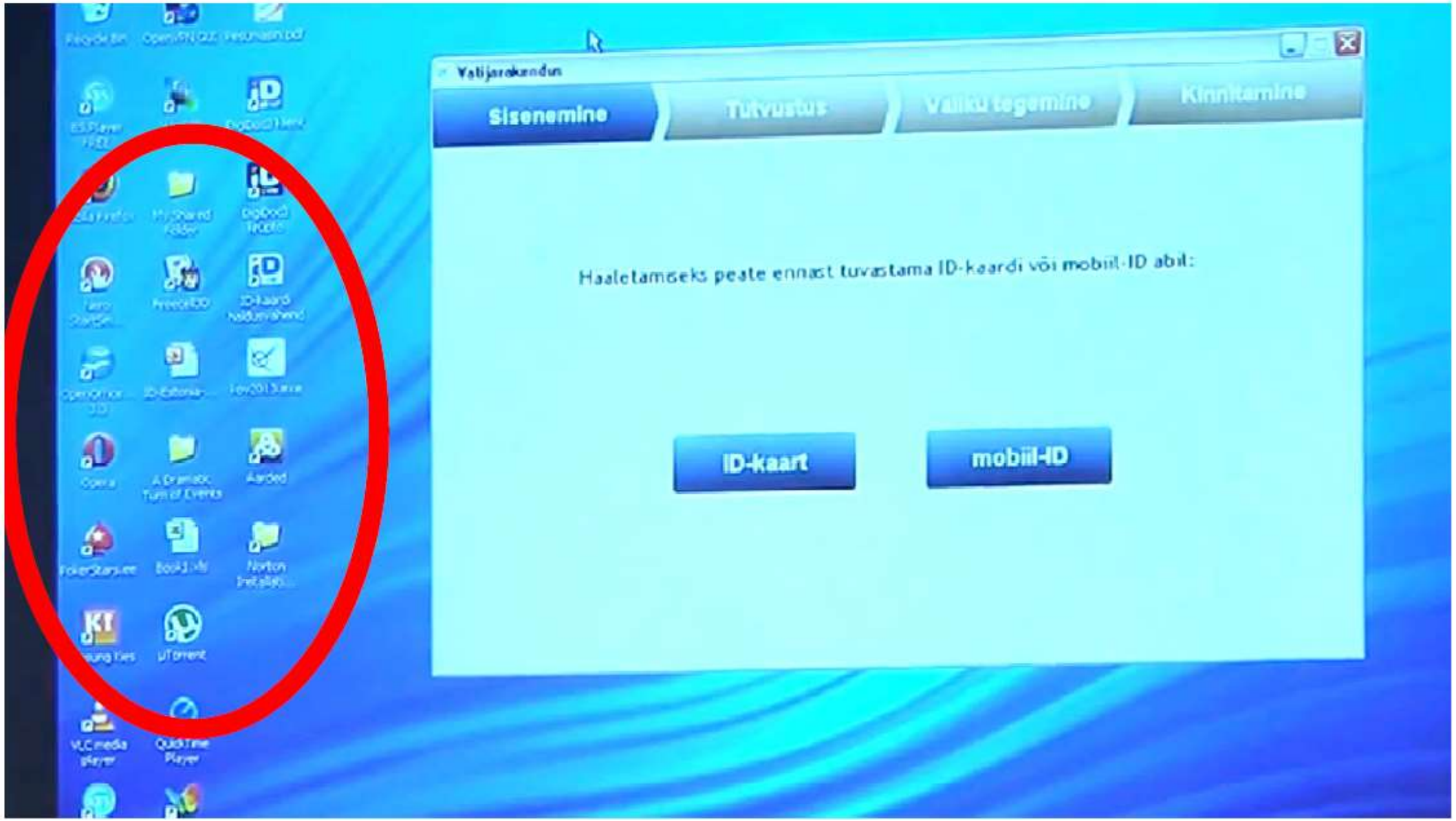
Our security is better than Google's.

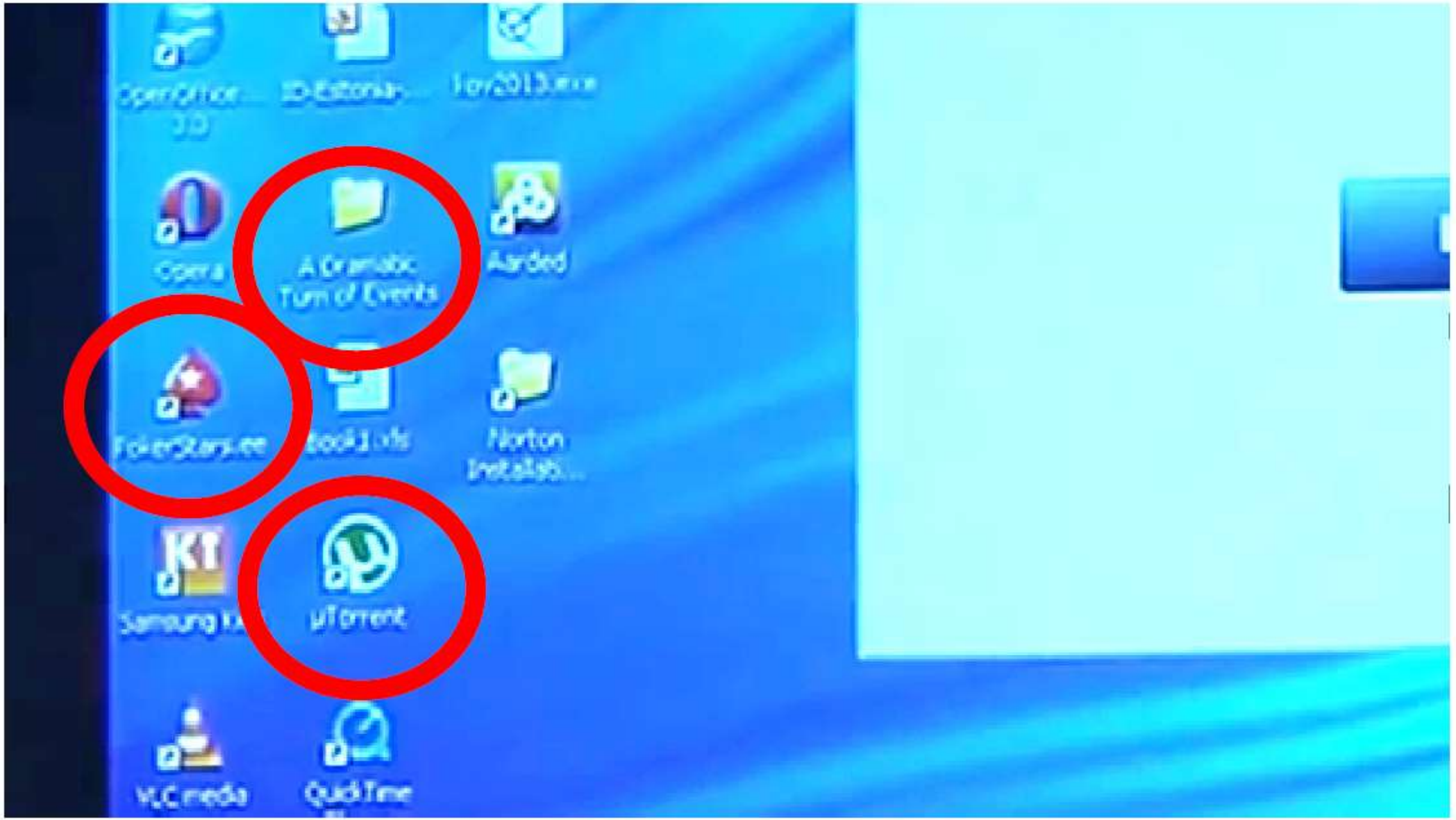
— Toomas Hendrik Ilves
President of Estonia

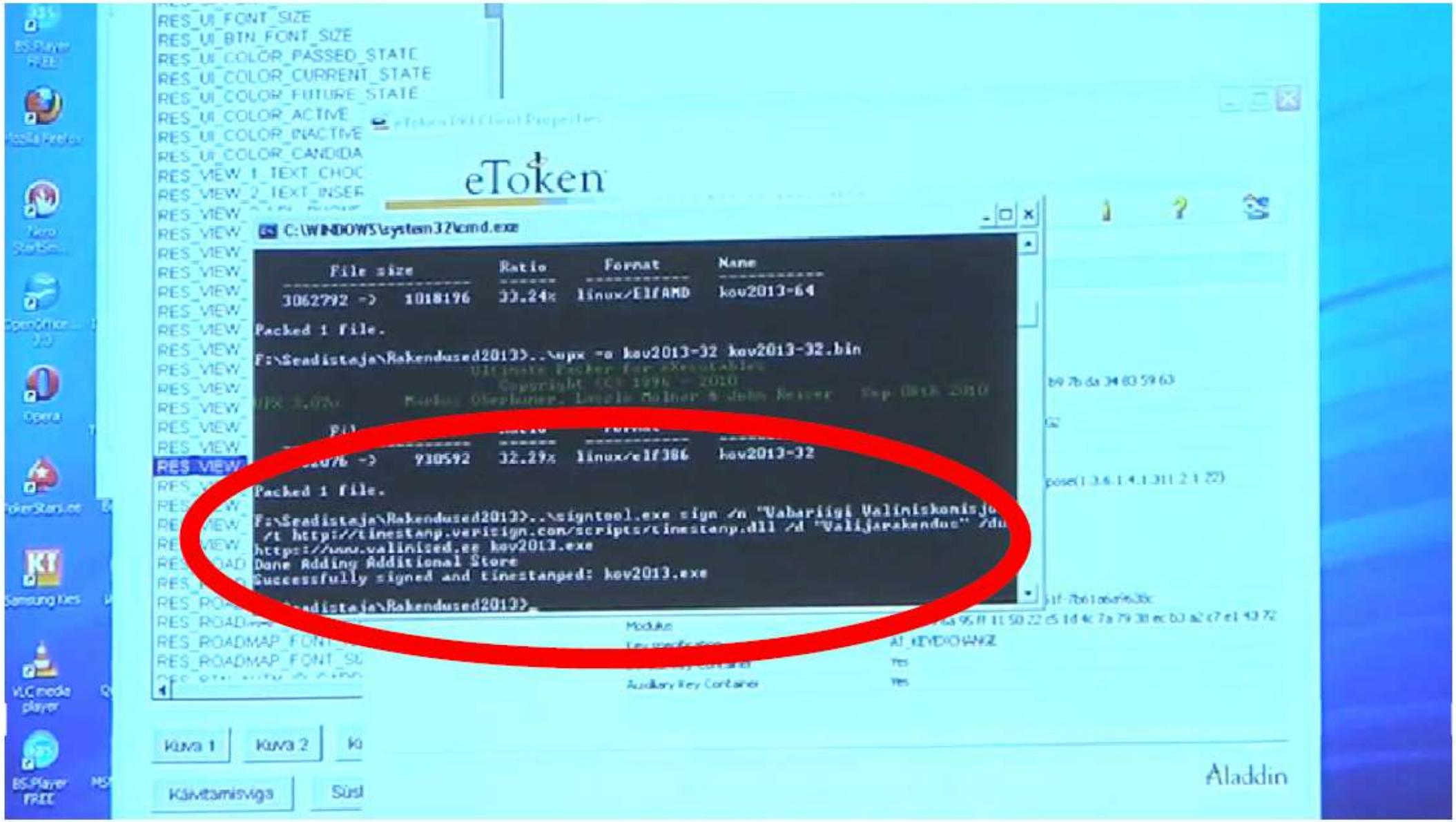

SHARP
Conference Series
Official YouTube Videos
00:13

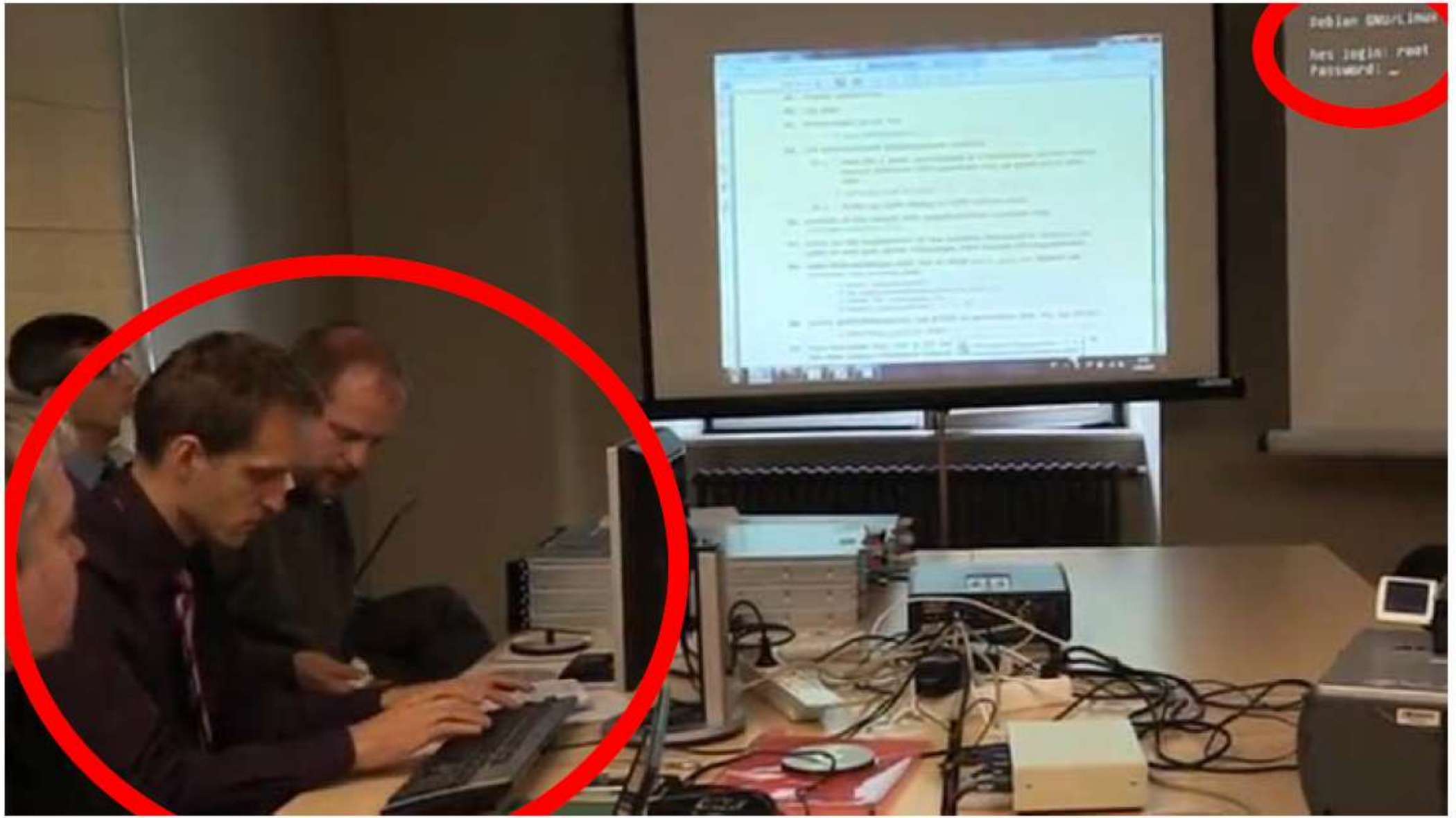


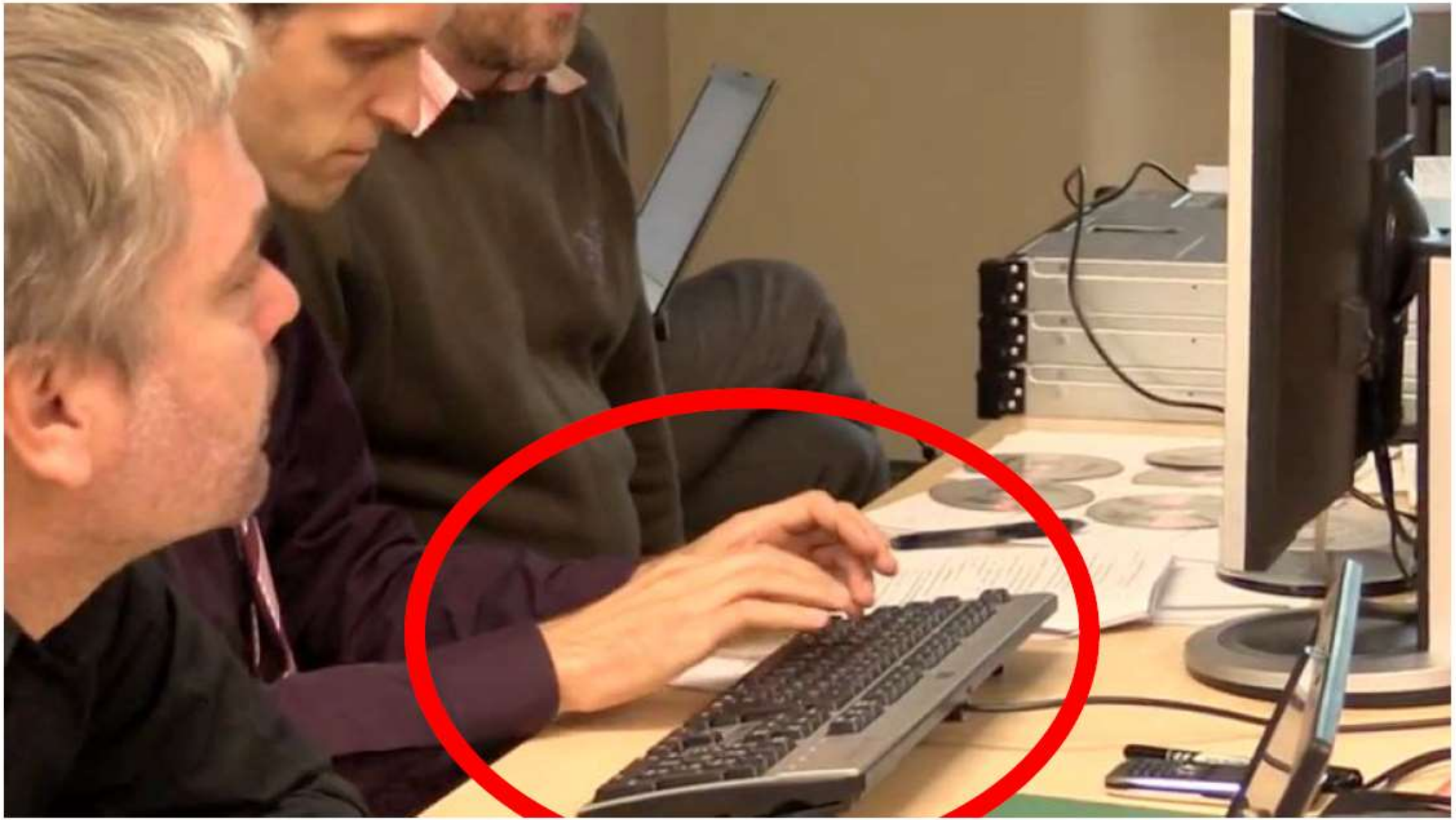

flo's freeware
Utilities and Source Codes for Windows
Info
Mailing List
Project Archive
Notepad2
Current Release: Version 4.2.25
Development Version: 5.0.26-beta4
Project last updated: October 28, 2012
The Story so far...
A few years ago, I found myself writing my first PHP projects using metapad. When I was looking around f
text editors with syntax highlighting, I have come across the Scintilla source code editing component. I wa
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 progra
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]


Valijarakendus
Sisenemine
Tuvastus
Valiku tegemine
Kinnitamine
Haaletamseks peate ennast tuvastama ID-kaardi või mobiil-ID abil:
ID-kaart
mobiil-ID


A Dramatic Turn of Events
µTorrent
QuickTime


eToken
C:\WINDOWS\system32\cmd.exe
File size Ratio Format Name
3062792 -> 1018196 33.24% linux/ElfAMD kov2013-64
Packed 1 file.
F:\Seadistaja\Rakendused2013>..\upx -o kov2013-32 kov2013-32.bin
930592 32.29% linux/elf386 kov2013-32
Packed 1 file.
F:\Seadistaja\Rakendused2013>..\signtool.exe sign /n "Vabariigi Valimiskomisjo
/t http://timestamp.verisign.com/scripts/timstamp.dll /d "Valijarakendus" /du
https://www.valimised.ee kov2013.exe
Done Adding Additional Store
Successfully signed and timestamped: kov2013.exe
Kuva 1
Kuva 2
Kävitamisviga
Aladdin


Debian GNU/Linux
box login: root
Password:



CERT Estonia

"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"


FAIL
1234*
failblog.org


Security Fail
failblog.org

Aber betrifft uns das überhaupt?

Middle school student charged with cybercrime in Holiday

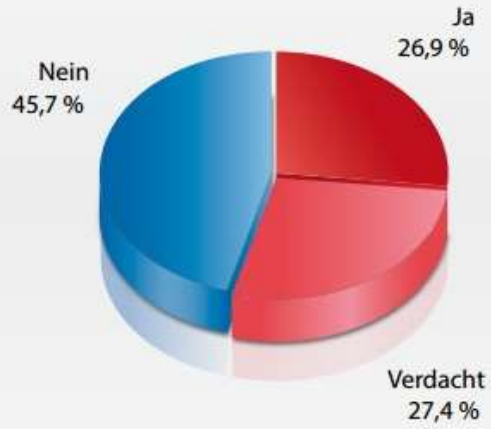
Green had previously received a three-day suspension for accessing the system inappropriately. Other students also got in trouble at the time, he said. It was a well-known trick, Green said, because the password was easy to remember: a teacher's last name. He said he discovered it by watching the teacher type it in.

The school district is in the process of changing the network password, district spokeswoman Linda Cobbe said.

Studie: Industriespionage 2014

Gab es in Ihrem Unternehmen konkrete Spionagefälle?

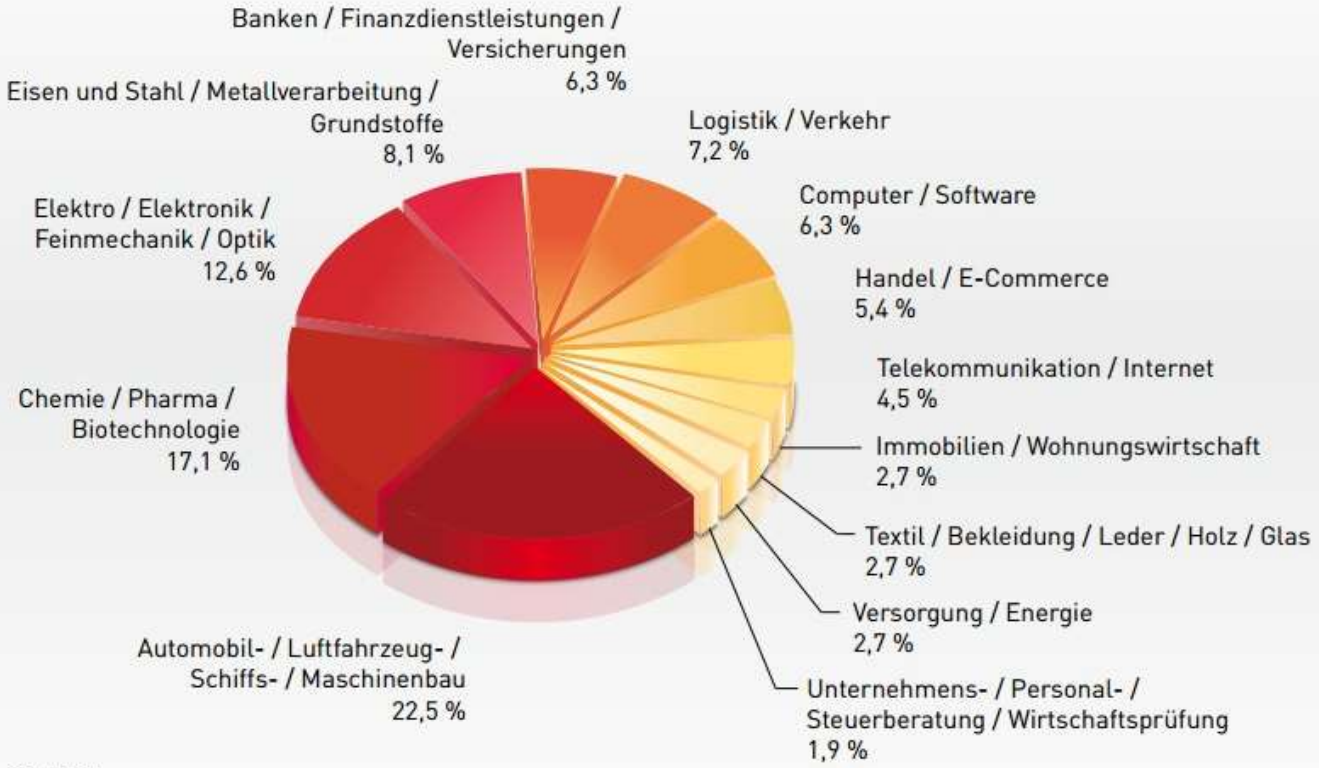
Deutschland



GRAFIK 2

Geschädigte Branchen

Deutschland



GRAFIK 6

Quelle: Corporate Trust

Nach Hackerangriff: Bundestagsnetzwerk wird mehrere Ta komplett abgeschaltet

Von Sven Röbel und Maik Baumgärtner

DPA

Bundestagspräsident Norbert Lammert: Schlechte Nachricht für die Abgeordneten

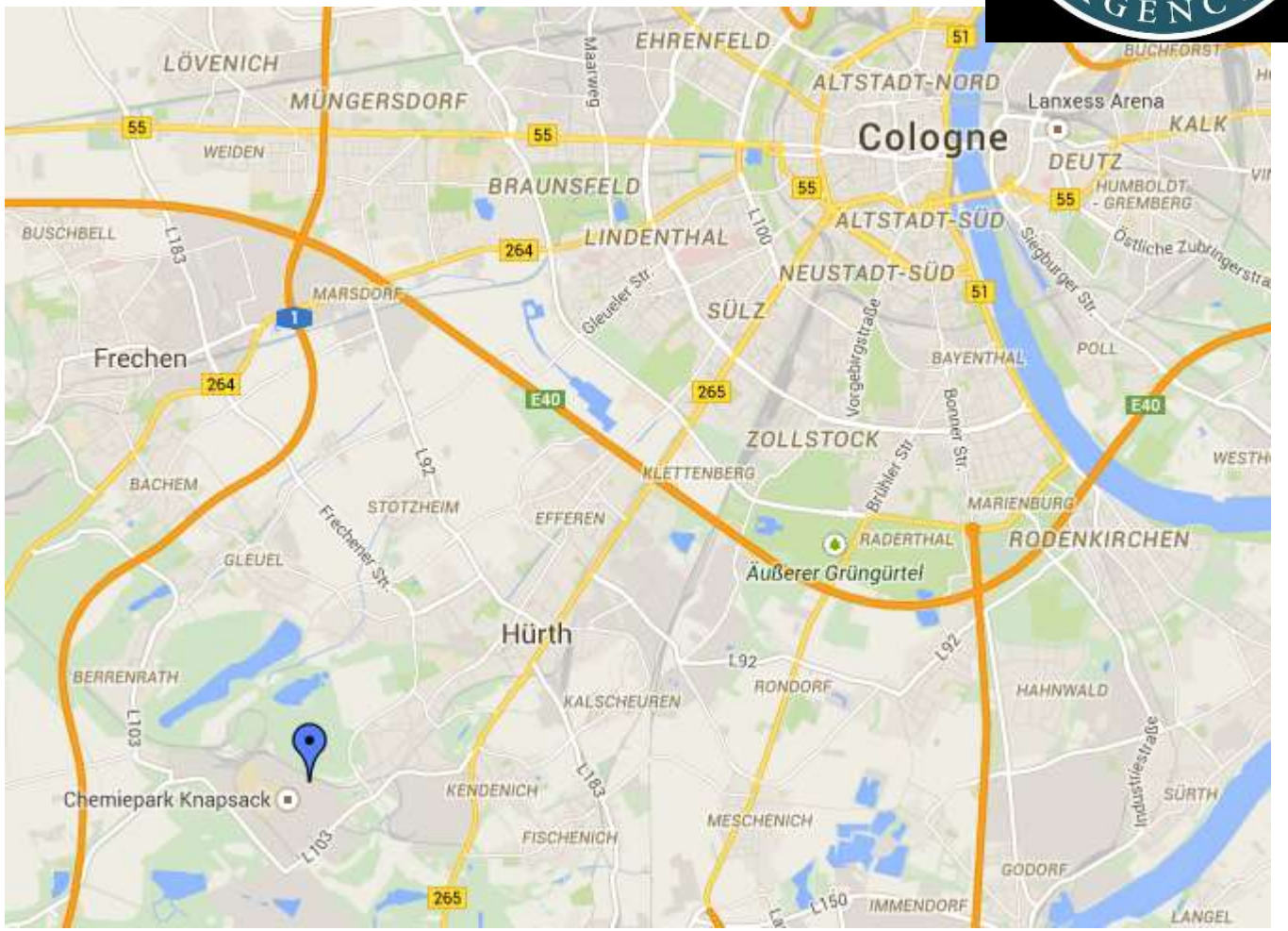
Nach dem Cyberangriff auf den Bundestag werden bald Teile des IT-Systems neu aufgesetzt. Für die Abgeordneten ist das ärgerlich: Sie müssen tagelang auf das Bundestagsnetzwerk verzichten.

Neue Dokumente von WikiLeaks

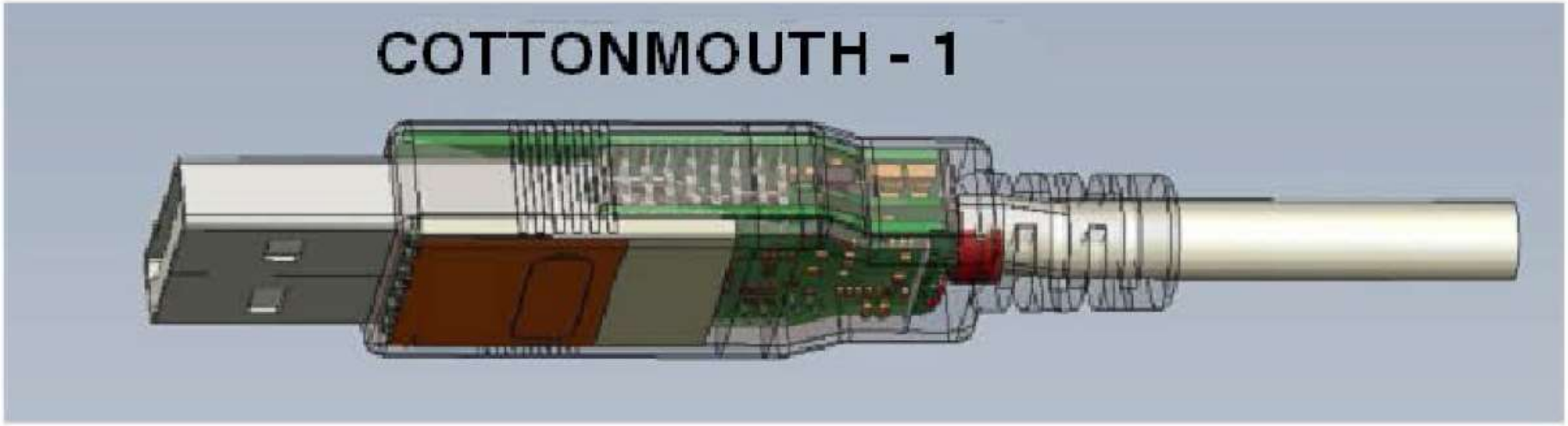
Großer NSA-Lauschangriff auf Bundesregierung

TOPI	Selector	Subscriber_ID	Information_Need	TOPI_Add_Date	Priority	IN_Explainer
S2C32	+49228682XXXX	MOF ASCHENBRENNER	2002-388*	101215	2	Germany: Political Affairs
S2C32	+4922817XXXX	OFF 400 FOR ECON POLICY	2002-388*	101215	2	Germany: Political Affairs
S2C32	+4922817XXXX	OFF 400 FOR ECON POLICY	2002-388*	101215	2	Germany: Political Affairs
S2C32	+4922817XXXX	OFF 400 FOR ECON POLICY	2002-388*	101215	2	Germany: Political Affairs
S2C32	+49228682XXXX	BUNDESMINISTERIUM DER FINANZEN MONEY LOAN DEPT	2003-2777*	101215	2	Multi-country: International Finance Developments
S2C32	+49228682XXXX	GE INT BS FIN MIN CZAKERT	2003-2777*	101215	2	Multi-country: International Finance Developments
S2C51	+49691344XXXX	EUROPEAN CENTRAL BANK	2003-2777*	110111	3	Multi-country: International Finance Developments
S2C32	+49228682XXXX	GERMAN FIN MIN STATE SEC	2002-388*	101215	2	Germany: Political Affairs
S2C32	+49228682XXXX	GERMAN MINIST FINANCE	2002-388*	101215	2	Germany: Political Affairs
S2C32	+49228682XXXX	GE INT TR MIN OF FIN HEND	2002-388*	101215	2	Germany: Political Affairs

Stellar Professional Communication Systems GmbH ®



(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.



Page 149

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

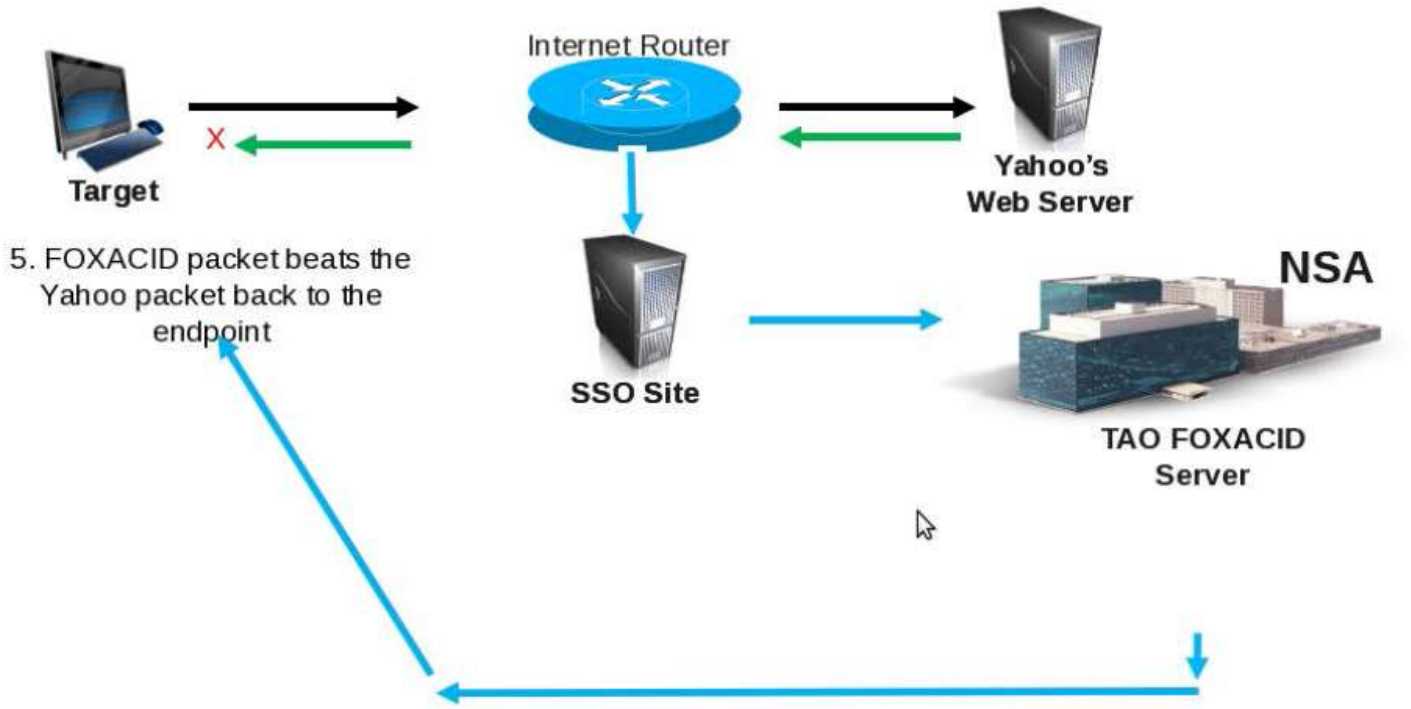
(TS//SI//REL TO USA,FVEY) The CTX4000 is a portable continuous wave (CW) radar unit. It can be used to illuminate a target system to recover different off net information. Primary uses include VAGRANT and DROPMIRE collection.

(TS//SI//REL TO USA,FVEY) The CTX4000 provides the means to collect signals that otherwise would not be collectable, or would be extremely difficult to collect and process. It provides the following features:

- Frequency Range: 1 - 2 GHz.
- Bandwidth: Up to 45 MHz
- Output Power: User adjustable up to 2 W using the internal amplifier; external amplifiers make it possible to go up to 1 kW.
- Phase adjustment with front panel knob

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

What can we do?

- Im WWW
  - mit HTTPS Everywhere TLS enforcen
  - https://www.eff.org/de/https-everywhere

HTTPS Everywhere

  - Mit TOR wirklich anonym surfen
  - https://www.torproject.org/

Tor

What can we do?

- In der Kommunikation
  - Emails verschlüsseln mit PGP
  - https://www.gnupg.org/

GnuPG

  - Mit OTR NSA-Sicher chatten
  - https://de.wikipedia.org/wiki/Off-the-Record_Messaging

Off-the-Record Messaging

What can we do?

- Auf dem Handy verschlüsselt telefonieren und chatten
  - Auf Android mit Redphone und Textsecure
  - https://whispersystems.org/

  - Auf Iphone mit Signal
  - https://whispersystems.org/

What can we do?

- Auf dem eigenen Rechner
  - Die Festplatte verschlüsseln mit Truecrypt
  - http://www.heise.de/download/truecrypt.html

  - Und Passwörter mit Keepass
  - http://keepass.info/

What can we do?

- Oder das Gesamtpaket: TailsOS
- https://tails.boum.org/


ID#: 31337
Name: Scriptkiddie
Federal Bureau of Investigation


NATIONAL SECURITY
ALL
YOUR
DATA
AGENCY