

Critical look at Estonian E-voting protocol

Helger Lipmaa and Sven Heiberg

Tallinn University and Cybernetica AS
Estonia

Outline

- Personal perspective (highly opinionated)
 - Cultural background
 - Birth pains of Estonian e-voting from our view
- Description of e-voting protocol
- Critique
- Correspondence to constitution?
- Estonian e-voting experience up to now

Estonian e-voting: nutshell

- Estonian culture:
 - Highly dynamic, newly democratic, do not trust authorities (incl academia)
 - No legacy systems. Can build instead of renovating
- E-voting in Estonia reflects that:
 - It functions, people welcome it as a sign of 21st century
 - Academic criticisms (security, ...) are ignored
 - Democracy is new: criticism based on importance of proper voting in democratic societies --- ignored
 - If broken, it will be replaced on the go

Personal Perspective (HL)

- PhD – 1999
- 2000-2010 – spent 7 years abroad („foreigner“)
 - 2000-2005 Finland (Helsinki UT, 2001+, professor)
 - 2006-2008 UK (University College London)
- Currently Tallinn University (professor) + Cybernetica AS (senior researcher)
- *Note: Cybernetica AS produces Estonian e-voting software, but **no** protocols. Opinions are strictly my/our own*

Personal Perspective (HL)

- 1999:
 - Invited Berry Schoenmakers to lecture in Estonia
 - Got interested in e-voting as a research topic
 - Estonia was preparing for digital signature law, id card, ... passively pushed e-voting?
- ~2000: Started to supervise a talented Estonian student, Oleg Mürk
- Late 2000/early 2001
 - Contacted by Estonian authorities, to investigate possibility of nationwide Internet voting in Estonia

Personal Perspective (HL)

- 2001 May:
 - Submitted a joint report (with Oleg Mürk, in Estonian, 37 pages) about existing e-voting protocols to Estonian government
 - Recommendation: start preparing for e-voting, but a lot of research is needed
- Then: silence. Whispers in the dark:
 - Our report was interpreted like we were anti e-voting
 - Decision not to involve people from academia anymore

E-valimiste realiseerimisvõimaluste analüüs

Helger Lipmaa

helger@tml.hut.fi

<http://www.tml.hut.fi/~helger>

Oleg Mürk

olegm@ut.ee

<http://www.ut.ee/~olegm>

9. aprill 2001. a.

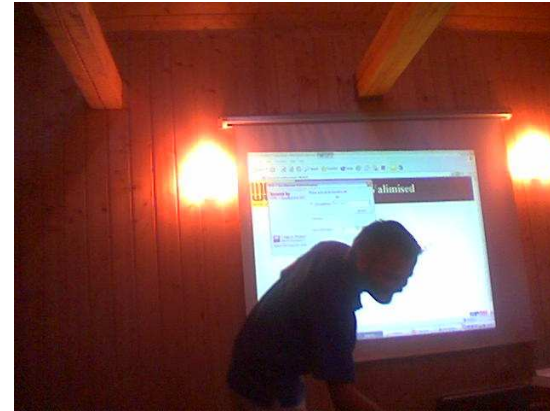
Personal Perspective (HL)

- 2003 Spring:
 - Panel on e-voting in Tallinn, with some ministers, etc
- 2003 Summer:
 - Kickoff meeting of Estonian e-voting interest group: members of electoral committee, security heads of local banks, ...
 - I was the only researcher
 - I gave an overview about research on e-voting
 - Homomorphic schemes, mixnets, ...
 - People were confused
 - Guy from electoral committee: what do you mean by “you don’t trust us”?



Personal Perspective (HL)

- The same meeting, 2003 Summer:
 - Tarvi Martens gave a presentation about the “double envelope” scheme
 - Essentially the same scheme is used also now
- 2004: e-voting seminar in Tartu, Estonia
 - Participants: Berry Schoenmakers, Jens Groth, people from Estonian interest group
 - Then-leader of working group: We mainly do it for hype



2003, First Nokia Phone with Camera

Personal Perspective (HL)

- (2009: involved in Norway)
- (2009: invited talk at VOTEID 2009)
- Next try, 2010:
 - We tried to explain the Norwegian solution
 - This was answered by blank stares
- **VOTEID 2011 in Estonia**
- OTOH, when I am abroad, people ask me why Estonia uses such protocols



Personal Perspective (SH)

- Active in professional software development since 1999
- Programmer, architect, project leader
- More concerned about making things work than breaking them
- Not scientist

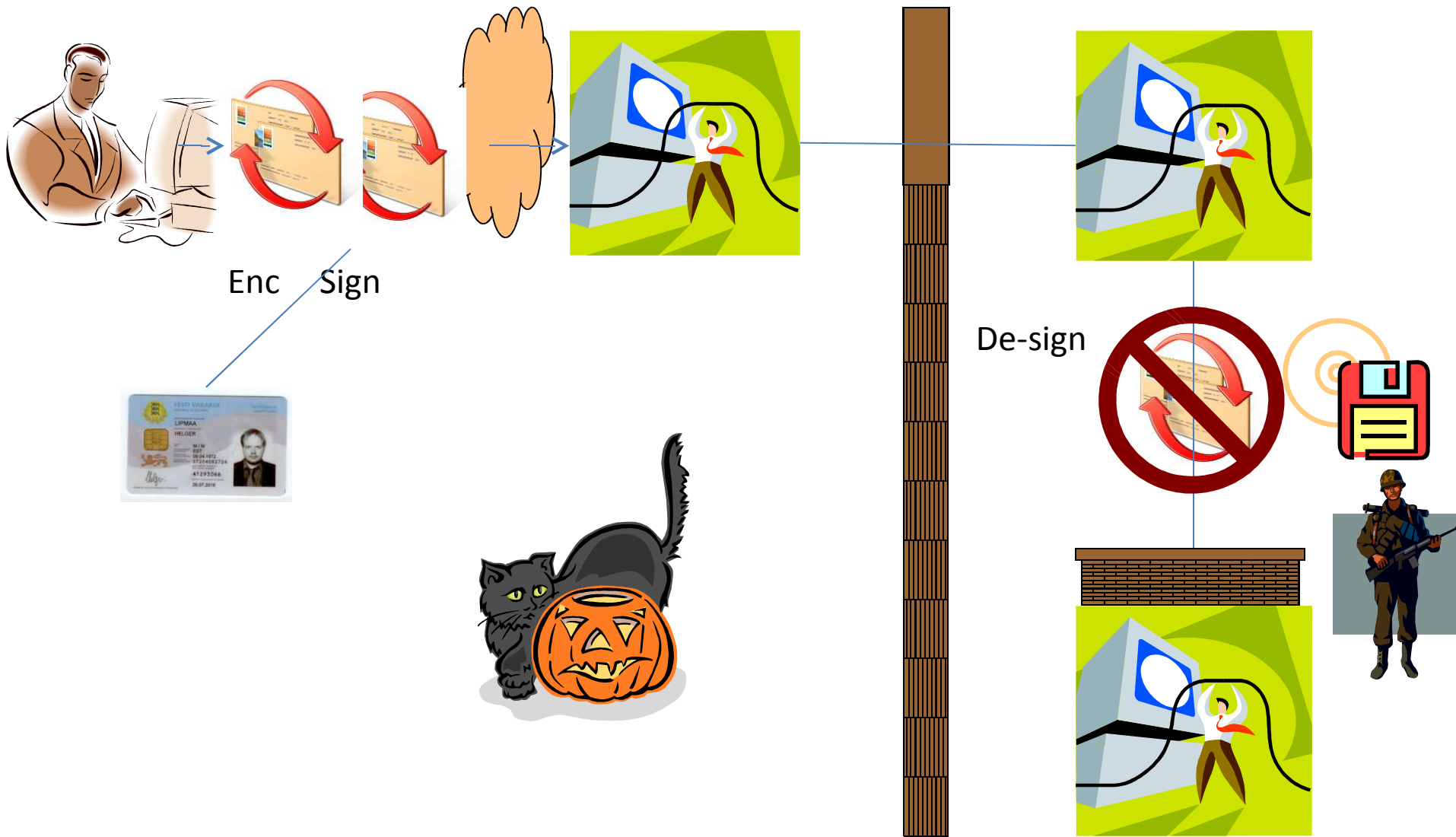
Personal Perspective (SH)

- E-voting software development project started in 2004
 - Implement double-envelope scheme
 - Support for various hardware/OS/browser combinations
 - Support various types of simultaneous elections (local government, parliament, referendums)
- 2005 – successful pilot
- Since then – various facelifts to the working system, the concept stays same
- 2009 – Norwegian project

Estonia: Prerequisites

- Access to Internet
 - Public access-points, people used to e-banking
 - Most pubs/restaurants have free wifi
- Legally accepted digital signatures
 - Digital Signature Act since 2000
- Infrastructure for digital signatures
 - Nationwide PKI since 2002
 - ID-card: RSA capable chipcard
 - Used for authentication and digital signatures

Estonian E-voting protocol



Who can attack?

- Computer user
 - Wrong user
 - Coercion/vote buying
- Voter PC
 - Any kind of malware
- Big Bad Internet
- Voting Servers
- Journalists

“Bad” Voter

- Voter authenticates themselves by using Estonian ID-card
 - Do we trust ID-card (out of scope)?
 - Do we trust drivers?
- Vote coercion/buying
 - Alleviated by revoting (possibly p-voting)
 - If this does not help: “you have bigger problems than e-voting security”



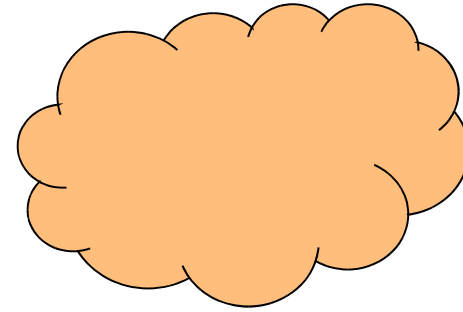
“Bad” Voter PC

- Malware, Trojans, viruses, ...
- No privacy against malicious PC
- Non-verifiable against mal. PC
- Trojan can also sign for you
- “You have bigger problems than e-voting security”



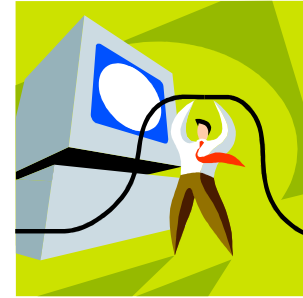
“Bad” Internet

- Votes are encrypted and signed
- No obvious attacks, except DDOS
- Only one central voting server!



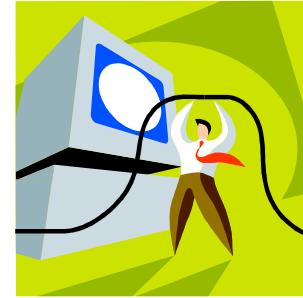
“Bad” Voting Servers

- 3 servers: Vote Forwarding Server, Storing Server, Counting Server
- There is some non-public auditing
- Forwarding Server:
 - Online server, receives  votes
- Storing Server:
 - Behind firewall, receives  votes, removes signatures
- Counting Server:
 - Completely offline, receives  votes on CD, physically secured



“Bad” Forwarding Server

- Online server, receives  votes



Can't forge or read (alone)



Can selectively drop votes



Can collaborate with coercer/vote buyer



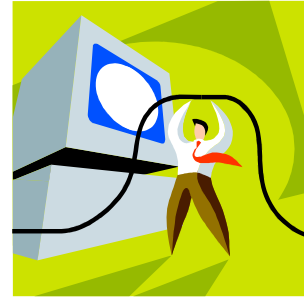
Possible DDOS, ... attacks



No verifiability

“Bad” Storing Server

- Intranet server, receives votes



- :) Can't forge or read (alone)
- :(Can selectively drop votes
- :(Can collaborate with coercer/vote buyer
- :(**No verifiability**

“Bad” Counting Server

- Offline server, receives  votes



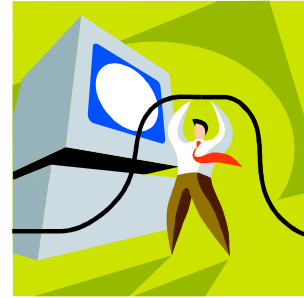
Can tally incorrectly



Or just (selectively) stop
functioning



No verifiability



“Bad” Process

- Security is mostly “guaranteed” by organizational means
- Watchdogs against DDOS
- Auditing traffic between servers
- SS->CS by secure physical means
- *Who guards the guardians?*
- Need to trust people and processes blindly
- Electoral Committee: “Why not?”



“Bad” Journalists: PR attacks

- Successful PR attack against e-voting may reduce trust
=> back to p-voting
- My/Norwegian/... solution:
 - Involve local academics in the process, have international reviews, ...
- Estonian solution:
 - Make process so simple that John Doe can understand how it works => in the case of attacks John Doe blames himself for not being clever enough
 - Obviously John Doe does not understand cryptography
 - Estonians don't trust academia/...

Constitution

- §1 – Estonia is independent and sovereign democratic republic. The supreme power is vested in the people.
- §56 – People exercise their power through citizens' right to vote.
- §156 – Local governments are elected in free elections for three years. Elections shall be general, uniform and direct. The ballot is secret.

Requirements by Constitution

- Elections are free
 - You decide how to vote
- Elections are general
 - All citizens have right to vote
- Elections are uniform
 - All votes are equal
- Elections are direct
 - The vote is given to a concrete candidate
- The ballot is secret
 - No-one has to know whether and how you voted

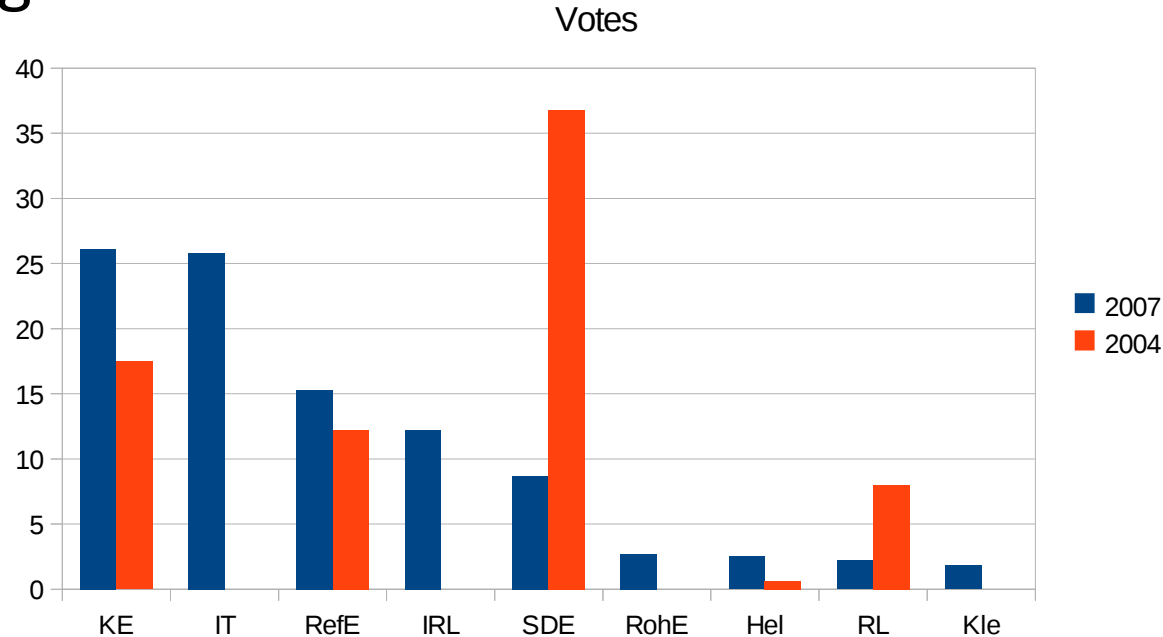


Estonian E-voting: Story

- 2005, Local government, **9 317 (0.9%)**
- 2007, Parliament, **30 275 (3,4%)**
- 2009, European Parliament, **58 669 (6,5%)**
- 2009, Local government, **104 413 (9,5%)**
 - 44% of advance voters were also e-voters
 - E-votes were sent out of 82 countries

What if?

- Europarlament elections 2009: 58669 evotes
- Difference between #1/#2: 1046 votes (1 mandate), both got about 103000 votes



Norwegian Experience (2009)

- Different attitude from government: security is paramount
- Big question: achieving security when voter PCs are corrupted
- We proposed a new setting and a new protocol
 - „Code-verification voting“
 - Published at ESORICS 2010
- Norway uses another protocol, but the same setting
- I am continuing research, improvements on both protocols
- Well-organized process, main criticism: research and implementation should have been carried out separately
 - Same company was supposed to do crypto and p-voting

Questions?

