Internet voting in Estonia: risk modelling and vote verification

Sven Heiberg, Jan Willemson
Cybernetica, STACC

22.05.2012

Risk modelling

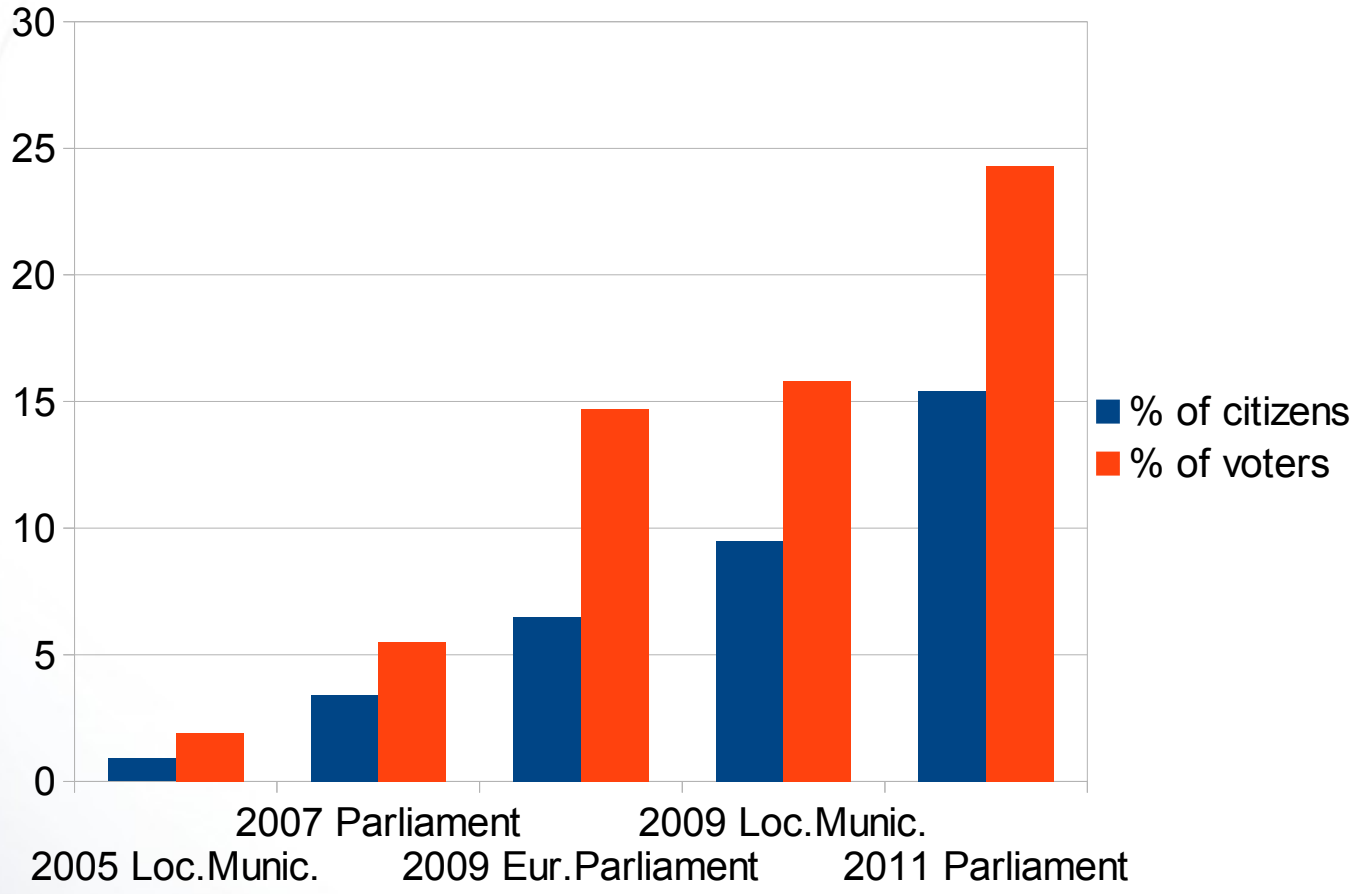
Internet voting (i-voting)

- I-voting is a form of electronic voting
  - Vote is cast with a voting tool
  - Vote is transported to election officials over the internet
  - It is possible to vote without any paper
- The term “electronic voting” also covers other methods we will not consider
  - Electronic verification of paper ballots
  - Code voting

A bit of history

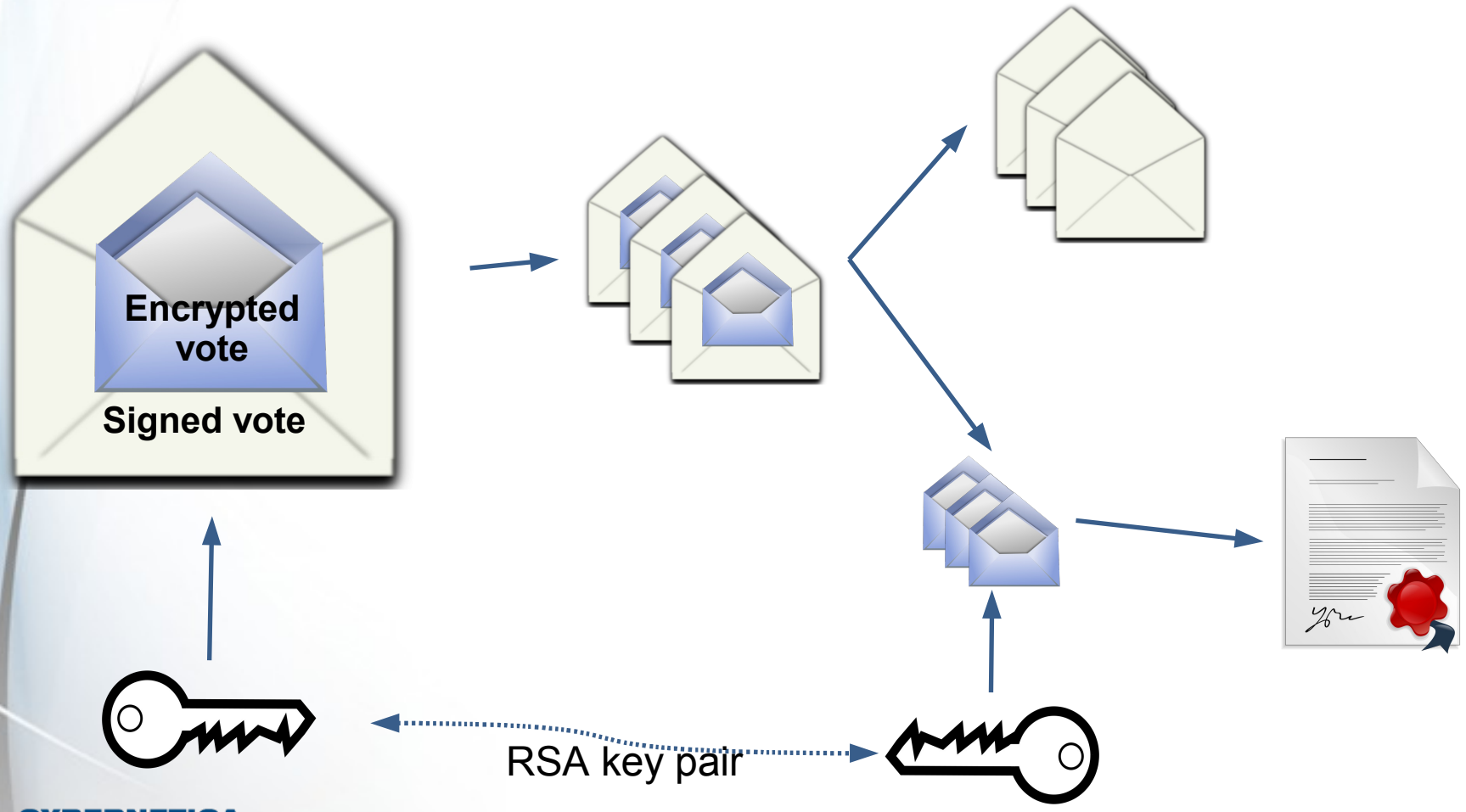
- First reports concerning Internet voting in Estonia were written in 2001
- The basic principles of i-voting were agreed upon in 2003
- These principles stood until 2011
  - Mimicking postal double-envelope voting
  - Accepting potential insecurity of voters' computers

I-voting in Estonia



CYBERNETICA

The protocol used this far



Parliamentary election 2011

- Election rigging malware developed by a student
  - Wanted public attention, attempted revocation
- Voting application defect used in political battle
- Anti-i-voting propaganda
  - Local municipalities' workshop, the Red Book
  - Stop internet voting

Threat modelling

- Critical information system must be accompanied by a threat model
  - The current threat model was developed in 2003, but the world has changed
- So we tried to create a threat model that would be easy to maintain and update for emerging threats
- We chose attack trees based approach

Root-node problem

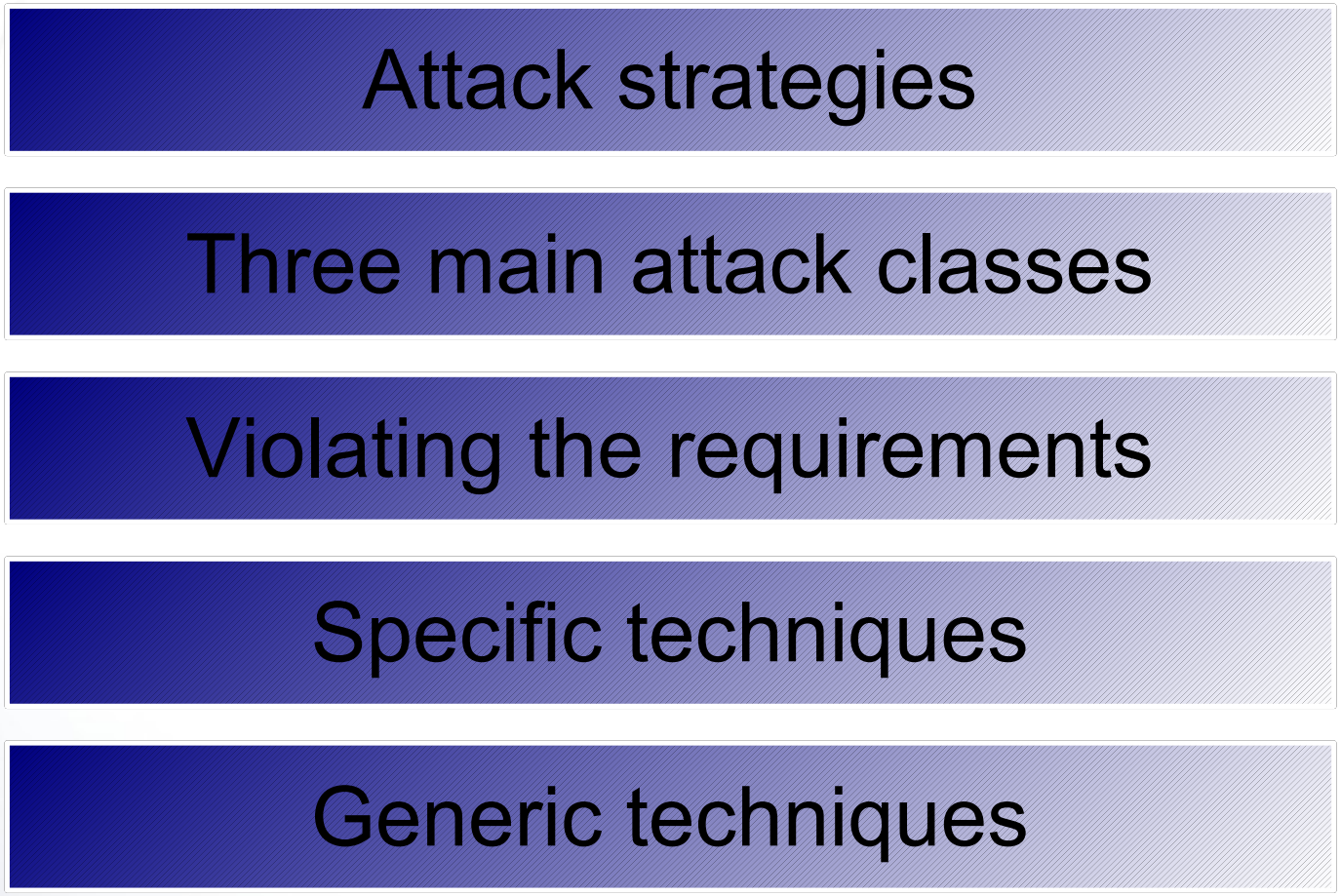
- Proposed root-nodes in literature
  - Change result of election successfully [Lazarus *et al.* 2011]
  - Attack voting equipment OR Attack voting process OR Insider threats [Pardue *et al.* 2010]
  - Large-scale votes' theft OR Large-scale disfranchisement of votes OR Large-scale votes' buying and selling OR Large-scale privacy violation [Buldas and Mägi 2007]

What is the purpose of elections?

- Delegating the power (formally vested into people) to a small set of representatives
- Hence, the real target of attacks (a.k.a. root node of attack tree) should be

Increase influence in the society

Meta-structure of the tree



The requirements for elections

- Only eligible voters can vote
- Voting expresses free will
- All citizens have right to vote
- All votes are equal
- The vote is cast directly by the voter
- The votes are secret
- Tallied and published correctly
- All cast ballots are taken into account
- Voters have access to elections

Manipulation attacks

- Manipulation attacks attempt to change the election outcome by directly/indirectly manipulating with a voting result
  - Most analysed attack category
  - 1 additional seat in Estonia costs approximately 5000 additional votes
  - In order to be successful the attack must remain hidden and the beneficiary secret
  - Technically complex, expensive, illegal

Revocation attacks

- Revocation attacks attempt to change the election outcome by revoking unsuitable voting result
  - Parties score differently in voting methods
  - Requires a proven violation of the rights with possible impact to the result
  - In order to be successful the attack must become visible, but the beneficiary has to remain secret
  - Beneficiary can stage the attack (illegal)

Reputation attacks

- Reputation attacks attempt to change the attitude towards unsuitable voting method
  - Reputation attacks are all about talking – no real attack has to take place
  - Nothing has to be hidden, the attack can not be easily distinguished from democratic process easily, it is perfectly legal

Generic techniques

- Involve institutions
- Involve the public
- Attack persons
- Use malware
- Attack the transport channel
- Attack the central system

Attacker's advantage

- Consider an attacker who wants to manipulate the election outcome
  - He starts with a manipulation attack
    - He fails – attack is discovered, but he manages to keep the beneficiary secret
  - He now changes strategy and tries to revoke the voting result altogether
    - He fails – Supreme Court decides that the attack had no real effect
  - He continues with propaganda
    - The success depends on the quality of his PR team

Vote verification

Aftermath of 2011 parliamentary elections

- Assumptions made in 2003 no longer hold
  - Creating specifically crafted malware has become accessible to moderately motivated students
  - I-voting has become so significant that it makes sense to attack it

Aims of verifiability

- Fight against real manipulation attacks
- Discourage potential real attackers
- Prevent revocation and reputation attacks
  - This item is actually the most important one, since reputation attacks are cheap, risk-free and can be expected to have huge impact

Levels of verifiability

- By Popoveniuc, Kelsey, *et al.*
  - Presented ballots are well-formed
  - Cast ballots are well-formed
  - Recorded as cast
  - Tallied as recorded
  - The two last sets are consistent
  - Only „Recorded as cast“ votes are tallied
- In Estonia we target the „Recorded as cast“ level

Verifiability: The Problem

- It is very easy to attack the voter's computer environment
  - That's why we need verification
- If we would rely on the same computer for verification, we would not achieve much against malware
- Hence, we need alternative environments and/or channels
  - They tend to be non-universal and/or expensive

Towards optimal solution

- We have to find an equilibrium between different contradictory requirements
  - Security
    - Already these requirements are contradictory
  - Usability
  - Availability
  - Possibility to implement

Methods of verification

- Electronic verification of paper voting
  - Scratch and Vote, Wombat, Prêt à Voter
  - Our target is pure Internet voting
- Electronic voting, verification using alternative channels/environments
  - Code voting
  - Verification codes
  - Vote auditing
- In Estonia, verification codes or vote auditing work the best

Alternative channels

- Postal service can be used to send sheets with verification codes
  - In Estonia, real addresses are not known
  - Generating and sending sheets is expensive
- E-mail
  - E-mail addresses are not known
  - E-mails will be read on the same computer
- SMS
  - Phone numbers are not known
  - SMS is not authenticated

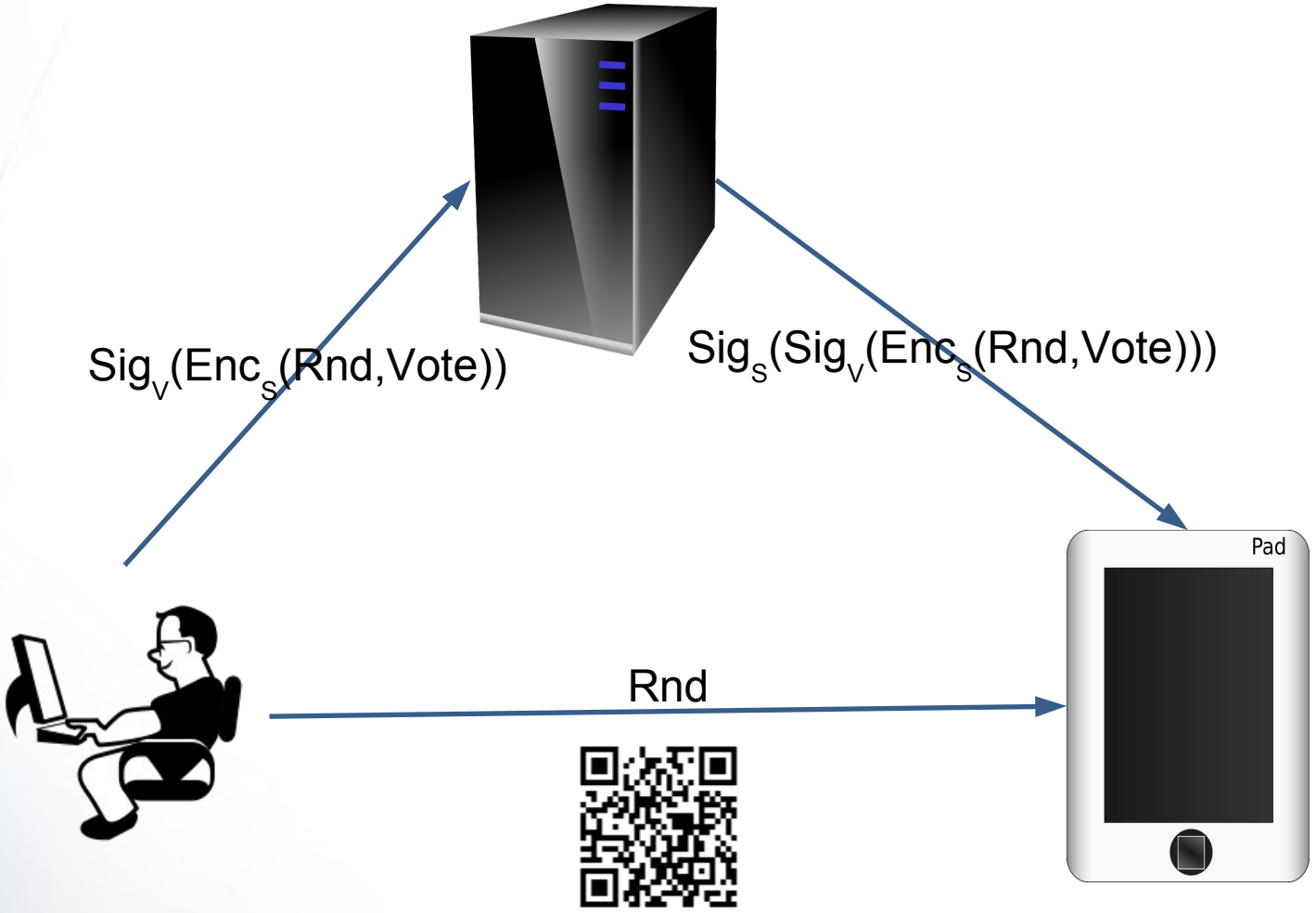
Alternative environments

- Second PC for handling codes or auditing
  - We may require voters to use a different PC for verification, but how many would do so?
- Another computing platform
  - A mobile device!
  - PC applications do not run on them, and for us this is a good thing

Codes or auditing?

- When considering the solution with verification codes, just an alternative platform does not solve the problems of unknown addresses and authentication of code sheets
- Hence, the decision was taken to apply the vote auditing scenario with a mobile device

Voting with vote auditing



Verification: some details

- Rnd moves from PC to mobile device via QR code
- Verification essentially cracks the encrypted vote by brute force
  - In practice, we have up to 400 candidates in one district, cracking takes a few seconds on a moderate smartphone

The scheme: pros and cons

- Pro: Incrementality w.r.t. present system
- Pro: Minimal extra overhead to usability
- Con: Not everyone has access to a mobile device
  - Not everyone has a computer, either
  - The mobile device can be shared
  - Technology is developing very rapidly, smart phones are outselling regular ones since 2011, the next elections are in 2013
  - You can get an Android phone for 0 EUR
  - It is enough to verify 2% of votes to catch large-scale manipulation attacks

Thank you!

- Discussions