The Norwegian 2011 Internet voting project
Guaranteed secure?

Thomas Tjøstheim
Security advisor Hordaland Fylkeskommune
AGENDA

- E-voting
  - What it is
  - Why it is challenging

- The Norwegian Internet voting system
  - About the project, ”E-valg 2011”
  - Main points of the solution

- Threat discussion
E-Voting

- Electronics
  - Casts votes
  - Count votes
- Remote e-voting
  - Casting votes in an uncontrolled environment
- Advantages?
  - Quicker
  - Improved accuracy
  - Better availability?
    - Better adapted for physically challenged
  - Increased voter turnout?
Why is it so hard to design a voting system?

- No neutral third parties
  - The voters can cheat
  - The system can cheat
  - Coercers and vote buyers

- Conflicting requirements
  - Verifiability vs. anonymity

- Any successful attack would be very high profile
Is it possible to design and develop a secure remote e-voting system?

- The experts are skeptical
  - Peter Ryan: “I’m not advocating remote voting for political elections. The political context will be variable in different countries, so it will be up to the politicians to determine what risks are acceptable.”
  - Kristian Gjøsteen: “With realistic attack models (the attacker knows everything the voter knows) for remote internet voting probably make it impossible to achieve both true voter verifiability and coercion-resistance.”
  - Arent: “Voting in your underwear does not seem a valid option—at least not at this moment.”
Remote e-voting

- Five non technical reasons against remote e-voting (Oostveen)
  1. Secret and free election
  2. ”Digital divide”
  3. Cultural effect
     - Gathering of people and ”civic ritual”
  4. Organizational problem
     - Online helpdesk
     - Many roles (e-voting + p-voting)
  5. Behavioral changes
     - Loosing feedback from the environment
The "E-VALG 2011" Project

- What it is?
  - Establish and deploy a solution for electronic voting and election administration in 10 selected municipalities (<200,000 voters) in time for the "kommunestyre and fylkesting" election in 2011
  - Started in 2008 (Pre-project in 2006)

- Some main points of the solution
  - Authentication: E-id (MinID)
  - Combines voting over the Internet with traditional poll place voting.
  - Paper vote overrides all electronic votes
  - Can revote any number of times electronically

- Partners
  - ErgoGroup: administration module
  - Scytl: Remote e-voting module
E-VALG 2011 Solution

- Show animation!
Cryptographic main points

- **Double envelope system**
  - Encrypt vote with public election key
  - Sign encrypted vote with own private key
  - $E_{\text{privVOTER}}(E_{\text{pubELECTION}}(B))$

- **Election private keys**
  - Before the election generate three secret parameters $a1$, $a2$ and $a3$
  - Such that $a1 + a2 = a3 \pmod{q}$.
  - The ballot box gets $a2$
  - The receipt code generator gets $a3$
  - The decryption service gets $a1$. (Divided into shares…)
Cryptographic main points

- Reencryption mix net
- The ballot box and a receipt generator cooperate to compute a sequence of receipt codes for the submitted ballot.
- For more details see

E-voting in other countries
E-valg 2011 Process

- Openness
  - Project
  - Solution
  - Selection and requirements process
  - Source code

- Reference groups
  - Security reference group
  - Political reference group
  - Municipality reference group
  - User reference group

- External verification
  - DNV and others
  - Independent experts
    - Barry Schoenmaker and David Wagner
    - Melanie Volkamer and Olivier Spycher
E-VALG 2011 Debate

- Very little discussion so far
  - Complex topic
  - Information from KRD
    - Blog
  - Norwegians trust in the Norwegian government

- Media
  - Focus on principles
    - UN’s Human rights
    - Illegal trial according to the Norwegian election law §1-1 claiming that all elections should be free and secret.
    - Family voting
    - Vote buying
    - Breach of tradition

- Little focus on technical solution
Our efforts

- **End of 2009 established an independent security group**
  - 8-10 people in Bergen and Oslo
  - 5 meetings with chief of security, Christian Bull
  - Developed a “concerns” list

- **Aim**
  - Analyse technical solution
  - Contribute with independent and constructive critique of the system.
Threat discussion

- Voting applet
- Receipt
- Ballot box
- Transition from e-voting phase to p-voting phase
- Mixing

- Trust model
- Authentication
- Ballot
- Election results
- Central infrastructure
- Etc.
Some selected threats

- Authentication solution
- Insider threats
- Vote buying

- Malware
- Denial of service attacks
Authentication of voters and PKI solution

- MinID (not eID as originally planned)
- A paradox is the fact that the authentication solution is proprietary
Authentication of voters and PKI solution

- Dilemma: How can the voters sign their vote without private keys?
  - Solution: Pre generate RSA signing keys for each voter…
Insider threats

- **Authority knowledge**
  - List correspondence between voters and receipts
  - **Countermeasure:** Physical destruction of hardware? Cooperation with Norsk Tipping, use similar method as for Flax lottery tickets.
Insider vulnerabilities

- **Information leakage**
  - Officials can leak information about who voted in the electronic election and votes that were overwritten by a p-vote.
  - ISP and mobile companies can reveal info about who voted in the e-voting phase.

- **Ballot stuffing**
  - Voting officials add votes for people who haven’t voted.

  ❖ Countermeasure: Voting officials with conflicting interests?
Insider threats

- Reconstruction of the decryption key
- Countermeasure: Private key split between different organisations.
  - Brønnøysund
  - DSB

Ballot box Key + Decryption Key = Receipt generator Key
Vote buying

- **Ways to prove how a voter voted**
  - Voter shows SMS together with voting card
  - Prove encryption of ballot by revealing randomisation factor
  - Countermeasure: revoting and overwriting e-vote with a p-vote

- **Vote buyers dilemma**
  - Assurance of correct vote?
  - How to setup a vote buying market?
  - Penalties: 3 years for vote buyer, 6 months for vote seller
## Statistics from Estonia

<table>
<thead>
<tr>
<th>Election Type</th>
<th>E-votes</th>
<th>% Multiple E-votes</th>
<th>% E-vote cancelled by p-vote</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parliamentary election - EU</td>
<td>58.699</td>
<td>1.55%</td>
<td>0.09%</td>
</tr>
<tr>
<td>Local election</td>
<td>104.413</td>
<td>2.27%</td>
<td>0.09%</td>
</tr>
</tbody>
</table>
Malware

- Trojan changes vote
  - Countermeasure: Voter checks receipt
- Discussion
  - How many people will have to check their receipts?
  - What if a voter falsely claims an incorrect receipt?
  - Receipt for each different candidate enough? (Does not consider ranking of candidates)
  - How to differ between vote changed due to malware and vote changed due to system errors?
Malware

- Trojan records vote
  - Countermeasures: None? Anti-Trojan software?
- Fake election client
  - Applet eliminates possibility of voting for some parties/candidates
  - Countermeasure: Signed applet(?)
Denial of Service attacks

- Connection to central infrastructure
- Connection from receipt code server to voter

- Countermeasures:
  Difficult? Internet voting period spread over time…
Understandability and usability

- Explanations available at different levels
- Verifiability
  - Voters understands concept of receipts?
- How easy is it to vote?
  - Will grandma understand?
- Level of openness
  - Many public errors can be problematic…
Summary

Remote-voting: Difficult to achieve true voter verifiability and coercion resistance. Also complex and difficult to explain to the voters

- **Pros**
  - Accessibility
  - Voter turnout(?)
  - Cheaper(?)
  - Accuracy
  - Openness

- **Cons**
  - Single point of failure
  - Attacks might scale better
  - Will grandma understand it?
  - Private service providers
  - Less manual control?
  - Centralization
Questions?