Seminar: (In)Security of Online Voting
Summer Semester 2021

Marius Momeu\textsuperscript{1}, Fabian Kilger\textsuperscript{1}, Michael Heinl\textsuperscript{2}

\textsuperscript{1}Chair of IT Security, Department of Informatics, Technical University of Munich (TUM)
\textsuperscript{2}Department Production Protection & Industrial Security, Fraunhofer AISEC

2\textsuperscript{nd} February, 2021
Motivation

• Why online voting? Arguments regularly presented in public debates include:
  – increased voter turnout
    • citizens with disabilities
    • occupied citizens
    • citizens traveling / living abroad
    • young citizens
  – reduced election costs
  – reduced contact (contain pandemics)
• However, online voting systems are very security-sensitive
Objectives

⇒ In this seminar, you are going to **assess state-of-the-art** technologies that facilitate reliable online voting, **real-life implementations adopted by nations**.

⇒ **And most importantly**, you are going to
  - **write a paper** about your findings,
  - **give feedback** to (two of) your colleagues’ papers,
  - **give a talk** at the end of the semester.
Topics

- **Technologies**
  - Homomorphic encryption, zero-knowledge proofs (ZKPs), mixnets (ciphertext shuffling)
  - Distributed ledger technologies, byzantine fault tolerance (BFT), consensus
  - Smart card security
  - Trusted Execution Environments (TEEs)

- **Implementations**
  - The Estonian voting system
  - The Swiss voting system
  - Apps used in the US’s midterm elections
<table>
<thead>
<tr>
<th>Phase</th>
<th>Task Description</th>
<th>Date Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase I</td>
<td>Topic announcement</td>
<td>07.03.2021 – 07.03.2021</td>
</tr>
<tr>
<td>Phase II</td>
<td>Choosing topic</td>
<td>07.03.2021 – 14.03.2021</td>
</tr>
<tr>
<td>Phase III</td>
<td>Familiarizing with literature</td>
<td>15.03.2021 – 14.04.2021</td>
</tr>
<tr>
<td>Phase IV</td>
<td>Writing (first draft) - lightweight feedback from tutors</td>
<td>15.04.2021 – 26.05.2021</td>
</tr>
<tr>
<td>Phase V</td>
<td>Writing (final draft) - thorough feedback from tutors</td>
<td>27.05.2021 – 23.06.2021</td>
</tr>
<tr>
<td>Phase VI</td>
<td>Peer reviewing - feedback from fellow students</td>
<td>24.06.2021 – 30.06.2021</td>
</tr>
<tr>
<td>Phase VII</td>
<td>Writing (&quot;camera ready&quot;) + Presentation Slides</td>
<td>01.07.2021 – 07.07.2021</td>
</tr>
<tr>
<td>Phase VIII</td>
<td>Final talks - feedback from tutors on the final talk</td>
<td>12.07.2021 – 26.07.2021</td>
</tr>
</tbody>
</table>
Sessions

Session I  Introduction to Scientific Writing
Session II More on Scientific Writing
Session III Hints on Paper Reviewing
Session IV Hints on Public Speaking
Session V  Final Talks
Grading

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 %</td>
<td>Final Paper (Content, Style, Language, Scope, ...)</td>
</tr>
<tr>
<td>40 %</td>
<td>Presentation (Content, Speaking, Style, Timeliness, ...)</td>
</tr>
<tr>
<td>5 %</td>
<td>Peer Review</td>
</tr>
<tr>
<td>5 %</td>
<td>Participation</td>
</tr>
</tbody>
</table>

**Σ 100 %** Total
Optional

⇒ **Analysis report** on an online voting platform of choice
  → commercial or open-source
  → one that is not tackled in this seminar
  → will bring you bonus points to the final grade
Orga

⇒ **When?**
   - with presentations from tutors and optionally from you (updates on your findings)
   - online or hybrid (depending on the regulations)
   - exact weekday and time TBA
   - final talks at the end of the semester

⇒ **Capacity**
   - **9 students**: individual work (no groups)
   - no qualification challenge
   - don’t forget to register in the matching system!

⇒ Master’s and Bachelor’s students are welcome

⇒ Language of instruction: **English**

⇒ **Moodle** for accessing seminar material
Some Background
Election Requirements

Theory

According to Article 38 (1) of the German Basic Law:

- General
- Direct
- Free
- Equal
- Secret
Election Requirements
Practice
Election Requirements
Practice (2)

- Universal verifiability
- Individual verifiability
- Usability
- Flexible application
- No exclusion
- Correctability
- Robustness
- Correctness
- Integrity
- Completeness

- Anonymity
- Receipt-freeness
- Impossibility of vote buying
- Coercion-resistance
- No forced abstention
- Comprehensibility
- Archiving
- No canvassing
- Equal voting power
- Equal choice
- No interim results
Election Requirements
Practice (2)

- Universal verifiability
- Individual verifiability
- Usability
- Flexible application
- No exclusion
- Correctability
- Robustness
- Correctness
- Integrity
- Completeness

- Anonymity
- Receipt-freeness
- Impossibility of vote buying
- Coercion-resistance
- No forced abstention
- Comprehensibility
- Archiving
- No canvassing
- Equal voting power
- Equal choice
- No interim results
Election Requirements
Practice (2)

- Universal verifiability
- Individual verifiability
- Usability
- Flexible application
- No exclusion
- Correctability
- Robustness
- Correctness
- Integrity
- Completeness

- Anonymity
- Receipt-freeness
- Impossibility of vote buying
- Coercion-resistance
- No forced abstention
- Comprehensibility
- Archiving
- No canvassing
- Equal voting power
- Equal choice
- No interim results
Election Requirements
Practice (2)

- Universal verifiability
- Individual verifiability
- Usability
- Flexible application
- No exclusion
- Correctability
- Robustness
- Correctness
- Integrity
- Completeness

- Anonymity
- Receipt-freeness
- Impossibility of vote buying
- Coercion-resistance
- No forced abstention
- Comprehensibility
- Archiving
- No canvassing
- Equal voting power
- Equal choice
- No interim results
Secure Platform Problem

- Online voting usually takes place on **private devices**
- These devices are not under the control of the election authority (.= uncontrolled environments)
- A potential compromise by malware has to be assumed
Technologies
Homomorphic Encryption

- **Asymmetric-key** (e.g., RSA, ElGamal, etc.) and symmetric-key cryptosystems
- The *result of certain operations on a set encrypted plaintexts is the encrypted result of the same operation applied on the plaintexts directly*
- Therefore, facilitates **private computations**
- Shuffling homomorphic ciphertexts used by mixnets to ensure **voter anonymity**
- Facilitate **individual and universal verifiability using ZKPs**
- **Zero-Knowledge Proof** $$\iff$$ proof that a statement is true without revealing additional knowledge (secrets) that facilitate the proof
Technologies

Distributed Ledger Technologies

- In the form of **distributed database** or **public bulletin board**
  - blockchain, directed acyclic graph (DAG), hashgraph, etc.
- For example, goals of blockchain are very related
  - Anonymity
  - Verifiability
  - Integrity
  - No single point of failure
- Blockchain currencies can be easily converted to votes:
  - Each voter is given an address in the blockchain with 1 token/coin
  - The voter sends its coins to the address it is voting for.
  - After some deadline, the address with the most coins is the winner of the poll
- **Available DLT-based systems are not yet ready for online voting!**
Existing Implementations
Switzerland

- Managed by SwissPost using Scytl’s e-voting protocol
- Voters receive **secret candidate choice codes** via post
- Used to cast their votes on a **web platform**
- **Confirmation codes** sent back electronically for validation
- Building blocks
  - ElGamal cryptosystem
  - Reliable as long as one server-side component stays honest
  - Bayer & Groth mixnet - homomorphically encrypted votes shuffled before decryption
  - Individual verifiability
  - Universal verifiability
- **However, researchers have proven it is flawed**
Resources

Reading Material

⇒ **Literature access**
   → https://scholar.google.com/
   → https://semanticscholar.org/
   → https://dblp.uni-trier.de/
   → https://arxiv.org/

⇒ **Get around paywalls** using: https://www-ub-tum-de.eaccess.ub.tum.de/datenbanken

⇒ **Researchers’ homepages can be valuable!**
   → the paper, source code, raw data, instructions, technical information
Outro

Questions?

Thank you!

Marius Momeu
momeu@sec.in.tum.de

Fabian Kilger
kilger@sec.in.tum.de

Michael Heinl
michael.heinl@aisec.fraunhofer.de