Automatic Verification of Remote Electronic Voting Protocols

Michael Backes, Cătălin Hrițcu, Matteo Maffei
Saarland University, Saarbrücken, Germany
Did you know that...

- ... in Germany, in the latest parliamentary elections **18.7%** of the votes were cast by post?
Did you know that …

• … in Germany, in the latest parliamentary elections **18.7%** of the votes were cast by post?

• this is a form of **remote voting**
Remote voting (by post)

- More convenient than supervised voting
- This should increase voter participation
Remote voting (by post)

- More convenient than supervised voting
- This should increase voter participation
- Voting by post raises many security concerns
  - An autograph signature does not authenticate the voter
  - An envelope does not guarantee secrecy or integrity
  - The post is not always a secure channel
  - Extremely easy to sell your vote
  - You can coerce voters to vote as you like
Remote voting (by post)

- More convenient than supervised voting
- This should increase voter participation
- Voting by post raises many security concerns
  - An autograph signature does not authenticate the voter
  - An envelope does not guarantee secrecy or integrity
  - The post is not always a secure channel
  - Extremely easy to sell your vote
  - You can coerce voters to vote as you like
- Still, this has been used in Germany for 50+ years
Remote electronic voting

- Seems even cheaper and even more convenient
- Promises better security (than voting by post at least)
- the security properties can be cryptographically enforced
Remote **electronic** voting

- Seems even cheaper and even more convenient
- Promises better security (than voting by post at least)
  - the security properties can be cryptographically enforced

Different security risks
- Easier to launch large-scale attacks and erase evidence
- Clients are the weakest link: e.g. remotely exploitable software flaws, viruses, Internet worms, trojans, lack of physical security, social engineering attacks, etc.
- Network also vulnerable: e.g. voter demographic-based DDOS, cache poisoning DNS attacks, etc.
desired properties

- eligibility
- non-reusability
- inalterability
- fairness
- completeness
- correctness
- vote-privacy
- robustness
- scalability
- availability
- accuracy
- democracy
- fault tolerance
- no forced-abstention attacks
- receipt-freeness
- coercion-resistance
- universal verifiability
- individual verifiability
- availability
desired properties

- Careful formalization and automatic verification of these properties important before widespread adoption
eligibility

inalterability  non-reusability

vote-privacy

no forced-abstention attacks

receipt-freeness

coercion-resistance

• Careful formalization and automatic verification of these properties important before widespread adoption
soundness

eligibility

inalterability non-reusability

vote-privacy
no forced-abstention attacks
receipt-freeness
coercion-resistance

• Careful formalization and automatic verification of these properties important before widespread adoption
• Careful formalization and automatic verification of these properties important before widespread adoption
What we did

- General technique for
  - modeling remote electronic voting protocols (in the applied pi-calculus)
  - and automatically verifying their security
- New formal definitions of
  - soundness - trace property
  - coercion-resistance - observational equivalence
  - both definitions amenable to automation (e.g. ProVerif)
- Proved that our coercion-resistance implies vote-privacy, immunity to forced-abstention attacks & receipt-freeness
- Automatically verified the security of the JCJ protocol
Soundness (eligibility, non-reusability, inalterability)

Hi, I’m Alice
Soundness (eligibility, non-reusability, inalterability)

Hi, I’m Alice

eligible(Alice)
Soundness (eligibility, non-reusability, inalterability)

Hi, I’m Alice

eligible(Alice)
Hi, I'm Alice

eligible(Alice)

Hi, I'm Alice

vote(Alice, pink)
Soundness (eligibility, non-reusability, inalterability)

Hi, I’m Alice

vote(Alice, pink)

eligible(Alice)
Hi, I'm Alice

eligible(Alice)

vote(Alice, pink)
Soundness (eligibility, non-reusability, inalterability)

Hi, I’m Alice

eligible(Alice)

vote(Alice, pink)

pink

blue
Soundness (eligibility, non-reusability, inalterability)

Hi, I'm Alice

eligible(Alice)

Hi, I'm Alice

vote(Alice, pink)
Soundness (eligibility, non-reusability, inalterability)

Hi, I’m Alice

eligible(Alice)

vote(Alice, pink)

tally(pink)
Soundness (eligibility, non-reusability, inalterability)

Hi, I’m Alice

Trace: $t_1$ eligible(Alice) $t_2$ vote(Alice, pink) $t_3$ tally(pink)
Soundness (eligibility, non-reusability, inalterability)

Hi, I’m Alice

Trace: t1 eligible(Alice) t2 vote(Alice, pink) t3 tally(pink)
Soundness (eligibility, non-reusability, inalterability)

Hi, I'm Alice

Trace: t1 eligible(Alice) t2 vote(Alice, pink) t3 tally(pink)

and the trace t1 t2 t3 is also sound (injective matching)
Vote-privacy

Voters
Alice
Bob
Charlie
Vote-privacy

Voters
- Alice
- Bob
- Charlie

Results
- pink party
- blue party
Vote-privacy

**Voters**
- Alice
- Bob
- Charlie

**Results**
- pink party
- blue party

**“Detailed” results**
- Alice .......... pink party
- Bob .......... blue party
- Charlie ......... blue party
Vote-privacy

Voters
Alice
Bob
Charlie

Results
pink party
blue party

“Detailed” results
Alice ............ pink party
Bob .............. blue party
Charlie ........ blue party
Definition of vote-privacy

[Delaune, Kremer & Ryan; CSF ’06]
Definition of vote-privacy

∀

indistinguishable from

[Delaune, Kremer & Ryan; CSF ’06]
Definition of vote-privacy

[Delaune, Kremer & Ryan; CSF ’06]
Definition of vote-privacy

[Delaune, Kremer & Ryan; CSF ’06]
Definition of vote-privacy

[Delaune, Kremer & Ryan; CSF ’06]
Immunity to forced-abstention
Receipt-freeness

- Cryptographic setting [Benaloh & Tuinstra; STOC '94]
Receipt-freeness

- Cryptographic setting [Benaloh & Tuinstra; STOC ’94]

- We adapted definition by [Delaune, Kremer & Ryan; CSF ’06] to remote voting
Coercion-resistance

- Cryptographic setting [Juels, Catalano & Jakobsson; WPES 2005]

\[ S[\text{pink blue}] \]  \equiv  \[ S[\text{pink blue}] \]

\Rightarrow \text{receipt-freeness (up to abstraction)}
Coercion-resistance

- Cryptographic setting [Juels, Catalano & Jakobsson; WPES 2005]

\[ \text{receipt-freeness (up to abstraction)} \]
Coercion-resistance

- Cryptographic setting [Juels, Catalano & Jakobsson; WPES 2005]

- Proved: coercion-resistance \(\Rightarrow\) no forced-abstention \(\Rightarrow\) vote-privacy

\[ S[ ] \approx S[ ] \Rightarrow \text{receipt-freeness (up to abstraction)} \]
# Definitions of coercion-resistance

<table>
<thead>
<tr>
<th></th>
<th>JCJ-WPES’05</th>
<th>DKR-CSF’06</th>
<th>DKR-TR’08</th>
<th>current</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>setting</strong></td>
<td>remote voting</td>
<td>supervised voting</td>
<td>supervised voting</td>
<td>remote voting</td>
</tr>
<tr>
<td><strong>automation</strong></td>
<td>no (crypto)</td>
<td>no (adaptive simulation)</td>
<td>no (∀C. P≈Q)</td>
<td>yes (≈)</td>
</tr>
<tr>
<td><strong>vote-privacy</strong></td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><strong>no simulation attacks</strong></td>
<td>yes</td>
<td>n/a</td>
<td>n/a</td>
<td>yes</td>
</tr>
<tr>
<td><strong>no forced-abstention</strong></td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td><strong>no randomization attacks (?)</strong></td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td><strong>receipt-freeness</strong></td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes (up to abstraction)</td>
</tr>
</tbody>
</table>
Analysis of JCJ

- first coercion-resistant protocol for remote voting [Juels, Catalano & Jakobsson; WPES ’05]
- forms the basis of many recent protocols (e.g. Civitas [Clarkson, Chong & Myers; S&P ’08])
- Analysis performed with ProVerif
  - automatic protocol analyzer using Horn-clause resolution
  - we use our symbolic abstraction of zero-knowledge [Backes, Maffei & Unruh; S&P ’08]
  - analyzing observational equivalence required (re)writing the specification in the shape of a biprocess
  - verification of JCJ succeeds, which yields security guarantees for unbounded number of voters, sessions, etc.
Future work

• Currently: analyzing a model of Civitas
Future work

- Currently: analyzing a model of Civitas
- Currently: defining and analyzing other properties
  - Individual verifiability (trace property)
  - Immunity to randomization attacks (privacy property)
Future work

• Currently: analyzing a model of Civitas
• Currently: defining and analyzing other properties
  • Individual verifiability (trace property)
  • Immunity to randomization attacks (privacy property)
• Different techniques for trace properties
  • type systems - e.g. our type system for ZK [WITS ’08]
Future work

- Currently: analyzing a model of Civitas
- Currently: defining and analyzing other properties
  - Individual verifiability (trace property)
  - Immunity to randomization attacks (privacy property)
- Different techniques for trace properties
  - type systems - e.g. our type system for ZK [WITS ’08]
- Different techniques for observational equivalence
  - for instance using symbolic bisimulation [DKR, SecCo ’07]
Future work

- Currently: analyzing a model of Civitas
- Currently: defining and analyzing other properties
  - Individual verifiability (trace property)
  - Immunity to randomization attacks (privacy property)
- Different techniques for trace properties
  - type systems - e.g. our type system for ZK [WITS ’08]
- Different techniques for observational equivalence
  - for instance using symbolic bisimulation [DKR, SecCo ’07]
- More accurate protocol models
  - The ultimate goal is to analyze implementations
Backup slides
Simplified JCJ protocol

Hi, I’m Alice
Simplified JCJ protocol

Hi, I’m Alice

\( cred \) (private channel)

\( \{ cred, r_1 \}_{pk(kT)} \)
Hi, I’m Alice

cred

(Private channel)

\{cred, r_1\}_{pk(kT)}

\{cred, r_2\}_{pk(kT)}, \{pink\}_{pk(kT)}, ZK
Hi, I'm Alice

Simplified JCJ protocol

\[ \text{cred} \]

(private channel)

\[ \{ \text{cred}, r_1 \}_{pk(kT)} \]

\[ \{ \text{cred}, r_2 \}_{pk(kT)}, \{ \text{pink} \}_{pk(kT)} \]

ZK
Hi, I'm Alice

Simplified JCJ protocol

cred

(pk(kT))

(cred, r_1)

ZK

cred, r_2

(pk(kT))

{cred, r_1}_{pk(kT)}

{cred, r_2}_{pk(kT)}, \{pink\}_{pk(kT)}, ZK
Hi, I’m Alice

credible \{cred, r_1\}_{pk(kT)}

(private channel)

credible \{cred, r_2\}_{pk(kT)}, \{pink\}_{pk(kT)}, ZK
Hi, I’m Alice

Simplified JCJ protocol

cred

\{ cred, r_1 \}_{pk(kT)}

\{ cred, r_2 \}_{pk(kT)}, \{ pink \}_{pk(kT)}, ZK

pink