Security in E-Voting

Prof. Dr. Ralf Küsters

Information Security and Cryptography
University of Trier
Germany
Electronic Voting

DRE

optical scanner
Electronic Voting

Used in many countries

- USA
- Estonia
- Switzerland
- Brasil
- India
- ... 

but also for low-stake elections, e.g.,

- Gesellschaft für Informatik
- Sozialwahl
- ...

Many e-voting companies

- e.g., Scytl (Spain), Polyas (Germany)

One project member, Dr. Tomasz Truderung, joined this company.
E-voting machines a fire

By Dawn Kawamoto
Staff Writer, CNET News

September 14, 2006 1:42 PM PDT

Concerns about electronic voting reliability has been heavily criticize resurfaced this week in a recently published University study.

Released on Wednesday, the Princeton report, "Security Analysis of the Diebold AccuVote-T Machine," says that the e-voting machine, procured by Diebold Election Systems, was vulnerable to malfunctions and potential voter fraud.

The Princeton report (click here for PDF) renewed debate over electronic voting systems near and ongoing.

Another election mess in Florida

Big doubts about a narrow victory

Dec 7th 2006 | washington, dc | From the print edition

SINCE it is a place where alligator wrestling is a recognised pastime and tourists wear hats with Mickey Mouse ears, you might think that Florida would be immune to election embarrassment. But after its punch-card ballots threw the 2000 presidential election into chaos, the state made a decisive move. It outlawed punch-cards and spent millions on touch-screen voting machines instead.

"There'll never be a hanging, dangling, or

and potential voter fraud.

"There'll never be a hanging, dangling, or
Manipulation of voting machines?!

Many problems with e-voting systems have been reported: USA, Netherlands, India, etc.

Programming errors?!
Objectives: My Project/E-Voting Reference Scenario

- Implement an e-voting system
  * Privacy and verifiability
  * Demonstrator/benchmark for RS$^3$
  * Implemented in Java

- Cryptographic aspects of e-voting
  * Widely applicable definitions of central security properties
  * Cryptographic security analysis of prominent e-voting protocols/systems
  * New attacks
  * Systematic design of e-voting systems (including sElect)

  [CCS 2010; SP 2011; JCS 2012; SP 2012; SP 2014; EuroSP 2016; SP 2016]
Objectives: My Project/E-Voting Reference Scenario

- Cryptographic code-level analysis of (Java) systems

  * Develop general methods and techniques
  * Combine techniques from
    - Language-based information flow and
    - Cryptography

- Apply to Java systems that use cryptography

  * Using tools such as Joana (Snelting et al.) and KeY (Beckert et al.)

Ultimate goal:

certified on code level
Objectives: My Project/E-Voting Reference Scenario

- Implement an e-voting system

  * Privacy and verifiability
  * Demonstrator/benchmark for RS$^3$
  * Implemented in Java

- Cryptographic aspects of e-voting

  * Widely applicable definitions of central security properties
  * Cryptographic security analysis of prominent e-voting protocols/systems
  * New attacks
  * Systematic design of e-voting systems (including sElect)

[CCS 2010; SP 2011; JCS 2012; SP 2012; SP 2014; EuroSP 2016; SP 2016]
New web-based remote e-voting system:

- Lightweight system meant for low-risk elections
  * design (e.g., simple crypto)
  * usability

- Fully automated verification (if voter client is trusted)

- Human verifiability (if voter client is not trusted)

- Rigorous cryptographic analysis
  verifiability, accountability, privacy

- Cryptographic analysis on code-level

- Has been used in mock elections
sElect: Overview

Voting booth

Voting booth

Serve static JS/CSS/HTML code

Voter

Browser

Receipt

Collecting server

Mix net

plain Chaumian mix net (only nested encryption, no ZKPs, no verifiability)

Bulletin board(s)
Chaumian Mixnet

Similar to TOR.
Your Favorite Superhero Election

(election identifier: F42C 99DD 2A66 FA6E E469 01D0 297B 1AAC BB9D 767F)

Please enter a code consisting of 9 randomly chosen characters:

Voter provided verification code

wk%m5=Q!v

These code will be part of the verification code which will allow you to check whether your vote has been properly counted.
Your Favorite Superhero Election

(election identifier: F42C 99DD 2A66 FA6E E469 01D0 297B 1AAC BB9D 767F)

Who is Your Favorite Superhero?

- Iron Man
- Batman
- Wonder Woman
- Spider Man
- Dr. Manhattan
- Hulk
- Superman

\[ b_i = E_{M_m}(\ldots E_{M_1}(c_i, v_i)\ldots) \]

wk%m5=Q!v442F0105

Provided by the voter
Generated by the browser

Cast your vote
Your Favorite Superhero Election

(election identifier: F42C 99DD 2A66 FA6E E469 01D0 297B 1AAC BB9D 767F)

Your ballot has been accepted by the collecting server.

When the election is over, you can manually check that your ballot is in the final tally. If you want to do this, you need to

save/write down the following verification code

and look it up in the result of the election: it should appear next to your choice.

Your verification code: wk%m5=Q!v442F0105

The first 9 characters are the code you entered, while the remaining part was generated randomly by the system.

Thank you!
Your Favorite Superhero Election
(election identifier: F42C 99DD 2A66 FA6E E469 01D0 297B 1AAC BB9D 767F)

The election is closed and the result is ready and available.

To see the result and check your verification code, you can now

[go to the result web page]

Independently, an automatic verification procedure is being carried out to check that the ballot with the following verification code has in fact been counted: wk%m5=Q!v442F0105

Verification successful ✔️

Fully automated verification!
Your Favorite Superhero Election

(election identifier: F42C 99DD 2A66 FA6E E469 01D0 297B 1AAC BB9D 767F)

The election is closed and the result is ready and available.

To see the result and check your verification code, you can now

go to the result web page

Independently, an automatic verification procedure is being carried out to check that the ballot with the following verification code has in fact been counted: &a_1a:8c93823E9CF

VERIFICATION FAILED: ballot with verification code &a_1a:8c93823E9CF is missing!

Looking for the misbehaving party.

Ballot &a_1a:8c93823E9CF has been dropped by the collecting server

The following data contains information necessary to hold the misbehaving party accountable. Please copy it and provide to the voting authorities.

```json
{"electionID":"f42c99dd2a66fa6ee46901d0297b1aacbb9d767f","signature":"7499d1e5e2c10ed849"}
```
Your Favorite Superhero Election

(election identifier: F42C 99DD 2A66 FA6E E469 01D0 297B 1AAC BB9D 767F)

The election is closed and the result is ready and available.

To see the result and check your verification code, you can now

go to the result web page

Independently, an automatic verification procedure is being carried out to check that the ballot with the following verification code has in fact been counted: wk%m5=Q!v442F0105

Verification successful ✔️
Description
This is the election of the Greatest Superhero Ever.

List of Votes

Please check that your choice is listed next to your verification code.

<table>
<thead>
<tr>
<th>verification code</th>
<th>choice</th>
</tr>
</thead>
<tbody>
<tr>
<td>am&lt;:-)62680BDE436</td>
<td>Dr. Manhattan</td>
</tr>
<tr>
<td>b27sh:][11CA826F</td>
<td>Spider Man</td>
</tr>
<tr>
<td>vb!{as32FBAA5E3E9</td>
<td>Bugs Bunny</td>
</tr>
<tr>
<td>wk%m5=Q!v442F0105</td>
<td>Bugs Bunny</td>
</tr>
</tbody>
</table>
New web-based remote e-voting system:

- Lightweight system meant for low-risk elections
  * design (e.g., simple crypto)
  * usability

- Fully automated verification (if voter client is trusted)

- Human verifiability (if voter client is not trusted)

- Rigorous cryptographic analysis
  verifiability, accountability, privacy

- Cryptographic analysis on code-level

- Has been used in mock elections
Objectives: My Project/E-Voting Reference Scenario

- Implement an e-voting system
  * Privacy and verifiability
  * Demonstrator/benchmark for RS$^3$
  * Implemented in Java

- Cryptographic aspects of e-voting
  * Widely applicable definitions of central security properties
  * Cryptographic security analysis of prominent e-voting protocols/systems
  * New attacks
  * Systematic design of e-voting systems (including sElect)

[CCS 2010; SP 2011; JCS 2012; SP 2012; SP 2014; EuroSP 2016; SP 2016]
Objectives: My Project/E-Voting Reference Scenario

- Cryptographic code-level analysis of (Java) systems

  * Develop general methods and techniques
  * Combine techniques from
    - Language-based information flow and
    - Cryptography

- Apply to Java systems that use cryptography

  * Using tools such as Joana (Snelting et al.) and KeY (Beckert et al.)

Ultimate goal:
The CVJ Framework

Goal: security/cryptographic analysis directly on code-level (Java)
(rather than in more abstract cryptographic model)

cryptographic privacy property of Java system

Combination of technique from cryptography and language-based security

non-interference property (language-based security)
Non-Interference

Given: Java system $S$

Tools for checking NI of Java programs:

Joana, KeY, JIF, Maude, ...
The CVJ Framework

Goal: security/cryptographic analysis directly on code-level (Java) (rather than in more abstract cryptographic model)

cryptographic privacy property of Java system

Combination of technique from cryptography and language-based security

Successfully applied to:
Client/Server-System
Cloud Storage System
using Joana.

non-interference property (language-based security)
Let’s apply this to e-voting systems (sElect)

Cryptographic vote privacy

E-Voting System (e.g., sElect)

election result

Cannot be done by fully automated tool

Tool has to prove functional correctness

Requires theorem prover
Hybrid Approach — Main Idea

[CSF 2015]

Use

as much as possible

an automated tool for NI

in combination with

only when and where necessary

a theorem prover
What about an E-Voting System?

E-Voting System (e.g., sElect)

cannot be handled by fully automated tool

Tool has to prove functional correctness

Requires theorem prover

Use hybrid approach
Case studies: E-Voting

Successfully applied to variant of sElect

Analyzed mix server of sElect

Strong cryptographic vote privacy property
(formulated as a cryptographic indistinguishability game in Java)

CVJ Framework: reduced problem to NI checking

Hybrid approach: used combination of Joana and KeY
Objectives: My Project/E-Voting Reference Scenario

- Cryptographic code-level analysis of (Java) systems
  
  * Develop general methods and techniques
  * Combine techniques from
    - Language-based information flow and
    - Cryptography

- Apply to Java systems that use cryptography
  
  * Using tools such as Joana (Snelting et al.) and KeY (Beckert et al.)

Ultimate goal:

CVJ Framework + Hybrid Approach

certified on code level
Objectives: My Project/E-Voting Reference Scenario

Ultimate Goal

Thank you!

certified on code level

Beginning of the project

New insights into e-voting systems
CVJ Framework
Hybrid Approach
Several case studies
Greatly improved tools
New e-voting system

now