Evaluating RIES using the proposed Protection Profile

Hugo Jonker  Eindhoven University of Technology & University of Luxembourg
Melanie Volkamer  University of Passau
rationale

Why RIES?

Why the protection profile (PP)?
rationale

Why RIES?
- used for parlementarian elections
- security not thoroughly investigated

Why the protection profile (PP)?
Why RIES?
- used for parliamentarian elections
- security not thoroughly investigated

Why the protection profile (PP)?
- Common Criteria (CC) = internationally accepted security standard
- PP (part of CC) has been recently developed
- test-case: how to apply the PP?
This PP, Core Requirements for Remote Electronic Voting:

- aimed at "regular" elections
- geared towards interface
requirements

- OverhasteProtection
- Correction
- Confirmation
- OneVoterOneVote
- VoteCount
- AnonElectionCommittee
- after-Integrity
- Cancel
- After-BallotBox
- EndElection
- IntegrityElectionCommittee

- SecretElectionCommittee
- Malfunction
- Log
- StartVoteCount
- SecretMessage
- AuthElectionCommittee
- UnauthorisedVoter
- NoProof
- after-ElectionSecrecy
- IntegrityMessage
- ElectionSecrecy
History:

- originally developed for water management board elections used in different regional elections, successful
- adapted for ex-pat voting (RIES-KOA, 2006)
- based on academic work, actively monitored by researchers, OSCE, WVSCN.NL
History:

- originally developed for water management board elections used in different regional elections, successful
- adapted for ex-pat voting (*RIES-KOA, 2006*)
- based on academic work, actively monitored by researchers, OSCE, WVSCN.NL

Noteworthy aspects:

- integrates mail-voting and e-voting
- 3 phases: pre-election, election, post election
- verifiability by hashes and commitments
Per voter:

- identity \( i \), secret key \( sk(i) \)
- “personalised” list of candidates \( C_i \)
Per voter:

- identity $i$, secret key $sk(i)$
- "personalised" list of candidates $C_i$

\[
\begin{array}{|c|c|}
\hline
i & \quad \text{can}_1 \\
\hline
\vdots & \vdots \\
\hline
n & \quad \text{can}_n \\
\hline
\end{array}
\]

$C$
Verifiability

Per voter:

- identity $i$, secret key $sk(i)$
- “personalised” list of candidates $C_i$

<table>
<thead>
<tr>
<th>$i$</th>
<th>$can_1$</th>
<th>$can_2$</th>
<th>$can_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$n$</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

$h_{sk(i)}$
Per voter:

- **identity** $i$, secret key $sk(i)$
- “personalised” list of candidates $C_i$

\[
\begin{array}{c|c}
\text{can}_1 & \cdots \text{can}_n \\
\hline
1 & \vdots \\
\vdots & \vdots \\
n & \vdots \\
\end{array}
\]  

\[
\begin{array}{c|c}
\text{can}_1 & \cdots \text{can}_n \\
\hline
1 & \vdots \\
\vdots & \vdots \\
n & \vdots \\
\end{array}
\]

$C$  

\[
\begin{array}{c|c}
\text{can}_1 & \cdots \text{can}_n \\
\hline
1 & \vdots \\
\vdots & \vdots \\
n & \vdots \\
\end{array}
\]

$C_i$

\[
\begin{array}{c|c}
\text{can}_1 & \cdots \text{can}_n \\
\hline
1 & \vdots \\
\vdots & \vdots \\
n & \vdots \\
\end{array}
\]

$C_i$

\[
\begin{array}{c|c}
\text{can}_1 & \cdots \text{can}_n \\
\hline
1 & \vdots \\
\vdots & \vdots \\
n & \vdots \\
\end{array}
\]

$C_i$

\[
\begin{array}{c|c}
\text{can}_1 & \cdots \text{can}_n \\
\hline
1 & \vdots \\
\vdots & \vdots \\
n & \vdots \\
\end{array}
\]
verifiability

Per voter:

- identity \( i \), secret key \( sk(i) \)
- “personalised” list of candidates \( C_i \)

\[
\begin{array}{c|c}
1 & can_1 \\
\vdots & \vdots \\
n & can_n \\
\end{array}
\]

\[
\begin{array}{c|c}
1 & h_{sk(i)}(i) \\
\vdots & \vdots \\
n & h_{sk(i)}(can_n) \\
\end{array}
\]

\[ C \rightarrow h_{sk(i)} \rightarrow C_i \]
Per voter:

- identity \( i \), secret key \( sk(i) \)
- “personalised” list of candidates \( C_i \)

\[
\begin{array}{c|c}
\hline
i & \text{can}_1 \\
\vdots & \vdots \\
n & \text{can}_n \\
\hline
\end{array}
\quad
\begin{array}{c|c}
\hline
h_{sk(i)}(i) & \text{can}_1 \\
\vdots & \vdots \\
h_{sk(i)}(i) & \text{can}_n \\
\hline
\end{array}
\quad
\begin{array}{c|c}
\hline
m(h_{sk(i)}(i)) & \text{can}_1 \\
\vdots & \vdots \\
m(h_{sk(i)}(i)) & \text{can}_n \\
\hline
\end{array}
\]

\( C \) \rightarrow \( C_i \) \rightarrow \( (published: m(C_i)) \)
pre-election

via post office

authority

publish $C$

voter$_i$

publish $m(C_i)$

$sk_i$
over ssl channel

\[ V \triangleq V \cup vot_{i} \]

\[ receipt(vot_{i}) \]

\[ vot_{i} = h_{sk(i)}(can_{i}) \]
post election

**Introduction**

**Protection profile**

**RIES**
- about
- verifiability
- pre-election
- election phase
- post election

**Analysis**

**Conclusions**

---

**verify** \( vote_i \in V \)

**verify** \( R = m(V) \)

**counter**

**publish** \( V \)

**announce result** \( R \)
approach

- not full blown CC-analysis
- based on available documentation
- extended with information gained from discussions / meetings
## objective | outcome
--- | ---
OverhasteProtection | PASS
Correction | PASS
Confirmation | PASS
OneVoterOneVote | PASS
VoteCount | PASS
AnonElectionCommittee | PASS
after-Integrity | PASS
Cancel | PASS
after-BallotBox | PASS
<table>
<thead>
<tr>
<th>objective</th>
<th>outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>EndElection</td>
<td>INCONCL</td>
</tr>
<tr>
<td>IntegrityElectionCommittee</td>
<td>INCONCL</td>
</tr>
<tr>
<td>SecretElectionCommittee</td>
<td>INCONCL</td>
</tr>
<tr>
<td>Malfunction</td>
<td>INCONCL</td>
</tr>
<tr>
<td>Log</td>
<td>INCONCL</td>
</tr>
<tr>
<td>StartVoteCount</td>
<td>INCONCL</td>
</tr>
<tr>
<td>SecretMessage</td>
<td>FAIL</td>
</tr>
<tr>
<td>AuthElectionCommittee</td>
<td>FAIL</td>
</tr>
<tr>
<td>UnauthorisedVoter</td>
<td>FAIL</td>
</tr>
<tr>
<td>NoProof</td>
<td>FAIL</td>
</tr>
<tr>
<td>after-ElectionSecrecy</td>
<td>FAIL</td>
</tr>
<tr>
<td>IntegrityMessage</td>
<td>FAIL</td>
</tr>
<tr>
<td>ElectionSecrecy</td>
<td>FAIL</td>
</tr>
</tbody>
</table>
document lacking (SSL configuration)
■ documentation lacking (SSL configuration)
■ voter proofs available
- documentation lacking (SSL configuration)
- voter proofs available
- self-tests? availability of ballot box?
  logging? starting/stopping guards?
- documentation lacking (SSL configuration)
- voter proofs available
- self-tests? availability of ballot box?
  logging? starting/stopping guards?
- authorised voters only!
on RIES

- documentation lacking (SSL configuration)
- voter proofs available
- authorised voters only!

Impact:
Suggestions for improvements will be in paper and communicated to voting officials and RIES developers.
■ emphasis on interfaces and correctness
on PP

- emphasis on interfaces and correctness
- not enough requirements on environment
- emphasis on interfaces and correctness
- not enough requirements on environment
- strong assumptions
on PP

- emphasis on interfaces and correctness
- not enough requirements on environment
- strong assumptions
- compliance does not imply a secure voting system
on PP

- emphasis on interfaces and correctness
- not enough requirements on environment
- strong assumptions
- compliance does not imply a secure voting system
- compliance does (strongly) indicate a correct and somewhat secure voting system
emphasize on interfaces and correctness
- not enough requirements on environment
- strong assumptions
- compliance does not imply a secure voting system
- compliance does (strongly) indicate a correct and somewhat secure voting system

Future work:
on PP

- emphasis on interfaces and correctness
- not enough requirements on environment
- strong assumptions
- compliance does not imply a secure voting system
- compliance does (strongly) indicate a correct and somewhat secure voting system

Future work:

- widen scope of PP to accommodate RIES (and similar)
- extend coverage of PP to catch more security
Thank you for your attention!

hugo.jonker@uni.lu

http://satoss.uni.lu/hugo/