Verifying Privacy by Little Interaction and No Process Equivalence

Denis Butin and Giampaolo Bella
Introduction

- E-voting protocols increasingly used
- Key property: voter privacy / ballot secrecy
- Inductive Method: protocol verification through theorem proving
- Extended for e-voting privacy analysis
- Example: FOO’92
Extensions for E-voting Protocols — Motivation

- Analysis of e-voting dominated by ProVerif automatic verifier
- Powerful, but sometimes limited
- Motivation to fill in the gaps with complementary, alternative approach
Privacy in e-voting

aaa
Related Work

- Ryan / Kremer / Delaune: applied pi calculus, partially mechanized through ProVerif
- Observational equivalence: traces in which two voters swap their votes are equivalent in a sense
- Parts of the proof done by hand
Method: the Inductive approach

- Mathematical induction on protocol steps
- Dolev-Yao threat model

- Tool support: Isabelle/HOL interactive theorem prover
# Protocols Verified in Isabelle So Far

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Class</th>
<th>Year</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahalom</td>
<td>Key sharing, authentication</td>
<td>1996</td>
<td>Paulson</td>
</tr>
<tr>
<td>NS symmetric</td>
<td>Key sharing</td>
<td>1996</td>
<td>Paulson &amp; Bella</td>
</tr>
<tr>
<td>Otway-Rees (with variants)</td>
<td>Authentication</td>
<td>1996</td>
<td>Paulson</td>
</tr>
<tr>
<td>Woo-Lam</td>
<td>Authentication</td>
<td>1996</td>
<td>Paulson</td>
</tr>
<tr>
<td>Otway-Bull</td>
<td>Authentication</td>
<td>1996</td>
<td>Paulson</td>
</tr>
<tr>
<td>NS asymmetric</td>
<td>Authentication</td>
<td>1997</td>
<td>Paulson</td>
</tr>
<tr>
<td>TLS</td>
<td>Multiple</td>
<td>1997</td>
<td>Paulson</td>
</tr>
<tr>
<td>Kerberos IV</td>
<td>Mutual authentication</td>
<td>1998</td>
<td>Bella</td>
</tr>
<tr>
<td>Kerberos BAN</td>
<td>Mutual authentication</td>
<td>1998</td>
<td>Bella &amp; Bella</td>
</tr>
<tr>
<td>SET suite</td>
<td>Multiple</td>
<td>2000+</td>
<td>Bella et al.</td>
</tr>
<tr>
<td>Abadi et al. certified e-mail</td>
<td>Accountability</td>
<td>2003</td>
<td>Bella et al.</td>
</tr>
<tr>
<td>Shoup-Rubin smartcard</td>
<td>Key distribution</td>
<td>2003</td>
<td>Bella</td>
</tr>
<tr>
<td>Zhou-Gollmann</td>
<td>Non-repudiation</td>
<td>2003</td>
<td>Paulson &amp; Bella</td>
</tr>
<tr>
<td>Kerberos V</td>
<td>Mutual authentication</td>
<td>2007</td>
<td>Bella</td>
</tr>
<tr>
<td>TESLA</td>
<td>Broadcast authentication</td>
<td>2009</td>
<td>Schaller et al.</td>
</tr>
<tr>
<td>Meadows distance bounding</td>
<td>Physical</td>
<td>2009</td>
<td>Basin et al.</td>
</tr>
<tr>
<td>Multicast NS symmetric</td>
<td>Key sharing</td>
<td>2011</td>
<td>Martina</td>
</tr>
<tr>
<td>Franklin-Reiter</td>
<td>Byzantine</td>
<td>2011</td>
<td>Martina</td>
</tr>
<tr>
<td>Onion routing</td>
<td>Anonymising</td>
<td>2011</td>
<td>Li &amp; Pang</td>
</tr>
</tbody>
</table>
E-voting Protocols

- New properties: privacy, verifiability, coercion-resistance...
- Partially studied with applied pi calculus, but with little mechanisation
- Often require modelling new crypto primitives
E-voting protocols: properties

- Eligibility
- Fairness
- Privacy / Receipt freeness / Coercion resistance – linkability concept (hard)
- Individual / Universal verifiability
The FOO Protocol

- Fujioka, Okamoto and Ohta, 1992
- Two election officials, bit commitment, blind signatures
- Signed, blinded commitment on a vote
- 6 steps
Specifying Blind Signatures

- Directly in `Message.thy` — limitation of operators interplay
- Solution: as part of inductive model

\[
\begin{aligned}
evsb &\in \text{foo}; \ Crypt (\text{priSK V}) \ BSBody \in \text{analz (spies \ evsb)}; \\
BSBody &= \ Crypt b (\ Crypt c (\text{Nonce N})); \ b \in \text{symKeys}; \\
Key b &\in \text{analz (spies \ evsb)}
\end{aligned}
\]

\[\Rightarrow \ Notes \ Spy (\ Crypt (\text{priSK V}) (\ Crypt c (\text{Nonce N}))) \neq \ evsb \in \text{foo}\]
What Is Privacy in E-Voting?

- Crucial point: privacy is NOT confidentiality of vote...
- ...But unlinkability of voter and vote
- In Pro-Verif, done with observational equivalence between swapped votes
Privacy in the Inductive Method: *aanalz*

```
primrec aanalz :: "agent => event list => msg set set"
where
  aanalz_Nil:  "aanalz A [] = {}"
| aanalz_Cons:
  "aanalz A (ev # evs) =
  (if A = Spy then
   (case ev of
      Says A' B X ⇒
       (if A' ∈ bad then aanalz Spy evs
        else if isAnms X
        then insert ({Agent B} ∪ (analzplus {X} (analz(knows Spy evs)))) (aanalz Spy evs)
        else insert ({Agent A'} Un {Agent B} ∪ (analzplus {X} (analz(knows Spy evs)))) (aanalz Spy evs)
      )
      | Gets A' X ⇒ aanalz Spy evs
      | Notes A' X ⇒ aanalz Spy evs)
   else aanalz A evs)"
```

Extract associations from honest agent’s messages
Privacy in the Inductive Method: *asynth*

**inductive_set**

*asynth :: msg set set → msg set set*

*for as :: msg set set where*

*asynth_Builder [intro]:*

\[
\begin{align*}
[a1 \in as; a2 \in as; m \in a1; m \in a2; m \neq \text{Agent Adm}; m \neq \text{Agent Co}] \\
\implies a1 \cup a2 \in asynth as
\end{align*}
\]

Build up association sets from associations with common elements. Only pairwise so far!
Privacy in the Inductive Method: Theorem Statement

**theorem foo_V_privacy_asynth:**

\[
\left[ \text{Says V Adm \{Agent V, } \right.
\left. \text{Crypt (priSK V) (Crypt b (Crypt c (Nonce Nv)))\}} \in \text{set evs; } \right.
\left. a \in (\text{asynth (aanalz Spy evs))}; \right.
\left. \text{Nonce Nv} \in a; V \notin \text{bad}; V \neq \text{Adm}; V \neq \text{Col}; evs \in \text{foo}\right]
\implies \text{Agent V} \neq a
\]

If a regular voter started the protocol, the corresponding vote and identity are unlinkable.
Privacy in the Inductive Method: Proving Process

- Genericity of steps 2 and 4 yields proof complexity
- Genericity is natural consequence of respecting guarantee availability
- Strategy: map components in asynth to possible origins in aanalz
- Taxonomy of structures of elements in aanalz
- Divide & conquer
Conclusions

- Flexibility of Inductive Method confirmed...
- ... but limitations related to message datatype extension
- Very different approach from most used tools (ProVerif, Scyther)...
- ... hence potential for complementarity!
Future Work

- Need stronger association synthesis — proof complexity challenge
- Analyse more recent e-voting protocols
Questions?