Deciding equivalence properties in security protocols

Vincent Cheval, Steve Kremer, Itsaka Rakotonirina

INRIA Nancy Grand-Est, LORIA
Security protocols

Google SSO  BAC (e-passport)

Helios (e-voting)

TLS 1.3 (prior ver.)  WPA2 (wifi)
Security protocols

Google SSO
Armando et al. (2008)

BAC (e-passport)
Chothia and Smirnov (2010)

Helios (e-voting)
Cortier and Smyth (2011)

TLS 1.3 (prior ver.)
Cremers et al. (2016)

WPA2 (wifi)
Vanhoef and Piessens (2017)
Security protocols

The attacker can...

- Read / Write
- Intercept

But they do not...

- Break cryptography
- Use side channels
Security protocols

The attacker can...
- Read / Write
- Intercept

But they do not...
- Break cryptography
- Use side channels

Dolev-Yao models
Concurrent systems where dishonest parties have complete control over inter-process communication
but cryptography is idealised
Security properties

Reachability
- Bad event in one system

Equivalence
- Privacy as indistinguishability

Authentication
- (weak) secrecy

Anonymity
- Vote privacy

Unlinkability
Security properties

Reachability  
Bad event in one system

Authentication

(weak) secrecy

Equivalence  
Privacy as indistinguishability

Anonymity

Vote privacy

Unlinkability
## Tool support

<table>
<thead>
<tr>
<th>Tamarin</th>
<th>Maude-NPA</th>
<th>ProVerif</th>
<th>Akiss</th>
<th>SAT-equiv</th>
<th>SPEC</th>
</tr>
</thead>
</table>

### Equivalence

Privacy as indistinguishability
Tool support

Equivalence
Privacy as indistinguishability

may not terminate  bounded number of protocol sessions

Tamarin   Maude-NPA   ProVerif   Akiss   SAT-equiv   SPEC
**Tool support**

**Equivalence**
Privacy as indistinguishability

- may not terminate
- bounded number of protocol sessions

- Tamarin
- Maude-NPA
- ProVerif
- Akiss
- SAT-equiv
- SPEC

- approximation of equivalence (false attacks)
## Tool support

<table>
<thead>
<tr>
<th>Tamarin</th>
<th>Maude-NPA</th>
<th>ProVerif</th>
<th>Akiss</th>
<th>SAT-equiv</th>
<th>SPEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>bounded number of protocol sessions</td>
<td>bounded number of protocol sessions</td>
<td>bounded number of protocol sessions</td>
<td>bounded number of protocol sessions</td>
<td>bounded number of protocol sessions</td>
<td>bounded number of protocol sessions</td>
</tr>
<tr>
<td>may not terminate</td>
<td>may not terminate</td>
<td>may not terminate</td>
<td>may not terminate</td>
<td>may not terminate</td>
<td>may not terminate</td>
</tr>
<tr>
<td>approximation of equivalence (false attacks)</td>
<td>approximation of equivalence (false attacks)</td>
<td>approximation of equivalence (false attacks)</td>
<td>approximation of equivalence (false attacks)</td>
<td>approximation of equivalence (false attacks)</td>
<td>approximation of equivalence (false attacks)</td>
</tr>
<tr>
<td>crypto limited to a few (common) primitives</td>
<td>crypto limited to a few (common) primitives</td>
<td>crypto limited to a few (common) primitives</td>
<td>crypto limited to a few (common) primitives</td>
<td>crypto limited to a few (common) primitives</td>
<td>crypto limited to a few (common) primitives</td>
</tr>
</tbody>
</table>

### Equivalence

Privacy as indistinguishability
Contributions

DEEPSEC prover

- may not terminate
- approximation of equivalence (false attacks)
- crypto limited to a few (common) primitives
- bounded number of protocol sessions
Contributions

DEEPSEC prover

- may not terminate
- approximation of equivalence (false attacks)
- exact procedure for trace equivalence
- crypto limited to a few (common) primitives
- any subterm convergent constructors/destructors
- bounded number of protocol sessions
Contributions

DEEPSEC prover

- may not terminate
- approximation of equivalence (false attacks)
- exact procedure for trace equivalence
- crypto limited to a few (common) primitives
- any subterm convergent constructors/destructors
- bounded number of protocol sessions
- running implementation
- tight complexity analysis of the problem
ANALYSING FINITE PROCESSES
The problem

[Diagram with skull and crossbones and stick figures]

[8/17]
The problem

Public outputs
increases attacker’s knowledge

Public inputs
crafted by the attacker
The problem

Public outputs
increases attacker’s knowledge

Public inputs
crafted by the attacker

source of infiniteness
The problem

Public outputs
increases attacker’s knowledge

source of infiniteness

Public inputs
crafted by the attacker
The problem

Public outputs
increases attacker’s knowledge

Symbolic knowledge base

source of infiniteness

Public inputs
crafted by the attacker

Symbolic inputs
finite
Handling the symbolic setting

Symbolic knowledge base  +  Symbolic inputs
Handling the symbolic setting

<table>
<thead>
<tr>
<th>Symbolic knowledge base</th>
<th>+</th>
<th>Symbolic inputs</th>
</tr>
</thead>
</table>

**Symbolic constraints**

to characterize symbolic traces
Handling the symbolic setting

Symbolic knowledge base + Symbolic inputs

Symbolic constraints
to characterize symbolic traces

\[ X \vdash ? x \]

Deducibility constraints
ability for the attacker to craft \( x \) (modulo crypto primitives)

\[ x \equiv y \]

Equations
equality of two terms
Decidability

\[ X \vdash ? x \]

Deducibility constraints
ability for the attacker to craft $x$
(modulo crypto primitives)

\[ x = y \]

Equations
equality of two terms
Decidability

\[ X \vdash ? x \]

Deducibility constraints
ability for the attacker to craft \( x \) (modulo crypto primitives)

\[ X = y \]

Equations
equality of two terms

**Ingredients**

- Most general solutions of a symbolic trace

  +

- Tree of sets of symbolic traces
  built by constraint solving
  equivalence = reachability of a BAD node
## Comparison to other tools

<table>
<thead>
<tr>
<th>#Agents</th>
<th>Wide-Mouth Frog (strong secrecy)</th>
<th>Helios Vanilla (vote privacy)</th>
<th>Helios Weeding</th>
<th>Helios Zero-KP</th>
<th>Helios W revote</th>
<th>Helios ZKP revote</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6 ✓</td>
<td>6 ⚠</td>
<td>6 ✓</td>
<td>6 ✓</td>
<td>11 ⚠</td>
<td>11 ✓</td>
</tr>
<tr>
<td></td>
<td>12 ✓</td>
<td>22min</td>
<td>OOM</td>
<td>OOM</td>
<td>OOM</td>
<td>2h 42min</td>
</tr>
<tr>
<td></td>
<td>23 ✓</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
</tr>
<tr>
<td></td>
<td></td>
<td>22min</td>
<td>OOM</td>
<td>OOM</td>
<td>OOM</td>
<td>2h 42min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3s</td>
<td>1s</td>
<td>2s</td>
<td>2h 42min</td>
</tr>
<tr>
<td></td>
<td></td>
<td>47s</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>2h 42min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>2h 42min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>2h 42min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>2h 42min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>2h 42min</td>
</tr>
</tbody>
</table>

- ✓ security proof
- ⚠ security violation
- — cannot be specified
- OOM out of memory
## Comparison to other tools

<table>
<thead>
<tr>
<th>#Agents</th>
<th>AKISS</th>
<th>SATEQUIV</th>
<th>DEEPSEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 ✓</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
</tr>
<tr>
<td>12 ✓</td>
<td>22min</td>
<td>&lt;1s</td>
<td>3s</td>
</tr>
<tr>
<td>23 ✓</td>
<td>OOM</td>
<td>&lt;1s</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#Agents</th>
<th>AKISS</th>
<th>SATEQUIV</th>
<th>DEEPSEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 ⚠</td>
<td>47s</td>
<td>—</td>
<td>&lt;1s</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#Agents</th>
<th>AKISS</th>
<th>SATEQUIV</th>
<th>DEEPSEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 ✓</td>
<td>OOM</td>
<td>—</td>
<td>1s</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#Agents</th>
<th>AKISS</th>
<th>SATEQUIV</th>
<th>DEEPSEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 ✓</td>
<td>OOM</td>
<td>—</td>
<td>2s</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#Agents</th>
<th>AKISS</th>
<th>SATEQUIV</th>
<th>DEEPSEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 ⚠</td>
<td>OOM</td>
<td>—</td>
<td>2s</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#Agents</th>
<th>AKISS</th>
<th>SATEQUIV</th>
<th>DEEPSEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 ✓</td>
<td>OOM</td>
<td>—</td>
<td>2h 42min</td>
</tr>
</tbody>
</table>

✓ security proof  ⚠ security violation  — cannot be specified  OOM out of memory
Couldn’t it be more efficient?
For subterm convergent crypto

- **Passive attacker**
  - PTIME
  - with fixed cryptographic primitives

- **Active attacker**
  - coNP-complete
  - if no `else` branches +
  - each honest agent uses a different channel
For subterm convergent crypto

- **Passive attacker**
  - PTIME
    - with fixed cryptographic primitives
  - coNP-complete in general

- **Active attacker**
  - coNP-complete
    - if no `else` branches + each honest agent uses a different channel
  - coNEXP-complete in general

New!
But in practice?

Unlinkability

Vote privacy
But in practice?

**Observation**

In practice, we check equivalence of processes with similar structure.

Unlinkability

Vote privacy
But in practice?

**Observation**
In practice, we check equivalence of processes with similar structure

**Future work**
Speed-up of the procedure in practical cases by using symmetry reductions
Conclusion

logical flaws of security protocols
Conclusion

Exact Analysis
without approximations
+ full finite fragment

logical flaws of security protocols
Conclusion

Exact Analysis
without approximations
+ full finite fragment

logical flaws of security protocols

“Optimal” Complexity
coNEXP-hardness
of the problem
Conclusion

Implementation
available at
https://deepsec-prover.github.io

Exact Analysis
without approximations
+ full finite fragment

logical flaws of
security protocols

“Optimal” Complexity
coNEXP-hardness
of the problem