Privacy-supporting cloud-based conference systems: protocol and verification

Myrto Arapinis, Sergiu Bursuc, Mark Ryan

School of Computer Science, University of Birmingham
Security of cloud computing

Does user have to trust the service provider?

- Confidentiality ← main issue
- Integrity
- Availability
EasyChair: the little Facebook

<table>
<thead>
<tr>
<th>Year</th>
<th>#confs</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>2</td>
</tr>
<tr>
<td>2003</td>
<td>3</td>
</tr>
<tr>
<td>2004</td>
<td>7</td>
</tr>
<tr>
<td>2005</td>
<td>66</td>
</tr>
<tr>
<td>2006</td>
<td>276</td>
</tr>
<tr>
<td>2007</td>
<td>629</td>
</tr>
<tr>
<td>2008</td>
<td>1312</td>
</tr>
<tr>
<td>2009</td>
<td>2183</td>
</tr>
<tr>
<td>2010</td>
<td>3306</td>
</tr>
<tr>
<td>2011</td>
<td>&gt;3690</td>
</tr>
<tr>
<td>2012</td>
<td>&gt;161</td>
</tr>
<tr>
<td>2013</td>
<td>&gt;5</td>
</tr>
</tbody>
</table>
EasyChair data about Mark Ryan, 2005-2011

Reviewed papers by A.Gordon (CSF’11), D.Ghica (FCS’11), G.Steel (ESORICS’10), M.Fisher (FM’10), P.Panagaden (LICS’09), and others. Recommended reject for all of them.

Had papers reviewed by S.Kremer (S&P’10), A.Martin (TRUST’09), M.Huth (POPL’08), J.Fiadeiro (CAV’09), etc. They all recommended accept.
EasyChair data about Mark Ryan, 2005-2011

Reviewed papers by A.Gordon (CSF’11), D.Ghica (FCS’11), G.Steel (ESORICS’10), M.Fisher (FM’10), P.Panagaden (LICS’09), and others. Recommended *reject* for all of them.

Had papers reviewed by S.Kremer (S&P’10), A.Martin (TRUST’09), M.Huth (POPL’08), J.Fiadeiro (CAV’09), etc. They all recommended *accept*.

- number of papers submitted: 25
- number of papers accepted: 17
- Acceptance rate: 0.68
- number of papers reviewed: 107
- number of times recommended accept: 24
- Recomendation agr. w. outcome: 28%
EasyChair data about Mark Ryan, 2005-2011

Reviewed papers by A.Gordon (CSF’11), D.Ghica (FCS’11), G.Steel (ESORICS’10), M.Fisher (FM’10), P.Panagaden (LICS’09), and others. Recommended reject for all of them.

Had papers reviewed by S.Kremer (S&P’10), A.Martin (TRUST’09), M.Huth (POPL’08), J.Fiadeiro (CAV’09), etc. They all recommended accept.

<table>
<thead>
<tr>
<th>Number of papers submitted</th>
<th>25</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of papers accepted</td>
<td>17</td>
</tr>
<tr>
<td>Acceptance rate</td>
<td>0.68</td>
</tr>
<tr>
<td>Number of papers reviewed</td>
<td>107</td>
</tr>
<tr>
<td>Number of times recommended accept</td>
<td>24</td>
</tr>
<tr>
<td>Recommendation agr. w. outcome</td>
<td>28%</td>
</tr>
</tbody>
</table>

Probability CSF 2012 re-invites him 0.2
Prob. will win ACM Turing award $2^{-11.2}$
Initialization
create $Conf$, $K_{conf}$, $pub(conf)$, $priv(conf)$

Conf, $R_1, \ldots, R_\ell$

Submission
$K_{conf}$

$DB_{conf} \leftarrow (A, \{A, P, k\}_{pub(conf)})::DB_{conf}$

create $P, k$
Chair | Cloud | Reviewer | Author
---|---|---|---
Reviewing | 

\[ [(A_1, \{ subm_1 \}_{pub(conf)}); \ldots ; (A_n, \{ subm_n \}_{pub(conf)})] \leftarrow DB_{conf} \]

pick \( R_1, \ldots , R_n \in \{ R_1, \ldots , R_\ell \} \)
\( DB \leftarrow \{ (\{ subm_1 \}_{K_{conf}}, R_1); \ldots ; (\{ subm_n \}_{K_{conf}}, R_n) \} \)

\( \{ i_1, \ldots , i_k \} \leftarrow \{ i \mid (A_i, P_i, R) \in DB \} \)
\( DB_R \leftarrow [\{ subm_{i_1} \}_{K_{conf}}; \ldots ; \{ subm_{i_k} \}_{K_{conf}}] \)

pick \( s_1, \ldots , s_k \in S \)
create \( r_1, \ldots , r_k \)
\( DB'_R \leftarrow [\{ subm_{i_1} , r_1 , s_1 \}_{K_{conf}}; \ldots ; \{ subm_{i_k} , r_k , s_k \}_{K_{conf}}] \)

\( DB_{rev} \leftarrow DB'_R @ DB_{rev} \)
\[
\{\{A_1', P_1', k_1', r_1', s_1'\}\}_K^{conf}; \ldots ; \{\{A_n', P_n', k_n', r_n', s_n'\}\}_K^{conf} \}
\]

\[DB_{\text{rev}} \leftarrow DB_{\text{rev}}\]

\[DB_{\text{rnk}} \leftarrow \{(s_1', \{A_1', P_1', k_1', r_1'\}_K^{conf}); \ldots ; (s_n', \{A_n', P_n', k_n', r_n'\}_K^{conf})\}\]

\[DB_{\text{res}} \leftarrow \{(rk_1', \{A_1', P_1', k_1', r_1'\}_K^{conf}); \ldots ; (rk_n', \{A_n', P_n', k_n', r_n'\}_K^{conf})\}\]

\[\text{pick } o_1, \ldots , o_n \in \{\text{acc, rej}\}\]

\[DB_{\text{notif}} \leftarrow \{(A_1', \{P_1', r_1', o_1\}_k'); \ldots ; (A_n', \{P_n', r_n', o_n\}_k')\}\]

\[\text{if } A_i' = A \]

\[(A_i', \{P_i', r_i', o_i\}_k')\]
Formal verification
Formal model

Term algebra $\mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$

$\mathcal{X} = x, y, z, \ldots$
$\mathcal{N} = a, b, c, k_1, k_2, \ldots$
$\Sigma = \{ \text{senc}(\_, \_, \_), \text{sdec}(\_, \_), \text{pub}(\_), \text{aenc}(\_, \_, \_), \text{adec}(\_, \_), \langle \_, \_ \rangle, \text{proj}_1(\_), \text{proj}_2(\_) \}$

Process calculus ProVerif [Blanchet’2001]

$P, Q, R ::= 0$

$P \mid Q$

$!P$

$new \ n; P$

(let $M = D$ in $P$ else $Q$

$\text{in}(c, M); P$

$\text{out}(c, M); P$
Term rewriting

\[
\begin{align*}
s\text{dec}(x, s\text{enc}(x, y, z)) & \rightarrow z & \text{proj}_1(\langle x, y \rangle) & \rightarrow x \\
\text{a\text{dec}}(x, \text{a\text{enc}}(\text{pub}(x), y, z)) & \rightarrow z & \text{proj}_2(\langle x, y \rangle) & \rightarrow y
\end{align*}
\]

Process reduction

\[
\begin{align*}
\text{out}(c, M).P \mid \text{in}(c, x).Q & \rightarrow P \mid Q\{M/x\} \\
\text{let } M = D \text{ in } P \text{ else } Q & \rightarrow P\sigma, \text{ if } D \Downarrow N \& \sigma = \mu(M, N) \\
\text{let } M = D \text{ in } P \text{ else } Q & \rightarrow Q, \text{ otherwise}
\end{align*}
\]
Observational equivalence

Observation $P \downarrow c$:

$$\exists C[\_] \exists Q, \exists M. \quad P \rightarrow^* C[\text{out}(c, M).Q]$$

Largest equivalence relation s.t. $P \sim Q$ implies

1. $P \downarrow c \implies Q \downarrow c$
2. $P \rightarrow^* P' \implies \exists Q'. Q \rightarrow^* Q' \& P' \sim Q'$
3. $\forall C[\_]. \quad C[P] \sim C[Q]
Secrecy in conference systems

Papers: \( P_{\text{conf}} \rightsquigarrow P_{\text{conf}}^\text{p}[-] \)

Reviews: \( P_{\text{conf}} \rightsquigarrow P_{\text{conf}}^\text{r}[-] \)

- Secrecy of papers: \( P_{\text{conf}}^\text{p}[\text{pap}] \sim P_{\text{conf}}^\text{p}[\text{pap}'] \)
- Secrecy of reviews: \( P_{\text{conf}}^\text{r}[\text{rev}] \sim P_{\text{conf}}^\text{r}[\text{rev}'] \)
Unlinkability in conference systems

**Author-Score:**

\[ P_{\text{conf}}^{\text{AS}}(a, \text{one})|P_{\text{conf}}^{\text{AS}}(b, \text{two}) \sim P_{\text{conf}}^{\text{AS}}(a, \text{two})|P_{\text{conf}}^{\text{AS}}(b, \text{one}) \]

**Reviewer-Score:**

\[ P_{\text{conf}}^{\text{RS}}(ra, \text{one})|P_{\text{conf}}^{\text{RS}}(rb, \text{two}) \sim P_{\text{conf}}^{\text{RS}}(ra, \text{two})|P_{\text{conf}}^{\text{RS}}(rb, \text{one}) \]

**Author-Reviewer:**

\[ P_{\text{conf}}^{\text{AR}}(a, ra)|P_{\text{conf}}^{\text{AR}}(b, rb) \sim P_{\text{conf}}^{\text{AR}}(a, rb)|P_{\text{conf}}^{\text{AR}}(b, ra) \]
Conclusions

“ToughChair”

- C does not know $p$ and $r$
- C knows $A$, $R$, and $s$, but
  - does not know the link $A \leftrightarrow s$
  - does not know the link $R \leftrightarrow s$
  - does not know the link $A \leftrightarrow R$

Formalising the properties, and verifying them.

Implementation by Matt Roberts and Joshua Phillips

toughchair.markryan.eu

The future

- A more systematic way to formalise the properties
- More cloud computing examples