CoCon: A Conference Management System with Verified Document Confidentiality

Sudeep Kanav Peter Lammich Andrei Popescu

Technische Universität München
Overview

What?

• Implementation of CoCon, a config. manag. sys.
• Verification in Isabelle of its information flow

Why?

• Anonymity and integrity concerns
Overview

What?

- Implementation of CoCon, a conf. manag. sys.
Overview

What?

- Implementation of CoCon, a conf. manag. sys.
- Verification in Isabelle of its information flow
Overview

What?
- Implementation of CoCon, a conf. manag. sys.
- Verification in Isabelle of its information flow

Why?
Overview

What?
- Implementation of CoCon, a conf. manag. sys.
- Verification in Isabelle of its information flow

Why?
- Anonymity and integrity concerns
It is our pleasure to inform you that your paper has been accepted to the IEEE Symposium of Security and Privacy (Oakland) 2012.
It is our pleasure to inform you that your paper has been accepted to the IEEE Symposium of Security and Privacy (Oakland) 2012.

We are sorry to inform you that your paper was not one of those accepted for this year’s conference. We apologize for an earlier ”acceptance” notification. It was due to a system error.
It is our pleasure to inform you that your paper has been accepted to the IEEE Symposium of Security and Privacy (Oakland) 2012.

We are sorry to inform you that your paper was not one of those accepted for this year’s conference. We apologize for an earlier "acceptance" notification. It was due to a system error.
Overview

What?
- Implementation of CoCon, a conf. manag. sys.
- Verification in Isabelle of its information flow

Why?
- Anonymity and integrity concerns
Overview

What?
- Implementation of CoCon, a conf. manag. sys.
- Verification in Isabelle of its information flow

Why?
- Anonymity and integrity concerns
- System with complex information flow
Overview

What?
- Implementation of CoCon, a conf. manag. sys.
- Verification in Isabelle of its information flow

Why?
- Anonymity and integrity concerns
- System with complex information flow
- Knowledge on how to approach similar systems
CoCon’s Architecture

Isabelle Specification → code generation → Scala Program → REST Web Service → Web Application
CoCon’s Architecture

Isabelle Specification \(\rightarrow\) code generation \(\rightarrow\) Scala Program

- REST Web Service
- Web Application

http://vmnipkow1.informatik.tu-muenchen.de

Used it for Isabelle 2014 Workshop
System Specification

Multi-user, multi-conference system

- **Users:**
  - ID and password

- **State:**
  - papers, authors, reviews, discussions, notifications, ...

- **Actions:**
  - register paper, upload new version,
  - bid on papers (if committee), assign reviewer (if chair), ...

- **Outputs:**
  - download paper, read review, list committee members, ...
End Product of System Specification

step : state → act → out × state
Verified Confidentiality Properties

What, when, by whom
Verified Confidentiality Properties

What, when, by whom can be learned about
Verified Confidentiality Properties

What, when, by whom can be learned about the documents in the system (papers, reviews, discussions, preferences)
<table>
<thead>
<tr>
<th>Source</th>
<th>Declassification Trigger</th>
<th>Declassification Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper Content</td>
<td>Paper Authorship</td>
<td>Last Uploaded Version</td>
</tr>
<tr>
<td></td>
<td>Paper Authorship or PC Membership&lt;sup&gt;B&lt;/sup&gt;</td>
<td>Nothing</td>
</tr>
<tr>
<td>Review</td>
<td>Review Authorship</td>
<td>Last Edited Version Before Discussion and All the Later Versions</td>
</tr>
<tr>
<td></td>
<td>Review Authorship or Non-Conflict PC Membership&lt;sup&gt;D&lt;/sup&gt;</td>
<td>Last Edited Version Before Notification</td>
</tr>
<tr>
<td></td>
<td>Review Authorship or Non-Conflict PC Membership&lt;sup&gt;D&lt;/sup&gt; or PC Membership&lt;sup&gt;N&lt;/sup&gt; or Paper Authorship&lt;sup&gt;N&lt;/sup&gt;</td>
<td>Nothing</td>
</tr>
<tr>
<td>Discussion</td>
<td>Non-Conflict PC Membership</td>
<td>Nothing</td>
</tr>
<tr>
<td>Decision</td>
<td>Non-Conflict PC Membership</td>
<td>Last Edited Version</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership or PC Membership&lt;sup&gt;N&lt;/sup&gt; or Paper Authorship&lt;sup&gt;N&lt;/sup&gt;</td>
<td>Nothing</td>
</tr>
<tr>
<td>Reviewer Assignment to Paper</td>
<td>Non-Conflict PC Membership&lt;sup&gt;R&lt;/sup&gt;</td>
<td>Non-Conflict PC Membership of Reviewers and Number of Reviewers</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership&lt;sup&gt;R&lt;/sup&gt; or Paper Authorship&lt;sup&gt;N&lt;/sup&gt;</td>
<td>Non-Conflict PC Membership of Reviewers</td>
</tr>
</tbody>
</table>

Phase Stamps: B = Bidding, D = Discussion, N = Notification, R = Review
<table>
<thead>
<tr>
<th>Source</th>
<th>Declassification Trigger</th>
<th>Declassification Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper Content</td>
<td>Paper Authorship</td>
<td>Last Uploaded Version</td>
</tr>
<tr>
<td></td>
<td>Paper Authorship or PC Membership(^B)</td>
<td>Nothing</td>
</tr>
<tr>
<td>Review</td>
<td>Review Authorship</td>
<td>Last Edited Version Before Discussion and All the Later Versions</td>
</tr>
<tr>
<td></td>
<td>Review Authorship or Non-Conflict PC Membership(^D)</td>
<td>Last Edited Version Before Notification</td>
</tr>
<tr>
<td></td>
<td>Review Authorship or Non-Conflict PC Membership(^D) or PC Membership(^N) or Paper Authorship(^N)</td>
<td>Nothing</td>
</tr>
<tr>
<td>Discussion</td>
<td>Non-Conflict PC Membership</td>
<td>Nothing</td>
</tr>
<tr>
<td>Decision</td>
<td>Non-Conflict PC Membership</td>
<td>Last Edited Version</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership or PC Membership(^N) or Paper Authorship(^N)</td>
<td>Nothing</td>
</tr>
<tr>
<td>Reviewer Assignment to Paper</td>
<td>Non-Conflict PC Membership(^R)</td>
<td>Non-Conflict PC Membership of Reviewers and Number of Reviewers</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership(^R) or Paper Authorship(^N)</td>
<td>Non-Conflict PC Membership of Reviewers</td>
</tr>
</tbody>
</table>

Phase Stamps: \(B =\) Bidding, \(D =\) Discussion, \(N =\) Notification, \(R =\) Review
<table>
<thead>
<tr>
<th>Source</th>
<th>Declassification Trigger</th>
<th>Declassification Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper Content</td>
<td>Paper Authorship</td>
<td>Last Uploaded Version</td>
</tr>
<tr>
<td></td>
<td>Paper Authorship or PC Membership&lt;sup&gt;B&lt;/sup&gt;</td>
<td>Nothing</td>
</tr>
<tr>
<td>Review</td>
<td>Review Authorship</td>
<td>Last Edited Version Before Discussion and All the Later Versions</td>
</tr>
<tr>
<td></td>
<td>Review Authorship or Non-Conflict PC Membership&lt;sup&gt;D&lt;/sup&gt;</td>
<td>Last Edited Version Before Notification</td>
</tr>
<tr>
<td></td>
<td>Review Authorship or Non-Conflict PC Membership&lt;sup&gt;D&lt;/sup&gt; or PC Membership&lt;sup&gt;N&lt;/sup&gt; or Paper Authorship&lt;sup&gt;N&lt;/sup&gt;</td>
<td>Nothing</td>
</tr>
<tr>
<td>Discussion</td>
<td>Non-Conflict PC Membership</td>
<td>Nothing</td>
</tr>
<tr>
<td>Decision</td>
<td>Non-Conflict PC Membership</td>
<td>Last Edited Version</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership or PC Membership&lt;sup&gt;N&lt;/sup&gt; or Paper Authorship&lt;sup&gt;N&lt;/sup&gt;</td>
<td>Nothing</td>
</tr>
<tr>
<td>Reviewer Assignment</td>
<td>Non-Conflict PC Membership&lt;sup&gt;R&lt;/sup&gt;</td>
<td>Non-Conflict PC Membership of Reviewers and Number of Reviewers</td>
</tr>
<tr>
<td>to Paper</td>
<td>Non-Conflict PC Membership&lt;sup&gt;R&lt;/sup&gt; or Paper Authorship&lt;sup&gt;N&lt;/sup&gt;</td>
<td>Non-Conflict PC Membership of Reviewers</td>
</tr>
</tbody>
</table>

Phase Stamps: B = Bidding, D = Discussion, N = Notification, R = Review
<table>
<thead>
<tr>
<th>Source</th>
<th>Declassification Trigger</th>
<th>Declassification Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper Content</td>
<td>Paper Authorship</td>
<td>Last Uploaded Version</td>
</tr>
<tr>
<td></td>
<td>Paper Authorship or PC Membership^{B}</td>
<td>Nothing</td>
</tr>
<tr>
<td>Review</td>
<td>Review Authorship</td>
<td>Last Edited Version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Before Discussion and All the Later Versions</td>
</tr>
<tr>
<td></td>
<td>Review Authorship or Non-Conflict PC Membership^{D}</td>
<td>Last Edited Version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Before Notification</td>
</tr>
<tr>
<td></td>
<td>Review Authorship or Non-Conflict PC Membership^{D} or PC Membership^{N} or Paper Authorship^{N}</td>
<td>Nothing</td>
</tr>
<tr>
<td>Discussion</td>
<td>Non-Conflict PC Membership</td>
<td>Nothing</td>
</tr>
<tr>
<td>Decision</td>
<td>Non-Conflict PC Membership</td>
<td>Last Edited Version</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership or PC Membership^{N} or Paper Authorship^{N}</td>
<td>Nothing</td>
</tr>
<tr>
<td>Reviewer Assignment to Paper</td>
<td>Non-Conflict PC Membership^{R}</td>
<td>Non-Conflict PC Membership of Reviewers and Number of Reviewers</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership^{R} or Paper Authorship^{N}</td>
<td>Non-Conflict PC Membership of Reviewers</td>
</tr>
</tbody>
</table>

Phase Stamps: B = Bidding, D = Discussion, N = Notification, R = Review
<table>
<thead>
<tr>
<th>Source</th>
<th>Declassification Trigger</th>
<th>Declassification Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper Content</td>
<td>Paper Authorship</td>
<td>Last Uploaded Version</td>
</tr>
<tr>
<td></td>
<td>Paper Authorship or PC Membership&lt;sup&gt;B&lt;/sup&gt;</td>
<td>Nothing</td>
</tr>
<tr>
<td>Review</td>
<td>Review Authorship</td>
<td>Last Edited Version</td>
</tr>
<tr>
<td></td>
<td>Review Authorship or</td>
<td>Before Discussion and</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership&lt;sup&gt;D&lt;/sup&gt;</td>
<td>All the Later Versions</td>
</tr>
<tr>
<td></td>
<td>Review Authorship or</td>
<td>Last Edited Version</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership&lt;sup&gt;D&lt;/sup&gt; or PC Membership&lt;sup&gt;N&lt;/sup&gt;</td>
<td>Before Notification</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership&lt;sup&gt;D&lt;/sup&gt; or PC Membership&lt;sup&gt;N&lt;/sup&gt;</td>
<td>Nothing</td>
</tr>
<tr>
<td>Discussion</td>
<td>Non-Conflict PC Membership</td>
<td>Nothing</td>
</tr>
<tr>
<td>Decision</td>
<td>Non-Conflict PC Membership</td>
<td>Last Edited Version</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership or PC Membership&lt;sup&gt;N&lt;/sup&gt;</td>
<td>Nothing</td>
</tr>
<tr>
<td>Reviewer Assignment to Paper</td>
<td>Non-Conflict PC Membership&lt;sup&gt;R&lt;/sup&gt;</td>
<td>Non-Conflict PC Membership of Reviewers and Number of Reviewers</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership&lt;sup&gt;R&lt;/sup&gt; or Paper Authorship&lt;sup&gt;N&lt;/sup&gt;</td>
<td>Non-Conflict PC Membership of Reviewers</td>
</tr>
</tbody>
</table>

Phase Stamps: B = Bidding, D = Discussion, N = Notification, R = Review
<table>
<thead>
<tr>
<th>Source</th>
<th>Declassification Trigger</th>
<th>Declassification Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper Content</td>
<td>Paper Authorship</td>
<td>Last Uploaded Version</td>
</tr>
<tr>
<td></td>
<td>Paper Authorship or PC Membership(^B)</td>
<td>Nothing</td>
</tr>
<tr>
<td>Review</td>
<td>Review Authorship</td>
<td>Last Edited Version Before Discussion and All the Later Versions</td>
</tr>
<tr>
<td></td>
<td>Review Authorship or Non-Conflict PC Membership(^D)</td>
<td>Last Edited Version Before Notification</td>
</tr>
<tr>
<td></td>
<td>Review Authorship or Non-Conflict PC Membership(^D) and PC Membership(^N) or Paper Authorship(^N)</td>
<td>Nothing</td>
</tr>
<tr>
<td>Discussion</td>
<td>Non-Conflict PC Membership</td>
<td>Nothing</td>
</tr>
<tr>
<td>Decision</td>
<td>Non-Conflict PC Membership</td>
<td>Last Edited Version</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership or PC Membership(^N) or Paper Authorship(^N)</td>
<td>Nothing</td>
</tr>
<tr>
<td>Reviewer Assignment to Paper</td>
<td>Non-Conflict PC Membership(^R)</td>
<td>Non-Conflict PC Membership of Reviewers and Number of Reviewers</td>
</tr>
<tr>
<td></td>
<td>Non-Conflict PC Membership(^R) or Paper Authorship(^N)</td>
<td>Non-Conflict PC Membership of Reviewers</td>
</tr>
</tbody>
</table>

Phase Stamps: \(B = \text{Bidding}, D = \text{Discussion}, N = \text{Notification}, R = \text{Review}\)
Bounded-Deducibility Security

\( \phi \) : Event \( \rightarrow \) Bool
\( f \) : Event \( \rightarrow \) Val

V = "filter with \( \phi \), then apply \( f \), event-wise"

List(Event) List(Val)

List(Obs)
Bounded-Deducibility Security

\[ \varphi : \text{Event} \rightarrow \text{Bool} \quad f : \text{Event} \rightarrow \text{Val} \]
\[ V = \text{"filter with } \varphi \text{, then apply } f \text{, event-wise"} \]

\[ \text{List(Event)} \xrightarrow{V} \text{List(Val)} \]

List(Obs)
Bounded-Deducibility Security

\[ \gamma : \text{Event} \rightarrow \text{Bool} \]
\[ g : \text{Event} \rightarrow \text{Obs} \]

\[ E = "\text{filter with } \gamma, \text{ then apply } g, \text{ event-wise}" \]
Bounded-Deducibility Security

\[ T : \text{Event} \rightarrow \text{Bool} \]

\[ \text{List(Event)} \rightarrow \text{List(Val)} \]

\[ \text{E} \]

\[ \text{List(Obs)} \]
Bounded-Deducibility Security

\[ T : \text{Event} \rightarrow \text{Bool} \quad \text{B relation on List(Val)} \]

\[ \begin{array}{c}
T \\
\downarrow \\
E \\
\downarrow \\
\text{List(Obs)}
\end{array} \quad \begin{array}{c}
\text{List(Event)} \quad V \\
\downarrow \\
\text{List(Val)} \quad \text{B}
\end{array} \]
Bounded-Deducibility Security

Unless $T$ occurs, $E$ can learn nothing about $V$ beyond $B$
Bounded-Deducibility Security

Unless $T$ occurs, $E$ can learn nothing about $V$ beyond $B$
Bounded-Deducibility Security

Unless T occurs, E can learn nothing about V beyond B.
Bounded-Deducibility Security

Unless $T$ occurs, $E$ can learn nothing about $V$ beyond $B$
Bounded-Deducibility Security

Unless T occurs, E can learn nothing about V beyond B

T \rightarrow \text{List(Event)} \rightarrow V \rightarrow \text{List(Val)} \rightarrow B

E \downarrow

\text{List(Obs)} \rightarrow 0 \rightarrow 0
Bounded-Deducibility Security

Unless $T$ occurs, $E$ can learn nothing about $V$ beyond $B$
Bounded-Deducibility Security

Unless T occurs, E can learn nothing about V beyond B

\[ T \xrightarrow{\text{List(Event)}} V \xrightarrow{\text{List(Val)}} B \]

\[ E \xleftarrow{\text{List(Obs)}} \]

\[ \text{o o} \]
Bounded-Deducibility Security

Unless $T$ occurs, $E$ can learn nothing about $V$ beyond $B$
Bounded-Deducibility Security

Proof by unwinding

\[ \text{T} \xrightarrow{\text{List(Event)}} \text{V} \xrightarrow{\text{List(Val)}} \text{B} \]

\[ \text{E} \xrightarrow{\text{List(Obs)}} \]

\[ \text{v} \quad \text{v} \]

\[ \text{v} \quad \text{B} \quad \text{v} \]

\[ \text{v} \]
Bounded-Deducibility Security

Proof by unwinding
Action

T \quad \text{List(Event)} \quad V \quad \text{List(Val)} \quad B

E

List(Obs)
Bounded-Deducibility Security

Proof by unwinding
Action / Reaction: Match

\[
\begin{align*}
\text{T} & \quad \text{List(Event)} & \quad V & \quad \text{List(Val)} & \quad B \\
E & \quad \text{List(Obs)} & \quad \text{oo}
\end{align*}
\]
Bounded-Deducibility Security

Proof by unwinding
Action

\[ T \xrightarrow{V} \text{List(Event)} \xrightarrow{V} \text{List(Val)} \]

\[ \text{List(Obs)} \xrightarrow{E} \text{List(Event)} \]

\[ \text{List(Obs)} \xrightarrow{V} \text{List(Event)} \]

\[ \text{List(Event)} \xrightarrow{V} \text{List(Val)} \]

\[ \text{List(Val)} \]
Bounded-Deducibility Security

Proof by unwinding
Action / Reaction: Ignore

T \rightarrow V \rightarrow \text{List(Val)}

E

List(Event) \rightarrow \text{List(Obs)}

oo
Bounded-Deducibility Security

Proof by unwinding
Action

\[ \text{List(Event)} \rightarrow \text{List(Val)} \]

\[ \text{List(Obs)} \rightarrow \]
Bounded-Deducibility Security

Proof by unwinding
Action / Reaction: Match

\[ \begin{align*}
T & \xrightarrow{V} \text{List(Val)} \\
\text{List(Event)} & \end{align*} \]

\[ \begin{align*}
\text{List(Obs)} & \xrightarrow{E} \text{List(Event)} \\
& \end{align*} \]

\[ \text{List(Obs)} \xrightarrow{oo} \text{List(Obs)} \]
Bounded-Deducibility Security

Proof by unwinding
Independent action . . .

\[
\begin{align*}
T & \quad \text{List(Event)} & \quad V & \quad \text{List(Val)} & \quad B \\
\text{List(Obs)} & \quad \text{oo} & \quad \text{oo}
\end{align*}
\]
Bounded-Deducibility Security

Proof by unwinding
Independent action

List(Event)  \(\rightarrow\)  List(Val)  B

E
List(Obs)  oo  oo
Bounded-Deducibility Security

Proof by unwinding
Independent action

\[
\begin{align*}
T & \quad \text{List(Event)} & V & \quad \text{List(Val)} & B \\
E & \quad \text{List(Obs)} & \text{oo} & \text{oo}
\end{align*}
\]
Bounded-Deducibility Security

Proof by unwinding

\[ \mathcal{B} \mapsto \Delta \subseteq \text{State} \times \text{List(Val)} \times \text{State} \times \text{List(Val)} \]

\[ \text{List(Event)} \]

\[ \text{T} \]

\[ \text{List(Obs)} \]

\[ \text{oo} \]

\[ \text{oo} \]
Bounded-Deducibility Security

Proof by unwinding

\[ B \rightsquigarrow \Delta \subseteq \text{State} \times \text{List(Val)} \times \text{State} \times \text{List(Val)} \]

Diagram:

- \( T \) \( \rightarrow \) \( \text{List(Event)} \) \( \overset{V}{\longrightarrow} \) \( \text{List(Val)} \) \( \rightarrow \) \( B \)

- \( E \)

- \( \text{List(Obs)} \)

- \( \text{oo} \) \( \text{oo} \)
Proof by Unwinding
Proof by Unwinding

\[ \Delta \subseteq \text{State} \times \text{List(Val)} \times \text{State} \times \text{List(Val)} \]
Proof by Unwinding

\[ \Delta \subseteq \text{State} \times \text{List(Val)} \times \text{State} \times \text{List(Val)} \]

Strategy for:
- when to act independently
- when to react
- if react: when to match and when to ignore
Summary

- Generic parameterized security notion
- Associated unwinding proof method
- Instantiated to reason about CoCon’s confidentiality
Future Work – More Holistic Verification

Isabelle Specification

code generation

Scala Program

REST Web Service

Web Application
Related Work

Theoretical frameworks

- **Sutherland 1986**: Nondeducibility
- Mantel 2000: MAKS framework
- Halpern and O'Neill, 2008: Secrecy in multiagent systems

Mechanical verification

- Arapinis et al. 2012: ConfiChair
- de Amorim et al. 2014: A Verified Information Flow Architecture
Thank You

Organizing a verification-friendly workshop?
Please consider using CoCon.

CoCon’s website:
www4.in.tum.de/~popescua/rs3/GNE.html