CoCon: A Conference Management System with Verified Document Confidentiality

Sudeep Kanav Peter Lammich Andrei Popescu

Technische Universität München

Overview

What?

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

Why

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

Why

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.

Why

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.

WARNING: HotCRP version 2.47 (commit range 94ca5a0e43bd7dd0565c2c8dc7d8f710a206ab49 through 9c1b45475411ecb85d46bad1f76064881792b038) was subject to an information exposure where some authors could see PC comments. Users of affected versions should upgrade or set the following option in `Code/options.inc`: `$Opt["disableCapabilities"] = true;`

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

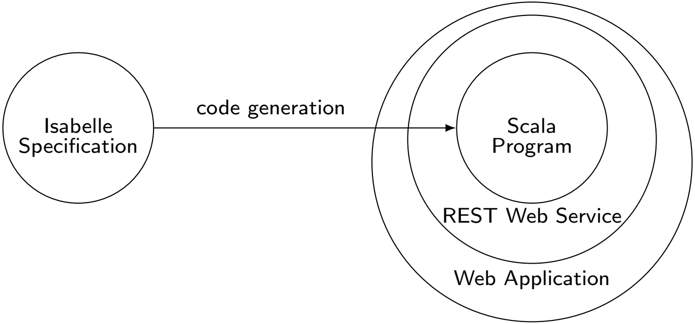
What?

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

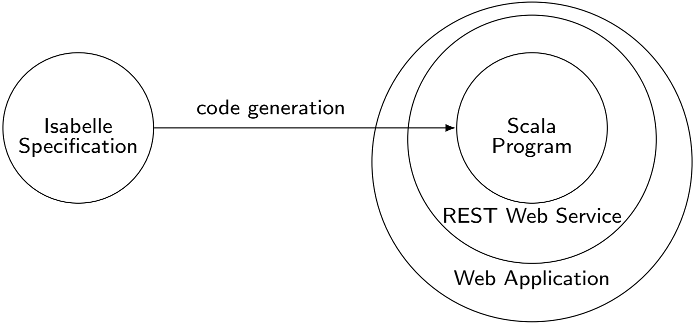
Why?

- Anonymity and integrity concerns
- System with complex information flow
- Knowledge on how to approach similar systems

CoCon's Architecture



CoCon's Architecture



`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

$$\mathsf{step} : \mathsf{state} \rightarrow \mathsf{act} \rightarrow \mathsf{out} \times \mathsf{state}$$

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)

Source	**Declassification Trigger**	**Declassification Bound**
Paper Content	Paper Authorship	Last Uploaded Version
	Paper Authorship or PC Membership^{B}	Nothing
Review	Review Authorship	Last Edited Version Before Discussion and All the Later Versions
	Review Authorship or Non-Conflict PC Membership^{D}	Last Edited Version Before Notification
	Review Authorship or Non-Conflict PC Membership^{D} or PC Membership^{N} or Paper Authorship^{N}	Nothing
Discussion	Non-Conflict PC Membership	Nothing
Decision	Non-Conflict PC Membership	Last Edited Version
	Non-Conflict PC Membership or PC Membership^{N} or Paper Authorship^{N}	Nothing
Reviewer Assignment to Paper	Non-Conflict PC Membership^{R}	Non-Conflict PC Membership of Reviewers and Number of Reviewers
	Non-Conflict PC Membership^{R} or Paper Authorship^{N}	Non-Conflict PC Membership of Reviewers

Phase Stamps: B = Bidding, D = Discussion, N = Notification, R = Review

Source	Declassification Trigger	Declassification Bound
Paper Content	Paper Authorship	Last Uploaded Version
	Paper Authorship or PC Membership^{B}	Nothing
Review	Review Authorship	Last Edited Version Before Discussion and All the Later Versions
	Review Authorship or Non-Conflict PC Membership^{D}	Last Edited Version Before Notification
	Review Authorship or Non-Conflict PC Membership^{D} or PC Membership^{N} or Paper Authorship^{N}	Nothing
Discussion	Non-Conflict PC Membership	Nothing
Decision	Non-Conflict PC Membership	Last Edited Version
	Non-Conflict PC Membership or PC Membership^{N} or Paper Authorship^{N}	Nothing
Reviewer Assignment to Paper	Non-Conflict PC Membership^{R}	Non-Conflict PC Membership of Reviewers and Number of Reviewers
	Non-Conflict PC Membership^{R} or Paper Authorship^{N}	Non-Conflict PC Membership of Reviewers

Phase Stamps: B = Bidding, D = Discussion, N = Notification, R = Review

Source	Declassification Trigger	Declassification Bound
Paper Content	Paper Authorship	Last Uploaded Version
	Paper Authorship or PC Membership^{B}	Nothing
Review	Review Authorship	Last Edited Version Before Discussion and All the Later Versions
	Review Authorship or Non-Conflict PC Membership^{D}	Last Edited Version Before Notification
	Review Authorship or Non-Conflict PC Membership^{D} or PC Membership^{N} or Paper Authorship^{N}	Nothing
Discussion	Non-Conflict PC Membership	Nothing
Decision	Non-Conflict PC Membership	Last Edited Version
	Non-Conflict PC Membership or PC Membership^{N} or Paper Authorship^{N}	Nothing
Reviewer Assignment to Paper	Non-Conflict PC Membership^{R}	Non-Conflict PC Membership of Reviewers and Number of Reviewers
	Non-Conflict PC Membership^{R} or Paper Authorship^{N}	Non-Conflict PC Membership of Reviewers

Phase Stamps: B = Bidding, D = Discussion, N = Notification, R = Review

Source	Declassification Trigger	Declassification Bound
Paper Content	Paper Authorship	Last Uploaded Version
	Paper Authorship or PC Membership^{B}	Nothing
Review	Review Authorship	Last Edited Version Before Discussion and All the Later Versions
	Review Authorship or Non-Conflict PC Membership^{D}	Last Edited Version Before Notification
	Review Authorship or Non-Conflict PC Membership^{D} or PC Membership^{N} or Paper Authorship^{N}	Nothing
Discussion	Non-Conflict PC Membership	Nothing
Decision	Non-Conflict PC Membership	Last Edited Version
	Non-Conflict PC Membership or PC Membership^{N} or Paper Authorship^{N}	Nothing
Reviewer Assignment to Paper	Non-Conflict PC Membership^{R}	Non-Conflict PC Membership of Reviewers and Number of Reviewers
	Non-Conflict PC Membership^{R} or Paper Authorship^{N}	Non-Conflict PC Membership of Reviewers

Phase Stamps: B = Bidding, D = Discussion, N = Notification, R = Review

Source	Declassification Trigger	Declassification Bound
Paper Content	Paper Authorship	Last Uploaded Version
	Paper Authorship or PC Membership^{B}	Nothing
Review	Review Authorship	Last Edited Version Before Discussion and All the Later Versions
	Review Authorship or Non-Conflict PC Membership^{D}	Last Edited Version Before Notification
	Review Authorship or Non-Conflict PC Membership^{D} or PC Membership^{N} or Paper Authorship^{N}	Nothing
Discussion	Non-Conflict PC Membership	Nothing
Decision	Non-Conflict PC Membership	Last Edited Version
	Non-Conflict PC Membership or PC Membership^{N} or Paper Authorship^{N}	Nothing
Reviewer Assignment to Paper	Non-Conflict PC Membership^{R}	Non-Conflict PC Membership of Reviewers and Number of Reviewers
	Non-Conflict PC Membership^{R} or Paper Authorship^{N}	Non-Conflict PC Membership of Reviewers

Phase Stamps: B = Bidding, D = Discussion, N = Notification, R = Review

Source	Declassification Trigger	Declassification Bound
Paper Content	Paper Authorship	Last Uploaded Version
	Paper Authorship or PC Membership[B]	Nothing
Review	Review Authorship	Last Edited Version Before Discussion and All the Later Versions
	Review Authorship or Non-Conflict PC Membership[D]	Last Edited Version Before Notification
	Review Authorship or Non-Conflict PC Membership[D] or PC Membership[N] or Paper Authorship[N]	Nothing
Discussion	Non-Conflict PC Membership	Nothing
Decision	Non-Conflict PC Membership	Last Edited Version
	Non-Conflict PC Membership or PC Membership[N] or Paper Authorship[N]	Nothing
Reviewer Assignment to Paper	Non-Conflict PC Membership[R]	Non-Conflict PC Membership of Reviewers and Number of Reviewers
	Non-Conflict PC Membership[R] or Paper Authorship[N]	Non-Conflict PC Membership of Reviewers

Phase Stamps: B = Bidding, D = Discussion, N = Notification, R = Review

Bounded-Deducibility Security

List(Event)

List(Val)

List(Obs)

Bounded-Deducibility Security

φ : Event $\rightarrow$ Bool $\qquad$ f : Event $\rightarrow$ Val

V = "filter with φ, then apply f, event-wise"

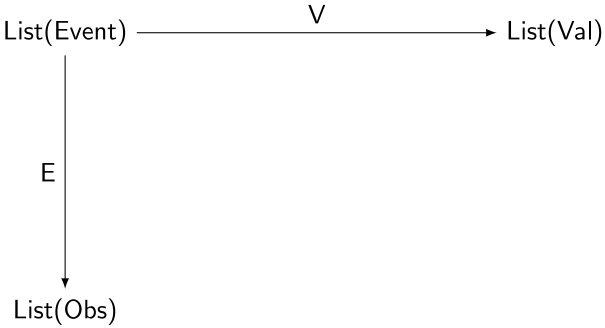
$$\text{List(Event)} \xrightarrow{\quad\quad\quad\quad\text{V}\quad\quad\quad\quad} \text{List(Val)}$$

List(Obs)

Bounded-Deducibility Security

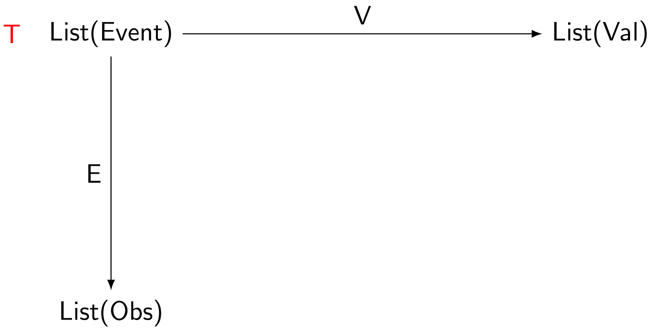
γ : Event $\rightarrow$ Bool $\qquad g$: Event $\rightarrow$ Obs

E = "filter with γ, then apply g, event-wise"



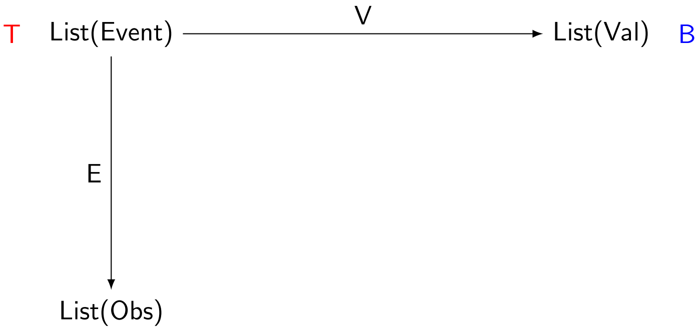
Bounded-Deducibility Security

T : Event → Bool



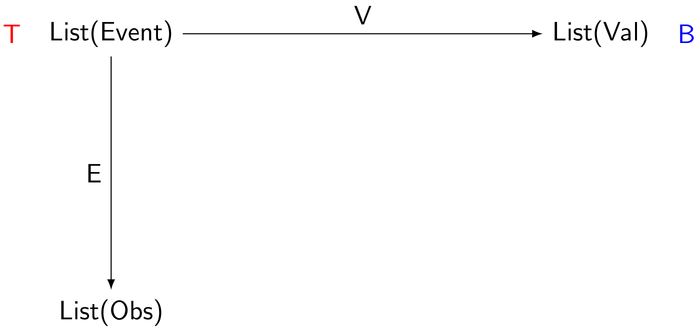
Bounded-Deducibility Security

T : Event → Bool   B relation on List(Val)



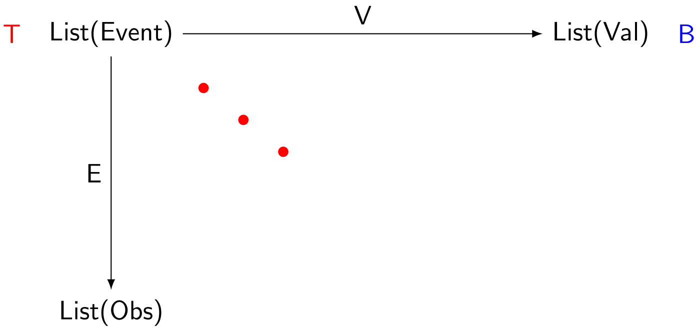
Bounded-Deducibility Security

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



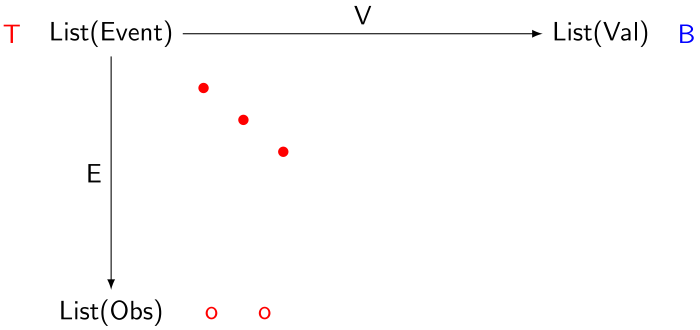
Bounded-Deducibility Security

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



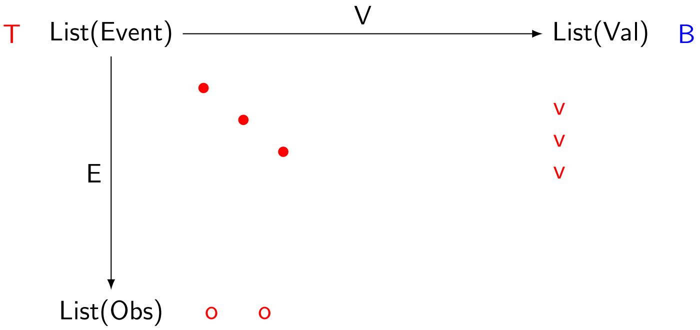
Bounded-Deducibility Security

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



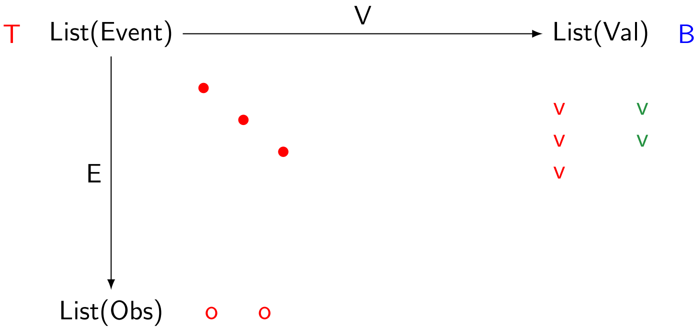
Bounded-Deducibility Security

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



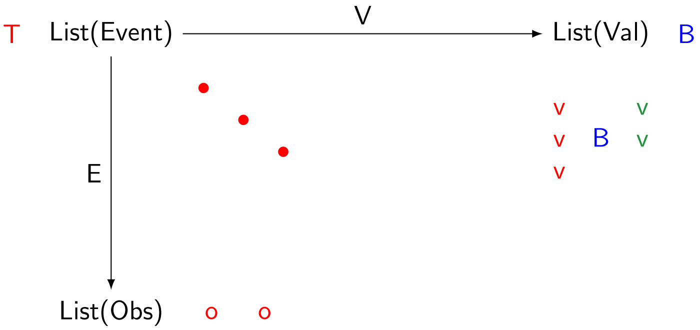
Bounded-Deducibility Security

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



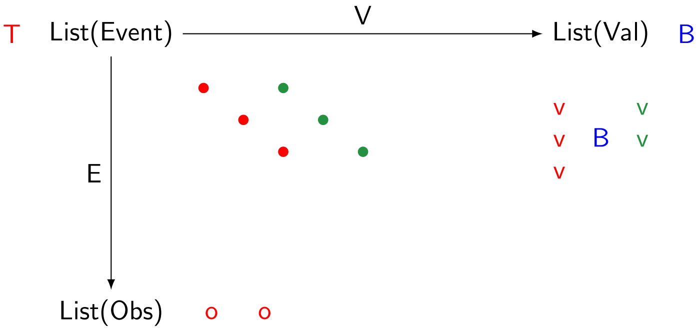
Bounded-Deducibility Security

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



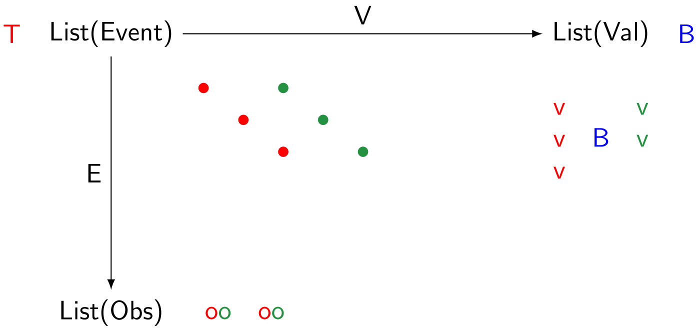
Bounded-Deducibility Security

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



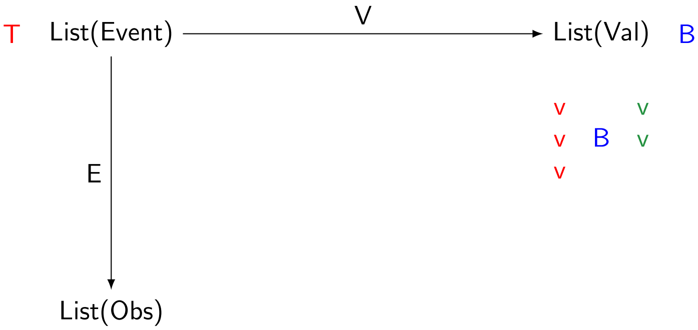
Bounded-Deducibility Security

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



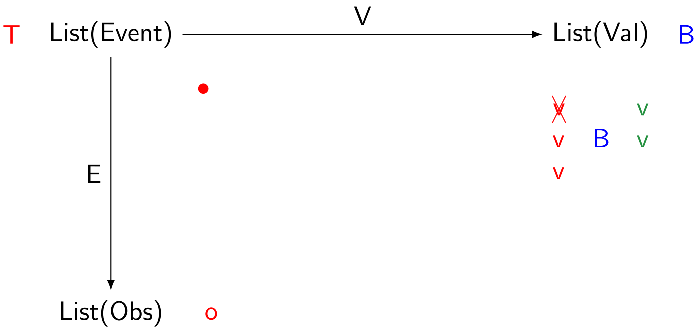
Bounded-Deducibility Security

Proof by unwinding



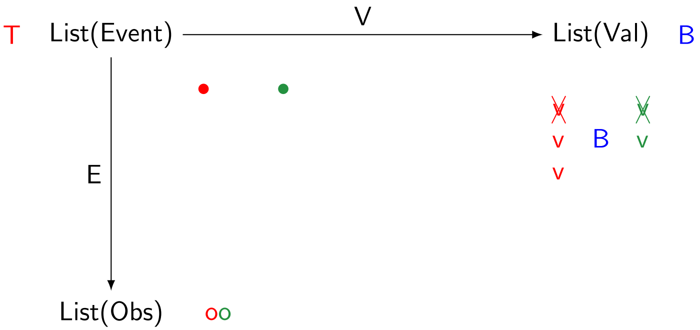
Bounded-Deducibility Security

Proof by unwinding
Action



Bounded-Deducibility Security

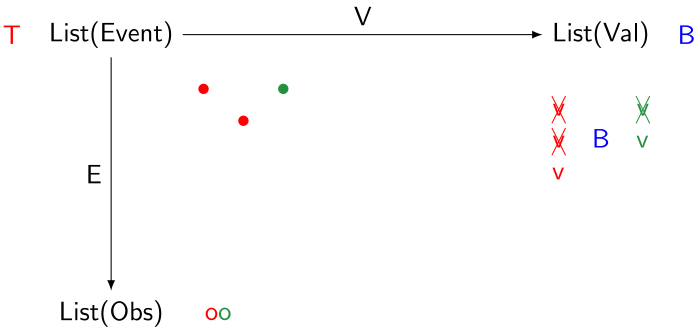
Proof by unwinding
Action / Reaction: Match



Bounded-Deducibility Security

Proof by unwinding

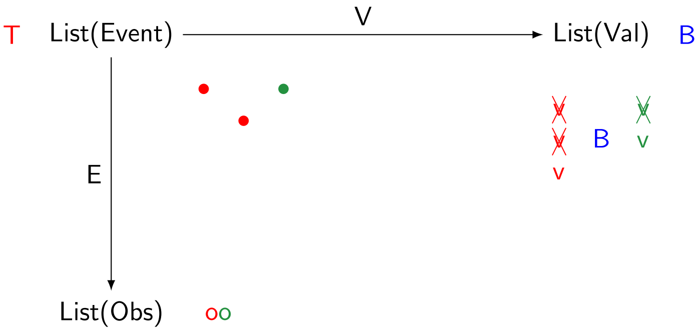
Action



Bounded-Deducibility Security

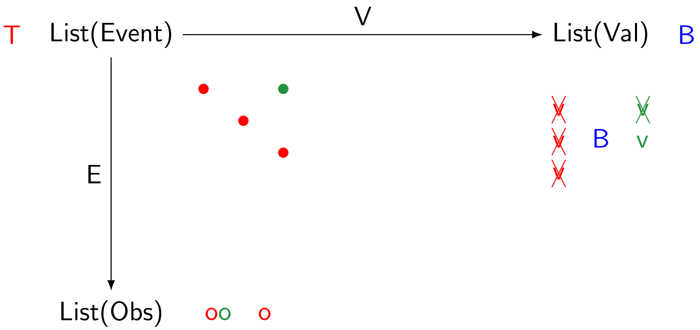
Proof by unwinding

Action / Reaction: Ignore



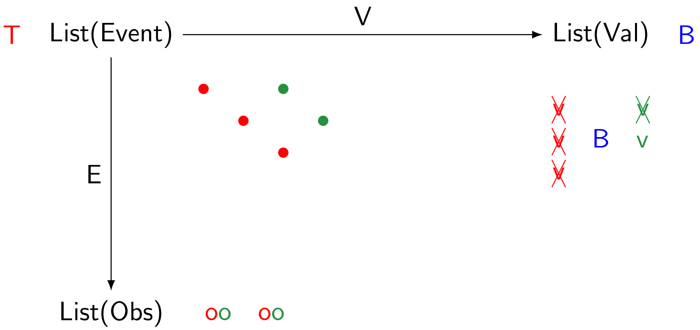
Bounded-Deducibility Security

Proof by unwinding
Action



Bounded-Deducibility Security

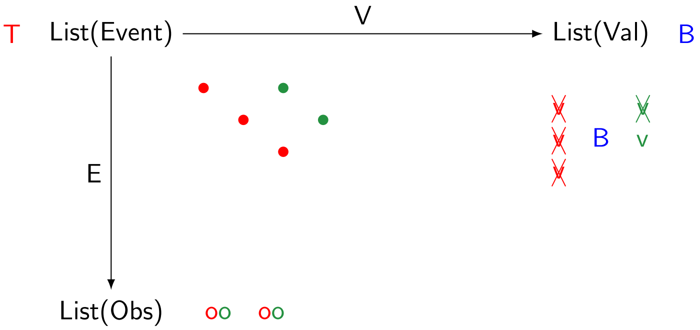
Proof by unwinding
Action / Reaction: Match



Bounded-Deducibility Security

Proof by unwinding

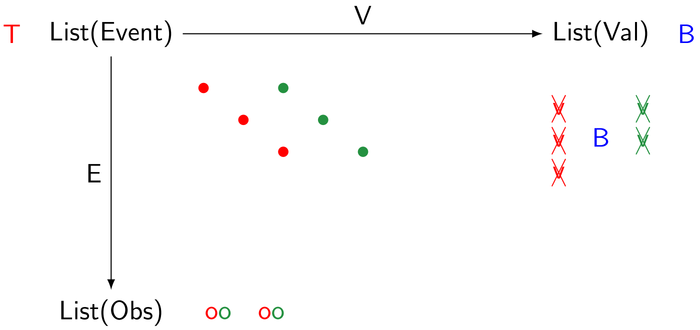
Independent action ...



Bounded-Deducibility Security

Proof by unwinding

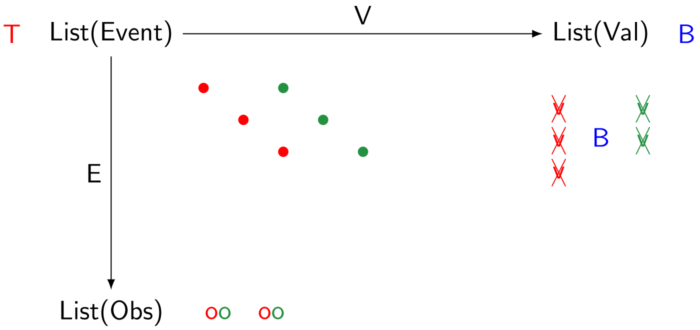
Independent action



Bounded-Deducibility Security

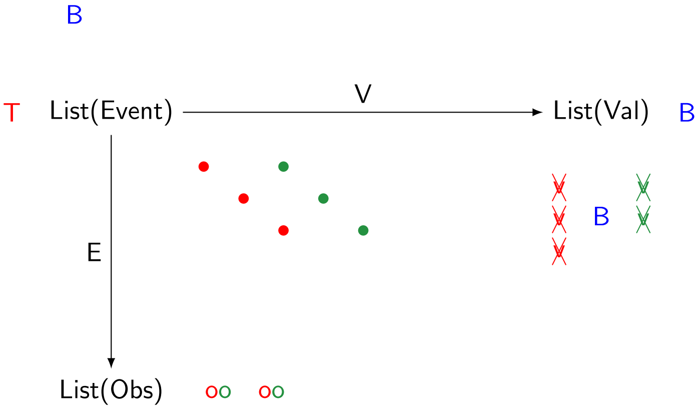
Proof by unwinding ✓

Independent action



Bounded-Deducibility Security

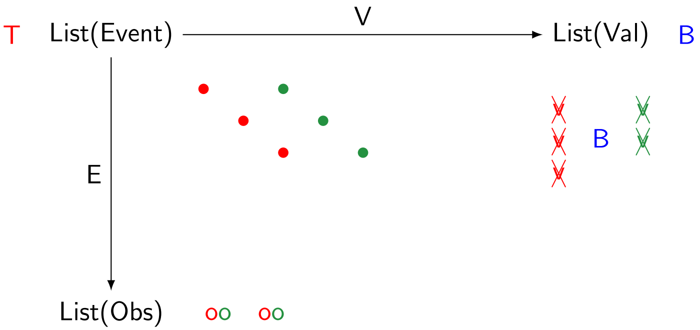
Proof by unwinding ✓



Bounded-Deducibility Security

Proof by unwinding ✓

$B \mapsto \Delta \subseteq \text{State} \times \text{List(Val)} \times \text{State} \times \text{List(Val)}$



Proof by Unwinding

Proof by Unwinding

$$\Delta \subseteq \mathsf{State} \times \mathsf{List}(\mathsf{Val}) \times \mathsf{State} \times \mathsf{List}(\mathsf{Val})$$

Proof by Unwinding

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

$+$

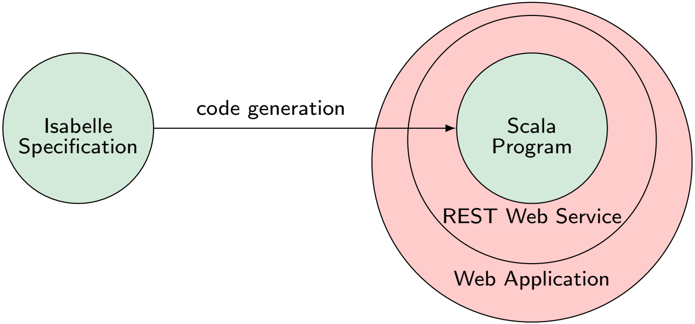
Strategy for:

- 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



Related Work

Theoretical frameworks

- **Sutherland 1986: Nondeducibility**
- Mantel 2000: MAKS framework
- Halpern and ONeill, 2008: Secrecy in multiagent systems
- Dimitrova et. al. 2012, Clarkson et. al 2014: Temporal Logics for Information Flow

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`