A Security Protocol Animator Tool for AVISPA

Yann Glouche¹ Thomas Genet¹

¹IRISA-INRIA, Rennes, France Team LANDE

Artist2 Security Workshop, 18th May 2006





A Security Protocol Animator Tool for AVISPA

2 The protocol animator

3 Experiments



Yann Glouche, Thomas Genet

A Security Protocol Animator Tool for AVISPA

2 The protocol animator

3 Experiments



A Security Protocol Animator Tool for AVISPA

Yann Glouche, Thomas Genet

2 The protocol animator





A Security Protocol Animator Tool for AVISPA

Yann Glouche, Thomas Genet





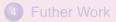


A Security Protocol Animator Tool for AVISPA



2 The protocol animator

3 Experiments



Yann Glouche, Thomas Genet

A Security Protocol Animator Tool for AVISPA

Experiments

Futher Work

The Need for a protocol animator in the AVISPA System

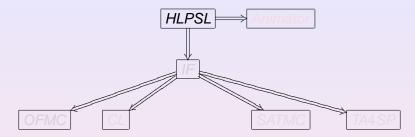
Avispa project

- AVISPA is a verification tool for cryptographic protocols.
- High Level Protocol Specification Language (HLPSL).
- Ability to use different techniques on the same protocol specification.

Experiments

Futher Work

The Need for a protocol animator in the AVISPA System

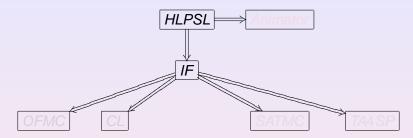


- On-the-Fly Model-Checker (OFMC)
- Constraint-Logic-based model-checker (CL)
- SAT-based Model-Checker (SATMC)
- Tree Automata Automatic Approximations for the Analysis of Security Protocol (TA4SP)

Experiments

Futher Work

The Need for a protocol animator in the AVISPA System

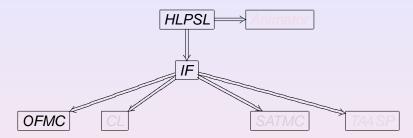


- On-the-Fly Model-Checker (OFMC)
- Constraint-Logic-based model-checker (CL)
- SAT-based Model-Checker (SATMC)
- Tree Automata Automatic Approximations for the Analysis of Security Protocol (TA4SP)

Experiments

Futher Work

The Need for a protocol animator in the AVISPA System

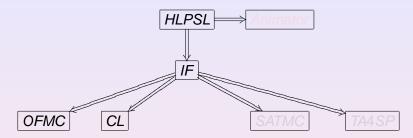


- On-the-Fly Model-Checker (OFMC)
- Constraint-Logic-based model-checker (CL)
- SAT-based Model-Checker (SATMC)
- Tree Automata Automatic Approximations for the Analysis of Security Protocol (TA4SP)

Experiments

Futher Work

The Need for a protocol animator in the AVISPA System

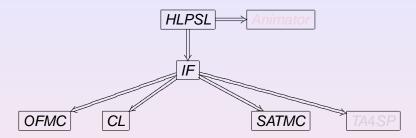


- On-the-Fly Model-Checker (OFMC)
- Constraint-Logic-based model-checker (CL)
- SAT-based Model-Checker (SATMC)
- Tree Automata Automatic Approximations for the Analysis of Security Protocol (TA4SP)

Experiments

Futher Work

The Need for a protocol animator in the AVISPA System

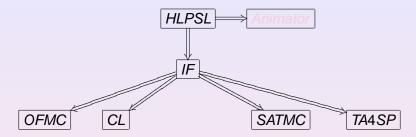


- On-the-Fly Model-Checker (OFMC)
- Constraint-Logic-based model-checker (CL)
- SAT-based Model-Checker (SATMC)
- Tree Automata Automatic Approximations for the Analysis of Security Protocol (TA4SP)

Experiments

Futher Work

The Need for a protocol animator in the AVISPA System

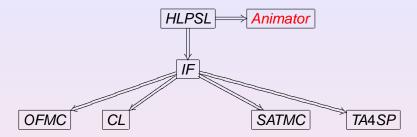


- On-the-Fly Model-Checker (OFMC)
- Constraint-Logic-based model-checker (CL)
- SAT-based Model-Checker (SATMC)
- Tree Automata Automatic Approximations for the Analysis of Security Protocol (TA4SP)

Experiments

Futher Work

The Need for a protocol animator in the AVISPA System



- On-the-Fly Model-Checker (OFMC)
- Constraint-Logic-based model-checker (CL)
- SAT-based Model-Checker (SATMC)
- Tree Automata Automatic Approximations for the Analysis of Security Protocol (TA4SP)

Experiments

Futher Work

The Need for a protocol animator in the AVISPA System

```
role a(...)
 State=0 \land RCV(start)
  = > State':=1 \wedge Na':=new()
       \land SND({Na'.A}_Kb)
 State=1 ∧ RCV(Na.Nb'_Ka)
  = > State':=2
        \land SND({Nb'}_Kb)
role b(...)
 State=0 \land RCV({Na'.A'}_Kb)
  = > State':=1 \wedge Nb':=new()
       \land SND({Na'.Nb}_Ka)
  State=1 \land RCV({Nb}_Kb)
  = > State':=2
```

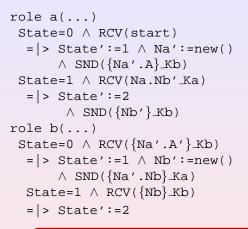
 $\begin{array}{l} A \rightarrow B : \{\textit{Na}, \textit{A}\}_{\textit{Kb}} \\ A \rightarrow B : \{\textit{Na}, \textit{Nb}\}_{\textit{Ka}} \\ A \rightarrow B : \{\textit{Nb}\}_{\textit{Kb}} \end{array}$

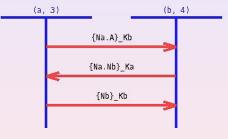
イロト イヨト イヨト イヨト

Experiments _____

Futher Work

The Need for a protocol animator in the AVISPA System





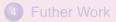
< ロ > < 団 > < 豆 > < 豆 >

The Need for a protocol animator

• \Rightarrow produce interactively MSC from an HLPSL specification.

2 The protocol animator

3 Experiments



Yann Glouche, Thomas Genet

・ロト ・日 ・ ・ ヨ ・ ・

A Security Protocol Animator Tool for AVISPA

Protocol specification

Protocol specifications in HLPSL are divided into roles.

Example (Protocol specification)

```
P Roles declaration
role a(A : agent...)
State=0 ^ RCV(start)
=|> State':=1 ^ Na':=new() ^ SND({Na'.A}_Kb)
State=1 ^ RCV(Na.Nb'.Ka) =|> State':=2 ^ SND({Nb'}_Kb)
role b(B : agent...)
State=0 ^ RCV({Na'.A'}_Kb)
=|> State':=1 ^ Nb':=new() ^ SND({Na'.Nb}_Ka)
State=1 ^ RCV({Nb}_Kb) =|> State':=2
```

role one_session(A, B : agent...) composition $a(A...) \land b(B...)$

Scenario declaration

one_session(alice, bob...)Aone_session(charlie, dane...

Protocol specification

Protocol specifications in HLPSL are divided into roles.

Example (Protocol specification)

```
• Roles declaration
role a(A : agent...)
State=0 ^ RCV(start)
=|> State':=1 ^ Na':=new() ^ SND({Na'.A}_Kb)
State=1 ^ RCV(Na.Nb'_Ka) =|> State':=2 ^ SND({Nb'}_Kb)
role b(B : agent...)
State=0 ^ RCV({Na'.A'}_Kb)
=|> State':=1 ^ Nb':=new() ^ SND({Na'.Nb}_Ka)
State=1 ^ RCV({Nb}_Kb) =|> State':=2
```

Scenario declaration

one_session(alice, bob...)Aone_session(charlie, dane...)

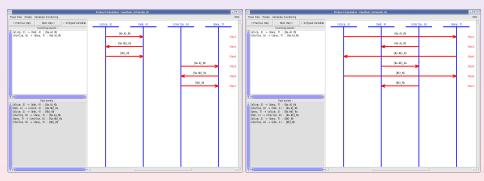
Futher Work

The protocol animator

V		Protocol Simulation : nee	dhare_Schreeder.tst		- 11
Trace Files Hodes Variables monitoring					HSC
C Provious stag Next stag 2	Untyped variables	(alice, 3)	(565, 4)	(charitie, 6)	(dany, 7)
Incoming events :					
$\begin{array}{c} \Delta (\operatorname{line}_{\mathcal{A}}, 3) \rightarrow (\operatorname{line}_{\mathcal{A}}, 4) \rightarrow (\operatorname{line}_{\mathcal{A}}, 3) \rightarrow (\operatorname{line}_{A$	×				

A Security Protocol Animator Tool for AVISPA

(日)



크

The features of current version

- Full support of HLPSL
- Interactive construction of MSC guided by the user because of
 - non deterministic protocols
 - choices in interleaved sessions
- usual undo/redo in constructed MSCs
- MSCs import/export

A Security Protocol Animator Tool for AVISPA

Yann Glouche, Thomas Genet

() < </p>

The features of current version

- Full support of HLPSL
- Interactive construction of MSC guided by the user because of
 - non deterministic protocols
 - choices in interleaved sessions
- usual undo/redo in constructed MSCs
- MSCs import/export

A Security Protocol Animator Tool for AVISPA



A B > A B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A

The features of current version

- Full support of HLPSL
- Interactive construction of MSC guided by the user because of
 - non deterministic protocols
 - choices in interleaved sessions
- usual undo/redo in constructed MSCs
- MSCs import/export

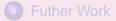
The features of current version

- Full support of HLPSL
- Interactive construction of MSC guided by the user because of
 - non deterministic protocols
 - choices in interleaved sessions
- usual undo/redo in constructed MSCs
- MSCs import/export

Image: Image:

2 The protocol animator





A Security Protocol Animator Tool for AVISPA

Yann Glouche, Thomas Genet

・ロト ・日下・ ・ ヨト・

We have applied the animator to several protocols

- all the protocols of the AVISPA Library
- a new protocol developped by Thomson called User Supervised Device Pairing (USDP) for pairing two devices

A Security Protocol Animator Tool for AVISPA

(日)

We have applied the animator to several protocols

- all the protocols of the AVISPA Library
- a new protocol developped by Thomson called User Supervised Device Pairing (USDP) for pairing two devices



Image: A matrix

We have applied the animator to several protocols

- all the protocols of the AVISPA Library
- a new protocol developped by Thomson called User Supervised Device Pairing (USDP) for pairing two devices



Image: Image:

We have applied the animator to several protocols

- all the protocols of the AVISPA Library
- a new protocol developped by Thomson called User Supervised Device Pairing (USDP) for pairing two devices



A B > A B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A
 B > A

Futher Work

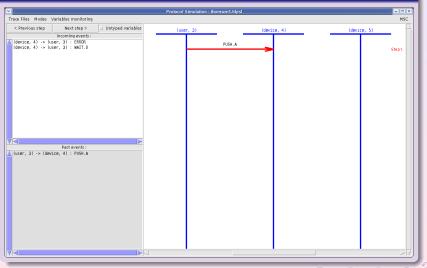
Experiments

An execution trace of Thomson's USDP protocol

	Protocol Simulation : thomson5.h	ilpsl		- D X
Trace Files Modes Variables monitoring				MSC
< Previous step Next step > Untyped variables	(user, 3)	(device, 4)	(device, 5)	X
Incoming events :				
(luser, 3) → Idevice, 4) : PISH.A				
7⊲	1			
Past events :				

Experiments

An execution trace of Thomson's USDP protocol



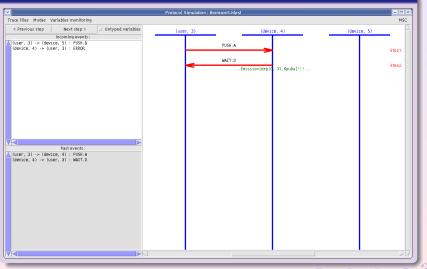
A Security Protocol Animator Tool for AVISPA

Yann Glouche, Thomas Genet

Futher Work

Experiments

An execution trace of Thomson's USDP protocol

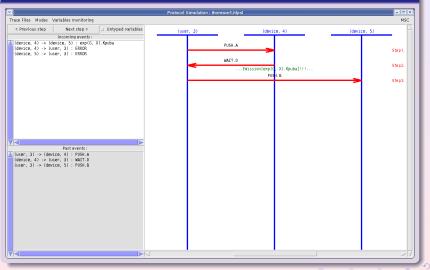


A Security Protocol Animator Tool for AVISPA

Futher Work

Experiments

An execution trace of Thomson's USDP protocol



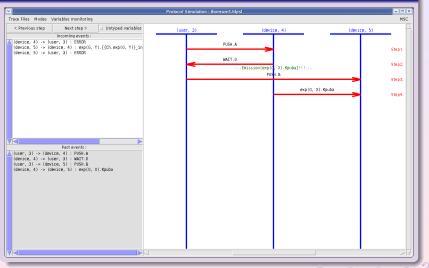
A Security Protocol Animator Tool for AVISPA

Yann Glouche, Thomas Genet

Futher Work

Experiments

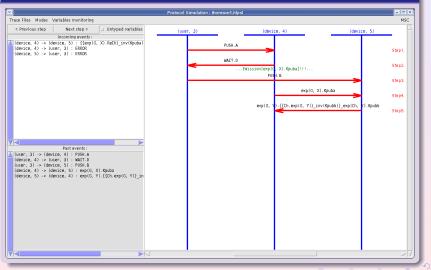
An execution trace of Thomson's USDP protocol



Futher Work

Experiments

An execution trace of Thomson's USDP protocol



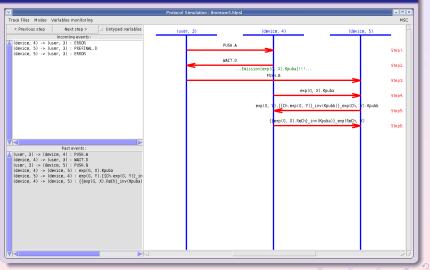
A Security Protocol Animator Tool for AVISPA

Yann Glouche, Thomas Genet

Futher Work

Experiments

An execution trace of Thomson's USDP protocol

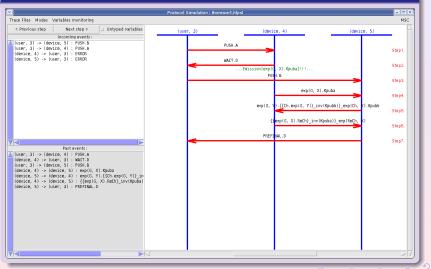


A Security Protocol Animator Tool for AVISPA

Futher Work

Experiments

An execution trace of Thomson's USDP protocol



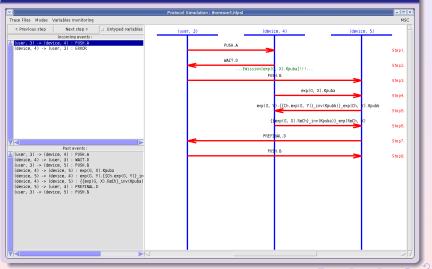
A Security Protocol Animator Tool for AVISPA

Yann Glouche, Thomas Genet

Futher Work

Experiments

An execution trace of Thomson's USDP protocol

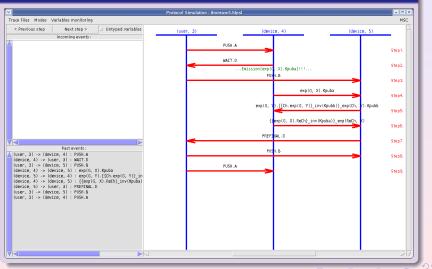


A Security Protocol Animator Tool for AVISPA

Futher Work

Experiments

An execution trace of Thomson's USDP protocol



A Security Protocol Animator Tool for AVISPA

Yann Glouche, Thomas Genet

2 The protocol animator

3 Experiments



A Security Protocol Animator Tool for AVISPA

Yann Glouche, Thomas Genet

・ロト ・日 ・ ・ ヨ ・ ・

Futher Work

A correct treatment of mathematical functions

• This is not yet fully functional when messages include *exp*, *xor*.

Integration of a mode to replay interactively the attacks

• Execute an intruder role who receive, replay, and treat all messages sent by an agent.

Futher Work

A correct treatment of mathematical functions

• This is not yet fully functional when messages include *exp*, *xor*.

Integration of a mode to replay interactively the attacks

 Execute an intruder role who receive, replay, and treat all messages sent by an agent.

A Security Protocol Animator Tool for AVISPA

Yann Glouche, Thomas Genet

= 990

・ロト ・ 四ト ・ ヨト ・ ヨト