SATMC: SAT-based Model-Checking of Security Protocols

Roberto Carbone

Security&Trust, CIT_irst, Bruno Kessler Foundation, Trento, Italy

joint work with
Alessandro Armando, Luca Compagna, Luca Zanetti

Tool session of FOSAD 2013

Bertinoro, September 4, 2013

Outline

Model checkers specifically tailored for security protocols have been remarkably successful in spotting flaws in protocols.

They rely on a number of simplifying assumptions:

Dolev-Yao (DY) Channels: controlled by an intruder, capable to overhear, divert, and fake messages.

Honest Principals (HP): required to react to messages of a specified form only.

Security Goals (SG): reachability properties.

Ok for simple protocols, but they prevent (or greatly complicate) the analysis of important real world protocols.

Model checkers specifically tailored for security protocols have been remarkably successful in spotting flaws in protocols.

They rely on a number of simplifying assumptions:

Dolev-Yao (DY) Channels: controlled by an intruder, capable to overhear, divert, and fake messages.

Honest Principals (HP): required to react to messages of a specified form only.

Security Goals (SG): reachability properties.

Ok for simple protocols, but they prevent (or greatly complicate) the analysis of important real world protocols.

Problems with the Common Assumptions

(DY) DY channels are not appropriate to model the behaviour of an attacker in

- **over-the-air protocols** (message interception unfeasible)
- **contract-signing protocols** (confidential, resilient channels)
- **browser-based protocols** (SSL/TLS channels)

(HP) Some protocols assume "non standard" behaviour of honest principals:

- **contract-signing protocols** (participants required to make progress)
- **browser-based protocols** (HTTP-redirect).

(SG) Some security goals cannot be (easily) expressed as reachability properties, e.g. fair exchange.

This Talk

1. Approach to security protocol analysis based on model checking of LTL formulae.
2. The approach does not rely on **(DY)**, **(HP)**, and **(SG)**.
3. Implementation in SATMC, a state of the art SAT-based Model Checker for security protocols.
4. Demo
5. Results: Effectiveness assessed against a number of real world protocols - Severe flaws found

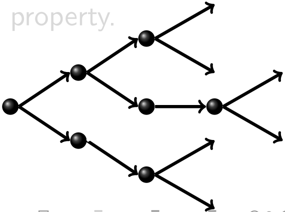
Outline

$$\overbrace{M}^{\text{model}} \models \overbrace{((C_I \wedge C_H) \Rightarrow G)}^{\text{LTL formula}}$$

- M: transition system modelling a superset of the behaviours of the honest agents and of the intruder.
- C_I: LTL formula constraining the behaviours of the intruder.
- C_H: LTL formula constraining the behaviours of honest principals.
- G: LTL formula encoding the expected security property.

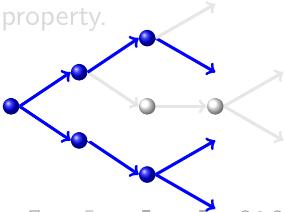
$$\overbrace{M}^{\text{model}} \models \overbrace{((C_I \wedge C_H) \Rightarrow G)}^{\text{LTL formula}}$$

- M: transition system modelling a superset of the behaviours of the honest agents and of the intruder.
- C_I: LTL formula constraining the behaviours of the intruder.
- C_H: LTL formula constraining the behaviours of honest principals.
- G: LTL formula encoding the expected security property.



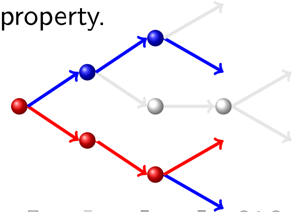
$$\overbrace{M}^{\text{model}} \models \overbrace{((C_I \wedge C_H) \Rightarrow G)}^{\text{LTL formula}}$$

- M: transition system modelling a superset of the behaviours of the honest agents and of the intruder.
- C_I: LTL formula constraining the behaviours of the intruder.
- C_H: LTL formula constraining the behaviours of honest principals.
- G: LTL formula encoding the expected security property.



$$\overbrace{M}^{\text{model}} \models \overbrace{((C_I \wedge C_H) \Rightarrow G)}^{\text{LTL formula}}$$

- M: transition system modelling a superset of the behaviours of the honest agents and of the intruder.
- C_I: LTL formula constraining the behaviours of the intruder.
- C_H: LTL formula constraining the behaviours of honest principals.
- G: LTL formula encoding the expected security property.



The Model

$$M \models (C_I \wedge C_H) \Rightarrow G$$

Transition system associated with the concurrent execution of a number of sessions of the protocol.

- **States:** sets of facts, i.e. ground atomic formulae
- **Transitions:** rewrite rules define mappings between sets of facts.

The Model: Facts

Fact	Meaning
$\mathtt{state}_{Role}(j, a, es, s)$	Principal a, playing role *Role*, is ready to execute step j in session s of the protocol.
$\mathtt{ak}(a, m)$	Principal a knows message m.
$\mathtt{sent}(rs, b, a, m, c)$	Principal rs has sent message m on channel c to principal a pretending to be principal b.
$\mathtt{rcvd}(a, b, m, c)$	Message m (supposedly sent by principal b) has been received on channel c by principal a

Note: $\mathtt{ik}(m)$ abbreviates $\mathtt{ak}(\mathrm{i}, m)$.

Example (State):

$$\mathtt{state}_{Init}(2, \mathrm{a}, [\mathrm{ka}, \mathrm{ka}^{-1}, \mathrm{kb}, \mathrm{na}], 1)\,.\,\mathtt{sent}(\mathrm{a}, \mathrm{a}, \mathrm{i}, \{\langle \mathrm{a}, \mathrm{na}\rangle\}_{\mathtt{ki}}, \mathrm{c})$$
$$.\,\mathtt{state}_{Resp}(1, \mathrm{b}, [\mathrm{kb}, \mathrm{kb}^{-1}, \mathrm{ka}], 1)\,.\,\mathtt{ik}(\mathrm{ka})\,.\,\mathtt{ik}(\mathrm{kb})$$

The Model: Rules for the Honest Agents

Message Delivery

$$\mathtt{\textbf{sent}}(\mathtt{RS}, \mathtt{B}, \mathtt{A}, \mathtt{M}, \mathtt{C}) \xrightarrow{\mathtt{receive}(\mathtt{A,B,RS,M,C})} \mathtt{\textbf{rcvd}}(\mathtt{A}, \mathtt{B}, \mathtt{M}, \mathtt{C}).\mathtt{\textbf{ak}}(\mathtt{A}, \mathtt{M})$$

Message Processing

$$\mathtt{\textbf{rcvd}}(\mathtt{A}, \mathtt{B}, \mathtt{M}, \mathtt{C}).\mathtt{\textbf{state}}_{Role}(j, \mathtt{A}, es, \mathtt{S}) \xrightarrow{\mathtt{send}_j(\mathtt{A,B,B1,\ldots,S})} \mathtt{\textbf{sent}}(\mathtt{A}, \mathtt{A}, \mathtt{B1}, \mathtt{M1}, \mathtt{C1}).\mathtt{\textbf{state}}_{Role}(l, \mathtt{A}, es', \mathtt{S})$$

The Model: Rules for the Intruder

Interception

$$\texttt{sent}(A, A, B, M, C) \xrightarrow{\texttt{intercept}(A,B,M,C)} \texttt{rcvd}(i, A, M, C).\texttt{ik}(M)$$

Overhearing

$$\texttt{sent}(A, A, B, M, C) \xrightarrow{\texttt{overhear}(A,B,M,C)} \texttt{sent}(A, A, B, M, C).\texttt{rcvd}(i, A, M, C).\texttt{ik}(M)$$

Faking

$$\texttt{ik}(M).\texttt{ik}(A).\texttt{ik}(B) \xrightarrow{\texttt{fake}(A,B,M,C)} \texttt{sent}(i, A, B, M, C).\texttt{ik}(M).\texttt{ik}(A).\texttt{ik}(B)$$

The Model: Inferential Capabilities of the Agents

$$\mathtt{ak}(\mathtt{A},\mathtt{M}) \,.\, \mathtt{ak}(\mathtt{A},\mathtt{K}) \xrightarrow{\mathtt{encrypt}(\mathtt{A},\mathtt{K},\mathtt{M})} \mathtt{ak}(\mathtt{A},\mathtt{M}) \,.\, \mathtt{ak}(\mathtt{A},\mathtt{K}) \,.\, \mathtt{ak}(\mathtt{A},\{\mathtt{M}\}_{\mathtt{K}})$$

$$\mathtt{ak}(\mathtt{A},\{\mathtt{M}\}_{\mathtt{K}}) \,.\, \mathtt{ak}(\mathtt{A},\mathtt{K}^{-1}) \xrightarrow{\mathtt{decrypt\_puk}(\mathtt{A},\mathtt{K},\mathtt{M})} \mathtt{ak}(\mathtt{A},\{\mathtt{M}\}_{\mathtt{K}}) \,.\, \mathtt{ak}(\mathtt{A},\mathtt{K}^{-1}) \,.\, \mathtt{ak}(\mathtt{A},\mathtt{M})$$

$$\mathtt{ak}(\mathtt{A},\{\mathtt{M}\}_{\mathtt{K}^{-1}}) \,.\, \mathtt{ak}(\mathtt{A},\mathtt{K}) \xrightarrow{\mathtt{decrypt\_prk}(\mathtt{A},\mathtt{K},\mathtt{M})} \mathtt{ak}(\mathtt{A},\{\mathtt{M}\}_{\mathtt{K}^{-1}}) \,.\, \mathtt{ak}(\mathtt{A},\mathtt{K}) \,.\, \mathtt{ak}(\mathtt{A},\mathtt{M})$$

$$\mathtt{ak}(\mathtt{A},\mathtt{M}_1) \,.\, \mathtt{ak}(\mathtt{A},\mathtt{M}_2) \xrightarrow{\mathtt{pairing}(\mathtt{A},\mathtt{M}_1,\mathtt{M}_2)} \mathtt{ak}(\mathtt{A},\mathtt{M}_1) \,.\, \mathtt{ak}(\mathtt{A},\mathtt{M}_2) \,.\, \mathtt{ak}(\mathtt{A},\langle \mathtt{M}_1,\mathtt{M}_2\rangle)$$

$$\mathtt{ak}(\mathtt{A},\langle \mathtt{M}_1,\mathtt{M}_2\rangle) \xrightarrow{\mathtt{decompose}(\mathtt{A},\mathtt{M}_1,\mathtt{M}_2)} \mathtt{ak}(\mathtt{A},\langle \mathtt{M}_1,\mathtt{M}_2\rangle) \,.\, \mathtt{ak}(\mathtt{A},\mathtt{M}_1) \,.\, \mathtt{ak}(\mathtt{A},\mathtt{M}_2)$$

$$M \models (C_I \wedge C_H) \Rightarrow G$$

Confidential Channel

A *channel ch is confidential to principal p* iff its **output** is exclusively accessible to a given receiver p:

$$\mathit{confidential}(ch, p) := \mathbf{G}\,\forall(\mathtt{rcvd}(A, B, M, ch) \Rightarrow A = p)$$

Resilient Channel

Any message will be eventually delivered to the intended recipient.

$$\mathit{resilient}(ch) := \mathbf{G}\,\forall(\mathtt{sent}(RS, A, B, M, Ch) \Rightarrow \mathbf{F}\,\mathtt{rcvd}(B, A, M, Ch))$$

- Capital letters denote variables.
- $\forall(\alpha)$ abbreviates the universal closure of α.
- Quantifiers are over finite domains (bounded analysis).

$$M \models (C_I \wedge C_H) \Rightarrow G$$

Principal *a* should not indefinitely wait for an answer

$$\mathbf{G}\,\forall(\mathtt{state}_R(j, a, \ldots) \Rightarrow \mathbf{F}\,\neg\mathtt{state}_R(j, a, \ldots))$$

Received messages will be eventually processed by principal *a*

$$\mathbf{G}\,\forall(\mathtt{rcvd}(a, P, M, C) \Rightarrow \mathbf{F}\,\neg\,\mathtt{rcvd}(a, P, M, C))$$

Specifying Security Properties

$$M \models (C_I \wedge C_H) \Rightarrow G$$

Authentication

b authenticates a on m in session s iff

$$authentication(b, a, m, s) :=$$
$$\mathbf{G}\,\forall(\mathtt{state}_{r_b}(final\_step, b, [a, \ldots, m, \ldots], s) \Rightarrow$$
$$\exists\,\mathbf{O}\,\mathtt{state}_{r_a}(initial\_step, a, [b, \ldots, m, \ldots], s))$$

Fair Exchange

"A principal cannot obtain a valid contract without allowing the remaining principal to also obtain a valid contract."

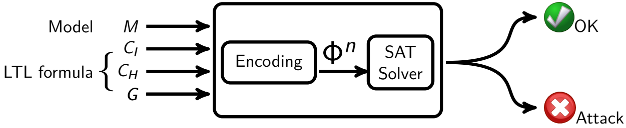
$$\mathbf{G}\,\forall(\mathtt{ak}(a, contract) \Rightarrow \mathbf{F}\,\mathtt{ak}(b, contract))$$

Outline

- SATMC reduces the security problem to propositional satisfiability problems (SAT).
- **Why SAT?**
  Dramatic speed-up of SAT solvers: problems with thousands of variables are now solved routinely in milliseconds.

- SATMC reduces the security problem to propositional satisfiability problems (SAT).
- **Why SAT?**
  Dramatic speed-up of SAT solvers: problems with thousands of variables are now solved routinely in milliseconds.

Encoding to SAT

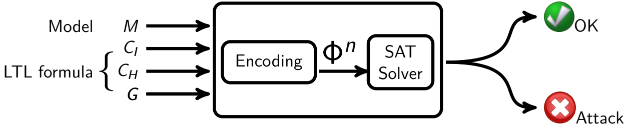


$$\Phi^n = I(p_0) \wedge \bigwedge_{i=0}^{n-1} T_i(p_i, \lambda_i, p_{i+1}) \wedge GC(p_0, \ldots, p_n)$$

Additional time-index parameter to each rule λ or fact p

Successful combination of

- SAT-reduction techniques developed for AI-planning
- Bounded model-checking techniques for reactive systems



$$\Phi^n = I(p_0) \wedge \bigwedge_{i=0}^{n-1} T_i(p_i, \lambda_i, p_{i+1}) \wedge GC(p_0, \ldots, p_n)$$

Additional time-index parameter to each rule λ or fact p

Successful combination of

- SAT-reduction techniques developed for AI-planning
- Bounded model-checking techniques for reactive systems

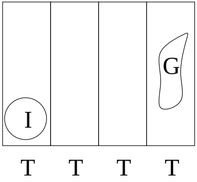
Over-approximation of the reachable states

- **Idea:** Use knowledge about the initial state to simplify the T_k's.
- **Approach:** Propagate information provided by the initial state for building an over-approximation of the forward search tree.

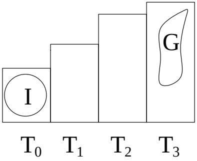
Over-approximation of the reachable states

- **Idea:** Use knowledge about the initial state to simplify the T_k's.
- **Approach:** Propagate information provided by the initial state for building an over-approximation of the forward search tree.

Linear Encoding



Graphplan-based encoding [2,3]



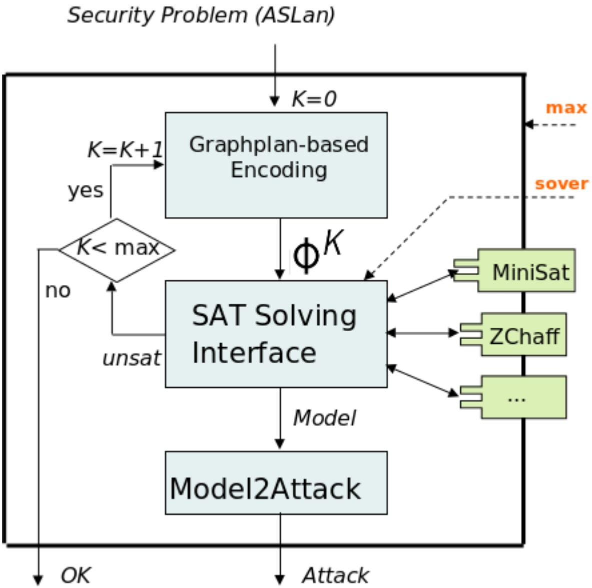
[1] H. Kautz, H. McAllester, and B. Selman. *Encoding Plans in Propositional Logic* (*KR'96*)
[2] A. Blum, and M. Furst. *Fast Planning through Planning Graph Analysis* (*IJCAI'95*)
[3] H. Kautz, and B. Selman. *Unifying SAT-based and Graph-based Planning* (*IJCAI'99*)

SAT-base model-checking for security Protocols

- Pros
  - leverages the speed-up of SAT solvers
  - Expressivity: LTL improves the scope of model checking for security protocols
- Cons
  - sometimes paid in terms of efficiency

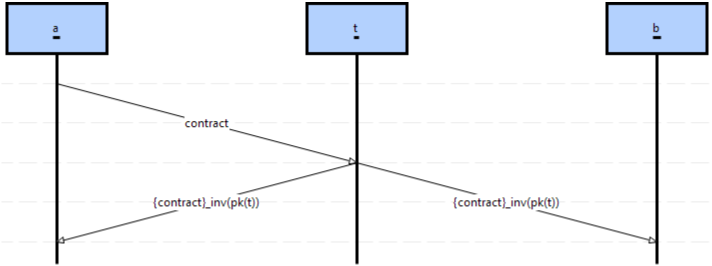
Outline

Implementation: Architecture



Outline

Demo: Toy Example



Outline

Usage

SATMC is used in several research prototypes and industrial tools:

- Back-end of the AVISPA Tool and AVANTSSAR Platform and the back-end of the forthcoming SPaCIoS Tool.
- Integrated in a SAP tool used to analyze SAP NetWeaver SAML Next Generation SSO.
- Used as an automated testcase generator in Tookan, a tool for analysing PKCS#11 security tokens

Some Results

- **Contract Signing protocols**
  - Optimistic Fair Exchange Protocol by Asokan, Shoup, and Waidner
  - Flaw detected in a version of the protocol "patched" by Mitchell & Shmatikov

A. Armando, R. Carbone and L. Compagna. **LTL Model Checking for Security Protocols**. In the proceedings of the 20th IEEE Computer Security Foundations Symposium (CSF20)

- **Strong authentication protocols**
  - user's credentials + other proofs of identity
  - serious vulnerabilities in protocols for two-factor and two-channel authentication for web applications.
  - an attacker can carry out a security-sensitive operation by using only one of the two authentication factors.

- **Contract Signing protocols**
  - Optimistic Fair Exchange Protocol by Asokan, Shoup, and Waidner
  - Flaw detected in a version of the protocol “patched” by Mitchell & Shmatikov

A. Armando, R. Carbone and L. Compagna. **LTL Model Checking for Security Protocols**. In the proceedings of the 20th IEEE Computer Security Foundations Symposium (CSF20)

- **Strong authentication protocols**
  - user's credentials + other proofs of identity
  - serious vulnerabilities in protocols for two-factor and two-channel authentication for web applications.
  - an attacker can carry out a security-sensitive operation by using only one of the two authentication factors.

A. Armando, R. Carbone and L. Zanetti. **Formal Modeling and Automatic Security Analysis of Two-Factor and Two-Channel Authentication Protocols**. In the proceedings of the International Conference on Network and System Security (NSS 2013). June, 2013.

- Flaw detected in Google's SAML-based SSO for Google Apps
- Authentication flaw in the most common use-case scenario of SAML 2.0 SSO Profile.
  (Errata by OASIS Security Services Technical Committee.)
- Cross-Site Scripting (XSS) vulnerabilities detected in:
  - SAML-based SSO for Google Apps
  - SimpleSAMLphp
  - Novell Access Manager v3.1

Browser-based Secu

sstc-saml-approved-errata-2.0.pdf (application/pdf Object) - Mozill

sstc-saml-approved-errata-2.0...

docs.oasis-open.org/security/saml/v2.0/sstc-saml

39 / 44 164%

OASIS

SAML Version 2.0 Errata 05

OASIS Approved Errata

01 May 2012

If no NameFormat v format:unspecified (see Section 8.2.1 of [SAMLCore]) is in effect.

E90: RelayState sanitization

Security analysis of SAML implementations in [Sec2011] suggests that guidance is needed to advise implementers how to avoid enabling a class of attacks involving misuse of the RelayState feature supported by SAML bindings. The TC thanks the following for their identification of the problem, and their assistance in drafting this material:

- Alessandro Armando, University of Genova and Fondazione Bruno Kessler
- Roberto Carbone, Fondazione Bruno Kessler
- Luca Compagna, SAP
- Jorge Cuellar, Siemens
- Giancarlo Pellegrino, SAP
- Alessandro Sorniotti, IBM
- The EU Projects AVANTSSAR, SPaCIoS, and SIAM

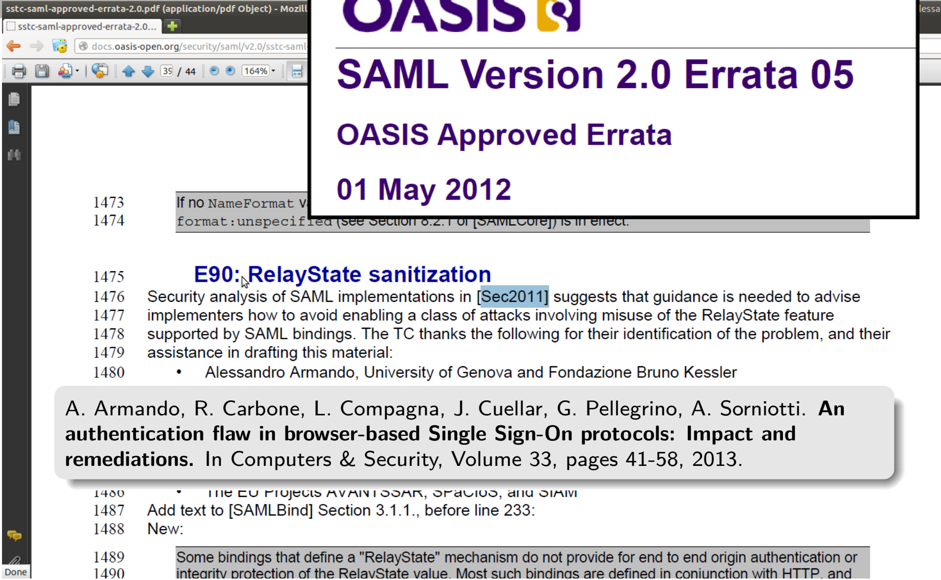
Add text to [SAMLBind] Section 3.1.1., before line 233:

New:

Some bindings that define a "RelayState" mechanism do not provide for end to end origin authentication or integrity protection of the RelayState value. Most such bindings are defined in conjunction with HTTP, and

Done

Browser-based Secu



OASIS

SAML Version 2.0 Errata 05

OASIS Approved Errata

01 May 2012

If no NameFormat v
format:unspecified (see Section 8.2.1 of [SAMLCore]) is in effect.

E90: RelayState sanitization

Security analysis of SAML implementations in [Sec2011] suggests that guidance is needed to advise implementers how to avoid enabling a class of attacks involving misuse of the RelayState feature supported by SAML bindings. The TC thanks the following for their identification of the problem, and their assistance in drafting this material:

- Alessandro Armando, University of Genova and Fondazione Bruno Kessler

A. Armando, R. Carbone, L. Compagna, J. Cuellar, G. Pellegrino, A. Sorniotti. **An authentication flaw in browser-based Single Sign-On protocols: Impact and remediations.** In Computers & Security, Volume 33, pages 41-58, 2013.

- The EU Projects AVANTSSAR, SPaCIoS, and SIAM

Add text to [SAMLBind] Section 3.1.1., before line 233:

New:

Some bindings that define a "RelayState" mechanism do not provide for end to end origin authentication or integrity protection of the RelayState value. Most such bindings are defined in conjunction with HTTP, and

Outline

Conclusions

- We have presented a general framework for security protocols based on model checking of LTL formulae allowing for the specification of:
  - assumptions on principals and channels
  - complex security properties

  that are normally not handled by state-of-the-art analysers.
- SATMC: SAT-based Model Checking of Security Protocols
- **It works!** Vulnerabilities detected on a number of important protocols:
  ASW, SAML 2.0 SSO Profile, Google's SAML-based SSO for Google Apps, Novell Access Manager, Strong Authentication protocols, . . .

Conclusions

- We have presented a general framework for security protocols based on model checking of LTL formulae allowing for the specification of:
  - assumptions on principals and channels
  - complex security properties

  that are normally not handled by state-of-the-art analysers.
- SATMC: SAT-based Model Checking of Security Protocols
- **It works!** Vulnerabilities detected on a number of important protocols:
  ASW, SAML 2.0 SSO Profile, Google's SAML-based SSO for Google Apps, Novell Access Manager, Strong Authentication protocols, ...

Conclusions

- We have presented a general framework for security protocols based on model checking of LTL formulae allowing for the specification of:
  - assumptions on principals and channels
  - complex security properties

  that are normally not handled by state-of-the-art analysers.
- SATMC: SAT-based Model Checking of Security Protocols
- **It works!** Vulnerabilities detected on a number of important protocols:
  ASW, SAML 2.0 SSO Profile, Google's SAML-based SSO for Google Apps, Novell Access Manager, Strong Authentication protocols, . . .

Thank you!

Acknowledgements:
This work was partially supported by

- SPaCIoS
  "Secure Provision and Consumption in the Internet of Services".
- SIAM
  "Automated Security Analysis of Identity and Access Management"