# Automatic Analysis of Security Protocols

#### Roberto Carbone

http://st.fbk.eu

Security & Trust Research Unit

Center for Information Technologies

Bruno Kessler Foundation





Sac

< 同 > < 三 >

# **Motivations**

- Security protocols and services are key to securing the ever-growing ecosystem of online applications (web, mobile, ...)
- But security solutions are notoriously difficult to get right. Many security-critical protocols and services have been designed and developed only to be found flawed years after their deployment.
- Due to the complex and unexpected interleaving of the protocols and services as well as to the possible interference of malicious agents.
- Very difficult to spot by traditional verification techniques (e.g., manual inspection and testing)
- Security-critical systems are a natural target for formal method techniques.

イロト イロト イヨト イヨト

# **Motivations**

- Security protocols and services are key to securing the ever-growing ecosystem of online applications (web, mobile, ...)
- But security solutions are notoriously difficult to get right. Many security-critical protocols and services have been designed and developed only to be found flawed years after their deployment.
- Due to the complex and unexpected interleaving of the protocols and services as well as to the possible interference of malicious agents.
- Very difficult to spot by traditional verification techniques (e.g., manual inspection and testing)
- Security-critical systems are a natural target for formal method techniques.

イロト イロト イヨト イヨト

#### Security-critical browser-based applications

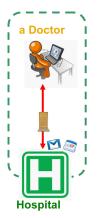
- 2 SATMC: a Bounded Model Checker for Security Protocols
- An Attack on the SAML-based SSO for Google Apps
- An Authentication Flaw in SAML SSO

#### 5 Conclusion

Sac

・ 同 ト ・ ヨ ト ・ ヨ

- Identity management ⇒ SAML-based Single Sign On



Sac

< 🗇 🕨

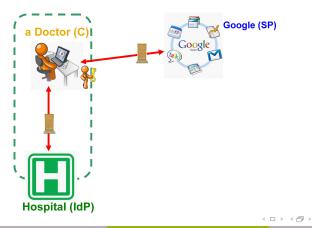
- Identity management ⇒ SAML-based Single Sign On



Sac

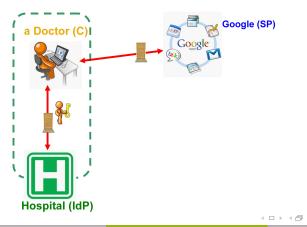
< 🗇 🕨

- Hospital outsources basic IT services ⇒ *Google Apps*
- Identity management ⇒ SAML-based Single Sign On



Sac

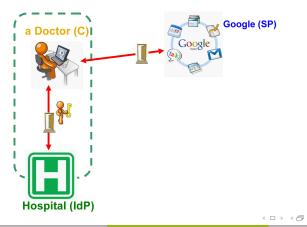
- Hospital outsources basic IT services ⇒ *Google Apps*
- Identity management ⇒ SAML-based Single Sign On



**H** 5

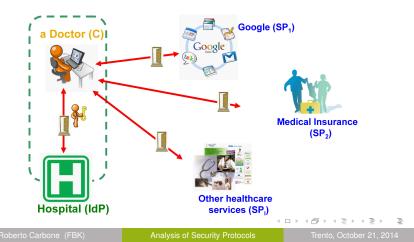
Sac

- Hospital outsources basic IT services ⇒ *Google Apps*
- Identity management ⇒ SAML-based Single Sign On

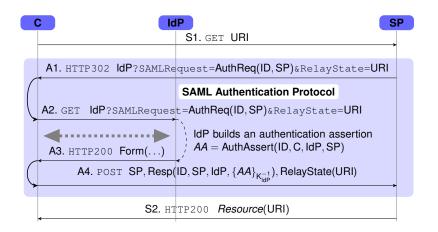


Sac

- Hospital outsources basic IT services ⇒ *Google Apps*
- Identity management ⇒ SAML-based Single Sign On

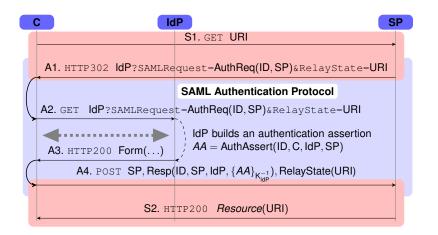


Sar



Sac

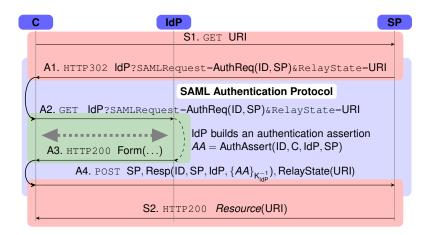
\* 伊ト \* ヨト \* ヨト



#### Assumption on Transport Protocols (TP1)

# Communication between C and SP is carried over a unilateral SSL/TLS channel.

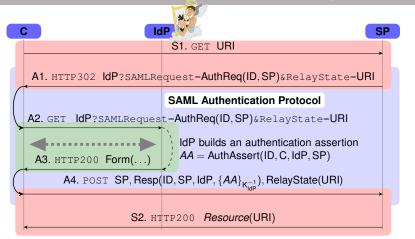
Roberto Carbone (FBK



#### Assumption on Transport Protocols (TP2)

# Communication between C and IdP is carried over a unilateral SSL/TLS channel that becomes bilateral once C authenticates on IdP.

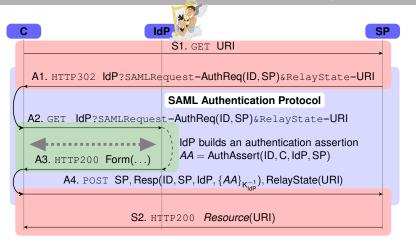
Roberto Carbone (FBK)



#### Trust Assumption (TA1)

IdP is not compromised, i.e. it is not under the control of an intruder and it abides by the rules of the protocol.

Roberto Carbone (FBK



#### Trust Assumption (TA2)

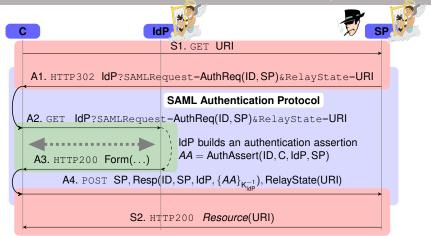
IdP is trusted by SP to generate authentication assertions about C.

Roberto Carbone (FBK)

Analysis of Security Protocols

Trento, October 21, 2014 5 / 2

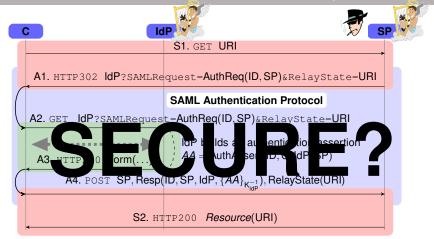
Sac



Important

We do not assume that all SPs whom C may play the protocol with are uncompromised.

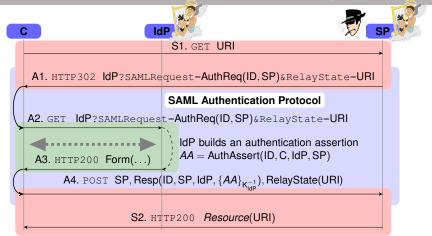
Roberto Carbone (FBK)



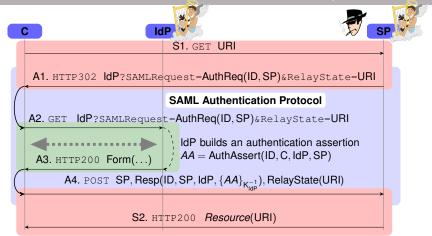
Trento, October 21, 2014 5 / 28

Sac

< ロ ト < 同 ト < 三 ト < 三 ト







# Security Goal (SAML Authentication Prococol) SP authenticates C

Roberto Carbone (FBK)

Analysis of Security Protocols

rento, October 21, 2014 5 /

nan



#### SATMC: a Bounded Model Checker for Security Protocols

#### An Attack on the SAML-based SSO for Google Apps

#### An Authentication Flaw in SAML SSO

#### 5 Conclusion

Sac

・ 同 ト ・ ヨ ト ・ ヨ

# SATMC: a Bounded Model Checker for Security Protocols

SATMC tackles problems of the form:



where

- P: transition system modeling honest participants.
- *I*: transition system modeling DY intruder.
- C: LTL formula constraining the behaviours of DY intruder on the communication channels.
- G: LTL formula encoding the expected security properties.
- Successful combination of
  - SAT-reduction techniques developed for AI-planning
  - Bounded model-checking techniques developed for reactive systems.

A. Armando, R. Carbone, L. Compagna. "SATMC: a SAT-based Model Checker for Security-critical Systems", In Proc. 20th international Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'14), 2014.

Roberto Carbone (FBK)

Analysis of Security Protocols

nar





#### An Attack on the SAML-based SSO for Google Apps

An Authentication Flaw in SAML SSO

#### 5 Conclusion

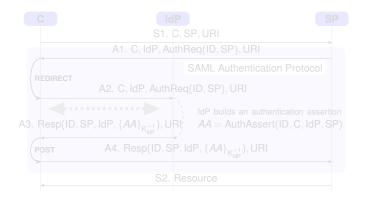
Sac

A B + A B + A B
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A

# The "SAML-based" SSO for Google Apps

Same as the SAML 2.0 Web Browser SSO Profile except for seemingly minor simplifications:

• ID and SP are not included in the authentication assertion.



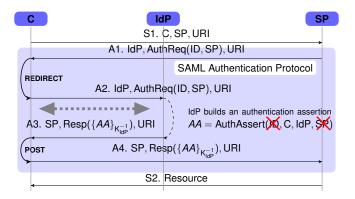
Sac

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

# The "SAML-based" SSO for Google Apps

Same as the SAML 2.0 Web Browser SSO Profile except for seemingly minor simplifications:

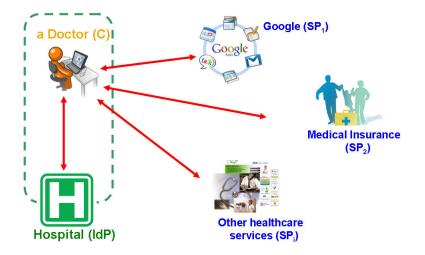
• ID and SP are not included in the authentication assertion.



Roberto Carbone (FBK)

A The local

#### Use Case Analysis

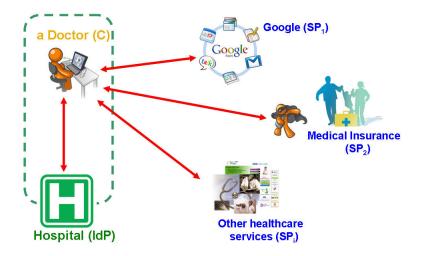


Э

990

< ロ > < 団 > < 豆 > < 豆 >

#### Use Case Analysis



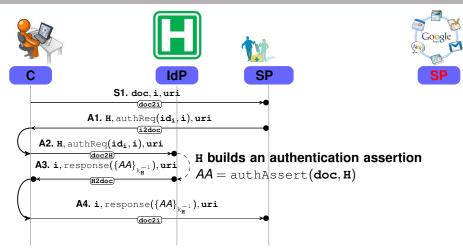
Trento, October 21, 2014 10 /

Э

990

<ロト < 回ト < 回ト < 回ト

# Attack on the SAML-based SSO for Google Apps



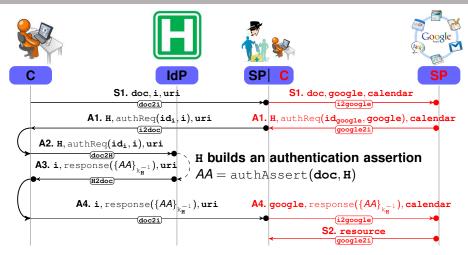
Roberto Carbone (FBK)

Analysis of Security Protocols

Trento October 21, 2014, 11 /

Sac

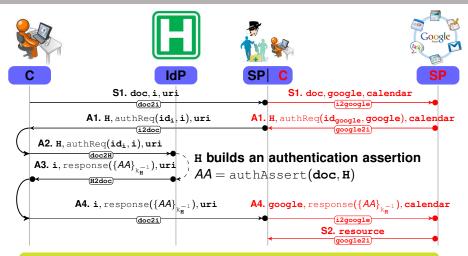
# Attack on the SAML-based SSO for Google Apps



Sac

・ ロ ト ・ 同 ト ・ 三 ト ・

# Attack on the SAML-based SSO for Google Apps



A. Armando, R. Carbone, L. Compagna, J. Cuéllar and L. Tobarra. Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-based Single Sign-On for Google Apps. In the Proceedings of the 6th ACM Workshop on Formal Methods in Security Engineering (FMSE 2008), 2008, Virginia, USA.

Roberto Carbone (FBK

Analysis of Security Protocols

) ९ (२ | / 28



2 SATMC: a Bounded Model Checker for Security Protocols

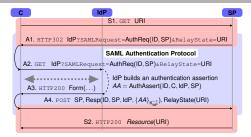
#### An Attack on the SAML-based SSO for Google Apps

#### An Authentication Flaw in SAML SSO

#### 5 Conclusion

Sac

・ 同 ト ・ ヨ ト ・ ヨ



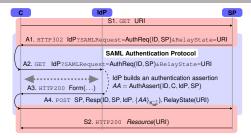
#### Assumption on Transport Protocols (TP1)

Communication between C and SP is carried over a unilateral SSL/TLS channel.

Roberto Carbone (FBK)

Trento, October 21, 2014 13 / 28

イロト イポト イヨト イヨト



#### Assumption on Transport Protocols (TP1)

Communication between C and SP is carried over a unilateral SSL/TLS channel.

But the standard does not specify whether the messages at steps S1 and A4 must be transported over the same SSL/TLS channel.

Roberto Carbone (FBK

Analysis of Security Protocols

T I O I I OI OOI I .

・ 同 ト ・ ヨ ト ・ ヨ

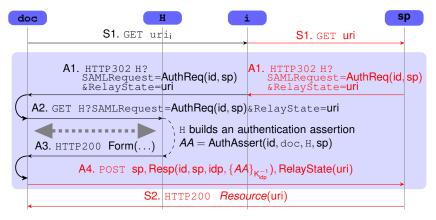
3/28

Reuse of the SSL/TLS channel apparently the most natural option, but difficult to achieve:

- Resuming SSL/TLS sessions.
  - the underlying TCP connection might be terminated,
  - an SSL server could not resume a previous session, or
  - the browser may very renegotiates the SSL session.
- **Software modularity.** The SW module that handles SAML messages may not have access to info of SSL/TLS.
- **Distributed SPs.** The SAML SP may be distributed over multiple machines, e.g., for work-balancing reasons.

イロト イポト イヨト イヨト

When run against the revised model, SATMC found the following attack:



Roberto Carbone (FBK)

Sac

イロト イポト イヨト イヨト



- 1484 Giancarlo Pellegrino, SAP
- 1485 Alessandro Sorniotti, IBM
- The EU Projects AVANTSSAR, SPaCloS, and SIAM
- 1487 Add text to [SAMLBind] Section 3.1.1., before line 233:
- 1488 New:

1489 Some bindings that define a "RelayState" mechanism do not provide for end to end origin authentication or 1490 integrity protection of the RelayState value. Most such bindings are defined in conjunction with HTTP, and

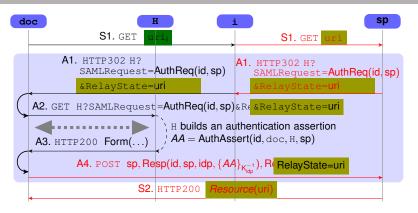


- 1400 THE EU FIUJEUS AVAINTOGAN, OFACIUS, ANU OIAIVI
- 1487 Add text to [SAMLBind] Section 3.1.1., before line 233:
- 1488 New:

1489 Some bindings that define a "RelayState" mechanism do not provide for end to end origin authentication or 1490 integrity protection of the RelayState value. Most such bindings are defined in conjunction with HTTP, and

イロト イポト イヨト イヨト

### Exploiting the Vulnerability



#### Delivery of unrequested resource

Force C to receive a different resource from that initially requested.

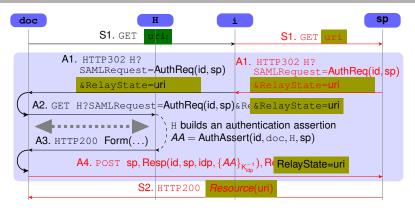
		(FBK)

Trento, October 21, 2014 17 /

Sac

<ロト < 回ト < 回ト < 回ト

### Exploiting the Vulnerability



### Launching pad for XSRF

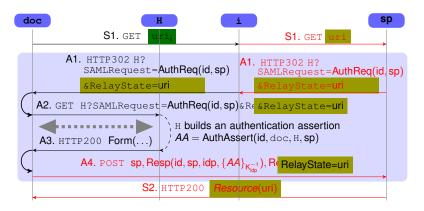
URI contains a URL-encoded command (e.g. a request to change of some settings).

Even more pernicious than classic XSRF, because XSRF requires C to have an active session with SP, which is not the case here.

Roberto Carbone (FBK)

Analysis of Security Protocols

### Exploiting the Vulnerability



### Launching pad for XSS

RelayState exposed to injection of malicious code. Although the standard recommends to protect the integrity of this field, this often is not the case.

Roberto Carbone (FBK)

Analysis of Security Protocols

Trento, October 21, 2014

イロト イポト イヨト イヨト

うへへ 17/28

### Impact of the vulnerability on the Google Apps

Our analysis of the SAML-based SSO for Google Apps showed that:



- RelayState was not sanitized and SAML SSO served as a launching pad for XSS.
- A malicious SP could force C to consume a resource from Google, for instance, visiting any page of the gmail service.
- A malicious SP could steal the cookies for the Google domain through XSS and could impersonate C on any Google application.

< ロ ト < 同 ト < 三 ト < 三 ト

### Impact of the vulnerability on simpleSAMLphp



- The SimpleSAMLphp stores the initially requested URI into the URL parameter ReturnTo.
- Although this field is not sanitized, no XSS could be mounted.
- The SP running SimpleSAMLphp use cookies that block the exploitation.

Sac

< ロ ト < 同 ト < 三 ト < 三 ト

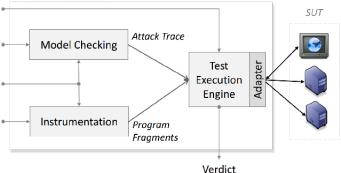
## Impact of the vulnerability on Novell Access Manager

- URI not associated with the RelayState field as mandated by the standard, but passed as URL-encoded parameter which was not sanitized by the SP.
- XSS attack was possible.

Novell.	Access Cateway Cateway
(L) GIT FIS	sting RES is never adeque sanisted, and can contai malicious code producin
	(f)
(2) 302 https://LAG/LAGBoke/tr+PATH6*SP/RES*	
(3) CET LACBroker's +PATHB'SP (FES'	<b>→</b>
(4) 302 https://UAG/nesp/app/ploginite+PKTHB*UAG/UAGBokw?*SP/RES**; SerCookie(IPC)	
(5) GET /LAG/hesp/app/plogin7c+FRTH81LAG/LAGBolau/197/RES11, Cockie/PC)	<b>_</b>
Authenrication Protocol	
(6) 200 FORMtarpet +LAC/LACBroker?SR/VES',LAREQ + < <spreadauthreq>&gt;3; SetCookie()</spreadauthreq>	
(7)/R051 /nidp/idff/sso target=LAG/LAGRokerTSF/RES*, LAREQ=< <signedauthreq>&gt;; Cookie(IPC)</signedauthreq>	*
. (8) 200 SetCookie() csoriet=top.window.location.hef ="[AC/LACBooke/"97183"]	string "LAC/LACBroker"SP/VES*** De could coreain malicious code. XSS #TEXCk II occurring here.
(9) CET / Inida / Idff / Iso2hd - Securit Com LIRAsid = OBcoston - credenta idioid = O Cocket/PC,	where of "LAC/LACBoher" "PyRES" should be samitized!
. (15) 200 FORMtanaet+LAG/LAGBoker/197 FES/, Scorn , User , ID, Scorn , Pastword 1	•
· · · · · · · · · · · · · · · · · · ·	
(11)POST /nidp/idff/sso target -LAG/LAGBoker?9P/RES', Ecom, User, ID +, Ecom, Password +; Cookie(PC,	►
(12) 200 top.location.html+'ssoftid+0'	-
(13) GET /nidp/sidW/ssoPoid+8; Cookie(PC,)	*
(14) 302 https://LAG/nesp/idff/spassertion_consume/SAMLart+&RelayState+MA++	-
(15) GET /nesp/idff/spasserion_consume/SAHLart+&feleyState=MA++; CookielPC,)	<b>}</b>
_ (16) 302 https://LAG/LAGBekw/TSP/RES*	
(17) /LAGBoker/SPIRES: CookielPC)	
. (18) 302 https://59/865 -GPC+	
(13) GIT RIS -CIPS	
(20) 802 HSI: SerContietPC =)	•
	cookie can be set to an arbitrary b value if string "\$9,985" ends
	with "-CPC" Cockle poisoning is possible. "99 RSS" should be sanitized
(22) (67 R8; Cooker(PC)	

# From Model Checking to Automated Security Testcase Generation and Execution

## SPaCI®S



Rober	to Carbo	ne (FBK)

Trento October 21 2014 21 /

Sar

・ 同 ト ・ ヨ ト ・ ヨ ト

### Ongoing Work...

	Carbon	

Trento, October 21, 2014 22 / 28

900

E

< □ > < □ > < □ > < □ > < □ >

## Security Threat Identification and Testing (STIATE)

EIT ICT Labs Activity 2014



- Goal: Bring the results of research projects to the market!
  - The STIATE Toolkit: an industrial strength API for model checking and automated testcase generation and execution (FBK) and front-end (SAP)
  - Methodology and guidance document for using the STIATE technology as part of Common Criteria developments. (DFKI)
  - Industry migration through application to uses cases of industrial complexity. (SAP, Reply)
  - Market solution toolkit to be market ready with consistent go to market strategy (Reply)

<ロト < 回ト < 回ト < 回ト

### Another Use Case for STIATE...



- Secure Call Authorization (SCA) is a commercial solution for multi-factor and two-channel authentication developed by AliasLab S.p.A.
  - user's mobile phone (second factor)
  - GSM/3G communication infrastructure (second channel)
- **Goal:** Formal Analysis of *SCA* using the STIATE Toolkit.

Sac

## Automatic Analysis of Browser-based Security Protocols



- Topic V, supervisors:
  R. Carbone and L. Compagna (SAP)
- The attacks described cannot be detected by the state-of-the-art penetration testing tools.
- Goal: Extend penetration testing tools!
- "Issue" of previous approaches: generation of the model

**Question:** Is it possible to detect the previous attacks without even specifying the model of the protocol?



イロト イポト イヨト イヨト

## Automatic Analysis of Browser-based Security Protocols



- Topic V, supervisors:
  R. Carbone and L. Compagna (SAP)
- The attacks described cannot be detected by the state-of-the-art penetration testing tools.
- Goal: Extend penetration testing tools!
- "Issue" of previous approaches: generation of the model

**Question:** Is it possible to detect the previous attacks without even specifying the model of the protocol?



イロト イポト イヨト イヨト

Automatic Analysis of Browser-based Security Protocols SECENTIS

- Topic V, supervisors: R. Carbone and L. Compagna (SAP)
- The attacks described cannot be detected by the state-of-the-art penetration testing tools.
- Goal: Extend penetration testing tools!
- Issue of previous approaches: generation of the model

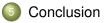
Question: Is it possible to detect the previous attacks without even specifying the model of the protocol? Answer: Avinash talk !

・ 同 ト ・ ヨ ト ・ ヨ ト





- 2 SATMC: a Bounded Model Checker for Security Protocols
- An Attack on the SAML-based SSO for Google Apps
- An Authentication Flaw in SAML SSO



Sac

・ 同下 ・ ヨト ・ ヨ

- Security protocols play pivotal role e.g. in web applications (SAML SSO, OpenID, OAuth, ...)
- Formal modeling and automatic analysis of security protocols can help unveil serious flaws and get the model right
- 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, ...
- Ongoing Work: Annibale (STIATE), Federico (AliasLab), Avinash (SECENTIS)

イロト 不同 ト イヨト イヨト

### Thank you!

Robert		

Trento, October 21, 2014 28 / 28

E

900

< □ > < □ > < □ > < □ > < □ >