

LICS 2023 Test-of-Time Award

An NP Decision Procedure for Protocol Insecurity with Xor

Yannick Chevalier, Ralf Küsters, Mathieu Turuani, Michaël
Rusinowitch

Intruder Deductions, Constraint Solving and Insecurity Decision in Presence of Exclusive Or

Hubert Comon-Lundh, Vitaly Shmatikov

Domain of Research: Security Protocols

Il Sole 24 ORE Accedi

Notizie | Economia | Norme e Tributi | Finanza | Commenti&Inchieste | **Tecnologia** | Cultura-Domenica

*** **TECNOLOGIA&BUSINESS** ***

[ILSOLE24ORE.COM](#) > Notizie Tecnologia e Business [ARCHIVIO](#)

L'Università di Genova salva Google dal «baco»

3 SETTEMBRE 2008

Condividi su: [f](#) [e](#) | vota su [DK](#) [NO](#) | [🖨](#) [📄](#) | [A](#) [A](#)

"Dai nostri archivi"

- 1 Borsa, Google e Microsoft deprimono Wall Street
- 1 Google scopre le Pmi
- 1 Secondo fronte: l'attivismo di Google
- 1 Magrini: «La nostra missione? Aggregare informazioni»
- 1 Google, l'Internet ultra veloce viaggerà sulle (vecchie) frequenze Tv

Anche ai gestori del più importante motore di ricerca del mondo può sfuggire qualcosa. Il brutto è quando si tratta di un problema serio: come una una falla nel sistema. Fortuna che stavolta a «salvare»Google ci abbia pensato l'Università di Genova. In particolare, il gruppo di ricerca del

Internet
of Things



Cryptology ePrint Archive

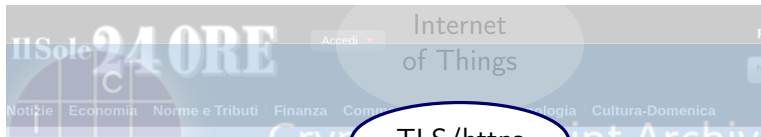
Paper 2008/310

Attacks on RFID Protocols

T. van Deursen and S. Radomirovic

Genova. In particolare, il gruppo di ricerca del

Domain of Research: Security Protocols



BEAST attack [edit]

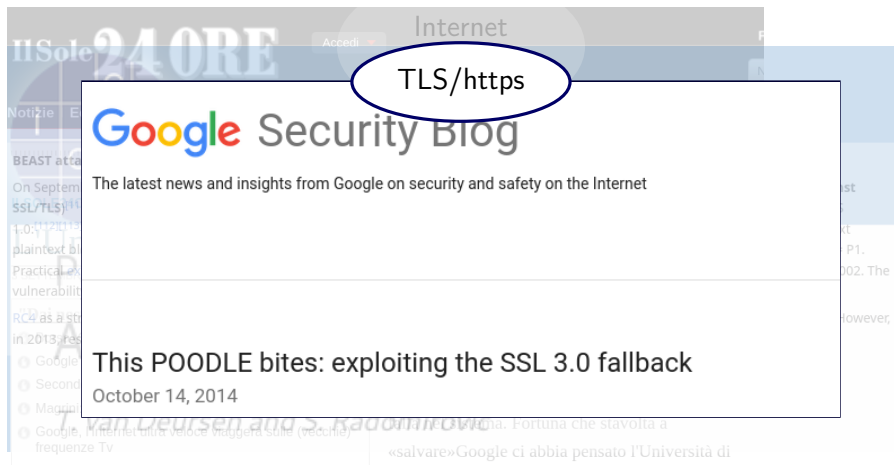
On September 23, 2011, researchers Thai Duong and Juliano Rizzo demonstrated a proof of concept called **BEAST (Browser Exploit Against SSL/TLS)**^[111] using a **Java applet** to violate **same origin policy** constraints, for a long-known **cipher block chaining** (CBC) vulnerability in TLS 1.0:^{[112][113]} an attacker observing 2 consecutive ciphertext blocks C_0, C_1 can test if the plaintext block P_1 is equal to x by choosing the next plaintext block $P_2 = x \oplus C_0 \oplus C_1$; as per CBC operation, $P_2 = E(C_1 \oplus P_2) = E(C_1 \oplus x \oplus C_0 \oplus C_1) = E(C_0 \oplus x)$, which will be equal to C_1 if $x = P_1$. Practical exploits had not been previously demonstrated for this vulnerability, which was originally discovered by Phillip Rogaway^[114] in 2002. The vulnerability of the attack had been fixed with TLS 1.1 in 2006, but TLS 1.1 had not seen wide adoption prior to this attack demonstration.

RC4 as a stream cipher is immune to BEAST attack. Therefore, RC4 was widely used as a way to mitigate BEAST attack on the server side. However, in 2013, researchers found more weaknesses in RC4. Thereafter enabling RC4 on server side was no longer recommended.^[115]

- 1 Google scopre le Pmi
- 2 Secondo fronte: l'attivismo di Google
- 3 Magnoli: «La nostra missione? Aggregare informazioni»
- 4 Google, l'Internet ultra veloce magenta sulle (vecchie) frequenze Tv

ricerca del mondo può sfuggire qualcosa. Il brutto è quando si tratta di un problema serio: come una una
T. van Deursen and S. Radomirovic
Fortuna che stavolta a
«salvare»Google ci abbia pensato l'Università di
Genova. In particolare, il gruppo di ricerca del

Domain of Research: Security Protocols



Internet

Accedi

24 ORE

Notizie E

BEAST attac

On Septem

SSL/TLS) 11

1.0; 112111

plaintext bl

Practical ex

vulnerabilit

RC4 as a st

in 2013, res

Google

Second

Maggio

Google, l'Internet più veloce maggera sola (vecchie)

frequenze Tv

Google

«salvare»Google ci abbia pensato l'Università di

Genova. In particolare, il gruppo di ricerca del

ist

KT

P1.

002. The

however,

Google

Security Blog

The latest news and insights from Google on security and safety on the Internet

This POODLE bites: exploiting the SSL 3.0 fallback

October 14, 2014

van Deursen and S. Radomirovic

Fortuna che stavolta a

«salvare»Google ci abbia pensato l'Università di

Genova. In particolare, il gruppo di ricerca del

Domain of Research: Security Protocols

Login with ...

Computer Science > Cryptography

[Submitted on 6 Jan 2016 (v1), last revised 8 Aug 2016 (this version, v4)]

A Comprehensive Formal Security Analysis of OAuth 2.0

[Daniel Fett](#), [Ralf Kuesters](#), [Guido Schmitz](#)

When proving the security of OAuth in our model, we discovered four attacks which break the security of OAuth. The vulnerabilities can be exploited in practice and are present also in OpenID Connect.

We propose fixes for the identified vulnerabilities, and then, for the first time, actually prove the security of OAuth in an expressive web model. In particular,

Domain of Research: Security Protocols

5G Networks

sciendo

Proceedings on Privacy Enhancing Technologies 2019

Ravishankar Borgaonkar, Lucca Hirschi*, Shinjo Park, and Altaf Shaik

New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols

Abstract: Mobile communications are used by more than two-thirds of the world population who expect security and privacy guarantees. The 3rd Generation Partnership Project (3GPP) group, responsible for the standardization of 3G, 4G, and 5G technologies, designed the Authentication and

AKA: the protection mechanism of the SQN can be defeated under specific replay attacks due to its use of Exclusive-OR (XOR) and a lack of randomness. We show how to leverage this vulnerability to break the confidentiality of SQN, thus defeating the purpose of a dedicated protection mechanism and breaking an explicit privacy requirement [6]. We show that partly learning

«salvare»Google ci abbia pensato l'Università di Genova. In particolare, il gruppo di ricerca del

Goal of Research: Security Assessment

Goal of Research: Security Assessment

- ▶ Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{Ack}$
Reader \rightarrow Tag : $h(Ack \oplus k \oplus r_0)$

Goal of Research: Security Assessment

- ▶ Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{Ack}$
Reader \rightarrow Tag : $h(Ack \oplus k \oplus r_0)$

- ▶ Security goal

Authentication through mutual
proof of knowledge of the
shared secret k

Goal of Research: Security Assessment

- ▶ Protocol from [4]

$$\begin{aligned} \text{Reader} &\rightarrow \text{Tag} && : r_0 \\ \text{Tag} &\rightarrow \text{Reader} && : r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{\text{Ack}} \\ \text{Reader} &\rightarrow \text{Tag} && : h(\text{Ack} \oplus k \oplus r_0) \end{aligned}$$

- ▶ Security goal

Authentication through mutual proof of knowledge of the shared secret k

- ▶ Context

Observed by an intruder Alice

Goal of Research: Security Assessment

▶ Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{Ack}$
Reader \rightarrow Tag : $h(Ack \oplus k \oplus r_0)$

▶ Security goal

Authentication through mutual
proof of knowledge of the
shared secret k

▶ Context

Observed by an intruder Alice

▶ Misuse by Alice

Reader \rightarrow Alice : r'_0

Goal of Research: Security Assessment

► Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{Ack}$
Reader \rightarrow Tag : $h(Ack \oplus k \oplus r_0)$

► Security goal

Authentication through mutual
proof of knowledge of the
shared secret k

► Context

Observed by an intruder Alice

► Misuse by Alice

Reader \rightarrow Alice : r'_0

Goal of Research: Security Assessment

▶ Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{\text{Ack}}$
Reader \rightarrow Tag : $h(\text{Ack} \oplus k \oplus r_0)$

▶ Security goal

Authentication through mutual
proof of knowledge of the
shared secret k

▶ Context

Observed by an intruder Alice

▶ Misuse by Alice

Reader \rightarrow Alice : r'_0
Alice chooses $r'_1 = r_0 \oplus r_1 \oplus r'_0$

Goal of Research: Security Assessment

► Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{\text{Ack}}$
Reader \rightarrow Tag : $h(\text{Ack} \oplus k \oplus r_0)$

► Security goal

Authentication through mutual
proof of knowledge of the
shared secret k

► Context

Observed by an intruder Alice

► Misuse by Alice

Reader \rightarrow Alice : r'_0
Alice chooses $r'_1 = r_0 \oplus r_1 \oplus r'_0$
Alice \rightarrow Reader: $r'_1, \underbrace{h(r'_0 \oplus r'_1 \oplus k)}_{\text{Ack}'}$

Goal of Research: Security Assessment

► Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{Ack}$
Reader \rightarrow Tag : $h(Ack \oplus k \oplus r_0)$

► Security goal

Authentication through mutual proof of knowledge of the shared secret k

► Context

Observed by an intruder Alice

► Misuse by Alice

Reader \rightarrow Alice : r'_0
Alice chooses $r'_1 = r_0 \oplus r_1 \oplus r'_0$
Alice \rightarrow Reader: $r'_1, \underbrace{h(r'_0 \oplus r'_1 \oplus k)}_{Ack'}$
 $Ack' = h(r'_0 \oplus r'_1 \oplus k)$

Goal of Research: Security Assessment

► Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{Ack}$
Reader \rightarrow Tag : $h(Ack \oplus k \oplus r_0)$

► Security goal

Authentication through mutual proof of knowledge of the shared secret k

► Context

Observed by an intruder Alice

► Misuse by Alice

Reader \rightarrow Alice : r'_0
Alice chooses $r'_1 = r_0 \oplus r_1 \oplus r'_0$
Alice \rightarrow Reader: $r'_1, \underbrace{h(r'_0 \oplus r'_1 \oplus k)}_{Ack'}$
 $Ack' = h(r'_0 \oplus r_0 \oplus r_1 \oplus r'_0 \oplus k)$

Goal of Research: Security Assessment

► Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{Ack}$
Reader \rightarrow Tag : $h(Ack \oplus k \oplus r_0)$

► Security goal

Authentication through mutual proof of knowledge of the shared secret k

► Context

Observed by an intruder Alice

► Misuse by Alice

Reader \rightarrow Alice : r'_0
Alice chooses $r'_1 = r_0 \oplus r_1 \oplus r'_0$
Alice \rightarrow Reader: $r'_1, \underbrace{h(r'_0 \oplus r'_1 \oplus k)}_{Ack'}$
 $Ack' = h(r'_0 \oplus r_0 \oplus r_1 \oplus r'_0 \oplus k)$

Goal of Research: Security Assessment

► Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{Ack}$
Reader \rightarrow Tag : $h(Ack \oplus k \oplus r_0)$

► Security goal

Authentication through mutual proof of knowledge of the shared secret k

► Context

Observed by an intruder Alice

► Misuse by Alice

Reader \rightarrow Alice : r'_0
Alice chooses $r'_1 = r_0 \oplus r_1 \oplus r'_0$
Alice \rightarrow Reader: $r'_1, \underbrace{h(r'_0 \oplus r'_1 \oplus k)}_{Ack'}$
 $Ack' = h(r_0 \oplus r_1 \oplus k)$

Goal of Research: Security Assessment

► Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{Ack}$
Reader \rightarrow Tag : $h(Ack \oplus k \oplus r_0)$

► Security goal

Authentication through mutual proof of knowledge of the shared secret k

► Context

Observed by an intruder Alice

► Misuse by Alice

Reader \rightarrow Alice : r'_0
Alice chooses $r'_1 = r_0 \oplus r_1 \oplus r'_0$
Alice \rightarrow Reader: $r'_1, \underbrace{h(r'_0 \oplus r'_1 \oplus k)}_{Ack'}$
 $Ack' = h(r_0 \oplus r_1 \oplus k) = Ack$

Goal of Research: Security Assessment

► Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{Ack}$
Reader \rightarrow Tag : $h(Ack \oplus k \oplus r_0)$

► Security goal

Authentication through mutual proof of knowledge of the shared secret k

► Context

Observed by an intruder Alice

► Misuse by Alice

Reader \rightarrow Alice : r'_0
Alice chooses $r'_1 = r_0 \oplus r_1 \oplus r'_0$
Alice \rightarrow Reader: $r'_1, \underbrace{h(r'_0 \oplus r'_1 \oplus k)}_{Ack'}$
 $Ack' = h(r_0 \oplus r_1 \oplus k) = Ack$
Reader \rightarrow Alice : $h(Ack' \oplus k \oplus r'_0)$

Goal of Research: Security Assessment

► Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{Ack}$
Reader \rightarrow Tag : $h(Ack \oplus k \oplus r_0)$

► Security goal

Authentication through mutual proof of knowledge of the shared secret k

► Context

Observed by an intruder Alice

► Misuse by Alice

Reader \rightarrow Alice : r'_0
Alice chooses $r'_1 = r_0 \oplus r_1 \oplus r'_0$
Alice \rightarrow Reader: $r'_1, \underbrace{h(r'_0 \oplus r'_1 \oplus k)}_{Ack'}$

$Ack' = h(r_0 \oplus r_1 \oplus k) = Ack$
Reader \rightarrow Alice : $h(Ack' \oplus k \oplus r'_0)$

► Consequence

Alice can impersonate a tag!

Goal of Research: Security Assessment

► Protocol from [4]

Reader \rightarrow Tag : r_0
Tag \rightarrow Reader: $r_1, \underbrace{h(r_0 \oplus r_1 \oplus k)}_{Ack}$
Reader \rightarrow Tag : $h(Ack \oplus k \oplus r_0)$

► Security goal

Authentication through mutual proof of knowledge of the shared secret k

► Context

Observed by an intruder Alice

Research goal: *Automatically find such attacks (messages involved and their derivation)*

► Misuse by Alice

Reader \rightarrow Alice : r'_0
Alice chooses $r'_1 = r_0 \oplus r_1 \oplus r'_0$
Alice \rightarrow Reader: $r'_1, \underbrace{h(r'_0 \oplus r'_1 \oplus k)}_{Ack'}$
 $Ack' = h(r_0 \oplus r_1 \oplus k) = Ack$
Reader \rightarrow Alice : $h(Ack' \oplus k \oplus r'_0)$

► Consequence

Alice can impersonate a tag!

Decidability Results

Decidability Results

Main results

Automated deduction techniques

Decidability Results

Main results

- ▶ Sufficient conditions on intruder deduction rules
Oracle rules

Automated deduction techniques

Decidability Results

Main results

- ▶ Sufficient conditions on intruder deduction rules
 - Oracle rules
- ▶ Applications
 - ▶ Exclusive-or (NP-completeness)
 - ▶ Prefix extraction: modeling of ECB block cypher

Automated deduction techniques

Decidability Results

Main results

- ▶ Sufficient conditions on intruder deduction rules
Oracle rules
- ▶ Applications
 - ▶ Exclusive-or (NP-completeness)
 - ▶ Prefix extraction: modeling of ECB block cypher

Automated deduction techniques

- ▶ Ordering techniques: **minimal attacks**

Decidability Results

Main results

- ▶ Sufficient conditions on intruder deduction rules
Oracle rules
- ▶ Applications
 - ▶ Exclusive-or (NP-completeness)
 - ▶ Prefix extraction: modeling of ECB block cypher

Automated deduction techniques

- ▶ Ordering techniques: **minimal attacks**
- ▶ Local proofs: **minimal derivations**

Decidability Results

Main results

- ▶ Sufficient conditions on intruder deduction rules
Oracle rules
- ▶ Applications
 - ▶ Exclusive-or (NP-completeness)
 - ▶ Prefix extraction: modeling of ECB block cypher

Automated deduction techniques

- ▶ Ordering techniques: **minimal attacks**
- ▶ Local proofs: **minimal derivations**
- ▶ Lifting: **pumping lemma**

Support in Cryptographic Protocol Analysis Tools

- ▶ Support through external reduction

Support in Cryptographic Protocol Analysis Tools

- ▶ Support through external reduction
CPSA, ProVerif: [5]

Support in Cryptographic Protocol Analysis Tools

- ▶ Support through external reduction
CPSA, ProVerif: [5]
- ▶ Incomplete support

Support in Cryptographic Protocol Analysis Tools

- ▶ Support through external reduction

CPSA, ProVerif: [5]

- ▶ Incomplete support

Maude-NPA: Through Narrowing with irreducibility constraints

Support in Cryptographic Protocol Analysis Tools

- ▶ **Support through external reduction**

CPSA, ProVerif: [5]

- ▶ **Incomplete support**

Maude-NPA: Through Narrowing with irreducibility constraints

Tamarin: Through reduction to AC-unification for some protocols

Support in Cryptographic Protocol Analysis Tools

- ▶ **Support through external reduction**

CPSA, ProVerif: [5]

- ▶ **Incomplete support**

Maude-NPA: Through Narrowing with irreducibility constraints

Tamarin: Through reduction to AC-unification for some protocols

- ▶ **Complete support**

Support in Cryptographic Protocol Analysis Tools

- ▶ **Support through external reduction**

CPSA, ProVerif: [5]

- ▶ **Incomplete support**

Maude-NPA: Through Narrowing with irreducibility constraints

Tamarin: Through reduction to AC-unification for some protocols

- ▶ **Complete support**

Cryptosense: complete for API analysis (without lifting)

Support in Cryptographic Protocol Analysis Tools

- ▶ **Support through external reduction**

CPSA, ProVerif: [5]

- ▶ **Incomplete support**

Maude-NPA: Through Narrowing with irreducibility constraints

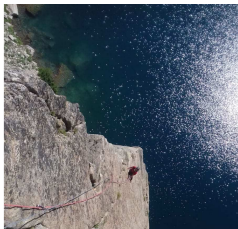
Tamarin: Through reduction to AC-unification for some protocols

- ▶ **Complete support**

Cryptosense: complete for API analysis (without lifting)

CL-AtSe: complete, also implements modular exponentiation, prefix rules,...

Hubert today



Equivalences of protocols

Anonymity

Outsider cannot tell if Alice or Bob plays:

$$P(A) | S \approx P(B) | S$$



Equivalences of protocols

Anonymity

Outsider cannot tell if Alice or Bob plays:

$$P(A) | S \approx P(B) | S$$



Ballot privacy

Outsider cannot tell who voted what:

$$V(A, v_1) | V(B, v_2) | S \approx V(A, v_2) | V(B, v_1) | S$$



Equivalences of protocols

Anonymity

Outsider cannot tell if Alice or Bob plays:

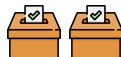
$$P(A) \mid S \approx P(B) \mid S$$



Ballot privacy

Outsider cannot tell who voted what:

$$V(A, v_1) \mid V(B, v_2) \mid S \approx V(A, v_2) \mid V(B, v_1) \mid S$$



Unlinkability

Outsider cannot tell if somebody plays twice:

$$! \nu i. ! \nu s. P(i, s) \approx ! \nu i. \nu s. P(i, s)$$



Equivalence of constraint systems

Reachability

$(P, \epsilon, \top) \rightarrow (P_1, \Phi_1, \mathcal{C}_1) \rightarrow \dots \rightarrow (P_n, \Phi_n, \mathcal{C}_n)$ with \mathcal{C}_n solvable?

Example: $h(r'_0 \oplus R'_1 \oplus k) = A$ with $r_0, r_1, h(r_0 \oplus r_1 \oplus k) \vdash R'_1, A$

Equivalence of constraint systems

Reachability

$(P, \epsilon, \top) \rightarrow (P_1, \Phi_1, \mathcal{C}_1) \rightarrow \dots \rightarrow (P_n, \Phi_n, \mathcal{C}_n)$ with \mathcal{C}_n solvable?

Example: $h(r'_0 \oplus R'_1 \oplus k) = A$ with $r_0, r_1, h(r_0 \oplus r_1 \oplus k) \vdash R'_1, A$

Equivalence

$\forall (P, \epsilon, \top) \xrightarrow{t} (P', \Phi_{P'}, \mathcal{C}_{P'}) \exists (Q, \epsilon, \top) \xrightarrow{t} (Q', \Phi_{Q'}, \mathcal{C}_{Q'})$
any possible experiment wrt. $\mathcal{C}_{P'}$ that succeeds on $\Phi_{P'}$
also works on $\Phi_{Q'}$ (and vice versa)

Example: xoring the first two messages yields the third one.



Cheval, Comon-Lundh, Delaune. *Automating Security Analysis: Symbolic Equivalence of Constraint Systems*. IJCAR'10.



Tiu, Dawson. *Automating Open Bisimulation Checking for the Spi Calculus*. CSF'10.



Baudet. *Security of cryptographic protocols : logical and computational aspects*. PhD, 2007.

Equivalences for unbounded sessions

Proverif

Can prove **diff-equivalence**: very strict, but often enough.



Blanchet, Abadi, Fournet. *Automated Verification of Selected Equivalences for Security Protocols*. LICS'05.

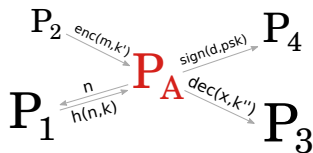
Tamarin

Very different from Proverif but similar capabilities.

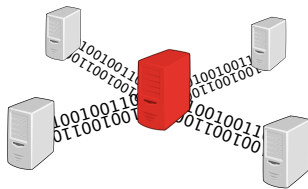


Basin, Dreier, Sasse. *Automated symbolic proofs of observational equivalence*. CCS'15.

Beyond the symbolic model (Dolev-Yao)



?



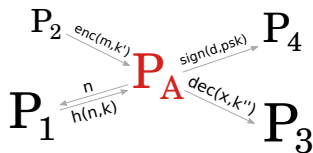
Symbolic

Explicit attacker capabilities.
Security against resulting class
of attackers.

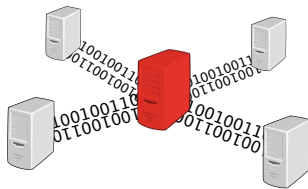
Computational

Any computation on bitstrings,
only constrained by crypto as-
sumptions.

Beyond the symbolic model (Dolev-Yao)



?



Symbolic

Explicit attacker capabilities.
Security against resulting class
of attackers.

Computational

Any computation on bitstrings,
only constrained by crypto as-
sumptions.



Bana, Comon. *Towards Unconditional Soundness: Computationally Complete Symbolic Attacker*. POST'12.



Bana, Comon. *A Computationally Complete Symbolic Attacker for Equivalence Properties*. CCS'14.

Data Privacy



- ▶ Shmatikov's numerous prizes related to privacy.
- ▶ Differential privacy papers at LICS 2021, 2020, 2019.
- ▶ Randomized security protocols at LICS 2017.

Bibliography

- [1] G. Steel, Deduction with XOR Constraints in Security API Modelling, CADE 2005 (start-up: CryptoSense, now SandboxAQ)
- [2] M. Turuani, *The CL-Atse Protocol Analyser*, RTA 2006
- [3] S. F. Doghmi, J. D. Guttman, and F. Javier Thayer, *Searching for Shapes in Cryptographic Protocols*, TACAS 2006
- [4] T. van Deursen and S. Radomirović, *Attacks on RFID protocols*, <https://eprint.iacr.org/2008/310>
- [5] R. Küsters and T. Truderung, *Reducing protocol analysis with XOR to the XOR-free case in the horn theory based approach*, ACM CCS 2008
- [6] S. Erbatur, S. Escobar, S. Kapur, Z. Liu, C. Lynch, C. Meadows, J. Meseguer, P. Narendran, S. Santiago, and R. Sasse, *Effective Symbolic Protocol Analysis via Equational Irreducibility Conditions*, ESORICS 2012 (basis for Maude-NPA equational reasoning)
- [7] J. D. Guttman, *Establishing and Preserving Protocol Security Goals*, J. of Comp. Sec. 2014.
- [8] D. Baelde, D. Delaune, I. Gazeau, S. Kremer, *Symbolic verification of privacy-type properties for security protocols with XOR* CSF 2017
- [9] J. Dreier, L. Hirschi, S. Radomirović, R. Sasse, *Automated Unbounded Verification of Stateful Cryptographic Protocols with Exclusive OR*, IEEE CSF 2018
- [10] D. Basin, J. Dreier, L. Hirschi, S. Radomirović, R. Sasse, V. Stettler, *A Formal Analysis of 5G Authentication (tamarin et xor)*, ACM CCS 2018
- [11] J. Dreier, L. Hirschi, S. Radomirović, R. Sasse, *Verification of Stateful Cryptographic Protocols with Exclusive OR*, J.of Comp.Sec. 2020