16|17 NOVEMBRE 2016

CITÉ DES SCIENCES ET DE L'INDUSTRIE - PARIS

Verification of Indistinguishability Properties

Stéphanie Delaune

Équipe EMSEC (IRISA), CNRS, France

November 16th, 2016

VIP in a nutshell

Verifiation of **I**ndistinguishability **P**roperties

- Projet JCJC Jeunes Chercheuses Jeunes Chercheurs
- January 2012 - June 2016
- `http://www.lsv.ens-cachan.fr/Projects/anr-vip/`

VIP in a nutshell

Verifiation of **I**ndistinguishability **P**roperties

- Projet JCJC Jeunes Chercheuses Jeunes Chercheurs
- January 2012 - June 2016
- `http://www.lsv.ens-cachan.fr/Projects/anr-vip/`

Research Themes

- Formal verification of security protocols
- Privacy-related security properties: unlinkability, anonymity, . . .

Applications: e-auction protocols, e-passeport, e-voting protocols, RFID protocols, routing protocols in mobile ad hoc networks, . . .

Les rencontres du NUMÉRIQUE de l'ANR

Cryptographic protocols everywhere!

16 | 17 NOVEMBRE 2016

Cryptographic protocols everywhere !

Cryptographic protocols

- small programs designed to secure communication (*e.g.* secrecy, authentication, anonymity, . . .)
- use cryptographic primitives (*e.g.* encryption, signature, ...)

The network is unsecure!

Communications take place over a public network like the Internet.

Cryptographic protocols everywhere !

Cryptographic protocols

- small programs designed to secure communication (*e.g.* secrecy, authentication, anonymity, . . .)
- use cryptographic primitives (*e.g.* encryption, signature, ...)

It becomes more and more important to protect our privacy.

Electronic passport

An electronic passport is a passport with an RFID tag embedded in it.

The RFID tag stores:

- the information printed on your passport,
- a JPEG copy of your picture.

Electronic passport

An electronic passport is a passport with an RFID tag embedded in it.

The RFID tag stores:

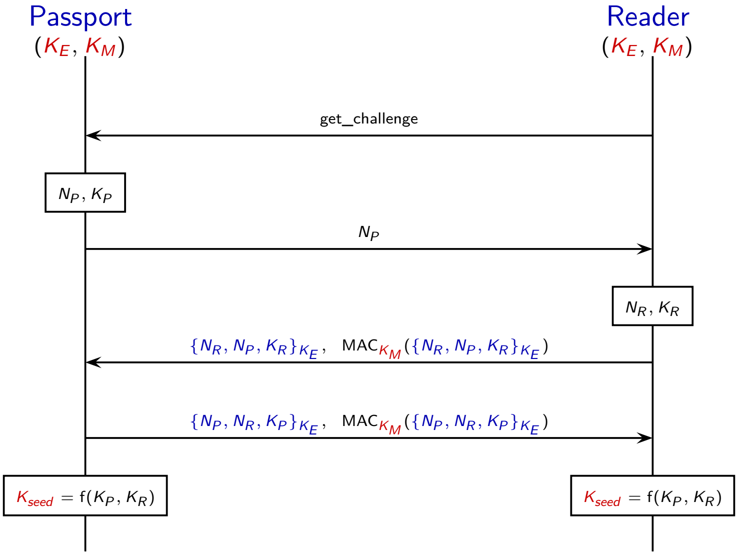
- the information printed on your passport,
- a JPEG copy of your picture.

The Basic Access Control (BAC) protocol is a key establishment protocol that has been designed to also ensure unlinkability.

ISO/IEC standard 15408

Unlinkability aims to ensure *that a user may make multiple uses of a service or resource without others being able to link these uses together.*

BAC protocol



How cryptographic protocols can be attacked?

How cryptographic protocols can be attacked?

Logical attacks

- can be mounted even assuming perfect cryptography,
  $\hookrightarrow$ replay attack, man-in-the middle attack, ...
- subtle and hard to detect by "eyeballing" the protocol

How cryptographic protocols can be attacked?

Logical attacks

- can be mounted even assuming perfect cryptography,
  $\hookrightarrow$ replay attack, man-in-the middle attack, ...
- subtle and hard to detect by "eyeballing" the protocol

Examples

- An authentication flaw in the Needham-Schroeder protocol (1995);
- An authentication flaw in the Single Sign-On protocol used *e.g.* in GMail (2008);
- A traceability attack on the BAC protocol used in e-passport (2010).

A sucessful approach: formal symbolic verification

Main goal: provides a rigorous framework and automatic tools to analyse security protocols and find their flaws.

A sucessful approach: formal symbolic verification

Main goal: provides a rigorous framework and automatic tools to analyse security protocols and find their flaws.

TAMARIN
Tamarin prover interactive mode

ProVerif

AVANTSSAR

Some sucess stories

- Attack on the Needham-Schroeder protocol discovered using the FDR model checker [Lowe, 1995];
  $\longrightarrow$ 17 years after the publication of the protocol!
- Authentication flaw in the Single Sign-On protocol discovered using the Avantssar platform [Armando *et al.*, 2008].

A sucessful approach: formal symbolic verification

Main goal: provides a rigorous framework and automatic tools to analyse security protocols and find their flaws.

TAMARIN Tamarin prover interactive mode   ProVerif   AVANTSSAR

State of the art: Most of the existing verification tools were dedicated to the analysis of standard security goals (*i.e.* secrecy and authentication).

Vip

Main Objective of the VIP project

Develop foundations and practical tools to allow the formal analysis of privacy properties (*e.g.* anonymity, unlinkability)

Les rencontres du NUMÉRIQUE de l'ANR

Main issues of the VIP project

16 | 17 NOVEMBRE 2016

Beyond secrecy and authentication properties

Unlinkability aims to ensure *that a user may make multiple uses of a service or resource without others being able to link these uses together*.

Beyond secrecy and authentication properties

Unlinkability aims to ensure *that a user may make multiple uses of a service or resource without others being able to link these uses together*.

More formally, an observer/attacker can not observe the difference between the two following situations:

1. a situation where the same passport may be used twice (or even more);
2. a situation where each passport is used at most once.

Beyond secrecy and authentication properties

Unlinkability aims to ensure *that a user may make multiple uses of a service or resource without others being able to link these uses together*.

More formally, an observer/attacker can not observe the difference between the two following situations:

1. a situation where the same passport may be used twice (or even more);
2. a situation where each passport is used at most once.

Goal of the VIP project: Develop algorithms and tools for checking the notion of trace equivalence that is used to express that P and Q are indistinguishable from the attacker's point of view.

Beyond standard cryptographic primitives

Modern applications often rely on non-classical cryptographic primitives.

Exclusive-or in RFID technology

$$
\begin{aligned}
x \oplus x &= 0 & \qquad x \oplus (y \oplus z) &= (x \oplus y) \oplus z \\
x \oplus 0 &= x & \qquad x \oplus y &= y \oplus x
\end{aligned}
$$

Blind signature in e-voting systems.

Beyond standard cryptographic primitives

Modern applications often rely on non-classical cryptographic primitives.

Exclusive-or in RFID technology

$$\begin{aligned} x \oplus x &= 0 & \qquad x \oplus (y \oplus z) &= (x \oplus y) \oplus z \\ x \oplus 0 &= x & x \oplus y &= y \oplus x \end{aligned}$$

Blind signature in e-voting systems.

Goal of the VIP project: Take into account these algebraic properties since some attacks exploit these properties.

A need for a modular approach

Real life protocols are usually complex and composed of several sub-protocols.

Verifying each sub-protocol in isolation is **not** sufficient!

Goal of the VIP project: Identify sufficient and reasonable conditions under which a modular security analysis is possible.

Les rencontres du NUMÉRIQUE de l'ANR

Results of the VIP project

16 | 17 NOVEMBRE 2016

The results in a nutshell

We improve the state of the art regarding trace equivalence checking.

- Decidability results
  ⟶ we provide the first decidability results in the unbounded setting

  Rémy Chrétien's PhD thesis (defended in Jan. 2016)
  Expert Technique au Ministère de la Défense

- Modular analysis
  ⟶ we provide some good design principles to make sure that protocols can be analysed in isolation, and used in more complex environment.

- Practical verification tools
  ⟶ we developed several prototypes

- Case studies:
  ⟶ e-passport, RFID protocols, e-voting protocols

Practical verification tools for checking trace equivalence

$\longrightarrow$ they are available on the webpage of the VIP project.

Bounded number of sessions:

- Apte supports protocols with conditional branches;
- Akiss handles a wide variety of primitives (*e.g.* blind signature, xor, ...).
  $\longrightarrow$ The work on the xor operator has been completed by Ivan Gazeau (post-doc on the VIP project), and has made possible the analysis of several RFID protocols.

Unbounded number of sessions:

- we extended ProVerif to prove more equivalences;
- Ukano (based on ProVerif) is devoted to the analysis of unlinkability for 2-party protocols.

Case studies: E-passport

We analyse several protocols issued from the e-passport application, as specified by the ICAO standard.

Main results

- several linkability attacks on the BAC protocol using Apte;
- the first formal security proof of the fixed version of BAC using Ukano;
- the discovery of several vulnerabilities on PACE (successor of BAC);
- a modular security analysis of BAC with PA and AA (two authentication protocols used in the e-passport application) assuming that the good design principles we proposed are fulfilled.

Les rencontres du NUMÉRIQUE de l'ANR

Conclusion

16|17 NOVEMBRE 2016

In a nutshell

Cryptographic protocols are:

- difficult to design and also difficult to analyse;
- particularly vulnerable to logical attacks.

Strong encryption schemes are necessary . . .

. . . **but this is not sufficient!**

In a nutshell

Cryptographic protocols are:

- difficult to design and also difficult to analyse;
- particularly vulnerable to logical attacks.

What kind of protocols are we able to analyse today?

- classical security properties (i.e. secrecy, authentication); and
- **privacy-type properties** on small protocols, and for relatively standard primitives.

Regarding the applications that are coming, this is not sufficient !

POPSTAR in a nutshell (2017-2021)

PI: Stéphanie Delaune, **CNRS**, France

Reasoning about **Physical properties** Of **security Protocols**
with an Application To **contactless Systems**

Main issues:

- specificities of contactless systems are not well understood;
- a lack of formal model to reason about these systems.

Main outcomes:

- solid foundations to reason about physical properties;
- new algorithms and tools to analyse the security and privacy of modern protocols;
- make the upcoming generation of nomadic contactless devices more secure.