Formal verification of security protocols - the Squirrel prover

Stéphanie DELAUNE

FPS - December 11, 2023

Cryptographic protocols everywhere !

Cryptographic protocols

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

Cryptographic protocols everywhere !

Cryptographic protocols

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

The network is unsecure !

Communications take place over a public network like the Internet.

Cryptographic protocols everywhere !

Cryptographic protocols

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

They aim to secure our communications and protect our privacy.

Electronic passport

An e-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 e-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*.

An attack on the BAC protocol

An attack against unlinkability on the BAC protocol [Chothia et al., 2010]

Security

Defects in e-passports allow real-time tracking

This threat brought to you by RFID

The register - Jan. 2010

- This issue was due to overly specific error messages ;
- French passports were vulnerable.

Contactless payment

- In the first quarter of 2020, there was a 40% growth in contactless transactions.
- In France, 4.6 billion of transactions were paid contactless in 2020 (40%).

Authentication with physical proximity

We want to ensure that the transaction is performed by a legitimate credit card, but actually the one close to the reader during the transaction.

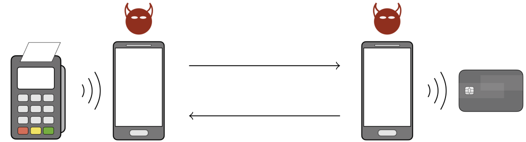
Contactless payment is vulnerable to relay attack

Do you know what you're paying for? How contactless cards are still vulnerable to relay attack

Publié: 2 août 2016, 18:19 CEST

The Conversation - Aug. 2016

How does it work ?



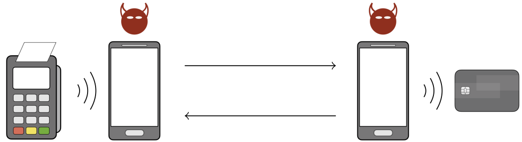
Contactless payment is vulnerable to relay attack

Do you know what you're paying for? How contactless cards are still vulnerable to relay attack

Publié: 2 août 2016, 18:19 CEST

The Conversation - Aug. 2016

How does it work ?



⟶ specific protocols, distance bounding protocols, have been designed to mitigate relay attack (included in the EMV specification since 2016)

How cryptographic protocols can be attacked ?

Several levels of attacks, which may exploit :

- weaknesses of cryptographic primitives ;
- flaws in the design of the protocol ;
- bugs in implementations.

How cryptographic protocols can be attacked ?

Several levels of attacks, which may exploit :

- weaknesses of cryptographic primitives ;
- flaws in the design of the protocol ;
- bugs in implementations.

Flaws in the design of the protocol

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

Two additional examples of logical attacks

An authentication flaw on the Needham Schroeder protocol

$$A \rightarrow B : \{A, N_A\}_{\mathsf{pub}(B)}$$
$$B \rightarrow A : \{N_A, N_B\}_{\mathsf{pub}(A)}$$
$$A \rightarrow B : \{N_B\}_{\mathsf{pub}(B)}$$

NS protocol (1978)

$$A \rightarrow B : \{A, N_A\}_{\mathsf{pub}(B)}$$
$$B \rightarrow A : \{N_A, N_B, B\}_{\mathsf{pub}(A)}$$
$$A \rightarrow B : \{N_B\}_{\mathsf{pub}(B)}$$

NS-Lowe protocol (1995)

Two additional examples of logical attacks

An authentication flaw on the Needham Schroeder protocol

$$\begin{aligned} A &\rightarrow B : \{A, N_A\}_{\mathsf{pub}(B)} \\ B &\rightarrow A : \{N_A, N_B\}_{\mathsf{pub}(A)} \\ A &\rightarrow B : \{N_B\}_{\mathsf{pub}(B)} \end{aligned}$$

NS protocol (1978)

$$\begin{aligned} A &\rightarrow B : \{A, N_A\}_{\mathsf{pub}(B)} \\ B &\rightarrow A : \{N_A, N_B, B\}_{\mathsf{pub}(A)} \\ A &\rightarrow B : \{N_B\}_{\mathsf{pub}(B)} \end{aligned}$$

NS-Lowe protocol (1995)

FREAK attack by Barghavan et al. (2015)

A logical flaw that allows a *man-in-the-middle* attacker to downgrade connections from 'strong' RSA to 'export grade' RSA.

$\longrightarrow$ websites affected by the vulnerability included those from the US federal government

How to verify the absence of logical flaws?

- dissect the protocol and test their resilience against well-known attacks;
  $\longrightarrow$ **this is not sufficient!**

How to verify the absence of logical flaws ?

- dissect the protocol and test their resilience against well-known attacks ;
  $\longrightarrow$ **this is not sufficient !**

- perform a manual security analysis
  $\longrightarrow$ **this is error-prone !**

How to verify the absence of logical flaws ?

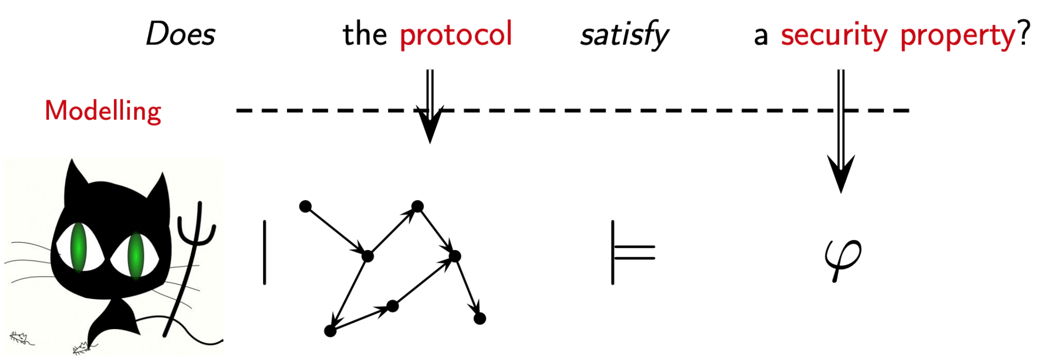
- dissect the protocol and test their resilience against well-known attacks ;
  $\longrightarrow$ **this is not sufficient !**

- perform a manual security analysis
  $\longrightarrow$ **this is error-prone !**

Our approach : formal verification using tools

We aim at providing a rigorous framework and verification tools (e.g. Squirrel) to analyse security protocols and find their logical flaws.

Outline



- I. Symbolic versus Computational model
- II. A novel approach : the Squirrel prover

Part I

Two main families of models : symbolic versus computational

Two main families of models

Symbolic models
[Dolev & Yao, 81]

Computational models
[Goldwasser & Micali, 84]

Two main families of models

Symbolic models

[Dolev & Yao, 81]

Messages are terms.

What the attacker can do.

Unclear guarantees.

Amenable to automation.

e.g. Proverif, Tamarin

Computational models

[Goldwasser & Micali, 84]

Messages are bitstrings.

What the attacker can **not** do.
Everything else is allowed ![1]

Stronger guarantees.

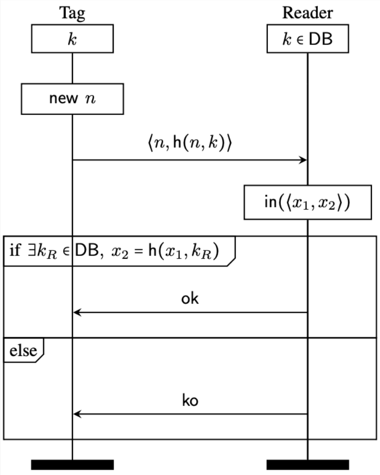
Harder to automate.

e.g. CryptoVerif

[1] The attacker is a probabilistic polynomial-time Turing machine.

Example : Basic Hash protocol

⟶ [Weis *et al.*, 03]



- Each tag stores a secret key k that is never updated.
- Readers have access to a database DB containing all the keys.

Security properties

- authentication : when the reader accepts a message, it has indeed been sent by a legitimate tag ;
- unlinkability : it is not possible to track tags.

Protocols as processes

$\longrightarrow$ a programming language with constructs for concurrency and communication

(applied-pi calculus [Abadi & Fournet, 01])

P, Q	$:=$	0	null process
	$\mid$	$\mathsf{in}(c, x); P$	input
	$\mid$	$\mathsf{out}(c, M); P$	output
	$\mid$	$\mathtt{new}\ n; P$	name generation
	$\mid$	$\mathtt{if}\ M = N\ \mathtt{then}\ P\ \mathtt{else}\ Q$	conditional
	$\mid$	$!P$	replication
	$\mid$	$(P \mid Q)$	parallel composition

Protocols as processes

$\longrightarrow$ a programming language with constructs for concurrency and communication

(applied-pi calculus [Abadi & Fournet, 01])

$$
\begin{array}{rcll}
P, Q & := & 0 & \text{null process} \\
& | & \mathrm{in}(c, x); P & \text{input} \\
& | & \mathrm{out}(c, M); P & \text{output} \\
& | & \texttt{new}\ n; P & \text{name generation} \\
& | & \texttt{if}\ \ M = N\ \texttt{then}\ \ P\ \texttt{else}\ \ Q & \text{conditional} \\
& | & !P & \text{replication} \\
& | & (P \mid Q) & \text{parallel composition} \\
& | & \texttt{insert}\ tbl(M); P & \text{insertion} \\
& | & \texttt{get}\ tbl(x)\ \texttt{st.}\ M = N\ \texttt{in}\ P\ \mathrm{else}\ Q & \text{lookup} \\
& | & \ldots &
\end{array}
$$

Basic Hash protocol in the symbolic setting

$\longrightarrow$ An abstract model, also known as Dolev-Yao model [Dolev &Yao, 81]

Modelling messages/computations

$$\begin{aligned} \Sigma &= \{\langle\ \rangle,\ \mathsf{proj}_1,\ \mathsf{proj}_2,\ \mathsf{h}\} \\ E &= \{\mathsf{proj}_1(\langle x_1, x_2\rangle) = x_1,\ \ \mathsf{proj}_2(\langle x_1, x_2\rangle) = x_2\} \end{aligned}$$

- all the function symbols are public (available to the attacker) ;
- no equation regarding the hash function.

Modelling protocols as processes, roughly a labelled transition system

$$!\,\mathsf{R}\ \mid\ (!\ \mathtt{new}\ k; \mathtt{insert}\ DB(k);\ !\ \mathsf{T}(k))$$

where :

- $\mathsf{T}(k) = \mathtt{new}\ n; \mathsf{out}(c, \langle n, \mathsf{h}(n, k)\rangle)$.
- $\mathsf{R} = \mathsf{in}(c, y); \mathtt{get}\ db(k)\ \mathtt{st.}\ \mathsf{h}(\mathsf{proj}_1(y), k) = \mathsf{proj}_2(y)\ \mathtt{in}\ \mathsf{out}(c, \mathsf{ok})\ \mathsf{else}\ \mathsf{out}(c, \mathsf{ko})$.

Basic Hash in the computational setting

$\longrightarrow$ The cryptographer's mathematical model for provable security

[Goldwasser & Micali, 84]

In computational model, properties only hold with overwhelming probability, under some assumptions on cryptographic primitives

Some usual cryptographic assumptions for a hash function :

- Collision Resistance (CR) : « $\mathsf{h}(n, k) = \mathsf{h}(n', k)$ implies $n = n'$ »
- PseudoRandom Function (PRF) : « $\mathsf{h}(n, k) \sim r$ »
- Existential UnForgeability (EUF) : ...

Existential UnForgeability (EUF)

There is a negligible probability of success for the following game, for any attacker $\mathcal{A}$ (i.e. any PPTM) :

- Draw k uniformly at random.
- $\langle u, v \rangle := \mathcal{A}^{\mathcal{O}}$ where $\mathcal{O}$ is the oracle $x \to \mathrm{h}(x, k)$.
- Succeed if $u = \mathrm{h}(v, k)$ and $\mathcal{O}$ has *not* been called on v.

Basic Hash in the computational setting : authentication

Existential UnForgeability (EUF)

There is a negligible probability of success for the following game, for any attacker $\mathcal{A}$ (i.e. any PPTM) :

- Draw k uniformly at random.
- $\langle u, v \rangle := \mathcal{A}^{\mathcal{O}}$ where $\mathcal{O}$ is the oracle $x \to \mathrm{h}(x, k)$.
- Succeed if $u = \mathrm{h}(v, k)$ and $\mathcal{O}$ has *not* been called on v.

Security proof : « Reader accepts m implies m emitted by a legitimate tag. »

- Assume reader accepts some m such that $\mathrm{proj}_2(m) = \mathrm{h}(\mathrm{proj}_1(m), k_i)$ for some i .
- By unforgeability, $\mathrm{proj}_1(m) = n_T$ for some session of tag T_i .
- The two projections of m are the two projections of the output of T_i. $\square$

Limitations of symbolic model

- Security assumptions can be imprecise (*cf.* EUF and PRF).
- Obtaining computational guarantees from the symbolic model is hard !

A fundamental problem

One should not specify what the attacker can do but what is safe.

Limitations of symbolic model

- Security assumptions can be imprecise (*cf.* EUF and PRF).
- Obtaining computational guarantees from the symbolic model is hard !

A fundamental problem

One should not specify what the attacker can do but what is safe.

The CCSA (Computational Complete Symbolic Attacker) approach, now implemented in the Squirrel prover, does just this, while keeping the modelling of messages as (abstract) terms with a computational semantics, to allow verification via automated reasoning.

Brief comparison of some exising verification tools

	DeepSec/Akiss	ProVerif/GSverif	Tamarin	**Squirrel**	CryptoVerif	EasyCrypt
unbounded traces	✗	✓	✓	✓	✓	✓
computational attacker	✗	✗	✗	✓	✓	✓
concrete security bounds	✗	✗	✗	✗	✓	✓
native concurrency	✓	✓	✓	✓	✓	✗
global mutable states	✓	✓	✓	✓	✗	✓
automation	↑	↗	↗	↘	↗	↓

Disclaimer :

Squirrel is less mature than any of the other tools

Part II

A Novel approach :
the Squirrel prover

What is Squirrel ?

A proof assistant for veryfing cryptographic protocols in the computational model.

`https://squirrel-prover.github.io/`

It is based on the CCSA approach :

G. Bana & H. Comon. CCS 2014.
A Computationally Complete Symbolic Attacker for Equivalence Properties.

History of Squirrel

Some papers related to Squirrel :

- 2012 : Towards Unconditional Soundess : CCSA — Bana & Comon
- 2014 : CCSA for equivalence properties — Bana & Comon
- 2017 : Some manual proofs of RFID protocols — Comon & Koutsos
- 2021 : Introduction of the meta-logic and the Squirrel prover — Baelde et al.
- 2022 : Mutable states and tactics to reason about them — Baelde et al.

Whats' new in 2023

A user manual and you can now play with Squirrel without installing it !

`https://squirrel-prover.github.io/jsquirrel/`

Current team : D. Baelde, A. Dallon, S. Delaune, C. Fontaine, C. Hérouard, C. Jacomme, A. Koutsos, J. Lallemand, S. Riou, J. Sauvage, G. Scerri, . . .

$\longrightarrow$ most of these people are at IRISA, LMF, and Inria Paris.

Squirrel prover

A tool for verifying security protocols in the computational model which takes in input :

- protocols written in a process algebra (as in symbolic models), and internally translated into a system of actions ;
- reachability and equivalence properties.

Squirrel prover

A tool for verifying security protocols in the computational model which takes in input :

- protocols written in a process algebra (as in symbolic models), and internally translated into a system of actions ;
- reachability and equivalence properties.

Squirrel is a proof assistant, i.e. users prove goals using sequence of tactics :

- logical tactics : apply, intro, rewrite, . . .
- cryptographic tactics : fresh, prf, euf, collision-resistant, . . .

$\longrightarrow$ All the reasoning about probabilities are hidden to the user, and each tactic is proved to be sound (manually once and for all).

Going back to the Basic Hash protocol

```
include Basic.

hash h
abstract ok : message
abstract ko : message.

name key  : index -> message

channel cT
channel cR.

process tag(i:index,k:index) =
  new nT; out(cT, <nT, h(nT,key(i))>).

process reader(j:index) =
  in(cT,x);
  if exists (i:index), snd(x) = h(fst(x),key(i)) then R1: out(cR,ok)
  else R2: out(cR,ko).

system [BasicHash] ((!_j R: reader(j)) | (!_i !_k T: tag(i,k))).
```

The process is immediately translated into a system of actions, i.e. a set of triples :

(input ; test ; output).

Basic Hash as a system of actions

Tag is modelled with **one action**, namely $T[i,k]$:

- input@$T[i,k]$;
- true ; and
- output@$T[i,k] = \langle n_T[i,k], \mathsf{h}(n_T[i,k], key[i])\rangle$.

Basic Hash as a system of actions

Tag is modelled with **one action**, namely $T[i,k]$:

- $\text{input@}T[i,k]$;
- true ; and
- $\text{output@}T[i,k] = \langle n_T[i,k], \text{h}(n_T[i,k], key[i])\rangle$.

Reader is modelled with **two actions**, namely $R_1[j]$ and $R_2[j]$:

- $\text{input@}R_1[j]$;
- $\exists i. snd(\text{input@}R_1[j]) = h(fst(\text{input@}R_1[j]), key[i])$;
- $\text{output@}R_1[j] = ok$;

- $\text{input@}R_2[j]$;
- $\forall i. snd(\text{input@}R_2[j]) \neq h(fst(\text{input@}R_2[j]), key[i])$;
- $\text{output@}R_2[j] = ko$.

Basic Hash - Authentication

```
lemma [BasicHash] authentication :
 forall (j:index), happens(R1(j)) =>
                   cond@R1(j) =>
                   (exists (i,k:index), T(i,k) < R1(j)
                             && fst(output@T(i,k)) = fst(input@R1(j))
                             && snd(output@T(i,k)) = snd(input@R1(j))).
Proof.
intro j Hap Hcond.
expand cond@R1(j).
destruct Hcond as [i0 HEq].
euf HEq.
intro [k0 [HOrd Eq]].
by exists i0, k0.
Qed.
```

⟶ The proof script contains logical tactics (here intro, exists) and also a crypto tactic (here euf).

$\longrightarrow$ All tactics have been proved to be sound manually once and for all.

For crypto axioms, they have been designed first at the base logic level (CCSA), and then lift at the meta-logic level, and their soundness have been established in two steps.

Example :

Base logic rule:

$$\frac{}{\Gamma, t = \mathsf{n} \vdash \phi} \quad \text{where } \mathsf{n} \notin \mathsf{st}(t)$$

Meta-logic rule:

$$\frac{\Gamma, \bigvee_{(\mathsf{n}[\vec{j}],\vec{k},c) \in \bar{\mathsf{st}}_{\mathcal{P}}(t)} \exists \vec{k}.c \wedge \vec{i} = \vec{j} \vdash \phi}{\Gamma, t = \mathsf{n}[\vec{i}] \vdash \phi}$$

Squirrel offline Demo - authentication on Basic Hash

basic-hash-auth.sp

```
  else R2: out(cR,ko).


system [BasicHash] ((!_j R: reader(j)) | (!_i !_k T: tag(i,k))).

lemma [BasicHash] authentication :
 forall (j:index), happens(R1(j)) =>
                   cond@R1(j) =>
                   (exists (i,k:index), T(i,k) < R1(j)
                              && fst(output@T(i,k)) = fst(input@R1(j))
                              && snd(output@T(i,k)) = snd(input@R1(j))).
Proof.
intro j Hap Hcond.
expand cond@R1(j).
destruct Hcond as [i0 HEq].
euf HEq.
intro [k0 [HOrd Eq]].
by exists i0, k0.
Qed.
```

```
[goal> Focused goal (1/1):
System: BasicHash
----------------------------------------
forall (j:index),
  happens(R1(j)) =>
  cond@R1(j) =>
  exists (i,k:index),
    T(i, k) < R1(j) &&
    fst (output@T(i, k)) = fst (input@R1(j)) &&
    snd (output@T(i, k)) = snd (input@R1(j))

U:%*-  *goals*       All L1       (Squirrel goals)
```

Squirrel offline Demo - authentication on Basic Hash

basic-hash-auth.sp

```
  else R2: out(cR,ko).


system [BasicHash] ((!_j R: reader(j)) | (!_i !_k T: tag(i,k))).

lemma [BasicHash] authentication :
 forall (j:index), happens(R1(j)) =>
                   cond@R1(j) =>
                   (exists (i,k:index), T(i,k) < R1(j)
                             && fst(output@T(i,k)) = fst(input@R1(j))
                             && snd(output@T(i,k)) = snd(input@R1(j))).
Proof.
intro j Hap Hcond.
expand cond@R1(j).
destruct Hcond as [i0 HEq].
euf HEq.
intro [k0 [HOrd Eq]].
by exists i0, k0.
Qed.
```

```
[goal> Focused goal (1/1):
System: BasicHash
Variables: j:index[const]
Hap: happens(R1(j))
Hcond: cond@R1(j)
----------------------------------------
exists (i,k:index),
  T(i, k) < R1(j) &&
  fst (output@T(i, k)) = fst (input@R1(j)) &&
  snd (output@T(i, k)) = snd (input@R1(j))

U:%*-  *goals*       All L1      (Squirrel goals)
```

Squirrel offline Demo - authentication on Basic Hash

basic-hash-auth.sp

```
  else R2: out(cR,ko).


system [BasicHash] ((!_j R: reader(j)) | (!_i !_k T: tag(i,k))).

lemma [BasicHash] authentication :
 forall (j:index), happens(R1(j)) =>
                   cond@R1(j) =>
                   (exists (i,k:index), T(i,k) < R1(j)
                              && fst(output@T(i,k)) = fst(input@R1(j))
                              && snd(output@T(i,k)) = snd(input@R1(j))).
Proof.
intro j Hap Hcond.
expand cond@R1(j).
destruct Hcond as [i0 HEq].
euf HEq.
intro [k0 [HOrd Eq]].
by exists i0, k0.
Qed.
```

```
[goal> Focused goal (1/1):
System: BasicHash
Variables: j:index[const]
Hap: happens(R1(j))
Hcond: exists (i:index), snd (input@R1(j)) = h (fst (input@R1(j)), key i)
----------------------------------------
exists (i,k:index),
  T(i, k) < R1(j) &&
  fst (output@T(i, k)) = fst (input@R1(j)) &&
  snd (output@T(i, k)) = snd (input@R1(j))

U:%*-  *goals*      All L1     (Squirrel goals)
```

Squirrel offline Demo - authentication on Basic Hash

basic-hash-auth.sp

```
  else R2: out(cR,ko).


system [BasicHash] ((!_j R: reader(j)) | (!_i !_k T: tag(i,k))).

lemma [BasicHash] authentication :
 forall (j:index), happens(R1(j)) =>
                   cond@R1(j) =>
                   (exists (i,k:index), T(i,k) < R1(j)
                              && fst(output@T(i,k)) = fst(input@R1(j))
                              && snd(output@T(i,k)) = snd(input@R1(j))).
Proof.
intro j Hap Hcond.
expand cond@R1(j).
destruct Hcond as [i0 HEq].
euf HEq.
intro [k0 [HOrd Eq]].
by exists i0, k0.
Qed.
```

```
[goal> Focused goal (1/1):
System: BasicHash
Variables: i0,j:index[const]
HEq: snd (input@R1(j)) = h (fst (input@R1(j)), key i0)
Hap: happens(R1(j))
----------------------------------------
exists (i,k:index),
  T(i, k) < R1(j) &&
  fst (output@T(i, k)) = fst (input@R1(j)) &&
  snd (output@T(i, k)) = snd (input@R1(j))

U:%*-  *goals*      All L1     (Squirrel goals)
```

Squirrel offline Demo - authentication on Basic Hash

basic-hash-auth.sp

```
  else R2: out(cR,ko).


system [BasicHash] ((!_j R: reader(j)) | (!_i !_k T: tag(i,k))).

lemma [BasicHash] authentication :
 forall (j:index), happens(R1(j)) =>
                   cond@R1(j) =>
                   (exists (i,k:index), T(i,k) < R1(j)
                              && fst(output@T(i,k)) = fst(input@R1(j))
                              && snd(output@T(i,k)) = snd(input@R1(j))).
Proof.
intro j Hap Hcond.
expand cond@R1(j).
destruct Hcond as [i0 HEq].
euf HEq.
intro [k0 [HOrd Eq]].
by exists i0, k0.
Qed.
```

```
[goal> Focused goal (1/1):
System: BasicHash
Variables: i0,j:index[const]
HEq: snd (input@R1(j)) = h (fst (input@R1(j)), key i0)
Hap: happens(R1(j))
----------------------------------------
(exists (k:index), T(i0, k) < R1(j) && fst (input@R1(j)) = nT (i0, k)) =>
exists (i,k:index),
  T(i, k) < R1(j) &&
  fst (output@T(i, k)) = fst (input@R1(j)) &&
  snd (output@T(i, k)) = snd (input@R1(j))

U:%*-  *goals*        All L1     (Squirrel goals)
in other actions:
  nT (i, k) auth. by key(i)
    (collision with fst (input@R1(j)) auth. by key(i0))
    in action T(i, k)
    in term <nT (i, k),h (nT (i, k), key i)>

Total: 1 occurrence
       0 of them are subsumed by another
       1 occurrence remaining
```

Squirrel offline Demo - authentication on Basic Hash

basic-hash-auth.sp

```
  else R2: out(cR,ko).


system [BasicHash] ((!_j R: reader(j)) | (!_i !_k T: tag(i,k))).

lemma [BasicHash] authentication :
 forall (j:index), happens(R1(j)) =>
                   cond@R1(j) =>
                   (exists (i,k:index), T(i,k) < R1(j)
                              && fst(output@T(i,k)) = fst(input@R1(j))
                              && snd(output@T(i,k)) = snd(input@R1(j))).
Proof.
intro j Hap Hcond.
expand cond@R1(j).
destruct Hcond as [i0 HEq].
euf HEq.
intro [k0 [HOrd Eq]].
by exists i0, k0.
Qed.
```

```
[goal> Focused goal (1/1):
System: BasicHash
Variables: i0,j,k0:index[const]
Eq: fst (input@R1(j)) = nT (i0, k0)
HEq: snd (input@R1(j)) = h (fst (input@R1(j)), key i0)
HOrd: T(i0, k0) < R1(j)
Hap: happens(R1(j))
----------------------------------------
exists (i,k:index),
  T(i, k) < R1(j) &&
  fst (output@T(i, k)) = fst (input@R1(j)) &&
  snd (output@T(i, k)) = snd (input@R1(j))

U:%*-  *goals*       All L1      (Squirrel goals)
```

Squirrel offline Demo - authentication on Basic Hash

basic-hash-auth.sp

```
  else R2: out(cR,ko).


system [BasicHash] ((!_j R: reader(j)) | (!_i !_k T: tag(i,k))).

lemma [BasicHash] authentication :
 forall (j:index), happens(R1(j)) =>
                  cond@R1(j) =>
                  (exists (i,k:index), T(i,k) < R1(j)
                           && fst(output@T(i,k)) = fst(input@R1(j))
                           && snd(output@T(i,k)) = snd(input@R1(j))).
Proof.
intro j Hap Hcond.
expand cond@R1(j).
destruct Hcond as [i0 HEq].
euf HEq.
intro [k0 [HOrd Eq]].
by exists i0, k0.
Qed.
```

```
[goal> lemma authentication is proved
```

```
U:%*-  *goals*     All L1     (Squir
```

Benchmark

Protocol name	LoC	Assumptions	Security Properties
Basic Hash	100	Prf, Euf	authentication & unlinkability
Hash Lock	130	Prf, Euf	authentication & unlinkability
LAK (with pairs)	250	Prf, Euf	authentication & unlinkability
MW	300	Prf, Euf, Xor	authentication & unlinkability
Feldhofer	270	Enc-Kp, Int-Ctxt	authentication & unlinkability
Private authentication	100	Cca_1, Enc-Kp	anonymity
Signed DDH [ISO 9798-3]	240	Euf, Ddh	authentication & strong secrecy
CANAuth	450	Euf	authentication
SLK06	80	Euf	authentication
YPLRK05	160	Euf	authentication

$\longrightarrow$ between 80 and 450 LoC (for the model and the proof script).

Conclusion

Formal symbolic verification

Take away :

- the two main tools today are ProVerif and Tamarin ;
- many success stories regarding reachability properties : they are able to analyse quite complex protocols and scenarios (mostly automatically)

Work in progress :

- allow some user interactions to help the prover ;
  $\longrightarrow$ available in Tamarin from the beginning, and now available also in ProVerif [Blanchet *et al.*, S&P'22]
- some equivalence properties (e.g. unlinkability) are still challenging to analyse ;
- each tool has its own specificities (syntax, semantics, own features, ...) : a need for a platform to ease interactions
  $\longrightarrow$ Sapic^{+} platform [Cheval *et al.*, USENIX'22]

Future developments on Squirrel

Squirrel is a new tool and it remains a lot to do . . .

Some work in progress :

- more complex protocols ;
- more powerful automation using e.g. SMT solvers ; (PhD of S. Riou)
- study of the translation from processes to actions ; (PhD of C. Hérouard)
- formally deriving crypto axioms / tactics from games ; (PhD of J. Sauvage)
- analysing post-quantum or hybrid protocols
- . . .

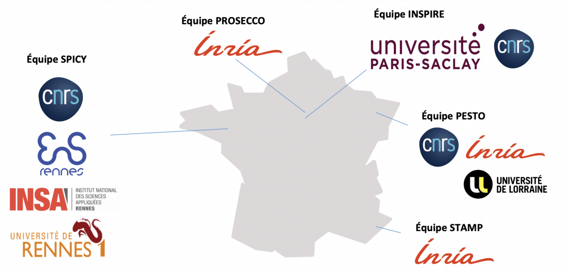
PEPR Cybersecurity (2022-2028)

Partners : 5 teams in France (Nancy, Paris, Rennes, Sophia)

https://pepr-cyber-svp.cnrs.fr

Job offers :

- PhDs
- Post-docs
- Engineers



⟶ contact me : stephanie.delaune@irisa.fr