Spicy team - Security & Privacy

Team leader: Stéphanie DELAUNE
January 15, 2024
Objective

Development of *methods* in order to systematically analyse the *security* and the *privacy* of the systems we are using in our daily life.

1. **Cryptographic protocols**: bluetooth, e-voting, distance bounding protocols, 
2. **Privacy**: vote-anonymity, untraceability, sanitization of data, 
3. **Formal methods**: process algebra, automated deduction, 

Team members

- 7 permanent researchers, and 5 PhD students;
- 1 engineer, and 1 DGA collaborator;
- 1 administrative assistant, and 1 project manager (SVP)

G. Avoine  M. Sabt  T. Allard  B. Fila  J. Lallemand  D. Baelde  S. Delaune
Team members

- 7 permanent researchers, and 5 PhD students;
- 1 engineer, and 1 DGA collaborator;
- 1 administrative assistant, and 1 project manager (SVP)

T. Claverie    C. Hérouard    P. Philippe    S. Riou    J. Sauvage
Team members

- 7 permanent researchers, and 5 PhD students;
- 1 engineer, and 1 DGA collaborator;
- 1 administrative assistant, and 1 project manager (SVP)

A. Dallon  C. Guichemerre  A. Patier  B. Josset
Research axis 1: Cryptographic protocols

Comprehensive analysis of all Bluetooth key-agreement protocols:


→ Best paper award at ESORICS’23

Digital Rights Management (DRM) systems:

- ANR JCJC DRAMA (2023-2026) - PI: M. Sabt;
- Gwendal Patat PhD thesis (defended in Dec. 2023);
- Ongoing work: formal analysis of Widevine using the Tamarin prover.

Research axis 2: Privacy

We are interested both in designing and attacking cryptographic protocols and/or data sanitization mechanisms.

**Antonin Voyez PhD thesis (CIFRE)**

| Supervised by T. Allard, G. Avoine, and E. Fromont (Lacodam) |
| Privacy Risk Analysis of Large-scale Temporal Data: Application to Electricity Consumption Data. |

**Part of the PhD thesis of Louis Béziaud**

| Supervised by T. Allard and S. Gambs (Montreal) |
| A framework designed to facilitate the organization of challenges dedicated to attacking existing data sanitization mechanisms. |
Research axis 3: Formal methods for security

### Squirrel prover

A proof assistant for verifying security protocols in the computational model.

→ All the reasoning about probabilities are hidden to the user.


What's new in 2023

A user manual and you can now play with Squirrel without installing it! [https://squirrel-prover.github.io/jsquirrel/](https://squirrel-prover.github.io/jsquirrel/)

→ thanks to T. Rubiano (before in D4, then in D1, and now in D3).
Research axis 3: Formal methods for security

**Squirrel prover**

A proof assistant for verifying security protocols in the computational model.

→ All the reasoning about probabilities are hidden to the user.


**Whats’ new in 2023**

A [user manual](https://squirrel-prover.github.io/jsquirrel/) and you can now play with Squirrel without installing it!

→ thanks to T. Rubiano (before in D4, then in D1, and now in D3).
Thanks for your attention