UMR IRISA

Activity Report 2021

Team SPICY

Security & PrIvaCY

D1 – Large Scale Systems

1 Team composition

The SPICY team was officially created in May 2021. Therefore, all the activities related to the first semester of year 2021 are not strictly speaking activities conducted in the SPICY team.

Researchers and faculty members

Tristan Allard	Associate Professor	Univ Rennes 1
Gildas Avoine	Professor	INSA Rennes
David Baelde	Professor	ENS Rennes
Stéphanie Delaune	Senior Researcher	CNRS – head of the team
Barbara Fila	Associate Professor (HdR)	INSA Rennes
Joseph Lallemand	Junior Researcher	CNRS
Mohamed Sabt	Associate Professor	Univ Rennes 1

Tristan Allard is member of the SPICY team since September 15th. He was before member of the DRUID team and his activities regarding the year 2021 are described in the DRUID activity report. David Baelde is member of the SPICY team since September 1st. He was before assistant professor at LMF (Saclay).

Engineers

Clément Hérouard	Sep 2021 to Aug 2022	ERC POPSTAR (CNRS)
Le Thanh Dung (Tito) Nguyen	Sep 2021 to Aug 2022	ERC POPSTAR (CNRS)
Javier Rojas-Balderrama	June 2020 to March 2022	

PhD students

Louis Béziaud	Jan 2019 to Feb 2023	Cominlabs PROFILE & UQÀM grant (cotutelle with UQÀM, Montreal)
Daniel De Almeida Braga	Sep 2018 to Aug 2021	Bourse DGA
Guillaume Didier	Sep 2019 to Aug 2022	IA DGA
Olivier Gimenez	Oct 2019 to Sep 2022	CIFRE with Orange Labs
Diane Leblanc-Albarel	Oct 2020 to Sep 2023	CNRS grant
Solène Moreau	Sep 2019 to Dec 2021	ERC POPSTAR (CNRS)
Gwendal Patat	Oct 2020 to Sep 2023	ministry grant
Thomas Rokicki	Oct 2019 to Sep 2022	ANR JCJC MIAOUS
Sadia Shamas	Feb 2021 to Jan 2024	ministry grant INSA
Antonin Voyez	June 2020 to June 2023	CIFRE grant with ENEDIS

Antonin Voyez is also member of the LACODAM team, and therefore his activities regarding the year 2021 are described in the LACODAM activity report.

Associate members

Antoine Dallon	Sep 2019 to Aug 2022	DGA-MI
Cyrille Wiedling	Sep 2019 to Aug 2022	DGA-MI

Administrative assistant

Aurélie Patier

2 Overall objectives

2.1 Overview

As reflected by the media, cybersecurity and especially cyberattacks, has become an important concern for professionals, politicians, as well as simple citizens. The growing importance of cybersecurity comes from the fact that nowadays all our activities rely on computing systems. This includes laptops, smartphones, and more generally many devices we are using in our daily life which are continuously connected to the Internet. To secure our communication and provide us with a secure way to access online services, **cryptographic protocols** have been developed and deployed. Designing cryptographic protocols is a highly error-prone task and these protocols are in constant evolution to face new applications. These protocols might fail because of mistakes in the specification itself, or some security issues may be introduced in their implementation. For instance, the long awaited 802.11 Wi-Fi Protected Access 3 (WPA-3), which has been released recently in order to replace WPA-2, suffers from vulnerabilities within both the protocol specification and implementation [VR20,BFS20]. Anomalies and shortcomings have also been discovered in some well-known standards such as Transport Layer Security (TLS) [BZD+16,BL16,CJ19].

Nowdays, we also live with the risk of leaking our personal data, and this risk needs to be mitigated. The recent adoption of the General Data Protection Regulation makes **privacy** a first-class citizen, and has to be considered along with security. To mitigate the issues mentioned above both in term of security and privacy, we can perform risk analysis, and we also propose to rely on **formal methods** with mathematical foundations to perform a rigorous analysis of a given protocol, or to allow the analysis of classes of protocols through the development of verification techniques and tools. In both cases, we advocate for the need of improving informal reasoning and manual proofs with the development of rigorous methods in order to systematically analyse the systems we are using in our daily life.

2.2 Scientific foundations

The research activities of Spicy are organized along three axes that are not disjoint, namely cryptographic protocols, privacy, and formal methods for security. We summarize the activities of each member of the Spicy in the table below.

[VR20] M. Vanhoef, E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd", *in : IEEE Symposium on Security and Privacy*, IEEE, p. 517–533, 2020.

[BFS20] D. D. A. Braga, P. Fouque, M. Sabt, "Dragonblood is Still Leaking: Practical Cache-based Side-Channel in the Wild", *in : ACSAC*, ACM, 2020.

[BZD+16] H. Böck, A. Zauner, S. Devlin, J. Somorovsky, P. Jovanovic, "Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS", *IACR Cryptol. ePrint Arch. 2016*, 2016, p. 475.

[BL16] K. Bhargavan, G. Leurent, "On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN", *in : ACM Conference on Computer and Communications Security*, ACM, p. 456–467, 2016.

[CJ19] C. Cremers, D. Jackson, "Prime, Order Please! Revisiting Small Subgroup and Invalid Curve Attacks on Protocols using Diffie-Hellman", *in : CSF*, IEEE, p. 78–93, 2019.

	Protocols	Privacy	Formal methods
Tristan Allard	⋆⋆	⋆⋆⋆	
Gildas Avoine	⋆⋆⋆	⋆⋆	
David Baelde	⋆	⋆	⋆⋆⋆
Stéphanie Delaune	⋆	⋆	⋆⋆⋆
Barbara Fila	⋆		⋆⋆⋆
Joseph Lallemand	⋆	⋆⋆	⋆⋆⋆
Mohamed Sabt	⋆⋆⋆		⋆

2.2.1 Axis 1: Cryptographic protocols

Spicy works on various topics related to cryptographic protocols, whatever the goal of the considered protocols, including design, cryptanalysis, and security proofs. We so consider ad hoc proofs in the computational model, but we also work on the development of generic methods and tools to mechanize and automate security proofs (see also Research Axis 3). Our protocol design activities is twofold, focusing on both low-ressource devices and privacy-related protocols. We also analyze many everyday-life protocols to identify their weaknesses. Our findings are in general twofold. First, we can find flaws in the design and sometimes we also demonstrate the feasibility of these attacks by implementing them. Second, we propose fixes to mitigate the discovered flaws. A final research direction in this part is to introduce original methodologies and techniques to perform generic attacks against real-life protocols.

2.2.2 Axis 2: Privacy

Privacy is becoming an important concern. In the Spicy team, as for cryptographic protocols, we are considering two directions: we can take the point of view of the attacker with the aim of establishing that a system or a set of data is not anonymous as claimed, but we also work on proposing new techniques to make existing systems privacy-compliant.

2.2.3 Axis 3: Formal methods

As we have seen, security protocols are often attacked. We therefore believe that it is necessary to design techniques to ensure that the security protocols we are using are safe, and to develop methods to evaluate and mitigate the risks. Many protocols once believed to be secure (relying, for instance, on informal security arguments or manual proofs) have been found to be flawed when formally modeled and analyzed. Spicy consequently considers formal methods for security as an important research goal.

2.3 Application domains

Spicy's work on design and cryptanalysis of cryptographic protocols also pass through attacks on real-life protocols, including LoRaWAN 1.0, SCP02, SCP10, 5G, WPA3 Dragonfly, FIDO U2F, WhatsApp, and ePassport's protocols. Such contributions aim at

advancing our knowledge on the analysis of protocols, to participate to the development of standards, and to make industrial aware of vulnerabilities in their security solutions.

3 Scientific achievements

3.1 PAKE Protocols in the Wild

Participants: Mohamed Sabt, Daniel De Almeida Braga.

*Joint work with Pierre-Alain Fouque (*Capsule*).*

Passwords are very popular on the web. However, most existing password-based authentication mechanisms can seriously be compromised by phishing attacks, server breaches and dictionary attacks. A better approach to rely on passwords for authentication is to leverage Password-Authenticated Key Exchange (PAKE) protocols. In its simplest form, a PAKE protocol allows two parties sharing nothing but a password) to establish a secure session. The security properties guaranteed by PAKEs make them appealing for numerous industrial solutions.

SRP is arguably the most widely used PAKE. It draws its popularity from its patent-free definition and the availability of efficient open-source implementations. In [5], we show that numerous SRP implementations do not resist against offline dictionary attacks. Indeed, we first identify some leakage vector in the client side of the OpenSSL SRP. Then, we exploit this leakage through micro-architectural cache-based attacks. We simplify the execution of our exploit by automating the whole process, including spying on executed instructions, interpreting the noisy cache measurements, and recovering the used password. Finally, we show how our attack concerns widely deployed solutions, such as Proton Mail and Apple Homekit. For each project, we point out the vulnerable component and the overall security implication of the attack. We also notified the impacted projects, and help in the patch process. Seven patches have been released following our work. Finally, we implement a Proof of Concept (PoC) on different projects [1]. We hope that these contributions raise awareness concerning the need of (formally verified) constant-time algorithms and implementations that do not rely on savvy developers to provide secure implementations.

3.2 Detecting Internet Traffic Hijacking

Participants: Gildas Avoine, Olivier Gimenez.

Joint work with Jacques Traoré (Orange Labs, Caen) and Ghada Arfaoui (Ornge Labs, Rennes)

We work on detecting Internet traffic hijacking, In 2021, we proposed a two-party cryptographic protocol [2] for detecting traffic hijacking over the Internet. Our proposal relies on a distance-bounding mechanism that measures the round-trip time of packets to decide whether an attack is ongoing. The protocol requires only two cryptographic operations per execution which leads to very few additional workload for the users. We

[1] https://gitlab.inria.fr/ddealmei/poc-openssl-srp

demonstrated the efficiency of the protocol using large-scale experiments and we discuss the choice of the decision function w.r.t. the false positive and negative cases. We now performe large-scale experiments.

3.3 Computational proofs of security protocols

Participants: David Baelde, Stéphanie Delaune, and Solène Moreau.

Joint work with Charlie Jacomme (CISPA, Germany), Adrien Koutsos (Inria Paris).

Given the central importance of designing secure protocols, providing solid mathematical foundations and computer-assisted methods to attest for their correctness is becoming crucial. Here, we elaborate on the formal approach introduced by Bana and Comon, which was originally designed to analyze protocols for a fixed number of sessions, and lacks support for proof mechanization. We propose a framework and an interactive prover allowing to mechanize proofs of security protocols for an arbitrary number of sessions in the computational model. We have implemented our approach within a new interactive prover, **the SQUIRREL prover**, taking as input protocols specified in the applied pi-calculus, and we have performed a number of case studies covering a variety of primitives (hashes, encryption, signatures, Diffie-Hellman exponentiation) and security properties (authentication, strong secrecy, unlinkability). This result has been published at S&P'21 [4]. We are working on an extension of this framework to handle protocols with mutable states (key updates, counters, *etc*).

3.4 Symbolic verification of cryptographic protocol implementations

Participants: Joseph Lallemand.

Joint work with David Basin, Peter Mueller, Christoph Sprenger, Linard Arquint, Felix Wolf (ETH Zürich)

Symbolic analysis of security protocols has lead to the creation of powerful automated tools to verify protocols, such as ProVerif or Tamarin. This automation however comes at the cost of a high abstraction level: the protocol verified is a very abstract model of the actual code that will be executed.

We propose a framework to bridge symbolic protocol verification and concrete implementation proofs at the code level. This way, we can establish code-level security guarantees while retaining the automation and comfort provided by symbolic protocol verifiers. More precisely, starting from a Tamarin model of a protocol, we extract a concrete specification, against which we then verify the protocol's implementation. That specification is expressed in separation logic, which is supported by many code verifiers, providing flexibility regarding the target implementation language. We prove the soundness of our approach, i.e. that it guarantees the implementation inherits the security properties proved on the abstract model. We also apply it to the Wireguard protocol (a widely deployed VPN system) to illustrate its generality. This work is under submission.

3.5 Decidability results regarding symbolic verification

Participants: Stéphanie Delaune, Antoine Dallon.

Joint work with Véronique Cortier (LORIA, Nancy), Vaishnavi Sundararajan (mostly done when she was post-doc in the Emsec *team from Nov 2018 to Nov 2019).*

We identify **a new decidable class of security protocols**, both for reachability and privacy-type properties. Our result holds for an unbounded number of sessions and for protocols with nonces. It covers all standard cryptographic primitives. Our class sets up three main assumptions. *(i)* Protocols need to be "simple", meaning that an attacker can precisely identify from which participant and which session a message originates from. We also consider protocols with no else branches (only positive test). *(ii)* Protocols should be type-compliant, which is intuitively guaranteed as soon as two encrypted messages of the protocol cannot be confused. *(iii)* Finally, we define the notion of a dependency graph, which, given a protocol, characterises how actions depend on the other ones (both sequential dependencies and data dependencies are taken into account). Whenever the graph is acyclic, then the protocol falls into our class. We show that many protocols of the literature belong to our decidable class, including for example some of the protocols embedded in the biometric passport. This result has been published in the journal JAR [1]. We are working on an extension of this work with the aim of providing a small bound on the number of sessions that need to be considered to detect an attack. As a consequence, tools for a bounded number of sessions could then be used to conclude that a protocol is secure for an unbounded number of sessions.

3.6 Formal modeling of security ceremonies

Participants: Barbara Fila, Sadia Shamas.

Joint work with Saša Radomirović (HWU, Scotland)

The classical security protocols are only interested in the exchange of cryptographic messages between communicating agents being it hardware (computers, servers, etc.) or software (processes, etc.). Such an approach is insufficient to capture problems resulting from human weaknesses (e.g., forgetting) or side channel investigation. In order to analyze the security protocols in a broader sense, we extend them to *security ceremonies* capturing not only the digital part of an exchange but also its entire physical and environmental context. In ceremonies, the notion of agents is extended with humans, and the communication can span over a variety of channels including physical, audio, visual, digital ones. The objects exchanged are no longer limited to cryptographic bistrings. The agents can transmit information, physical objects, emotions, etc.

We are currently working on formal model of security ceremonies. The objective is to find a suitable syntax to express them and then equip it with a semantics. Our ultimate goal is to devise a verification method for security ceremonies which we plan to automate with the help of the Tamarin tool. The main challenge lies in the modeling of the human behavior which might be non-deterministic and influenced by a number of internal and external factors, such as emotions, environment, political situation, etc.

3.7 Cryptanalytic Time-memory Trade-off

Participants: Gildas Avoine, Diane Leblanc-Albarel.

Joint work with Xavier Carpent (University of Nottingham, UK)

Cryptanalytic time-memory trade-offs (TMTOs) are techniques commonly used in computer security e.g., to crack passwords. However, TMTOs usually encounter in practice a bottleneck that is the time needed to perform the precomputation phase (preceding to the attack). We aim to improve this phase. In particular, in 2021, we introduced a technique, called distributed filtration-computation [3], that significantly reduces the precomputation time without any negative impact the online phase. Experiments performed on large problems with a 128-core computer perfectly match the theoretical expectations. We constructed a rainbow table for a space in approximately 8 hours instead of 50 hours for the usual way to generate a table. We also show that the efficiency of our technique is very close from the theoretical time lower bound. In order to still improve the precomputation phase, we now work on a new shape of tables.

3.8 Microarchitectural security

Participants: Guillaume Didier, Thomas Rokicki.

Joint work with Clémentine Maurice (Univ Lille), Pierre Laperdrix (Univ Lille)

We worked on several aspects of microarchitectural security. First, we underlined the role of the CPU Interconnect and the cache coherence in cache attacks and demonstrate that a better model of this component allows to improve the Flush+Flush attack [8]. Second, we focused on timing attacks in browsers, and in particular we studied the impact of the changes that were made to JavaScript timers [9]. We found out that, while the isolation recently provided by browsers is able to thwart some classes of attacks (e.g., some speculative execution attacks), browsers are in fact more vulnerable to hardware contention-based timing attacks now that they were a few years ago.

3.9 Cryptanalysis

Participants: Stéphanie Delaune.

*Joint work with Patrick Derbez (*Capsule*), Arthur Gontier (*Capsule*), Paul Huynh & Marine Minier (LORIA, Nancy), Victor Mollimard (*Capsule*), Charles Prud'homme (IMT Atlantique, Nantes).*

We aim at studying the resistance of block and stream ciphers through the development of new methods for automatically searching specific types of attacks or distinguishers.

We evaluate the resistance of ciphers against **differential cryptanalysis**. In particular, we propose automatic tools to find the best differential characteristics on the SKINNY block cipher. Notably, for SKINNY-128 in the SK model and for 13 rounds, we retrieve the results of Abdelkhalek et al. within a few seconds (to compare with 16 days) and we provide, for the first time, the best differential related-tweakey character-

istics up to 14 rounds for the TK1 model. We also obtain new results regarding the TK2 and the TK3 models. These results have been published at ACNS'21 [7].

We also consider **cube attack** which is a powerful cryptanalysis technique against symmetric primitives, especially for stream ciphers. One of the key step in a cube attack is recovering the superpoly. We propose a new model to recover the exact superpoly of a stream cipher given a cube. We propose two implementations of our model, one in MILP and one in CP, which are up to 10 times faster than the original division property-based model from Hao et al. (EuroCrypt'20), and consistently 30 to 60 times faster than the monomial prediction-based model from Hu et al (AsiaCrypt'20). This result has been accepted for publication at SAC'21 [6].

4 Software development

4.1 Squirrel

The Squirrel prover is a proof assistant for protocols. It is based on first-order logic and provides guarantees in the computational model. All the information regarding this development is available here:

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

In a nutshell, this tool is written in OCaml (about 10 000 lines of codes). Squirrel is an interactive prover for protocol verification:

- the user specifies a protocol in an input language (a variant of the applied pi-calculus) and some reachability or equivalence security goals;
- then, the user interacts with the prover by calling tactics, corresponding to inference rules, in order to verify the security properties;
- some automated reasoning is applied at each step.

The tool can be used in an interactive mode in Emacs using ProofGeneral. The two engineers, Clément Hérouard and Le Thanh Dung (Tito) Nguyen, who have been hired on the POPSTAR ERC project, are contributing to the development of this proof assistant. Figure 1 shows a screenshot of the tool with the specification of a protocol as well as an authentication goal on the left, and the proof can be seen on the right.

4.2 Bowtie++

Bowtie++ is a web-based application to perform risk analysis using bowtie diagrams. Bowtie diagrams are a graphical way of representing an unwanted event together with its causes end consequences. An example of a generic bowtie diagram is given in Figure 2.

Bowtie++ is developed jointly by SINTEF Norway (`https://www.sintef.no/en/`) and students at INSA Rennes supervised by Barbara Fila. The main functionalities of Bowtie++ include

- drawing of bowtie diagrams,

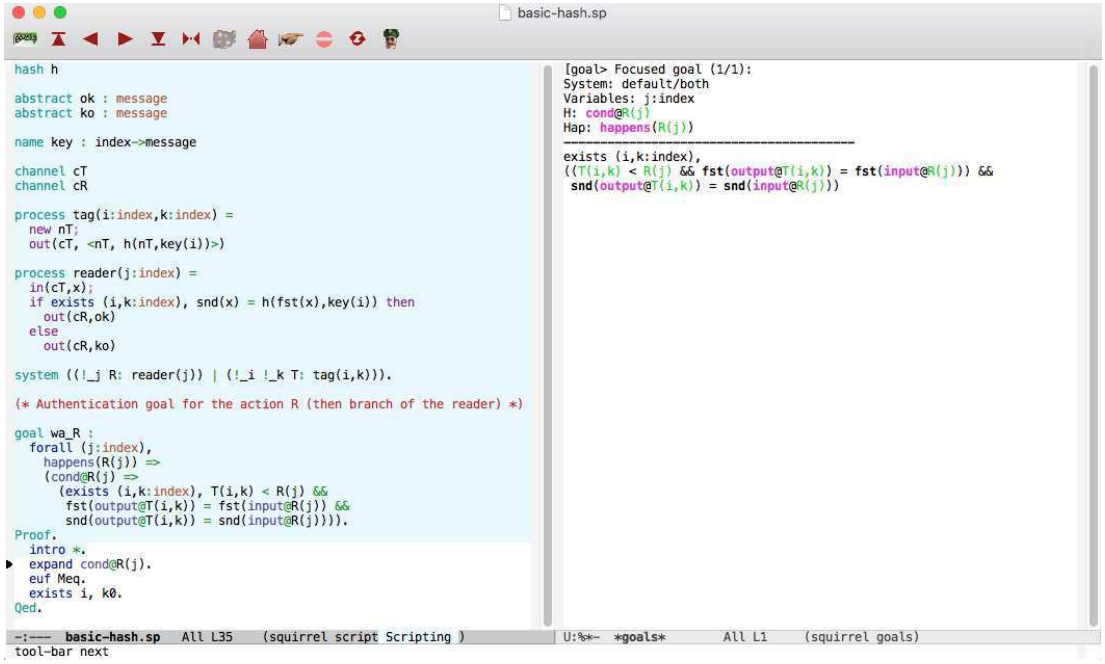

Figure 1: Screenshot of the Squirrel tool

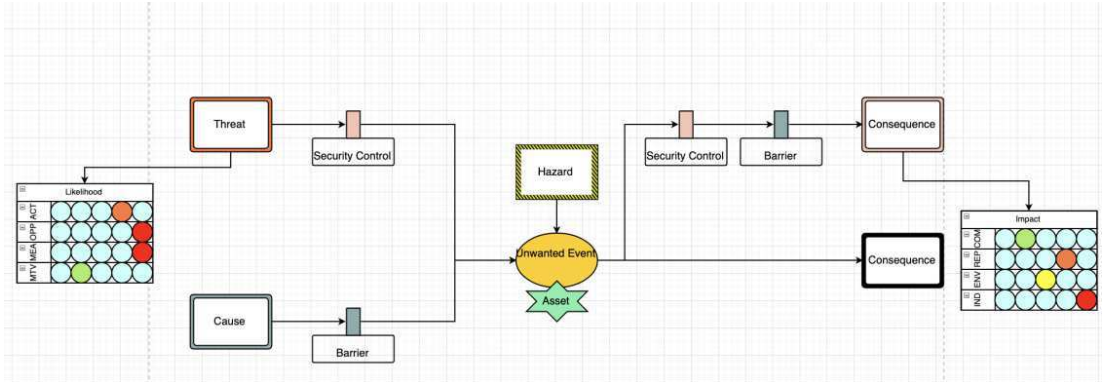

Figure 2: A generic bowtie diagram

- quantitative risk analysis using bowtie diagrams,
- sharing of bowtie diagrams.

Further information regarding Bowtie++ is available at `https://github.com/INSA-SINTEF/BowtiePlusPlus`.

5 Contracts and collaborations

5.1 ERC POPSTAR

Participants: David Baelde, Stéphanie Delaune, Clément Hérouard, Joseph Lallemand, Le Thanh Dung (Tito) Nguyen, Solène Moreau.

- Project type: H2020 ERC
- Dates: 02/17 - 07/22
- PI: Stéphanie Delaune (CNRS)
- Budget: 1 500 000 EUR
- URL: `https://popstar.irisa.fr`

Description. The main objective of the POPSTAR project is to develop foundations and practical tools to analyze modern security protocols that establish and rely on physical properties. The POPSTAR project will significantly advance the use of formal verification to contribute to the security analysis of protocols that rely on physical properties. This project is bold and ambitious, and answers the forthcoming expectation from consumers and citizens for high level of trust and confidence about contactless nomadic devices.

5.2 ANR TECAP

Participants: David Baelde, Stéphanie Delaune, Joseph Lallemand, Solène Moreau.

- Project type: ANR
- Dates: 01/2018 - 06/2022
- PI: Vincent Cheval (LORIA)
- PI local: Stéphanie Delaune (CNRS)
- Budget Spicy: About 15 000 EUR
- URL: `http://anr17-tecap.gforge.inria.fr/`

Description. Formal methods have been shown successful in proving security of cryptographic protocols and finding flaws. However manually proving the security of cryptographic protocols is hard and error-prone. Hence, a large variety of automated verification tools have been developed to prove or find attacks on protocols. These tools differ in their scope, degree of automation and attacker models. Despite the large number of automated verification tools, several cryptographic protocols still represent a real challenge for these tools and reveal their limitations. The aim of this project is to get the best of all these tools, meaning, on the one hand, to improve the theory and implementations of each individual tool towards the strengths of the others and, on the other hand, build bridges that allow the cooperations of the methods/tools.

5.3 ANR Decrypt

Participants: Stéphanie Delaune.

- Project type: ANR
- Dates: 2018 - 2022
- PI: Marine Minier (LORIA)
- PI local: Patrick Derbez (MdC UR1 -Capsule team)
- URL: `https://limos.fr/news_project/56`

Description. The objective of the Decrypt project is to facilitate the design of symmetric encryption primitives by proposing tools that allow cryptographers to:

1. facilitate the modelling of combinatorial problems underlying symmetric primitives;
2. efficiently solve these problems using constraint solvers that scale better than dedicated approaches;
3. provide guarantees on the solutions produced by the solvers;
4. give explanations of the results obtained.

5.4 Rennes Métropole

Participants: Mohamed Sabt, Gwendal Patat.

- Project type: Materials Funding
- Dates: 12/2021 - 12/2023
- PI: Mohamed Sabt (UR1)
- Budget: About 22 000 EUR

Description. The goal of this funding is to support Spicy that requires to implement their identified vulnerabilities on recent devices, including smart cards and smartphones. Moreover, the project also allows the team to acquire some professional reverse engineering license.

5.5 Grant CIFRE Orange Labs

Participants: Olivier Gimenez.

Description. The objective of this collaborative work is to design solutions to detect traffic diversion in 5G networks. The expected solution is based on the round-trip time of cryptographic messages exchanged over the network. Abnormal behaviors can so be detected using a statistical approach.

5.6 CNRS Grant - accompagnement jeunes chercheurs

Participants: Joseph Lallemand.

- Date: 01/2021 - 12/2021
- PI: Joseph Lallemand (CNRS)

- Budget: 10 000 EUR

Description. The CNRS supports newly recruited researchers to facilitate their integration into their host laboratory and to enable them to start their research activities on the basis of the research project they submitted to the CNRS competition.

6 Dissemination

6.1 Promoting scientific activities

6.1.1 Scientific Events Organisation

- Stéphanie Delaune co-organized with Sébastien Bardin the Cyber in Saclay School (online event), February 2021. The school gathered about a hundred participants among which about forty participated to online practical sessions.
- Stéphanie Delaune participated to the organization of the annual meeting for the GT-MFS working group (online event) of the GdR Sécurité Informatique (about 100 participants).

6.1.2 Scientific Events Selection

- Stéphanie Delaune was PC member of the 28th ACM Conference on Computer and Communications Security (CCS), Seoul, South Korea, November 14-19, 2021.
- Stéphanie Delaune was PC member of the 36th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), Rome, Italy, 29 June -2 July 2021.
- Stéphanie Delaune was PC member of the 19th International Conference on Applied Cryptography and Network Security (ACNS), Kamakura, Japan, 21-24 June 2021.
- Barbara Fila was a PC member of the Security track at the ACM Symposium on Applied Computing (SEC@SAC), Gwangju, Korea, March 22–26, 2021.

6.1.3 Journal

- Stéphanie Delaune was in the editorial board of Information Processing Letters (IPL) from 2019 to 2021.
- Stéphanie Delaune is in the editorial board of the ACM Transactions on Computational Logic (TOCL), since 2018.
- Stéphanie Delaune is in the editorial board of the ACM Transactions on Privacy and Security (TOPS), since 2020.

6.1.4 Leadership within the Scientific Community

- Gildas Avoine was the head of the GdR Sécurité Informatique (2015–2021).
- Gildas Avoine is the president of the scientific council of ANSSI (2019–2022).
- Gildas Avoine is in charge for the CNRS of the 65-million EUR national scientific program PEPR Cybersécurité (since 2021)

- Gildas Avoine was a member of the French "Alliance Allistene" (working group Cybersecurity) (2016–2021)
- Stéphanie Delaune was member of the executive boad GdR Sécurité Informatique (2016–2021).
- Stéphanie Delaune was co-Head (with Sébastien Bardin) of the working group GT-MFS "Méthodes Formelles pour la Sécurité" from GdR Sécurité Informatique (2017-2021).
- Stéphanie Delaune is in the steering committee of the Programming Languages and Analysis for Security (PLAS) workshop, since 2018.
- Stéphanie Delaune is in the steering committee of the Computer Security Foundations Symposium (CSF), since 2017.
- Stéphanie Delaune is member of the scientific council GdR IM, since 2018.

6.1.5 Scientific Expertise

- Gildas Avoine was a committee member for the research program "Grands Défis Cybersécurité" funded by SGPI (PIA3), from 2019 to 2021.
- Stéphanie Delaune was a committee member for the FWO (the counterpart of the ANR in Belgium) in 2020 & 2021 (1-day meeting to evaluate and rank about 30 proposals).

6.1.6 Comités de sélection

- Barbara Fila was a member of the hiring committee for a professorship position at Télécom SudParis (Spring 2021).
- Barbara Fila was a member of the hiring committees for CDD LRU positions in Cyberdefense (section 27) at ENSIBS (Spring 2021).

6.1.7 Research Administration

- Gildas Avoine is the head of the computer science lab of INSA Rennes since 2021 (about 50 scientists, including 20 faculty members)
- Gildas Avoine is an elected member of the computer science department council at INSA Rennes (2017–2025)
- Gildas Avoine was an elected member of the computer science lab council at INSA Rennes (2017–2021)
- Stéphanie Delaune was elected member of the laboratory council at IRISA (2017–2021).
- Stéphanie Delaune is member of the executive board of the EUR CyberSchool since its creation in 2020.
- Stéphanie Delaune is the head of the CyberSecurity axis at IRISA, since 2019.

6.2 Teaching, supervision

6.2.1 Teaching

For reseachers, all activities are given. For professors and assistant professors, only courses at the M. Sc. level are listed.

- Gildas Avoine lectures and is in charge of two 26-hour courses : Cryptography Engineering (M1 students, INSA Rennes) and Network Security (M1 students, INSA Rennes). He also co-lectures the network security course for the telecom department of INSA Rennes (M1 students).
- David Baelde is in charge of the training program preparing students for the French *agrégation d'informatique* at ENS Rennes, in which he also makes different kinds of interventions for a total volume of 42 hours eqTD.
- Barbara Fila co-lectures and is in charge of the 32-hour course "Languages and grammars" (4th-year students, INSA Rennes), the 26-hour course "Verification of security protocols" (5th-year students, INSA Rennes), and the 20-hour course "Security protocols" (5th-year students, Master SIF, University Rennes 1). She also is the administrative coordinator of the "Secure programing" course (4th-year students, INSA Rennes).
- Joseph Lallemand co-lectures the 26-hour course "Verification of security protocols" (5th-year students, INSA Rennes) and the 20-hour course "Security protocols" (M2 SIF, Univ Rennes 1).
- Mohamed Sabt lectures and is in charge of 40-hour course "System Security" (M1 students, Cyberschool, UR1), 48-hour course "Software Security" (M1 students, Cyberschool, UR1), and "Research Project" (M1 students, Cyberschool, UR1),

6.2.2 Supervision

- PhD: Solène Moreau, defended November 2021, supervised by David Baelde & Stéphanie Delaune
- PhD in progress: Louis Béziaud supervised by Tristan Allard & Sébastien Gambs
- PhD in progress: Daniel De Almeida Braga supervised by Pierre-Alain Fouque & Mohamed Sabt
- PhD in progress: Olivier Gimenez supervised by Gildas Avoine, Jacques Traoré,= & Ghada Arfaoui.
- PhD in progress: Arthur Gontier supervised by Stéphanie Delaune, Patrick Derbez & Charles Prud'homme
- PhD in progress: Diane Leblanc-Albarel supervised by Gildas Avoine
- PhD in progress: Gwendal Patat supervised by Pierre-Alain Fouque & Mohamed Sabt
- PhD in progress: Sadia Shamas supervised by Barbara Fila & Saša Radomirović
- PhD in progress: Antonin Voyez supervised by Tristan Allard, Gildas Avoine &Élisa Fromont.
- L3 Internship by Paul Robert (ENS Saclay), supervised by Stéphanie Delaune and Joseph Lallemand, Summer 2021.

Guillaume Didier and Thomas Rokicki are currently doing their PhD in the Spicy team. However, their advisor, Clémentine Maurice, is not anymore member of the Spicy team. She joined the Spirals group CRIStAL (Lille, France) last February.

6.2.3 Juries

- Katharina Boudgoust (PhD), Rennes, November 2021 (Stéphanie Delaune was "President")

- Marius Lombard-Platet (PhD), ENS Paris, September 2021 (Gildas Avoine was a reviewer)
- Adeline Roux-Langlois (HdR), Rennes, June 2021 (Stéphanie Delaune was "President")

6.3 Popularization

- Stéphanie Delaune wrote an article in the journal of the CNRS, *Between transparency and confidentiality, the challenges of electronic voting*, with Véronique Cortier, April 2021.

6.4 Awards

- The work about SRP [5] was highly appreciated by ProtonMail; The names of D. Braga, P. Fouque, and M. Sabt now appear in their Security Contributors[2].
- The work about Widevine in Android done by G. Patat and M. Sabt was awarded by the Hall of Fame of Google. In addition, it was published by the Android Security Bulletin[3]. This work is currently under submission.

7 Bibliography

Articles in referred journals and book chapters

[1] V. Cortier, S. Delaune, V. Sundararajan, "A Decidable Class of Security Protocols for Both Reachability and Equivalence Properties", *J. Autom. Reason. 65*, 4, 2021, p. 479–520.

Publications in Conferences and Workshops

[2] G. Arfaoui, G. Avoine, O. Gimenez, J. Traoré, "How Distance-Bounding Can Detect Internet Traffic Hijacking", *in : Cryptology and Network Security - 20th International Conference, CANS 2021, Vienna, Austria, December 13-15, 2021, Proceedings*, M. Conti, M. Stevens, S. Krenn (editors), *Lecture Notes in Computer Science*, *13099*, Springer, p. 355–371, 2021, https://doi.org/10.1007/978-3-030-92548-2_19.

[3] G. Avoine, X. Carpent, D. Leblanc-Albarel, "Precomputation for Rainbow Tables has Never Been so Fast", *in : Computer Security - ESORICS 2021 - 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4-8, 2021, Proceedings, Part II*, E. Bertino, H. Shulman, M. Waidner (editors), *Lecture Notes in Computer Science*, *12973*, Springer, p. 215–234, 2021, https://doi.org/10.1007/978-3-030-88428-4_11.

[4] D. Baelde, S. Delaune, C. Jacomme, A. Koutsos, S. Moreau, "An Interactive Prover for Protocol Verification in the Computational Model", *in : Proceedings of the 42nd IEEE Symposium on Security and Privacy (S&P'21)*, A. Oprea, T. Holz (editors), IEEE Computer Society Press, San Francisco, California, USA, May 2021.

[2] https://protonmail.com/blog/protonmail-security-contributors
[3] https://source.android.com/security/bulletin/2021-08-01#widevine

[5] D. D. A. Braga, P. Fouque, M. Sabt, "PARASITE: PAssword Recovery Attack against Srp Implementations in ThE wild", *in : CCS*, ACM, p. In press, 2021.

[6] S. Delaune, P. Derbez, A. Gontier, C. Prud'homme, "A Simpler Model for Recovering Superpoly on Trivium", *in : Proceedings of the 28th International Conference on Selected Areas in Cryptography (SAC'21)*, *Lecture Notes in Computer Science*, Springer, 2021.

[7] S. Delaune, P. Derbez, P. Huynh, M. Minier, V. Mollimard, C. Prud'homme, "Efficient Methods to Search for Best Differential Characteristics on SKINNY", *in : Proceedings of the 19th International Conference on Applied Cryptography and Network Security (ACNS'21)*, 2021.

[8] G. Didier, C. Maurice, "Calibration Done Right: Noiseless Flush+Flush Attacks", *in : Detection of Intrusions and Malware, and Vulnerability Assessment - 18th International Conference, DIMVA 2021, Virtual Event, July 14-16, 2021, Proceedings*, L. Bilge, L. Cavallaro, G. Pellegrino, N. Neves (editors), *Lecture Notes in Computer Science*, *12756*, Springer, p. 278–298, 2021, `https://doi.org/10.1007/978-3-030-80825-9\_14`.

[9] T. Rokicki, C. Maurice, P. Laperdrix, "SoK: In Search of Lost Time: A Review of JavaScript Timers in Browsers", *in : IEEE European Symposium on Security and Privacy, EuroS&P 2021, Vienna, Austria, September 6-10, 2021*, IEEE, p. 472–486, 2021, `https://doi.org/10.1109/EuroSP51992.2021.00039`.