IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2017

Project-Team PESTO

Proof techniques for security protocols

IN COLLABORATION WITH: Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

RESEARCH CENTER
Nancy - Grand Est

THEME
Security and Confidentiality

Table of contents

Project-Team PESTO

Creation of the Team: 2016 January 01, updated into Project-Team: 2016 November 01

Keywords:

Computer Science and Digital Science:

A2.4. - Verification, reliability, certification
A4.5. - Formal methods for security
A4.6. - Authentication
A4.8. - Privacy-enhancing technologies
A7.1. - Algorithms
A7.2. - Logic in Computer Science

Other Research Topics and Application Domains:

B6.3.2. - Network protocols
B6.3.4. - Social Networks
B6.6. - Embedded systems
B9.8. - Privacy

1. Personnel

Research Scientists

Vincent Cheval [Inria, Researcher]
Véronique Cortier [Deputy team leader, CNRS, Senior Researcher, HDR]
Steve Kremer [Team Leader, Inria, Senior Researcher, HDR]
Christophe Ringeissen [Inria, Researcher, HDR]
Michaël Rusinowitch [Inria, Senior Researcher, HDR]
Mathieu Turuani [Inria, Researcher]

Faculty Members

Jannik Dreier [Univ Lorraine, Associate Professor]
Abdessamad Imine [Univ Lorraine, Associate Professor, HDR]
Laurent Vigneron [Univ Lorraine, Professor, HDR]

Post-Doctoral Fellows

Sergiu Bursuc [Inria, ERC Spooc, from Feb 2017]
Sourya Joyee de [Inria, Fondation MAIF, from Mar 2017]
Constantin-Catalin Dragan [Inria, ERC Spooc]
Ivan Gazeau [Inria, ERC Spooc]

PhD Students

Younes Abid [Univ Lorraine, Fondation MAIF]
Haftay Gebreslasie Abreha [Cifre Cynapsys, coadvised by Madynes, from Sep 2017]
Antoine Dallon [ENS Cachan & LORIA, DGA funding]
Alicia Filipiak [Cifre Orange]
Charlie Jacomme [ENS Cachan, from Sep 2017]
Joseph Lallemand [Univ Lorraine, ERC Spooc]
Itsaka Rakotonirina [Univ Lorraine, ERC Spooc, from Oct 2017]
Ludovic Robin [Univ Lorraine, until Sep 2017]

Interns

Parag Bansal [Inria, from May 2017 until Jul 2017]
Hector Dang-Nhu [Ecole Normale Supérieure Paris, from Jun 2017 until Jul 2017]
Dibyendu Das [Inria, from Oct 2017 until Nov 2017]
Andrii Dychka [Univ Lorraine, from Jun 2017 until Aug 2017]
Sreekar Garlapati [Inria, from May 2017 until Jul 2017]
Valentin Salquebre [Univ Lorraine, from Aug 2017 until Sep 2017]

Administrative Assistants

Emmanuelle Deschamps [Inria]
Christelle Levêque [Univ Lorraine]

Visiting Scientist

Walid Belkhir [Univ Franche-Comté, from Feb 2017 until Jul 2017]

2. Overall Objectives

2.1. Context

The rise of the Internet and the ubiquity of electronic devices have changed our way of life. Many face to face and paper transactions have nowadays digital counterparts: home banking, electronic commerce, e-voting, ... and even partially our social life. This digitalisation of the world comes with tremendous risks for our security and privacy as illustrated by the following examples.

Financial transactions. According to the FEVAD (French federation of remote selling and e-commerce), in France 51.1 billion Euros have been spent through e-commerce in 2013 and fraud is estimated to 1.9 billion Euros by certissim. [1] As discussed in another white paper [2] by Dave Marcus (Director of Advanced Research and Threat Intelligence, McAfee) and Ryan Sherstobitoff (Threat Researcher, Guardian Analytics) bank fraud has changed dramatically. Fraudsters are aiming to steal increasingly higher amounts from bank accounts (with single transfers over 50,000 Euros) and develop fully automated attack tools to do so. As a consequence, protocols need to implement more advanced, multi-factor authentication methods.

Electronic voting. In the last few years several European countries (Estonia, France, Norway and Switzerland) organised *legally binding political elections* that allowed (part of the) voters to cast their votes remotely via the Internet. For example, in June 2012 French people living abroad ("expats") were allowed to vote via the Internet for parliament elections. An engineer demonstrated that it was possible to write a malware that could change the value of a cast vote without any way for the voter to notice. [3] In Estonia in the 2011 parliament election, a similar attack was reported by computer scientist Paavo Pihelgas who conducted a real life experiment with aware consenting test subjects. [4]

Privacy violations. Another security threat is the violation of an individual person's privacy. For instance the use of Radio-frequency identification (RFID) technology can be used to trace persons, e.g. in automatic toll-paying devices [5] or in public transportation. Even though security protocols are deployed to avoid tracing by third parties, protocol design errors enabled tracing of European e-passports. [6] Recently, a flaw was identified in the 3G mobile phone protocols that allows a third party, i.e., not only the operator, to trace telephones [43]. Also, anonymised data of social networks has been effectively used to identify persons by comparing data from several social networks. [7]

[1] Livre Blanc : La fraude dans le e-commerce, certissim.
[2] Dissecting Operation High Roller. https://en.wikipedia.org/wiki/Operation_High_Roller
[3] A video explaining the attack is available at http://www.youtube.com/watch?v=AsvLxY478xc
[4] The Supreme Court dismissed an electoral complaint regarding e-voting security. http://www.nc.ee/?id=1235
[5] A Pass on Privacy? The New York Times, July 17, 2005. http://www.nytimes.com/2005/07/17/magazine/17WWLN.html
[6] Defects in e-passports allow real-time tracking. The Register, January 26, 2010. http://www.theregister.co.uk/2010/01/26/epassport_rfid_weakness/
[7] Social sites dent privacy efforts. BBC, March 27, 2009. http://news.bbc.co.uk/2/hi/technology/7967648.stm

2.2. Objectives

The aim of the Pesto project is to build formal models and techniques, for computer-aided analysis and design of security protocols (in a broad sense). While historically the main goals of protocols were confidentiality and authentication the situation has changed. E-voting protocols need to guarantee privacy of votes, while ensuring transparency of the election; electronic devices communicate data by the means of web services; RFID and mobile phone protocols have to guarantee that people cannot be traced. Due to malware, security protocols need to rely on additional mechanisms, such as trusted hardware components or multi-factor authentication, to guarantee security even if the computing platform is a priori untrusted. Current existing techniques and tools are however unable to analyse the properties required by these new protocols and take into account the newly deployed mechanisms and associated attacker models.

3. Research Program

3.1. Modelling

Before being able to analyse and properly design security protocols, it is essential to have a model with a precise semantics of the protocols themselves, the attacker and its capabilities, as well as the properties a protocol needs to ensure.

Most current languages for protocol specification are quite basic and do not provide support for global state, loops, or complex data structures such as lists, or Merkle trees. As an example we may cite Hardware Security Modules that rely on a notion of *mutable global state* which does not arise in traditional protocols, see e.g. the discussion by Herzog [54].

Similarly, the properties a protocol should satisfy are generally not precisely defined, and stating the "right" definitions is often a challenging task in itself. In the case of authentication, many protocol attacks were due to the lack of a precise meaning, cf. [53]. While the case of authentication has been widely studied, the recent digitalisation of all kinds of transactions and services, introduces a plethora of new properties, including for instance anonymity in e-voting, untraceability of RFID tokens, verifiability of computations that are out-sourced, as well as sanitisation of data in social networks. We expect that many privacy anonymity properties may be modelled as particular observational equivalences in process calculi [49], or indistinguishability between cryptographic games [2], sanitisation of data may also rely on information-theoretic measures.

We also need to take into account that the attacker model changes. While historically the attacker was considered to control the communication network, we may nowadays argue that even (part of) the host executing the software may be compromised through, e.g., malware. This situation motivates the use of secure elements and multi-factor authentication with out-of-band channels. A typical example occurs in e-commerce: to validate an online payment a user needs to enter an additional code sent by the bank via sms to the user's mobile phone. Such protocols require the possession of a physical device in addition to the knowledge of a password which could have been leaked on an untrusted platform. The fact that data needs to be copied by a human requires these data to be *short*, and hence amenable to brute-force attacks by an attacker or guessing.

3.2. Analysis

3.2.1. Generic proof techniques

Most automated tools for verifying security properties rely on techniques stemming from automated deduction. Often existing techniques do however not apply directly, or do not scale up due to the state explosion problems. For instance, the use of Horn clause resolution techniques requires dedicated resolution methods [44][3]. Another example is unification modulo equational theory, which is a key technique in several tools, e.g. [52]. Security protocols, however require to consider particular equational theories that are not naturally studied in classical automated reasoning. Sometimes, even new concepts have been introduced. One example is the finite variant property [47], which is used in several tools, e.g., *Akiss* [3], Maude-NPA [52] and Tamarin [55].

Another example is the notion of asymmetric unification [51] which is a variant of unification used in Maude-NPA to perform important *syntactic* pruning techniques of the search space, even when reasoning modulo an equational theory. For each of these topics we need to design efficient decision procedures for a variety of equational theories.

3.2.2. Dedicated procedures and tools

We design dedicated techniques for automated protocol verification. While existing techniques for security protocol verification are efficient and have reached maturity for verification of confidentiality and authentication properties (or more generally safety properties), our goal is to go beyond these properties and the standard attacker models, verifying the properties and attacker models identified in Section 3.1. This includes techniques that:

- can analyse *indistinguishability* properties, including for instance anonymity and unlinkability properties, but also properties stated in simulation-based (also known as universally composable) frameworks, which express the security of a protocol as an ideal (correct by design) system;
- take into account protocols that rely on *mutable global state* which does not arise in traditional protocols, but is essential when verifying tamper-resistant hardware devices, e.g., the RSA PKCS#11 standard, IBM's CCA and the trusted platform module (TPM);
- consider attacker models for protocols relying on *weak secrets* that need to be copied or remembered by a human, such as multi-factor authentication.

These goals are beyond the scope of most current analysis tools and require both theoretical advances in the area of verification, as well as the design of new efficient verification tools.

3.3. Design

Given our experience in formal analysis of security protocols, including both protocol proofs and findings of flaws, it is tempting to use our experience to design protocols with security in mind and security proofs. This part includes both provably secure design techniques, as well as the development of new protocols.

3.3.1. General design techniques

Design techniques include *composition results* that allow one to design protocols in a modular way [48], [46]. Composition results come in many flavours: they may allow one to compose protocols with different objectives, e.g. compose a key exchange protocol with a protocol that requires a shared key or rely on a protocol for secure channel establishment, compose different protocols in parallel that may re-use some key material, or compose different sessions of a same protocol.

Another area where composition is of particular importance is Service Oriented Computing, where an "orchestrator" must combine some available component services, while guaranteeing some security properties. In this context, we work on the automated synthesis of the orchestrator or monitors for enforcing the security goals. These problems require to study new classes of automata that communicate with structured messages.

3.3.2. New protocol design

We also design new protocols. Application areas that seem of particular importance are:

- External hardware devices such as security APIs that allow for flexible key management, including key revocation, and their integration in security protocols. The security *fiasco* of the PKCS#11 standard [45], [50] witnesses the need for new protocols in this area.
- Election systems that provide strong security guarantees. We already work (in collaboration with the Caramba team) on a prototype implementation of an e-voting system, Belenios (http://belenios.gforge.inria.fr).
- Mechanisms for publishing personal information (e.g. on social networks) in a controlled way.

4. Application Domains

4.1. Formal methods for cryptographic protocols

Security protocols, such as TLS, Kerberos or ssh, are the main tool for securing our communications. The aim of our work is to propose models that are expressive enough to formally represent protocol executions in the presence of an adversary, formal definitions of the security properties to be satisfied by these protocols, and design automated tools able to analyse them and possibly exhibit design flaws.

4.2. Automated reasoning

Many techniques for symbolic verification of security are rooted in automated reasoning. A typical example is equational reasoning used to model the algebraic properties of a cryptographic primitive. Our work therefore aims to improve and adapt existing techniques or propose new ones when needed for reasoning about security.

4.3. Electronic voting

Electronic elections have in the last years been used in several countries for politically binding elections. The use in professional elections is even more widespread. The aim of our work is to increase our understanding of the security properties needed for secure elections, propose techniques for analysing e-voting protocols, design of state-of-the-art voting protocols, but also to highlight the limitations of e-voting solutions.

4.4. Privacy in social networks

Treatment of information released by users on social networks can violate a user's privacy. The goal of our work is to allow one a controlled information release while guaranteeing a user's privacy.

5. Highlights of the Year

5.1. Highlights of the Year

The paper [3] is listed in ACM Computing Reviews' 21st Annual Best of Computing list of notable books and articles [8] for 2016.

The voting system Belenios, developed in the Pesto and Caramba teams, has served as a basis of the development of two industrial systems (Docapost and Orange).

A 4-year ANR project on *Protocol Analysis — Combining Existing Tools* (TECAP) has been accepted. It will start in 2018 with Vincent Cheval as project leader.

6. New Software and Platforms

6.1. Akiss

AKISS: Active Knowledge in Security Protocols
KEYWORDS: Security - Verification

[8] http://www.computingreviews.com

FUNCTIONAL DESCRIPTION: Akiss (Active Knowledge in Security Protocols) is a tool for verifying indistinguishability properties in cryptographic protocols, modelled as trace equivalence in a process calculus. Indistinguishability is used to model a variety of properties including anonymity properties, strong versions of confidentiality and resistance against offline guessing attacks, etc. Akiss implements a procedure to verify equivalence properties for a bounded number of sessions based on a fully abstract modelling of the traces of a bounded number of sessions of the protocols into first-order Horn clauses and a dedicated resolution procedure. The procedure can handle a large set of cryptographic primitives, namely those that can be modeled by an optimally reducing convergent rewrite system.

- Contact: Steve Kremer
- URL: https://github.com/akiss

6.2. Belenios

Belenios - Verifiable online voting system
KEYWORD: E-voting
FUNCTIONAL DESCRIPTION: Belenios is an online voting system that provides confidentiality and verifiability. End-to-end verifiablity relies on the fact that the ballot box is public (voters can check that their ballots have been received) and on the fact that the tally is publicly verifiable (anyone can recount the votes). Confidentiality relies on the encryption of the votes and the distribution of the decryption key.

Belenios builds upon Helios, a voting protocol used in several elections. The main design enhancement of Belenios vs Helios is that the ballot box can no longer add (fake) ballots, due to the use of credentials.

- Participants: Pierrick Gaudry, Stéphane Glondu and Véronique Cortier
- Partners: CNRS - Inria
- Contact: Stéphane Glondu
- URL: http://belenios.gforge.inria.fr/

6.3. CL-AtSe

Constraint Logic based Attack Searcher
KEYWORDS: Security - Verification - Web Services
FUNCTIONAL DESCRIPTION: CL-AtSe is a Constraint Logic based Attack Searcher for security protocols and services. The main idea in CL-AtSe consists in running the protocol or set of services in all possible ways by representing families of traces with positive or negative constraints on the intruder knowledge, on variable values, on sets, etc. Thus, each run of a service step consists in adding new constraints on the current intruder and environment state, reducing these constraints down to a normalized form for which satisfiability is easily decidable, and decide whether some security property has been violated up to this point.

- Participants: Mathieu Turuani and Tigran Avanesov
- Contact: Mathieu Turuani
- URL: https://cassis.loria.fr/wiki/Wiki.jsp?page=Cl-Atse

6.4. Deepsec

DEciding Equivalence Properties in SECurity protocols
KEYWORDS: Security - Verification

FUNCTIONAL DESCRIPTION: DeepSec (DEciding Equivalence Properties in SECurity protocols) is a tool for verifying indistinguishability properties in cryptographic protocols, modelled as trace equivalence in a process calculus. Indistinguishability is used to model a variety of properties including anonymity properties, strong versions of confidentiality and resistance against offline guessing attacks, etc. DeepSec implements a decision procedure to verify trace equivalence for a bounded number of sessions and cryptographic primitives modeled by a subterm convergent destructor rewrite system. The procedure is based on constraint solving techniques. Several new features are currently being developed including the possibility to verify labelled bisimilarity and session equivalence. Optimizations to improve efficiency and interface improvements are also under development.

- Contact: Vincent Cheval
- URL: https://github.com/DeepSec-prover/deepsec

6.5. Tamarin

TAMARIN prover
KEYWORDS: Security - Verification
FUNCTIONAL DESCRIPTION: The TAMARIN prover is a security protocol verification tool that supports both falsification and unbounded verification of security protocols specified as multiset rewriting systems with respect to (temporal) first-order properties and a message theory that models Diffie-Hellman exponentiation, bilinear pairing, multisets, and exclusive-or (XOR), combined with a user-defined convergent rewriting theory. Its main advantages are its ability to handle stateful protocols and its interactive proof mode. Moreover, it has recently been extended to verify equivalence properties. The tool is developed jointly by the PESTO team, the Institute of Information Security at ETH Zurich, and the University of Oxford. In a joint effort, the partners wrote and published a user manual in 2016, available from the Tamarin website.

- Contact: Jannik Dreier
- URL: http://tamarin-prover.github.io/

6.6. SAPIC

SAPIC: Stateful Applied Pi Calculus
KEYWORDS: Security - Verification
FUNCTIONAL DESCRIPTION: SAPIC is a tool that translates protocols from a high-level protocol description language akin to the applied pi-calculus into multiset rewrite rules, that can then be analysed using the TAMARIN prover. TAMARIN has also been extended with dedicated heuristics that exploit the form of translated rules and favor termination.

SAPIC offers support for the analysis of protocols that include states, for example Hardware Security Tokens communicating with a possibly malicious user, or protocols that rely on databases. It also allows us to verify liveness properties and a recent extension adds a notion of location and reporting used for modelling trusted execution environments. It has been successfully applied on several case studies including the Yubikey authentication protocol, and extensions of the PKCS#11 standard. SAPIC also includes support for verifying liveness properties, which are for instance important in fair exchange and contract signing protocols, as well as support for constructions useful when modelling isolated execution environments.

SAPIC has been integrated as a plugin in TAMARIN and is now part of the TAMARIN distribution.

- Contact: Steve Kremer
- URL: http://sapic.gforge.inria.fr/

6.7. TypeEquiv

A type checker for privacy properties
KEYWORDS: Security - Cryptographic protocol - Privacy

FUNCTIONAL DESCRIPTION: TypeEquiv takes as input the specification of a pair of security protocols, written in a dialect of the applied-pi calculus, together with some type annotations. It checks whether the two protocols are in equivalence or not.

- Partner: Technische Universität Wien
- Contact: Véronique Cortier

7. New Results

7.1. Modelling

7.1.1. New protocol and adversary models

Participants: Jannik Dreier, Steve Kremer, Ludovic Robin.

Symbolic models for security protocol verification, following the seminal ideas of Dolev and Yao, come in many flavors, even though they share the same ideas. A common assumption is that the attacker has complete control over the network: he can therefore intercept any message. Depending on the precise model this may be reflected either by the fact that any protocol output is directly routed to the adversary, or communications may be among any two participants, including the attacker—the scheduling between which exact parties the communication happens is left to the attacker. These two models may seem equivalent at first glance and, depending on the verification tools, either one or the other semantics is implemented. In collaboration with Babel (IIT Bombay) we show that, unsurprisingly, they indeed coincide for reachability properties. However, when we consider equivalence properties, we prove that these two semantics are incomparable. We also introduce a new semantics, where internal communications are allowed but messages are always eavesdropped by the attacker. We show that this new semantics yields strictly stronger equivalence relations and identify two subclasses of protocols for which the three semantics coincide. These results were presented at POST'17 [16].

Isolated Execution Environments (IEEs), such as ARM TrustZone and Intel SGX, offer the possibility to execute sensitive code in isolation from other, potentially malicious programs, running on the same machine, or a potentially corrupted OS. A key feature of IEEs is the ability to produce reports binding cryptographically a message to the program that produced it, typically ensuring that this message is the result of the given program running on an IEE. In collaboration with Jacomme (ENS Cachan) and Scerri (Univ Bristol), Kremer presented a symbolic model for specifying and verifying applications that make use of such features. For this they introduced the SℓAPiC process calculus to reason about reports issued at given locations. They also provide tool support, extending the *SAPIC/TAMARIN* toolchain and demonstrate the applicability of their framework on several examples implementing secure outsourced computation (SOC), a secure licensing protocol and a one-time password protocol that all rely on such IEEs. This work has been published and presented at EuroS&P'17 [30].

Modern security protocols may involve humans in order to compare or copy short strings between different devices. Multi-factor authentication protocols, such as Google 2-factor or 3D-secure are typical examples of such protocols. However, such short strings may be subject to brute force attacks. In collaboration with Delaune (IRISA), we propose a symbolic model which includes attacker capabilities for both guessing short strings, and producing collisions when short strings result from an application of weak hash functions. We propose a new decision procedure for analysing (a bounded number of sessions of) protocols that rely on short strings. The procedure has been integrated in the *Akiss* tool and tested on protocols from the ISO/IEC 9798-6:2010 standard. This work has been published and presented at CSF'17 [26].

Most security properties are modelled as *safety* properties (*"bad things do not happen"*). Another important class of properties is that of *liveness* properties (*"eventually, good things happen"*). Reasoning about the class of *liveness* properties of cryptographic protocols, has received little attention in the literature, even though this class is vital in many security-sensitive applications, such as fair exchange protocols, or security layers in industrial control systems. In collaboration with Backes and Künnemann (Univ Saarland, Germany), Dreier and Kremer have designed a protocol and adversary model that are suitable for reasoning about liveness properties. Tool support is also provided by extending the *SAPIC/TAMARIN* tool chain and several case studies demonstrate the effectiveness of the approach. This work has been published and presented at EuroS&P'17 [17].

7.1.2. New properties

Participant: Jannik Dreier.

Industrial systems are nowadays regularly the target of cyberattacks, the most famous being Stuxnet[9]. At the same time such systems are increasingly interconnected with other systems and insecure media such as Internet. In contrast to other IT systems, industrial systems often do not only require classical properties like data confidentiality or authentication of the communication, but have special needs due to their interaction with the physical world. For example, the reordering or deletion of some commands sent to a machine can cause the system to enter an unsafe state with potentially catastrophic effects. To prevent such attacks, the integrity of the message flow is necessary.

In joint work with Lafourcade (Univ Clermont-Ferrand), Potet, and Puys (Univ Grenoble Alpes), Dreier developed a formal definition of Flow Integrity in the context of industrial systems. The framework is applied to two well-known industrial protocols: OPC-UA and MODBUS. Using *TAMARIN*, they identified several design flaws in some of the different versions of these protocols. They also discussed how to efficiently model counters and timestamps in *TAMARIN*, as they are key ingredients of the analyzed protocols. This work was presented at SECRYPT'17 [32], and won a Best Student Paper Award.

7.2. Analysis

7.2.1. Analysis of equivalence properties

Participants: Vincent Cheval, Véronique Cortier, Antoine Dallon, Ivan Gazeau, Steve Kremer, Joseph Lallemand, Itsaka Rakotonirina, Christophe Ringeissen.

Automatic tools based on symbolic models have been successful in analyzing security protocols. These tools are particularly well adapted for trace properties (e.g. secrecy or authentication). However, they often fail to analyse equivalence properties. Equivalence properties can express a variety of security properties, including in particular privacy properties (vote privacy, anonymity, untraceability). Several decision procedures have already been proposed but the resulting tools are often rather limited, and lack efficiency.

In the case of a passive adversary, Ringeissen, in collaboration with Marshall (Univ Mary Washington, USA) and Erbatur (LMU, Germany) present new combination techniques for the study of deducibility and static equivalence in unions of equational theories sharing constructors. This allows us to develop new modularity results for the decidability of deducibility and static equivalence. In turn, this should allow for the security analysis of protocols which previous disjoint combination methods could not address because their axiomatization corresponds to the union of non-disjoint equational theories. This work has been presented at CADE'17 [28].

[9] Stuxnet. https://en.wikipedia.org/wiki/Stuxnet

In case of an active adversary, and a bounded number of sessions, we made several advances. The *Akiss* tool has been extended in two directions. Gazeau and Kremer, in collaboration with Baelde (LSV, ENS Cachan) and Delaune (IRISA) have extended the underlying theory and the *Akiss* tool with support for exclusive or. They analyse unlinkability in several RFID protocols and resistance to guessing attacks of several password-based protocols. This work has been presented at CSF'17 [18]. Gazeau and Kremer also extended the *Akiss* tool to analyse protocols with else branches. This is particularly useful when verifying equivalence properties, as one needs to model precisely the error messages sent out when tests fail. While ignoring these branches may often be safe when studying trace properties this is not the case for equivalence properties, as for instance witnessed by an attack on the European electronic passport. One appealing feature of our approach is that our extension re-uses the saturation procedure which is at the heart of the verification procedure of *Akiss* as a black box, without need to modify it. As a result we obtain the first tool that is able verify equivalence properties for protocols that may use xor and else branches. We demonstrate the tool's effectiveness on several case studies, including the AKA protocol deployed in mobile telephony. This result was presented at ESORICS'17 [29]. Cortier and Dallon, in collaboration with Delaune (IRISA) propose a novel algorithm, based on graph planning and SAT-solving, which significantly improves the efficiency of the analysis of equivalence properties. The resulting implementation, SAT-Equiv, can analyze several sessions where most tools have to stop after one or two sessions. The approach has been presented at CSF'17 [20] for protocols with symmetric encryption and no else branches. Finally, Cheval, Kremer, and Rakotonirina have worked on complexity results for deciding equivalence properties and provide a decision procedure in the case of a bounded number of sessions. They showed that trace equivalence and labelled bisimilarity for a large variety of cryptographic primitives—those that can be represented by a subterm convergent destructor rewrite system— are both CoNEXP complete. Moreover, the procedure has been implemented in a new tool, *DeepSec*. Extensive experiments demonstrate that it is significantly more efficient than most other similar tools (being only slightly outperformed by SAT-Equiv in some specific examples), while at the same time raises the scope of the protocols that can be analysed. These results are currently under submission.

The previous results apply for a bounded number of sessions and may still be limited for a large number of sessions. In collaboration with Maffei and Grimm, Lallemand and Cortier have devised a novel approach [24] for proving equivalence properties. Instead of *deciding* equivalence, like for the previous approaches, they design a type system, sound w.r.t. equivalence. The resulting tool TypeEquiv can consider a bounded as well as an unbounded number of sessions, or a mix of both. It induces a significant speedup compared to previous tools for a bounded number of sessions and compares similarly to ProVerif for an unbounded number of sessions, with the advantage of a tighter treatment of bounded number of sessions. It can be applied to protocols with standard primitives and else branches.

7.2.2. Analysis of stateful security protocols

Participants: Vincent Cheval, Véronique Cortier, Jannik Dreier, Steve Kremer, Mathieu Turuani.

Many real-life protocols need to maintain a global state–such as counters, tables, or more generally, memory cells–that may be read and updated by parallel threads. Modelling such mutable, global state in protocols complicates the verification problem, in particular when analyzing an unbounded number of sessions.

The *SAPIC/TAMARIN* toolchain is one of the few tools that was designed to handle such global state. Dreier, Duménil (former intern in Pesto) and Kremer, in collaboration with Sasse (ETH Zurich, Switzerland) improve the underlying theory and the *TAMARIN* tool to allow for more general user-specified equational theories: the extension supports arbitrary convergent equational theories that have the finite variant property, making *TAMARIN* the first tool to support at the same time this large set of user-defined equational theories, protocols with global mutable state, an unbounded number of sessions, and complex security properties. The effectiveness of this generalization is demonstrated by analyzing several protocols that rely on blind signatures, trapdoor commitment schemes, and ciphertext prefixes that were previously out of scope. This work has been presented at POST'17 [27].

ProVerif is a very popular tool for the analysis of security protocols, that works very well in practice. However, in the case of protocols with global states, ProVerif typically fails in its analysis, due to its internal abstraction.

Instead of designing a new ad-hoc procedure, we devise a generic transformation of the security properties queried to ProVerif. We prove the soundness of our transformation and implement it into a front-end GSVerif. Our experiments show that our front-end (combined with ProVerif) outperforms the few existing tools, both in terms of efficiency and protocol coverage. We successfully apply our tool to a dozen of protocols of the literature including a deployed voting and a payment protocol. This work is under submission.

7.2.3. Analysis of e-voting protocols

Participants: Véronique Cortier, Constantin-Catalin Dragan, Mathieu Turuani.

Cortier and Dragan provide the first machine-checked proof of privacy-related properties (including ballot privacy) for an electronic voting protocol in the computational model. They target the popular Helios family of voting protocols, for which they identify appropriate levels of abstractions to allow for simplification and convenient reuse of proof steps across many variations of the voting scheme. The resulting framework enables machine-checked security proofs for several hundred variants of Helios and should serve as a stepping stone for the analysis of further variations of the scheme. In addition, they highlight some of the lessons learned regarding the gap between pen-and-paper and machine-checked proofs, and report on the experience with formalizing the security of protocols at this scale. This work has been presented at S&P'17 [21].

Turuani and Cortier, in collaboration with Galindo (Univ Birmingham), have analysed the e-voting protocol developed by Scytl and planned to be deployed in Switzerland. The formal analysis of both privacy and individual verifiability has been conducted in ProVerif. It required to develop a crafty encoding of the security properties in order to avoid the limitations of ProVerif in the presence of global states (here, no revoting). This first encoding yielded the preliminary ideas for the GSVerif tool mentioned in the previous section. Such a formal analysis is required by the Swiss Chancellerie and has been accepted at EuroSP'18 [23].

Norway used e-voting in its last political election both in September 2011 and September 2013. The underlying protocol was also developed by Scytl. Cortier, in collaboration with Wiedling, has conducted a formal analysis (by hand) of vote privacy of this protocol, considering several corruption scenarios [13].

7.2.4. Unification in Forward-Closed Theories

Participant: Christophe Ringeissen.

In collaboration with Marshall (Univ Mary Washington, USA) and Erbatur (LMU, Germany), we investigate the unification problem in equational theories involving forward-closed convergent term rewrite systems. In the class of forward-closed theories, unification is decidable and finitary since a convergent term rewrite system has a finite forward-closure if and only if it has the finite variant property. Actually, forward-closed theories are syntactic theories admitting a terminating mutation-based unification procedure. This can be shown by reusing a mutation-based unification algorithm originally developed for equational theories saturated by paramodulation, since a forward-closed theory is indeed a sufficient condition to get soundness and completeness. Building on this fact we develop a new mutation-based unification algorithm which is simpler, with regard to conflicts and number of rules, than the first algorithm. We then use this simplified algorithm as a component to develop a new method that solves the unification problem in unions of forward-closed theories with non-disjoint theories. The resulting algorithm can be viewed as a terminating instance of a procedure initiated for hierarchical combination. This work has been presented at the workshop UNIF'17 [33].

7.2.5. Analysis of Combinations of Protocols

Participant: Jannik Dreier.

When trying to prove the security of a protocol, one usually analyzes the protocol in isolation, i.e., in a network with no other protocols. But in reality, there will be many protocols operating on the same network, maybe even sharing data including keys, and an intruder may use messages of one protocol to break another. We call that a multi-protocol attack. In this work, we tried to find such attacks using the *TAMARIN* prover. We analyzed both examples that were previously analyzed by hand or using other tools, and found novel attacks. This work was presented at FPS'17 [31].

7.3. Design

7.3.1. E-voting protocols

Participants: Véronique Cortier, Alicia Filipiak.

Building upon a recently proposed voting scheme, BeleniosRF, we design a new voting scheme that ensures both verifiability and privacy against a compromised voting machine, as well as a compromised voting server. It assumes that the voter has two devices: one computer for casting a vote and another device (typically a smartphone or a tablet) to, optionally, audit the material (a voting sheet) sent to the voter. Neither the computer nor the smartphone learns how the voter voted unless they collude. The resulting protocol has been formally analysed in ProVerif w.r.t. both verifiability and privacy. Analysing verifiability in ProVerif cannot be done directly as it would require counting. Instead, we propose a set of properties that can be handled by ProVerif and that entail verifiability. This work is one of the contribution of the thesis manuscript of Alicia Filipiak and will be submitted.

7.3.2. Designing and proving an EMV-compliant payment protocol for mobile devices

Participants: Véronique Cortier, Alicia Filipiak.

In collaboration with Gharout, Traoré and Florent (Orange Labs), we devised a payment protocol that can be securely used on mobile devices, even infected by malicious applications. Our protocol only requires a light use of Secure Elements, which significantly simplifies certification procedures and protocol maintenance. It is also fully compatible with the EMV-SDA protocol and allows off-line payments for the users. We provide a formal model and full security proofs of the protocol using the *TAMARIN* prover. This work has been presented at EuroS&P'17 [22].

7.3.3. Composition and design of PKIs

Participants: Vincent Cheval, Véronique Cortier.

In protocol analysis one makes the (strong) assumption that honestly generated keys are available to all parties and that the link between identities and public keys is fixed and known to everyone. The abstraction is grounded in solid intuition but there are currently no theoretical underpinnings to justify its use. Cheval and Cortier, in collaboration with Warinschi (Univ Bristol, UK), initiate a rigorous study of how to use PKIs within other protocols, securely. They first show that the abstraction outlined above is in general unsound by exhibiting a simple protocol which is secure with idealized key distribution but fails in the presence of more realistic PKI instantiation. Their main result is a generic composition theorem that identifies under which conditions protocols that require public keys can safely use any PKI protocol (which satisfies a security notion which we identify). Interestingly, unlike most existing composition results in symbolic models they do not require full tagging of the composed protocols. Furthermore, the results confirm the recommended practice that keys used in the PKI should not be used for any other cryptographic task. This work has been presented at CSF'17 [19].

7.3.4. Privacy Protection in Social Networks

Participants: Younes Abid, Hector Dang-Nhu, Andrii Dychka, Abdessamad Imine, Michaël Rusinowitch, Valentin Salquebre.

In order to demonstrate privacy threats in social networks we show how to infer user preferences by random walks in a multiple graph representing simultaneously attributes and relationships links. For the approach to scale in a first phase we reduce the space of attribute values by partition in balanced homogeneous clusters. Following the Deepwalk approach, the random walks are considered as sentences. Hence unsupervised learning techniques from natural languages processing can be employed in a second phase to deduce semantic similarities of some attributes. We conduct initial experiments on real datasets to evaluate our approach. This work was presented at DEXA'17 [15].

7.3.5. Compressed and Verifiable Filtering Rules in Software-defined Networking

Participants: Haftay Gebreslasie Abreha, Michaël Rusinowitch.

In a joint project with EPI Madynes and Cynapsys, we are starting to work on the design, implementation and evaluation of multi-masked techniques for building a compressed and a verifiable filtering rules in Software Defined Networks with the possibility of distributing the workload processing among several packet filtering devices operating in parallel.

8. Bilateral Contracts and Grants with Industry

8.1. Scytl - Electronic Voting Systems

Participants: Véronique Cortier, Mathieu Turuani.

Since 2014, a collaboration agreement has been signed between Loria and Scytl, a Spanish company who is proposing solutions for the organization of on-line elections, including legally binding elections, in several countries. In this context, Scytl has signed a contract in 2016 with the Pesto team as well as the University of Birmingham (David Galindo) to design a formal proof of both verifiability and privacy of the protocol developed by Scytl, for a deployment in Switzerland. The result of the analysis will be presented at the conference EuroS&P'18 [23].

8.2. Canton of Geneva - Electronic Voting Systems

Participants: Véronique Cortier, Mathieu Turuani.

The canton of Geneva has signed a contract in October 2017 with Pesto and Caramba, as well as Manifold Security (Bogdan Warinschi and David Bernhard) to design a formal and cryptographic proof of individual and universal verifiability of the protocol developed by the canton of Geneva, for a deployment in Switzerland.

8.3. Docapost - Electronic Voting Systems

Participant: Véronique Cortier.

Docapost has signed a 18-month contract in September 2017, with Pesto and Caramba, to enhance the voting solution of Docapost, in particular with respect to verifiability.

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. CNRS

- CNRS PEPS INS2I 2016-2018 project ASSI *Analyse de Sécurité de Systèmes Industriels*, duration: 2 years, leader: Pascal Lafourcade (Univ Clermont-Ferrand), participant Pesto: Jannik Dreier, other participants: Marie-Laure Potet, Maxime Puys (Univ Grenoble-Alpes).

  The goal of the project is to develop an approach to verify protocols used in industrial control (SCADA) systems using tools such as *TAMARIN* or ProVerif. These protocols have specific security requirements such as flow integrity, going beyond the classical authentication and secrecy properties. The project also aims at analyzing different intruder models matching the particularities of industrial systems, and to develop specific modeling and verification techniques.

9.1.2. ANR

- ANR SEQUOIA *Security properties, process equivalences and automated verification*, duration: 4 years, since October 2014, leader: Steve Kremer, other partners: ENS Cachan, Univ Luxembourg. Most protocol analysis tools are restricted to analyzing reachability properties while many security properties need to be expressed in terms of some process equivalences. The increasing use of observational equivalence as a modeling tool shows the need for new tools and techniques that are able to analyze such equivalence properties. The aims of this project are *(i)* to investigate which process equivalences – among the plethora of existing ones – are appropriate for a given security property, system assumptions and attacker capabilities; *(ii)* to advance the state-of-the-art of automated verification for process equivalences, allowing for instance support for more cryptographic primitives, relevant for case studies; *(iii)* to study protocols that use low-entropy secrets expressed using process equivalences; *(iv)* to apply these results to case studies from electronic voting.
- ANR TECAP *Protocol Analysis — Combining Existing Tools*, duration: 4 years, starting in 2018, leader: Vincent Cheval, other partners: ENS Cachan, Inria Paris, Inria Sophia Antipolis, IRISA, LIX. Despite the large number of automated verification tools, several cryptographic protocols (e.g. stateful protocols) still represent a real challenge for these tools and reveal their limitations. To cope with these limits, each tool focuses on different classes of protocols depending on the primitives, the security properties, etc. Moreover, the tools cannot interact with each other as they evolve in their own model with specific assumptions. The aim of this project is to get the best of all these tools, meaning, to improve the theory and implementations of each individual tool towards the strengths of the others and, to build bridges that allow the cooperations of the methods/tools. We will focus in this project on the tools CryptoVerif, EasyCrypt, Scary, ProVerif, *TAMARIN*, *Akiss* and APTE. In order to validate the results obtained in this project, we will apply our results to several case studies such as the Authentication and Key Agreement protocol from the telecommunication networks, the Scytl and Helios voting protocols, and the low entropy authentication protocols 3D-Secure. These protocols have been chosen to cover many challenges that the current tools are facing.

9.1.3. Fondation MAIF

Project *Protection de l'information personnelle sur les réseaux sociaux*, duration: 3 years, started in October 2014. The goal of the project is to lay the foundation for a risk verification environment on privacy in social networks. Given social relations, this environment will rely on the study of metrics to characterize the security level for a user. Next, by combining symbolic and statistical techniques, an objective is to synthesize a model of risk behavior as a rule base. Finally, a verifier based on model-checking will be developed to assess the security level of user. Partners are Pesto (leader), Orpailleur and Fondation MAIF.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

- SPOOC (2015–2020) [10]— ERC Consolidator Grant on Automated Security Proofs of Cryptographic Protocols: Privacy, Untrusted Platforms and Applications to E-voting Protocols.

  The goals of the Spooc project are to develop solid foundations and practical tools to analyze and formally prove security properties that ensure the privacy of users as well as techniques for executing protocols on untrusted platforms. We will
  - develop foundations and practical tools for specifying and formally verifying new security properties, in particular privacy properties;
  - develop techniques for the design and automated analysis of protocols that have to be executed on untrusted platforms;
  - apply these methods in particular to novel e-voting protocols, which aim at guaranteeing strong security guarantees without need to trust the voter client software.

[10] https://members.loria.fr/SKremer/files/spooc/index.html

Steve Kremer is the leader of the project.

9.3. International Initiatives

9.3.1. Inria International Partners

- Collaboration with David Basin, Ralf Sasse and Lara Schmid (ETH Zurich), Cas Cremers (Univ Oxford), and Sasa Radomirovic (Univ Dundee) on the improvement of the *TAMARIN* prover
- Collaboration with Bogdan Warinschi (Univ Bristol) on defining game-based privacy for e-voting protocols and isolated execution environments
- Collaboration with Myrto Arapinis (Univ Edinburgh) on simplification results for the formal analysis of e-voting protocols
- Collaboration with Matteo Maffei (CISPA, Germany) on type systems for e-voting systems
- Collaboration with Michael Backes and Robert Künnemann (CISPA, Germany) on automated verification of security protocols
- Collaboration with Paliath Narendran's group (SUNY Albany) on automated deduction
- Collaboration with Hanifa Boucheneb's group (Polytechnique Montreal) on model-checking of collaborative systems
- Collaboration with John Mullins's group (Polytechnique Montreal) on information hiding

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- David Galindo (Univ Birmingham), June 2017
- Bogdan Warinschi (Univ Bristol), November 2017

10. Dissemination

10.1. Promoting Scientific Activities

V. Cortier was auditioned by the chamber of the workers in Luxembourg, on the security of electronic voting.

10.1.1. Scientific Events Selection

10.1.1.1. Program Committee Chair

- A. Imine: FPS 2017, 10th International Symposium on Foundations & Practice of Security, Nancy, October 23-25, 2017 (co-chair with J. M. Fernandez, Polytechnique Montreal, Canada)
- M. Rusinowitch: SCSS 2017, The 8th International Symposium on Symbolic Computation in Software Science, Gammarth, Tunisie, April 6-9, 2017 (co-chair with M. Mosbah, Univ Bordeaux)

10.1.1.2. Program Committee Member

- V. Cortier: E-VoteID 2018, POST 2018, E-VoteID 2017, CCS 2017, LICS 2017, SAC 2017, HotSpot 2017
- S. Kremer: Voting 2018, EuroS&P 2018, PLAS 2017, ESORICS 2017, Voting 2017, EuroS&P 2017
- C. Ringeissen: IJCAR 2018, UNIF 2018, WRLA 2018, FroCoS 2017, UNIF 2017
- M. Rusinowitch: CRISIS 2017, FPS 2017, ICISSP 2018, IWSPA 2018
- V. Cheval: TMPA 2017, SEC@SAC 2017

10.1.2. Journal

10.1.2.1. Editorial Board Member

- V. Cortier: Information & Computation, Journal of Computer Security, ACM Transactions on Privacy and Security (TOPS, previously TISSEC), Foundations and Trends (FnT) in Security and Privacy
- S. Kremer: ERCIM News

10.1.2.2. Scientific Committee Member

- L. Vigneron: Technique et Sciences Informatiques, Lavoisier

10.1.3. Invited Talks

- V. Cortier. Invited tutorial at Highlights 2017, London, UK, September 12th, 2017
- V. Cortier. Invited talk at FPS 2017, Nancy, France, October 2017
- V. Cortier. Invited talk at CIAA 2017, Marne-la-Vallée, France, June 2017
- V. Cortier. Invited talk at Workshop on the 20th Anniversary of LSV, Cachan, France, May 11th 2017
- V. Cortier. Invited tutorial at ETAPS 2017, Uppsala, Sweden, April 22nd, 2017
- V. Cortier. Invited talk at Models and Tools for Security Analysis and Proofs Workshop, affiliated with Eurocrypt 2017, Paris, France, April 29th 2017

10.1.4. Research Administration

Inria evaluation committee (S. Kremer)

Jury Junior Research Position Inria Rennes-Bretagne Atlantique (S. Kremer)

Jury Junior Research Position Inria Nancy-Grand Est (V. Cortier, committee chair)

Jury Professor at UMPC, LIP6 (V. Cortier)

Computer science commission of the Doctoral School, Univ Lorraine (L. Vigneron, chair)

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Licence:

  V. Cheval, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 69 hours (ETD), TELECOM Nancy

  J. Dreier, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 146 hours (ETD), TELECOM Nancy

- Master:

  V. Cortier, Security of flows, 20 hours, M2 Computer Science, TELECOM Nancy and Mines Nancy

  A. Imine, Security for XML Documents, 12 hours (ETD), M1, Univ Lorraine

  S. Kremer, Security Theory, 24 hours (ETD), M2 Computer science, Univ Lorraine

  C. Ringeissen, Decision Procedures for Software Verification, 18 hours (ETD), M2 Computer science, Univ Lorraine

  L. Vigneron, Security of information systems, 22.5 hours (ETD), M2 Computer science, Univ Lorraine

  L. Vigneron, Security of information systems, 24 hours (ETD), M2 MIAGE – Distributed Information Systems, Univ Lorraine

  L. Vigneron, Security of information systems, 16 hours (ETD), M2 MIAGE – Audit and Design of Information Systems, Univ Lorraine

- Summer School:

  V. Cortier and S. Kremer: Summer School on Models and Tools for Cryptographic Proofs, Nancy, June 2017

10.2.2. Supervision

- PhD in progress:

  Younes Abid, Privacy control for social networks, started in March 2015 (M. Rusinowitch)

  Antoine Dallon, Decision procedures for equivalence properties, started in November 2015 (V. Cortier and S. Delaune)

  Alicia Filipiak, Design and validation of security services for mobile platforms: smartphones and tablets, started in March 2015 (V. Cortier)

  Abreha Haftay Gebreslasie, Compressed and Verifiable Filtering Rules in Software-defined Networking, started in September 2017 (A. Lahmadi, M. Rusinowitch and A. Bouhoula)

  Charlie Jacomme, Security protocols: new properties, new attackers, new protocols, started in September 2017 (H. Comon and S. Kremer)

  Joseph Lallemand, Type systems for equivalence properties, started in September 2016 (V. Cortier)

  Itsaka Rakotonirina, Efficient verification of equivalence properties in cryptographic protocols, started in October 2017 (V. Cheval and S. Kremer)

  Ludovic Robin, Verification of cryptographic protocols using weak secrets, started in October 2014, defense scheduled early 2018 (S. Delaune and S. Kremer)

10.2.3. Juries

Examiner for Robin David, CEA and Loria (S. Kremer)

Reviewer for Ryan Stanley-Oakes, Univ Bristol (S. Kremer)

Examiner and president of the jury for Wazen Shbair, Univ Lorraine, Loria (V. Cortier)

Examiner and president of the jury for Hubert Godefroy, Univ Lorraine, Loria (V. Cortier)

Reviewer for Fabienne Eigner, Univ Saarbruecken (V. Cortier)

Reviewer for Mnacho Echenim, HDR, Univ Grenoble (M. Rusinowitch)

10.3. Popularization

- How to Explain Modern Security Concepts to your Children [11] (J. Dreier)
- Vote par Internet [41] (V. Cortier and S. Kremer)
- 2 days of debate on privacy at *Moments d'invention 2016*, organized by Grand Nancy (V. Cortier)
- booth at the *Open Government Summit* organized at Sénat (V. Cortier)
- Conference and debate at the *ISN day*, conference for teachers in computer science (V. Cortier)
- Interview for *silicon.fr* on weakening cryptosystems to allow limited access by authorities (S. Kremer)
- France 3 Lorraine radio interview on computer security (S. Kremer)
- Interview for *AFP* on electronic voting (S. Kremer)
- Interview for *AFP* and *Huffington Post* on electronic voting (V. Cortier)

11. Bibliography

Major publications by the team in recent years

[1] W. BELKHIR, Y. CHEVALIER, M. RUSINOWITCH. *Parametrized automata simulation and application to service composition*, in "J. Symb. Comput.", 2015, vol. 69, pp. 40–60

[2] D. BERNHARD, V. CORTIER, D. GALINDO, O. PEREIRA, B. WARINSCHI. *A comprehensive analysis of game-based ballot privacy definitions*, in "Proceedings of the 36th IEEE Symposium on Security and Privacy (S&P'15)", IEEE Computer Society Press, May 2015, pp. 499–516

[3] R. CHADHA, V. CHEVAL, S. CIOBÂCĂ, S. KREMER. *Automated verification of equivalence properties of cryptographic protocols*, in "ACM Transactions on Computational Logic", 2016, vol. 17, n° 4 [*DOI :* 10.1145/2926715], https://hal.inria.fr/hal-01306561

[4] P. CHOCRON, P. FONTAINE, C. RINGEISSEN. *A Polite Non-Disjoint Combination Method: Theories with Bridging Functions Revisited*, in "Proceedings of the 25th International Conference on Automated Deduction (CADE-25)", Lecture Notes in Computer Science, Springer, August 2015, vol. 9195, pp. 419-433, https://hal.inria.fr/hal-01157898

[5] R. CHRETIEN, V. CORTIER, S. DELAUNE. *Typing messages for free in security protocols: the case of equivalence properties*, in "Proceedings of the 25th International Conference on Concurrency Theory (CONCUR'14)", Rome, Italy, Lecture Notes in Computer Science, Springer, September 2014, vol. 8704, pp. 372-386

[6] S. KREMER, R. KÜNNEMANN. *Automated Analysis of Security Protocols with Global State*, in "2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014", IEEE Computer Society, 2014, pp. 163–178

[7] H. H. NGUYEN, A. IMINE, M. RUSINOWITCH. *Anonymizing Social Graphs via Uncertainty Semantics*, in "Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, (ASIA CCS'15), 2015", ACM, 2015, pp. 495–506

Publications of the year

Articles in International Peer-Reviewed Journals

[8] T. AVANESOV, Y. CHEVALIER, M. RUSINOWITCH, M. TURUANI. *Intruder deducibility constraints with negation. Decidability and application to secured service compositions*, in "Journal of Symbolic Computation", 2017, vol. 80, pp. 4 - 26 [*DOI :* 10.1016/J.JSC.2016.07.008], https://hal.inria.fr/hal-01405851

[9] T. AVANESOV, Y. CHEVALIER, M. RUSINOWITCH, M. TURUANI. *Satisfiability of General Intruder Constraints with and without a Set Constructor*, in "Journal of Symbolic Computation", 2017, vol. 80, pp. 27-61 [*DOI :* 10.1016/J.JSC.2016.07.009], https://hal.inria.fr/hal-01405842

[10] D. BASIN, C. CREMERS, J. DREIER, R. SASSE. *Symbolically Analyzing Security Protocols using Tamarin*, in "ACM SIGLOG News", October 2017 [*DOI :* 10.1145/3157831.3157835], https://hal.archives-ouvertes.fr/hal-01622110

[11] X. BULTEL, J. DREIER, P. LAFOURCADE, M. MORE. *How to Explain Modern Security Concepts to your Children*, in "Cryptologia", March 2017, vol. 41, n° 5 [*DOI :* 10.1080/01611194.2016.1238422], https://hal.archives-ouvertes.fr/hal-01397035

[12] V. CHEVAL, H. COMON-LUNDH, S. DELAUNE. *A procedure for deciding symbolic equivalence between sets of constraint systems*, in "Information and Computation", August 2017, vol. 255, pp. 94 - 125 [*DOI :* 10.1016/J.IC.2017.05.004], https://hal.inria.fr/hal-01584242

[13] V. CORTIER, C. WIEDLING. *A Formal Analysis of the Norwegian E-Voting Protocol*, in "Journal of Computer Security", March 2017 [*DOI :* 10.3233/JCS-15777], https://hal.inria.fr/hal-01647764

[14] N. GUETMI, A. IMINE. *Cloud patterns for mobile collaborative applications* , in "International Journal of Intelligent Information and Database Systems", September 2017, vol. 10, n^{o} 3/4, pp. 191-223 [*DOI :* 10.1504/IJIIDS.2017.10007786], https://hal.inria.fr/hal-01651504

International Conferences with Proceedings

[15] Y. ABID, A. IMINE, A. NAPOLI, C. RAÏSSI, M. RUSINOWITCH. *Two-phase preference disclosure in attributed social networks*, in "DEXA 2017 - 28th International Conference on Database and Expert Systems Applications", Lyon, France, LNCS, Springer, August 2017, vol. 10438, pp. 249-263 [*DOI :* 10.1007/978-3-319-64468-4_19], https://hal.inria.fr/hal-01649246

[16] K. BABEL, V. CHEVAL, S. KREMER. *On communication models when verifying equivalence properties*, in "6th International Conference on Principles of Security and Trust (POST)", Uppsala, Sweden, April 2017, https://hal.inria.fr/hal-01450898

[17] M. BACKES, J. DREIER, S. KREMER, R. KÜNNEMANN. *A Novel Approach for Reasoning about Liveness in Cryptographic Protocols and its Application to Fair Exchange*, in "2nd IEEE European Symposium on Security and Privacy (EuroS&P'17)", Paris, France, Proceedings of the 2nd IEEE European Symposium on Security and Privacy, Springer, April 2017, https://hal.inria.fr/hal-01396282

[18] D. BAELDE, S. DELAUNE, I. GAZEAU, S. KREMER. *Symbolic verification of privacy-type properties for security protocols with XOR*, in "CSF 2017 - 30th IEEE Computer Security Foundations Symposium", Santa Barbara, United States, August 2017, 15 p. , https://hal.inria.fr/hal-01533708

[19] V. CHEVAL, V. CORTIER, B. WARINSCHI. *Secure Composition of PKIs with Public Key Protocols*, in "CSF'17 - 30th IEEE Computer Security Foundations Symposium", Santa Barbara, United States, August 2017, pp. 144 - 158 [*DOI :* 10.1109/CSF.2017.28], https://hal.inria.fr/hal-01625766

[20] V. CORTIER, A. DALLON, S. DELAUNE. *SAT-Equiv: An Efficient Tool for Equivalence Properties*, in "30th IEEE Computer Security Foundations Symposium (CSF'17)", Santa Barbara, United States, July 2017, pp. 481 - 494 [*DOI :* 10.1109/CSF.2017.15], https://hal.inria.fr/hal-01624274

[21] V. CORTIER, C. DRAGAN, F. DUPRESSOIR, B. SCHMIDT, P.-Y. STRUB, B. WARINSCHI. *Machine-Checked Proofs of Privacy for Electronic Voting Protocols*, in "38th IEEE Symposium on Security and Privacy (S&P'17)", San Jose, United States, May 2017, pp. 993 - 1008 [*DOI :* 10.1109/SP.2017.28], https://hal.inria.fr/hal-01624270

[22] V. CORTIER, A. FILIPIAK, S. GHAROUT, J. TRAORÉ. *Designing and proving an EMV-compliant payment protocol for mobile devices*, in "2nd IEEE European Symposium on Security and Privacy (EuroSP'17)", Paris, France, April 2017, https://hal.inria.fr/hal-01408584

[23] V. CORTIER, D. GALINDO, M. TURUANI. *A formal analysis of the Neuchâtel e-voting protocol*, in "IEEE European Symposium on Security and Privacy 2018 (EuroS&P)", Londres, United Kingdom, April 2018, https://hal.inria.fr/hal-01647150

[24] V. CORTIER, N. GRIMM, J. LALLEMAND, M. MAFFEI. *A Type System for Privacy Properties*, in "CCS'17 - 24th ACM Conference on Computer and Communications Security", Dallas, United States, October 2017, pp. 409 - 423, https://hal.inria.fr/hal-01626109

[25] S. J. DE, A. IMINE. *Privacy Scoring of Social Network User Profiles through Risk Analysis*, in "CRiSIS 2017 - The 12th International Conference on Risks and Security of Internet and Systems", Dinard, France, September 2017, https://hal.inria.fr/hal-01651476

[26] S. DELAUNE, S. KREMER, L. ROBIN. *Formal verification of protocols based on short authenticated strings*, in "CSF 2017 - 30th IEEE Computer Security Foundations Symposium", Santa Barbara, United States, IEEE (editor), August 2017, 14 p. , https://hal.inria.fr/hal-01528607

[27] J. DREIER, C. DUMÉNIL, S. KREMER, R. SASSE. *Beyond Subterm-Convergent Equational Theories in Automated Verification of Stateful Protocols*, in "POST 2017 - 6th International Conference on Principles of Security and Trust", Uppsala, Sweden, Principles of Security and Trust, Springer, April 2017, vol. 10204, pp. 117-140, https://hal.inria.fr/hal-01450916

[28] S. ERBATUR, A. M. MARSHALL, C. RINGEISSEN. *Notions of Knowledge in Combinations of Theories Sharing Constructors*, in "26th International Conference on Automated Deduction", Göteborg, Sweden, L. DE MOURA (editor), Lecture Notes in Artificial Intelligence, Springer, August 2017, vol. 10395, pp. 60 - 76 [*DOI :* 10.1007/978-3-319-63046-5_5], https://hal.inria.fr/hal-01587181

[29] I. GAZEAU, S. KREMER. *Automated analysis of equivalence properties for security protocols using else branches*, in "22nd European Symposium on Research in Computer Security (ESORICS'17)", Oslo, Norway, Springer, 2017, https://hal.inria.fr/hal-01566035

[30] C. JACOMME, S. KREMER, G. SCERRI. *Symbolic Models for Isolated Execution Environments*, in "2nd IEEE European Symposium on Security and Privacy (EuroS&P'17)", Paris, France, C. HRIŢCU (editor), Proceedings of the 2nd IEEE European Symposium on Security and Privacy, Springer, April 2017, https://hal.inria.fr/hal-01396291

Conferences without Proceedings

[31] E. BLOT, J. DREIER, P. LAFOURCADE. *Formal Analysis of Combinations of Secure Protocols*, in "FPS 2017 - 10th International Symposium on Foundations & Practice of Security", Nancy, France, October 2017, pp. 1-15, https://hal.archives-ouvertes.fr/hal-01596010

[32] J. DREIER, M. PUYS, M.-L. POTET, P. LAFOURCADE, J.-L. ROCH. *Formally Verifying Flow Integrity Properties in Industrial Systems*, in "SECRYPT 2017 - 14th International Conference on Security and Cryptography", Madrid, Spain, July 2017, 12 p. , http://hal.univ-grenoble-alpes.fr/hal-01527913

[33] S. ERBATUR, A. M. MARSHALL, C. RINGEISSEN. *Non-Disjoint Combination with Forward-Closed Theories*, in "31th International Workshop on Unification, UNIF 2017", Oxford, United Kingdom, Adrià Gascón and Christopher Lynch, September 2017, https://hal.inria.fr/hal-01590782

Research Reports

[34] D. BAELDE, S. DELAUNE, I. GAZEAU, S. KREMER. *Symbolic verification of privacy-type properties for security protocols with XOR (extended version)*, Inria Nancy - Grand Est, 2017, 29 p. , https://hal.inria.fr/hal-01533694

[35] V. CORTIER, A. DALLON, S. DELAUNE. *SAT-Equiv: an efficient tool for equivalence properties*, LSV, ENS Cachan, CNRS, Inria, Université Paris-Saclay, Cachan (France) ; IRISA, Inria Rennes ; LORIA - Université de Lorraine ; CNRS, May 2017, https://hal.archives-ouvertes.fr/hal-01529966

[36] V. CORTIER, D. GALINDO, M. TURUANI. *A formal analysis of the Neuchâtel e-voting protocol*, Inria Nancy - Grand Est, October 2017, https://hal.inria.fr/hal-01616425

[37] S. DELAUNE, S. KREMER, L. ROBIN. *Formal verification of protocols based on short authenticated strings (extended version)*, Inria Nancy - Grand Est, 2017, https://hal.inria.fr/hal-01528603

[38] I. GAZEAU, T. CHOTHIA, D. DUGGAN. *Types for Location and Data Security in Cloud Environments*, Inria Nancy - Grand Est (Villers-lès-Nancy, France) ; University of Birmingham ; Stevens Institute of Technology, June 2017, https://hal.inria.fr/hal-01534567

[39] I. GAZEAU, S. KREMER. *Automated analysis of equivalence properties for security protocols using else branches (extended version)*, Inria Nancy, June 2017, 29 p. , https://hal.inria.fr/hal-01547017

[40] D. LE MÉTAYER, S. J. DE. *Privacy Risk Analysis to Enable Informed Privacy Settings*, Inria - Research Centre Grenoble – Rhône-Alpes, December 2017, n^{o} RR-9125, pp. 1-24, https://hal.inria.fr/hal-01660045

Scientific Popularization

[41] V. CORTIER, S. KREMER. *Vote par Internet*, in "Interstices", March 2017, Cet article met à jour la première version publiée en janvier 2013, https://hal.inria.fr/hal-01350400

Other Publications

[42] E. BLOT, J. DREIER, P. LAFOURCADE. *Formal Analysis of Combinations of Secure Protocols* , November 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01558552

References in notes

[43] M. ARAPINIS, L. MANCINI, E. RITTER, M. RYAN, N. GOLDE, K. REDON, R. BORGAONKAR. *New privacy issues in mobile telephony: fix and verification*, in "Proc. 19th ACM Conference on Computer and Communications Security (CCS'12)", ACM Press, 2012, pp. 205-216

[44] B. BLANCHET. *An Efficient Cryptographic Protocol Verifier Based on Prolog Rules*, in "Proc. 14th Computer Security Foundations Workshop (CSFW'01)", IEEE Comp. Soc. Press, 2001, pp. 82–96

[45] M. BORTOLOZZO, M. CENTENARO, R. FOCARDI, G. STEEL. *Attacking and Fixing PKCS#11 Security Tokens*, in "Proc. 17th ACM Conference on Computer and Communications Security (CCS'10)", ACM Press, 2010, pp. 260-269

[46] C. CHEVALIER, S. DELAUNE, S. KREMER, M. RYAN. *Composition of Password-based Protocols*, in "Formal Methods in System Design", 2013, vol. 43, pp. 369-413

[47] H. COMON-LUNDH, S. DELAUNE. *The finite variant property: How to get rid of some algebraic properties*, in "Proc. of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)", LNCS, Springer, 2005, vol. 3467, pp. 294-307

[48] V. CORTIER, S. DELAUNE. *Safely Composing Security Protocols*, in "Formal Methods in System Design", February 2009, vol. 34, n^{o} 1, pp. 1-36

[49] S. DELAUNE, S. KREMER, M. RYAN. *Verifying Privacy-type Properties of Electronic Voting Protocols*, in "Journal of Computer Security", July 2009, vol. 17, n^{o} 4, pp. 435-487

[50] S. DELAUNE, S. KREMER, G. STEEL. *Formal Analysis of PKCS#11 and Proprietary Extensions*, in "Journal of Computer Security", November 2010, vol. 18, n^{o} 6, pp. 1211-1245

[51] S. ERBATUR, D. KAPUR, A. M. MARSHALL, C. MEADOWS, P. NARENDRAN, C. RINGEISSEN. *On Asymmetric Unification and the Combination Problem in Disjoint Theories*, in "Proc. 17th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'14)", LNCS, Springer, 2014, pp. 274-288

[52] S. ESCOBAR, C. MEADOWS, J. MESEGUER. *Maude-NPA: Cryptographic Protocol Analysis Modulo Equational Properties*, in "Foundations of Security Analysis and Design V", LNCS, Springer, 2009, vol. 5705, pp. 1-50

[53] D. GOLLMANN. *What do we mean by entity authentication?*, in "Proc. Symposium on Security and Privacy (SP'96)", IEEE Comp. Soc. Press, 1996, pp. 46–54

[54] J. HERZOG. *Applying protocol analysis to security device interfaces*, in "IEEE Security & Privacy Magazine", July-Aug 2006, vol. 4, n^{o} 4, pp. 84–87

[55] B. SCHMIDT, S. MEIER, C. CREMERS, D. BASIN. *The TAMARIN Prover for the Symbolic Analysis of Security Protocols*, in "Proc. 25th International Conference on Computer Aided Verification (CAV'13)", LNCS, Springer, 2013, vol. 8044, pp. 696-701