IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2016

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:

2.4. - Verification, reliability, certification
4.5. - Formal methods for security
4.6. - Authentication
4.8. - Privacy-enhancing technologies
7.1. - Parallel and distributed algorithms
7.4. - Logic in Computer Science

Other Research Topics and Application Domains:

6.3.2. - Network protocols
6.3.4. - Social Networks
6.6. - Embedded systems
9.8. - Privacy

1. Members

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]

PhD Students

Younes Abid [Univ Lorraine, Fondation Maif, coadvised by Orpailleur]
Rémy Chrétien [ENS Cachan & LORIA, ANR Jeunes Chercheurs VIP (S. Delaune)]
Antoine Dallon [ENS Cachan & LORIA, DGA funding]
Alicia Filipiak [Cifre Orange]
Joseph Lallemand [Univ Lorraine, ERC Spooc, since September 2016]
Éric Le Morvan [Univ Lorraine, CNRS, until September 2016]
Huu Hiep Nguyen [Univ Lorraine, Cordi-S, until October 2016]
Ludovic Robin [Univ Lorraine]

Post-Doctoral Fellows

Constantin-Catalin Dragan [CNRS, FP7 ERC ProSecure]
Ivan Gazeau [Inria, ERC Spooc, since September 2016]
Peter Roenne [Inria, ANR Sequoia, until March 2016]

Visiting Scientist

Carlos Castro [UTFSM, 12 months, until June 2016]

Administrative Assistants

Emmanuelle Deschamps [Inria]
Delphine Hubert [Univ Lorraine]
Martine Kuhlmann [CNRS]

Others

Kushal Babel [2nd year student at IIT Bombay, India, from May 2016 until July 2016]
Charles Duménil [Master Mathématiques Nancy, M2, from April 2016 until September 2016]
Itsaka Rakotonirina [ENS Cachan/MPRI, M2, from May 2016 until July 2016]
Jonathan Proietto-Stallone [MIAGE Nancy, from March 2016 until August 2016]
Laura Trivino [IUT Nancy, from April 2016 until June 2016]
Clément Pascutto [ENS Paris, from June 2016 until July 2016]

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 billions Euros have been spent through e-commerce in 2013 and fraud is estimated to 1.9 billions 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 casted vote without any way for the voter to notice. 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. [3]

Privacy violations. Another security threat is the violation of an individual person's privacy. For instance the use of RFID technology can be used to trace persons, e.g. in automatic toll-paying devices [4] 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. [5] 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 [33]. Also, anonymised data of social networks has been effectively used to identify persons by comparing data from several social networks. [6]

[1] Livre Blanc: La fraude dans le e-commerce, certissim.
[2] Dissecting Operation High Roller. http://www.mcafee.com/uk/resources/reports/rp-operation-high-roller.pdf
[3] The Supreme Court dismissed an electoral complaint regarding e-voting security. http://www.nc.ee/?id=1235
[4] A Pass on Privacy? The New York Times, July 17, 2005. http://www.nytimes.com/2005/07/17/magazine/17WWLN.html
[5] Defects in e-passports allow real-time tracking. The Register, 26th January 2010. http://www.theregister.co.uk/2010/01/26/epassport_rfid_weakness/
[6] 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 [46].

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 [44]. 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 [40], 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 [34][3]. Another example is unification modulo equational theory, which is a key technique in several tools, e.g. [43]. 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 [38], which is used in several tools, e.g., *Akiss* [3], Maude-NPA [43] and Tamarin [47].

Another example is the notion of asymmetric unification [42] 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 will also 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 will include *composition results* that allow one to design protocols in a modular way [39], [36]. 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 will 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 will also design new protocols. Application areas that seem of particular importance are:

- External hardware devices such as security APIs that allow one for flexible key management, including key revocation, and their integration in security protocols. The security *fiasco* of the PKCS#11 standard [35], [41] 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

Steve Kremer gave a keynote talk at the 29th IEEE Computer Security Foundations Symposium (CSF'16).

5.1.1. Awards

Véronique Cortier, Antoine Dallon and Stéphanie Delaune received the EASST best paper award of the ETAPS conference for the paper [24].

BEST PAPER AWARD:

[24]
V. CORTIER, A. DALLON, S. DELAUNE. *Bounding the number of agents, for equivalence too*, in "5th International Conference on Principles of Security and Trust (POST'16)", Eindhoven, Netherlands, April 2016, pp. 211-232 [*DOI :* 10.1007/978-3-662-49635-0_11], https://hal.inria.fr/hal-01361286

6. New Software and Platforms

6.1. Akiss

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. The tool also includes the possibility for checking everlasting indistinguishability properties [32].

The tool is still under active development, including optimisations to improve efficiency, but also the addition of new features, such as the possibility to model protocols using weak secrets, and the addition of support for exclusive or.

The *Akiss* tool is freely available at https://github.com/akiss/akiss.

6.2. ATSE

We develop *CL-AtSe*, a Constraint Logic based Attack Searcher for cryptographic protocols, initiated and continued by the European projects *AVISPA*, AVANTSSAR (for web-services) and Nessos respectively. The *CL-AtSe* approach to verification consists in a symbolic state exploration of the protocol execution for a bounded number of sessions, thus is both correct and complete. *CL-AtSe* includes a proper handling of sets, lists, choice points, specification of any attack states through a language for expressing e.g., secrecy, authentication, fairness, or non-abuse freeness, advanced protocol simplifications and optimizations to reduce the problem complexity, and protocol analysis modulo the algebraic properties of cryptographic operators such as XOR (exclusive or) and Exp (modular exponentiation).

CL-AtSe has been successfully used to analyse protocols from e.g., France Telecom R&D, Siemens AG, IETF, Gemalto, Electrum in funded projects. It is also employed by external users, e.g., from the AVISPA's community. Moreover, *CL-AtSe* achieves good analysis times, comparable and sometimes better than other state-of-the art tools.

CL-AtSe has been enhanced in various ways. It fully supports the Aslan semantics designed in the context of the AVANTSSAR project, including Horn clauses (for intruder-independent deductions, e.g., for credential management), and a large fragment of LTL-based security properties. A Bugzilla server collects bug reports, and online analysis and orchestration are available on our team server (https://cassis.loria.fr). Large models can be analysed on the TALC Cluster in Nancy with parallel processing. *CL-AtSe* also supports negative constraints on the intruder's knowledge, which reduces drastically the orchestrator's processing times and allows separation of duties and non-disclosure policies, as well as conditional security properties, like: i) an authentication to be verified iff some session key is safe; ii) relying on a leaking condition on some private data instead of an honesty predicate to trigger or block some agent's property. This was crucial for e.g., the Electrum's wallet where all clients can be dishonest but security guarantees must be preserved anyway.

6.3. Belenios

In collaboration with the Caramba project-team, we develop an open-source private and verifiable electronic voting protocol, named *Belenios*. Our system is an evolution and a new implementation of an existing system, Helios, developed by Ben Adida, and used e.g., by UCL and the IACR association in real elections. The main differences with Helios are a cryptographic protection against ballot stuffing and a practical threshold decryption system that allows us to split the decryption key among several authorities, k out of n authorities being sufficient to decrypt. We will continue to add new cryptographic and protocol improvements to offer a secure, proved, and practical electronic voting system.

Belenios has been implemented (cf. http://belenios.gforge.inria.fr) by Stéphane Glondu (SED Team). Since 2015, it is used by CNRS for remote election among its councils and since 2016, it used by Inria to elect representatives in the "comités de centre" of each Inria center. It has also been used to elect the leader of the GdR-IM working groups C2 and Calcul Formel. It has also been used in smaller elections (e.g., to choose an invited speaker).

6.4. Tamarin

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 combined with a user-defined subterm-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.

TAMARIN is freely available at http://tamarin-prover.github.io/. In a joint effort, the partners wrote and published a user manual in 2016, available from the same website.

6.5. Sapic

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 be analysed using the *TAMARIN* prover. *TAMARIN* has also bee extended with dedicated heuristics that exploit the form of translated rules and favour 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, extensions of the PKCS#11 standard and fair exchange protocols.

SAPIC is freely available at http://sapic.gforge.inria.fr/.

7. New Results

7.1. Modelling

7.1.1. New protocol and adversary models

Participants: Jannik Dreier, Steve Kremer.

Isolated Execution Environments (IEEs), such as ARM TrustZone and Intel SGX, offer the possibility to execute sensitive code in isolation from other 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 accepted for publication at EuroS&P'17 [27].

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 (U. 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 accepted for publication at EuroS&P'17 [20].

7.1.2. New properties

Participants: Véronique Cortier, Jannik Dreier.

Defining security properties correctly is often a challenging problem on its own: too strict definitions may lack generality and exclude systems that should be considered as secure, while relaxing definitions may lead to accepting insecure systems.

In e-voting, *verifiability* is the property meant to defend against voting devices and servers that have programming errors or are outright malicious. While the first formal definitions of verifiability were devised in the late 1980s already, new verifiability definitions are still being proposed. The definitions differ in various aspects, including the classes of protocols they capture and even their formulations of the very core of the meaning of verifiability. This is an unsatisfying state of affairs, leaving the research on the verifiability of e-voting protocols and systems in a fuzzy state. Cortier, in collaboration with Galindo (U. Birmingham, UK), Küsters, Müller (U. Trier, Germany) and Truderung (Polyas GmbH, Germany), review all formal definitions of verifiability proposed in the literature and cast them in a framework proposed by the KTV framework, yielding a uniform treatment of verifiability. This enables a detailed comparison of the various definitions of verifiability from the literature and a discussion of advantages and disadvantages, limitations and problems. Finally, a general definition of verifiability is distilled, which can be instantiated in various ways. This work has been presented at S&P'16 [26].

Industrial systems are nowadays regularly the target of cyberattacks, the most famous being Stuxnet. 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 (Université Clermont-Ferrand), Potet, and Puys (University 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*, a cryptographic protocol verification tool, they identified several design flaws in some of the different versions of these protocols. We also discussed how to efficiently model counters and timestamps in *TAMARIN*, as they are key ingredients of the analyzed protocols. This work is currently under submission.

7.2. Analysis

7.2.1. Analysis of equivalence properties

Participants: Vincent Cheval, Véronique Cortier, Antoine Dallon, Ivan Gazeau, Steve Kremer, 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 (U. of 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.

In case of an active adversary, and a bounded number of sessions, we made several advances. In [14], Cheval and Kremer, in collaboration with Chadha (U. of Missouri, USA) and Ciobâcă (U. Iasi, Romania), present the theory underlying the *Akiss* tool, a Horn clause resolution based procedure for both under- and over-approximating trace equivalence. They show partial correctness for a large class of cryptographic primitives,

modelled as an arbitrary convergent equational theory that has the finite variant properties. Additionally, termination is shown for subterm convergent theories. Gazeau and Kremer, in collaboration with Baelde (LSV, ENS Cachan) and Delaune (IRISA) have extended the *Akiss* tool with support for exclusive or. They analyse unlinkability in several RFID protocols and resistance to guessing attacks of several password base protocols. 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. Finally, Cheval and Kremer propose a novel decision procedure for verifying trace equivalence. Unlike most existing tools, they support a rich class of cryptographic primitives and protocols that may use else branches. An implementation of the procedure is currently under development.

These results are currently under submission.

7.2.2. Simplification results

Participants: Véronique Cortier, Antoine Dallon, Steve Kremer.

Bounding the number of agent identies is a current practice when modeling a protocol. In 2003, it has been shown that one honest agent and one dishonest agent are indeed sufficient to find all possible attacks, for trace properties. This is no longer the case for equivalence properties, crucial to express many properties such as vote privacy or untraceability. As a first result of his PhD, Antoine Dallon has shown that it is sufficient to consider two honest agents and two dishonest agents for equivalence properties, for deterministic processes with standard primitives and without else branches. More generally, we show how to bound the number of agents for arbitrary constructor theories and for protocols with simple else branches. We show that our hypotheses are tight, providing counter-examples for non action-deterministic processes, non constructor theories, or protocols with complex else branches. This work has been presented at POST 2016 [24] and obtained the EASST best paper award of the ETAPS conference.

When verifying e-voting protocols, one of the difficulties is that they need to be secure for an arbitrary number of malicious voters. In collaboration with Arapinis (U. Edinburgh, UK), Cortier and Kremer identify a class of voting protocols for which only a small number of voters needs to be considered: if there is an attack on vote privacy, for an arbitrary number of honest and dishonest voters, then there is also an attack that involves at most 3 voters (2 honest voters and 1 dishonest voter). In the case where the protocol allows a voter to cast several votes and counts, e.g., only the last one, we also reduce the number of ballots required for an attack to 10, and under some additional hypotheses, 7 ballots. They illustrate the applicability of our results on several case studies, including different versions of Helios and Prêt-à-Voter, as well as the JCJ protocol. For some of these protocols the ProVerif tool is used to provide the first formal proofs of privacy for an unbounded number of voters. This work has been presented at ESORICS 2016 [19].

7.2.3. Analysis of stateful security protocols

Participants: Jannik Dreier, Charles Duménil, Steve Kremer.

In collaboration with Künnemann (U. Saarland, Germany), Kremer proposes *SAPIC* (stateful applied pi calculus), a process calculus with constructs for manipulation of a global state by processes running in parallel. They show that this language can be translated to multiset rewriting rules whilst preserving all security properties expressible in a dedicated first-order logic for security properties. The translation has been implemented in a prototype tool which uses the *TAMARIN* prover as a backend. The tool is applied to several case studies among which a simplified fragment of PKCS#11, the Yubikey security token, and an optimistic contract signing protocol. This work has been published in the Journal of Computer Security [15]. Dreier, Duménil 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 accepted for publication at POST'17.

7.2.4. Analysis of e-voting protocols

Participants: Véronique Cortier, Constantin-Catalin Dragan.

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 the 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 is submitted for publication.

7.2.5. Analysis of Electrum Bitcoin wallet

Participants: Michaël Rusinowitch, Mathieu Turuani.

Electrum is a popular Bitcoin wallet. We introduce a formal modeling in ASLan++ of the two-factor authentication protocol used by the Electrum Bitcoin wallet. This allows us to perform an automatic analysis of the wallet and show that it is secure for standard scenarios in the Dolev Yao model [30]. The result could be derived thanks to some advanced features of the Cl-Atse protocol analyzer such as the possibility to specify i) new intruder deduction rules with clauses and ii) non-deducibility constraints.

7.2.6. Satisfiability Modulo Bridging Theories

Participant: Christophe Ringeissen.

Bridging theories are equational theories defining recursive functions. They are useful to handle equational theories of interest in protocol analysis, as advocated in [48], where a locality approach is promoted to solve the satisfiability problem. In collaboration with Pascal Fontaine (Veridis project-team) and Paula Chocron (IIIA-CSIC Barcelona), we investigate a combination approach for the satisfiability problem modulo this particular non-disjoint union of theories, where a source theory is connected to a target one through a bridging function. In 2016, we have prepared a new full paper unifying previous results presented respectively at CADE 2015 [4] and FroCoS 2015. In that papers, we focused on source theories admitting term-generated models. In [21], we have also explored an extension to deal with terms modulo a congruence relation. This joint work with Raphaël Berthon (ENS Rennes) allows us to consider not only trees but also data structure theories such as lists, multisets and sets.

7.2.7. Analysis of Security Properties for an Unbounded Number of Sessions

Participants: Jonathan Proietto-Stallone, Mathieu Turuani, Laurent Vigneron.

The internship of Jonathan Proietto-Stallone has permitted to study the method described in [37] for analyzing protocols without bounding the number of sessions. We have clarified the formalization of this method, including the consideration of xor and exp operators, and implemented it in *CL-AtSe*.

7.3. Design

7.3.1. E-voting protocols

Participants: Véronique Cortier, Steve Kremer, Peter Roenne.

We propose a new voting scheme, BeleniosRF, that offers both receipt-freeness and end-to-end verifiability. It is receipt-free in a strong sense, meaning that even dishonest voters cannot prove how they voted. We provide a game-based definition of receipt-freeness for voting protocols with non-interactive ballot casting, which we name strong receipt-freeness (sRF). To our knowledge, sRF is the first game-based definition of receipt-freeness in the literature, and it has the merit of being particularly concise and simple. Built upon the Helios protocol, BeleniosRF inherits its simplicity and does not require any anti-coercion strategy from the voters. We implement BeleniosRF and show its feasibility on a number of platforms, including desktop computers and smartphones. This work has been presented at CCS 2016 [26].

Another challenging problem in e-voting is to provide guarantees when the voting platform itself is corrupted. Du-Vote [45] is a recently presented remote electronic voting scheme that aims to be malware tolerant, i.e., provide security even in the case where the platform used for voting has been compromised by dedicated malware. For this it uses an additional hardware token, similar to tokens distributed in the context of online banking. Du-Vote aims at providing vote privacy as long as either the vote platform or the vote server is honest. For verifiability, the security guarantees are even higher, as even if the token's software has been changed, and the platform and the server are colluding, attempts to change the election outcome should be detected with high probability. We provide an extensive security analysis of Du-Vote and show several attacks on both privacy as well as verifiability. We also propose changes to the system that would avoid many of these attacks. This work has been presented at Euro S&P 2016 [28].

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 accepted for publication at Euro S&P'17 [25].

7.3.3. Composition and design of PKIs

Participants: Vincent Cheval, Véronique Cortier.

Public Key Infrastructures (PKIs) is the backbone of public key cryptography, as it ensures that public keys can be correctly linked to identities. Their security typically relies on honest Certificate Authorities that distribute and/or generate keys to all parties. This trust assumption is a vulnerability exploited in numerous attacks. Recent proposals using public logs have succeeded in making certificate management more transparent and verifiable. However, those proposals involve a fixed set of authorities which means an oligopoly is created. Another problem with current log-based system is their heavy reliance on trusted parties that monitor the logs. Cheval, in collaboration with Ryan and Yu (U. Birmingham, UK) propose a distributed transparent key infrastructure (DTKI), which greatly reduces the oligopoly of service providers and allows verification of the behaviour of trusted parties. Their work also formalises the public log data structure and provides a formal analysis of the security that DTKI guarantees. The work has been published in The Computer Journal [17].

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 (U. 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 is currently under submission.

7.3.4. Physical Zero-Knowledge Proofs

Participant: Jannik Dreier.

In this work we develop physical algorithms to realize zero-knowledge proofs for Akari, Takuzu, Kakuro, and KenKen, which are logic games similar to Sudoku. The zero-knowledge proofs allow a player to show that he knows a solution without revealing it. These interactive proofs can be realized with simple office material as they only rely on cards and envelopes. They can thus be used for example for scientific outreach activities, or in teaching. Moreover, we also formalized our algorithms and proved their security. This joint work with Bultel (U. Clermont-Ferrand), Dumas (U. Grenoble Alpes), and Lafourcade (U. Clermont-Ferrand) was published at FUN 2016 [22].

7.3.5. Privacy Protection in Social Networks

Participants: Younes Abid, Abdessamad Imine, Huu Hiep Nguyen, Clément Pascutto, Michaël Rusinowitch, Laura Trivino.

Hiep Nguyen's PhD thesis addresses three privacy problems of social networks: graph anonymization, private community detection and private link exchange. The main goal is to provide new paradigms for publication of social graphs in noisy forms, private community detection over graphs as well as distributed aggregation of graphs via noisy link exchange processes. The graph anonymization problem is solved via two different semantics: uncertainty semantics and differential privacy. For uncertainty semantics, a general obfuscation model is proposed that keeps the expected node degree equal to those in the unanonymized graph. Over the last decade, a great number of algorithms for community detection have been proposed to deal with the increasingly complex networks. However, the problem of doing this in a private manner is rarely considered. We analyze the major challenges behind the problem and propose several schemes to tackle them under differential privacy from two perspectives: input perturbation and algorithm perturbation [29].

We address the problem of rapidly disclosing many friendship links using only legitimate queries (i.e., queries and tools provided by the targeted social network). Our study [18] sheds new light on the intrinsic relation between communities (usually represented as groups) and friendships between individuals. To develop an efficient attack we analysed group distributions, densities and visibility parameters from a large sample of a social network. By effectively exploring the target group network, our proposed algorithm is able to perform friendship and mutual-friend attacks along a strategy that minimizes the number of queries. Pascutto has established a state-of-the-art on inference techniques for social networks. Trivino has developed a user interface for privacy risk evaluation on social networks.

8. Bilateral Contracts and Grants with Industry

8.1. 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 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.

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. CNRS

- CNRS PEPS JCJC INS2I 2016 project VESPA *Verifying Equivalence Security in Protocols: Tools and Algorithms*, duration: 1 year, leader: Jannik Dreier, participant: Vincent Cheval.

  Privacy-related notions such as unlinkability and anonymity are usually expressed as equivalence properties, which are notoriously difficult to prove. Due to the complexity of the protocols and the properties, tool support is a must, yet currently rather limited. Notably, there is currently no tool that can verify unlinkability of the electronic passport for an unbounded number of sessions, or anonymity in certain classic electronic cash protocols. The goal of this project is to enable the proofs for these and similar protocols using two complementary approaches: (1) by significantly advancing the state of the art of the algorithms used inside the tools to improve handling of branching and cryptographic primitives, and (2) by providing new reduction results that simplify the tools' inputs.

- CNRS PEPS INS2I 2016 project ASSI *Analyse de Sécurité de Systèmes Industriels*, duration: 1 year, leader: Pascal Lafourcade (Université Clermont-Ferrand), participant PESTO: Jannik Dreier, other participants: Marie-Laure Potet, Maxime Puys (University 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. Most protocol analysis tools are restricted to analyzing reachability properties while many security properties need to be expressed in terms of some process equivalence. 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.

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 à la 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

- ProSecure (2011-2016) [7]— ERC Starting Grant Project on Provably secure systems: foundations, design, and modularity. The long-term aim of the project is to develop provably secure systems such as security protocols. The goal is to propose foundations for a careful analysis and design of large classes of up-to-date protocols. To achieve this goal, the project is structured in three main tasks. First, we develop general verification techniques for new classes of protocols that are of primary interest in nowadays life like e-voting protocols, routing protocols or security APIs. Second,

[7] http://prosecure.loria.fr

we consider the cryptographic part of the primitives that are used in such protocols (encryption, signatures, ...), obtaining higher security guarantees. Third, we propose modular results both for the analysis and design of protocols. Véronique Cortier is the leader of the project.

- SPOOC (2015–2020) [8]— 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.

  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 (University of Oxford), and Sasa Radomirovic (University of Dundee) on the improvement of the *TAMARIN* prover and the elaboration of a user manual.
- Collaboration with Bogdan Warinschi (Bristol University) on defining game-based privacy for e-voting protocols and isolated execution environments.
- Collaboration with Myrto Arapinis (University of 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 (Ecole Polytechnique de Montréal) on model-checking of collaborative systems.
- Collaboration with John Mullins's group (Ecole Polytechnique de Montréal) on information hiding.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Carlos Castro (UTSM Valparaíso, Chile), July 2015 - June 2016, partly funded as Inria invited researcher
- David Galindo (University of Bimingham), April 2016
- Bogdan Warinschi (University of Bristol), November 2016

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

10. Dissemination

10.1. Promoting Scientific Activities

The CNIL (Commission Nationale Informatique et Liberté) has official recommendations in terms of electronic voting.[9] These recommendations influence the design of e-voting systems that are deployed in France. However, some of the recommendations seem a bit outdated and dedicated to particular classes of systems. Even more importantly, the CNIL recommendations focus on vote privacy but do not say much about verifiability. Véronique Cortier, David Galindo, and Stéphane Glondu formulated new recommendations, submitted to the CNIL. They met some CNIL members to discuss how to integrate some of the propositions to the new version of the CNIL recommendations that should appear in 2017.

Moreover, Véronique Cortier was auditioned by the AFE (Assemblée des Francais de l'étranger) on the security of electronic voting. She has also presented the Belenios protocol to the MENESR (Ministère de l'Éducation National, de l'Enseignement Supérieur et de la Recherche) and to the Open Government Summit at the Sénat. Steve Kremer gave a talk on e-voting at the "Colloque Sécurité Informatique : mythes et réalité" organised by CNRS.

10.1.1. Scientific Events Selection

10.1.1.1. General Chair, Scientific Chair

- Véronique Cortier: HotSpot 2016, 4th Workshop on Hot Issues in Security Principles and Trust. Affiliated with ETAPS 2016.
- Steve Kremer: GRSRD 2016, Grande Region Security and Reliability Day, Nancy, March 2016 (co-chair with J. Pang, U. Luxembourg).

10.1.1.2. Program Committee Chair

- Véronique Cortier: HotSpot 2016, 4th Workshop on Hot Issues in Security Principles and Trust. Affiliated with ETAPS 2016.
- Michaël Rusinowitch: ACM International Workshop on Security And Privacy Analytics, New Orleans, LA, USA, March 11, 2016. (co-chair with Rakesh Verma, U. Houston).

10.1.1.3. Program Committee Member

- Véronique Cortier: LICS 2017, CCS 2016, Concur 2016, E-VoteID 2016, MFCS 2016, EuroS&P 2016.
- Steve Kremer : Voting 2017, Euro S&P 2017, FSTTCS 2016, ESORICS 2016, CSF 2016, Voting 2016, AsiaCCS 2016, ACISP 2016.
- Christophe Ringeissen: FroCoS 2017, UNIF 2017, WRLA 2016, UNIF 2016, IJCAR 2016.
- Michaël Rusinowitch: POST 2016, CRISIS 2016, STM 2016.
- Vincent Cheval: TMPA 2017

10.1.2. Journal

10.1.2.1. Editorial Board Member

- Véronique Cortier: Information & Computation, Journal of Computer Security, ACM Transactions on Information and System Security (TISSEC), Foundations and Trends (FnT) in Security and Privacy.

10.1.2.2. Scientific Committee Member

- Laurent Vigneron: Technique et Sciences Informatiques, Lavoisier.

10.1.3. Invited Talks

- Steve Kremer: 29th IEEE Computer Security Foundations Symposium (CSF'16).

10.1.4. Research Administration

Inria evaluation committee (Steve Kremer)

[9] https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000023174487

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

Jury Senior Research Position (Steve Kremer)

Jury Junior Research Position Inria Nancy-Grand Est (Véronique Cortier, president of the committee)

Jury Professor at Université de Lorraine (Véronique Cortier)

Jury Assistant Professor at Université de Lorraine (Michaël Rusinowitch)

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Licence:

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

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

- Master:

  Véronique Cortier, Security of flows, 20 hours, M2 Computer Science, Telecom Nancy and Mines Nancy, France.

  Abdessamad Imine, Security for XML Documents, 12 hours (ETD), M1, Lorraine University, France.

  Steve Kremer, Security Theory, 24 hours (ETD), M2 Computer science, Lorraine University, France.

  Christophe Ringeissen, Decision Procedures for Software Verification, 18 hours (ETD), M2 Computer science, Lorraine University, France.

  Laurent Vigneron, Security of information systems, 22.5 hours (ETD), M2 Computer science, Lorraine University, France.

  Laurent Vigneron, Security of information systems, 24 hours (ETD), M2 MIAGE – Distributed Information Systems, Lorraine University, France.

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

10.2.2. Supervision

- HDR defended in 2016:

  Abdessamad Imine, Data sharing in collaborative systems, defended on December 9.

- PhD defended in 2016:

  Rémy Chrétien, Decision procedures of equivalence properties, started in October 2012, Véronique Cortier and Stéphanie Delaune
  Huu Hiep Nguyen, Secure Collaboration in Mobile Social Networks, started in November 2013, Abdessamad Imine and Michaël Rusinowitch

- PhD discontinued in 2016:

  Éric Le Morvan, Secure composition of cryptographic protocols, started in October 2013, discontinued in June 2016, Véronique Cortier

- PhD in progress:

  Younes Abid, Privacy control for social networks, started in March 2015. Abdessamad Imine, Michaël Rusinowitch and Orpailleur co-advising.

  Antoine Dallon, Decision procedures for equivalence properties, started in November 2015, Véronique Cortier and Stéphanie Delaune

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

Joseph Lallemand, Type systems for equivalence properties, started in September 2016, Véronique Cortier

Ludovic Robin, Verification of cryptographic protocols using weak secrets, started in October 2014, Stéphanie Delaune and Steve Kremer

10.2.3. Juries

Reviewer for Yang Zhang PhD, Luxembourg (Michaël Rusinowitch)

Examiner for Stefania Dumbrova, Paris-Sud (Michaël Rusinowitch)

Examiner for Jiri Marsik, LORIA (Laurent Vigneron)

Examiner for Robin David, CEA (Steve Kremer)

10.3. Popularization

- Vote Électronique. Véronique Cortier. 1024 – Bulletin de la société informatique de France. Numéro 9, Novembre 2016.
- How to Explain Modern Security Concepts to your Children. Xavier Bultel, Jannik Dreier, Pascal Lafourcade, Malika More. Cryptologia, Taylor & Francis, 2016. [13]
- Comment sécuriser les communications ? Du bon usage des protocoles et de la cryptographie. Vincent Cheval, Joseph Lallemand – Séminaire *La Pépinière 4.1*, Oct 2016, Maisons pour la science au service des professeurs, Nancy.

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, S. CIOBACA, S. KREMER. *Automated Verification of Equivalence Properties of Cryptographic Protocols*, in "Programming Languages and Systems - 21st European Symposium on Programming, ESOP 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012. Proceedings", H. SEIDL (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 7211, pp. 108–127

[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

Doctoral Dissertations and Habilitation Theses

[8] R. CHRETIEN. *Automated analysis of equivalence properties for cryptographic protocols*, Université Paris-Saclay, January 2016, https://tel.archives-ouvertes.fr/tel-01277205

[9] H.-H. NGUYEN. *Social Graph Anonymization*, Universite de Lorraine, November 2016, https://hal.inria.fr/tel-01403474

Articles in International Peer-Reviewed Journals

[10] T. ABBES, A. BOUHOULA, M. RUSINOWITCH. *Detection of firewall configuration errors with updatable tree*, in "International Journal of Information Security", June 2016, vol. 15, n° 3, pp. 301-317 [*DOI :* 10.1007/s10207-015-0290-0], https://hal.inria.fr/hal-01320646

[11] 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

[12] 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

[13] X. BULTEL, J. DREIER, P. LAFOURCADE, M. MORE. *How to Explain Modern Security Concepts to your Children*, in "Cryptologia", November 2016, https://hal.archives-ouvertes.fr/hal-01397035

[14] R. CHADHA, V. CHEVAL, Ş. C. 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

[15] S. KREMER, R. KÜNNEMANN. *Automated Analysis of Security Protocols with Global State*, in "Journal of Computer Security", 2016, vol. 24, n° 5 [*DOI :* 10.3233/JCS-160556], https://hal.inria.fr/hal-01351388

[16] H. NGUYEN, A. IMINE, M. RUSINOWITCH. *Network Structure Release under Differential Privacy*, in "Transactions on Data Privacy", December 2016, vol. 9, n° 3, 26 p. , https://hal.inria.fr/hal-01424911

[17] J. YU, V. CHEVAL, M. RYAN. *DTKI: A New Formalized PKI with Verifiable Trusted Parties*, in "The Computer Journal", 2016, vol. 59, pp. 1695-1713 [*DOI :* 10.1093/COMJNL/BXW039], https://hal.archives-ouvertes.fr/hal-01403899

International Conferences with Proceedings

[18] Y. ABID, A. IMINE, A. NAPOLI, C. RAÏSSI, M. RUSINOWITCH. *Online link disclosure strategies for social networks*, in "The 11th International Conference on Risks and Security of Internet and Systems", Roscoff, France, The 11th International Conference on Risks and Security of Internet and Systems, September 2016, https://hal.inria.fr/hal-01402062

[19] M. ARAPINIS, V. CORTIER, S. KREMER. *When are three voters enough for privacy properties?*, in "21st European Symposium on Research in Computer Security", Heraklion, Crete, Greece, 21st European Symposium on Research in Computer Security, Springer, 2016, https://hal.inria.fr/hal-01351398

[20] 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, 2017, https://hal.inria.fr/hal-01396282

[21] R. BERTHON, C. RINGEISSEN. *Satisfiability Modulo Free Data Structures Combined with Bridging Functions*, in "14th International Workshop on Satisfiability Modulo Theories, affiliated with IJCAR 2016", Coimbra, Portugal, T. KING, R. PISKAC (editors), CEUR Workshop Proceedings, CEUR-WS.org, July 2016, n^{o} 1617, pp. 71–80, https://hal.inria.fr/hal-01389228

[22] X. BULTEL, J. DREIER, J.-G. DUMAS, P. LAFOURCADE. *Physical Zero-Knowledge Proofs for Akari, Takuzu, Kakuro and KenKen*, in "FUN with algorithms 2016", La Maddalena, Italy, E. DEMAINE, F. GRANDONI (editors), FUN with algorithms 2016, June 2016, https://hal.archives-ouvertes.fr/hal-01326059

[23] P. CHAIDOS, V. CORTIER, G. FUCHSBAUER, D. GALINDO. *BeleniosRF: A Non-interactive Receipt-Free Electronic Voting Scheme*, in "23rd ACM Conference on Computer and Communications Security (CCS'16)", Vienna, Austria, October 2016 [*DOI :* 10.1145/2976749.2978337], https://hal.inria.fr/hal-01377917

[24] *Best Paper*
V. CORTIER, A. DALLON, S. DELAUNE. *Bounding the number of agents, for equivalence too*, in "5th International Conference on Principles of Security and Trust (POST'16)", Eindhoven, Netherlands, April 2016, pp. 211-232 [*DOI :* 10.1007/978-3-662-49635-0_11], https://hal.inria.fr/hal-01361286.

[25] 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

[26] V. CORTIER, D. GALINDO, R. KUESTERS, J. MUELLER, T. TRUDERUNG. *SoK: Verifiability Notions for E-Voting Protocols*, in "36th IEEE Symposium on Security and Privacy (S&P'16)", San Jose, United States, May 2016, https://hal.inria.fr/hal-01280445

[27] 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, Proceedings of the 2nd IEEE European Symposium on Security and Privacy, Springer, 2017, https://hal.inria.fr/hal-01396291

[28] S. KREMER, P. RØNNE. *To Du or not to Du: A Security Analysis of Du-Vote*, in "IEEE European Symposium on Security and Privacy 2016", Saarbrucken, Germany, Proceedings of the IEEE European Symposium on Security and Privacy 2016, IEEE Computer Society, March 2016, https://hal.inria.fr/hal-01238894

[29] H. H. NGUYEN, A. IMINE, M. RUSINOWITCH. *Detecting Communities under Differential Privacy*, in "Workshop on Privacy in the Electronic Society - WPES 206", Vienna, Austria, October 2016, pp. 83 - 93, https://hal.inria.fr/hal-01393266

Conferences without Proceedings

[30] M. TURUANI, T. VOEGTLIN, M. RUSINOWITCH. *Automated Verification of Electrum Wallet*, in "3rd Workshop on Bitcoin and Blockchain Research", Christ Church, Barbados, February 2016, https://hal.inria.fr/hal-01256397

Books or Proceedings Editing

[31] R. VERMA, M. RUSINOWITCH (editors). *International Workshop on Security And Privacy Analytics*, IWSPA '16: Proceedings of the 2016 ACM on International Workshop on Security And Privacy Analytics, ACM, New Orleans, United States, 2016, https://hal.inria.fr/hal-01408625

References in notes

[32] M. ARAPINIS, V. CORTIER, S. KREMER, M. RYAN. *Practical Everlasting Privacy*, in "Principles of Security and Trust - Second International Conference, POST 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings", D. BASIN, J. MITCHELL (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 7796, pp. 21–40

[33] 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

[34] 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

[35] 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

[36] 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

[37] Y. CHEVALIER, L. VIGNERON. *Strategy for Verifying Security Protocols with Unbounded Message Size*, in "Journal of Automated Software Engineering", April 2004, vol. 11, n^{o} 2, pp. 141-166

[38] 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

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

[40] 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

[41] 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

[42] 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

[43] 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

[44] 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

[45] G. GREWAL, M. RYAN, L. CHEN, M. CLARKSON. *Du-Vote: Remote Voting with Untrusted Computers*, in "Proc. 28th IEEE Computer Security Foundations Symposium (CSF'11)", IEEE Computer Society Press, 2015

[46] 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

[47] 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

[48] V. SOFRONIE-STOKKERMANS. *Locality Results for Certain Extensions of Theories with Bridging Functions*, in "Automated Deduction - CADE-22, 22nd International Conference on Automated Deduction, Montreal, Canada, August 2-7, 2009. Proceedings", R. A. SCHMIDT (editor), Lecture Notes in Computer Science, Springer, 2009, vol. 5663, pp. 67–83