

# Security and Rewriting

Edited by

Hubert Comon-Lundh<sup>1</sup>, Ralf Küsters<sup>2</sup>, and Catherine Meadows<sup>3</sup>

1 ENS – Cachan, FR

2 Universität Trier, DE

3 Naval Research – Washington, US, meadows@itd.nrl.navy.mil

---

## Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 11332 “Security and Rewriting”.

**Seminar** 15.–18. August, 2011 – [www.dagstuhl.de/11332](http://www.dagstuhl.de/11332)

**1998 ACM Subject Classification** F.4.2 Grammars and Other Rewriting Systems

**Keywords and phrases** Rewriting, Security, Access Control, Protocol Verification

**Digital Object Identifier** 10.4230/DagRep.1.8.53


**Edited in cooperation with** Benedikt Schmidt

## 1 Executive Summary

*Hubert Comon-Lundh*

*Ralf Küsters*

*Catherine Meadows*

**License**  Creative Commons BY-NC-ND 3.0 Unported license  
© Hubert Comon-Lundh, Ralf Küsters, and Catherine Meadows

Security is a fundamental problem in computer science. Because of the possible catastrophic problems that can arise from poor security, the ability to mathematically prove and formally verify the security of computer systems is vital. Research has been ongoing in this area since the 1970’s and has been the subject of many Dagstuhl seminars, including (in the last three years) “Theoretical Foundations of Practical Information Security” (November 2008)<sup>1</sup>, and “Formal Protocol Verification Applied” (October 2007)<sup>2</sup>.

Research on formal proofs of security has demonstrated that rewriting techniques, including completion, narrowing, unification, play a central role in this area, for example:

- Formally modeling the properties of cryptographic primitives: fundamental properties of the cryptographic primitives are presented as algebraic theories and used as a basis for security analysis.
- Automatically proving security protocols: both the protocol and the attacker’s possible actions can be modeled as a rewrite system and unification algorithms play a central role in the security analysis of such systems.
- Formally specifying and verifying security policies: the (possibly infinite) set of allowed transitions may be represented as a finite rewriting system. The views on a documents or a class of documents may be specified by tree automata.

---

<sup>1</sup> <http://www.dagstuhl.de/08491>

<sup>2</sup> <http://www.dagstuhl.de/07421>



- Modeling and analysis of other security-critical applications: rewrite techniques are used to model and analyze the security of web services, APIs and systems for access control.

The goal of this seminar was (i) to bring together researchers who have a background in rewriting techniques and researchers who have a background in security applications (or both) (ii) to answer, among others, the following questions:

- Are there specific problems in rewriting that stems from security applications and would deserve some further research? For instance, do the algebraic theories of cryptographic primitives enjoy some specific properties? Are there restrictions that are relevant to the applications and that would yield more efficient unification/rewriting algorithms? Which new challenges does the addition of an arbitrary attacker context bring? What are the specific problems on tree automata that are brought by security applications?
- What are the limits/successes/failures of rewriting techniques in security applications?
- What are the emerging research areas at the intersection of security and rewriting?

## 2 Table of Contents

### Executive Summary

<i>Hubert Comon-Lundh, Ralf Küsters, and Catherine Meadows</i> . . . . .	53
--	----

### Overview of Talks

Automated Analysis of Access Control Policies <i>Alessandro Armando</i> . . . . .	57
Model Checking of Browser-based Single Sign-On Protocols: an Experience Report <i>Alessandro Armando</i> . . . . .	57
Real-world Key Exchange versus Symbolic Analysis - Where do we stand? <i>Cas Cremers</i> . . . . .	58
Security Analysis in Geometric Logic: To Models via Rewriting <i>Dan Dougherty</i> . . . . .	58
The Margrave policy-analysis tool <i>Dan Dougherty</i> . . . . .	58
Rewrite Specifications of Access Control Policies in Distributed Environments <i>Maribel Fernandez</i> . . . . .	59
Logical Protocol Analysis for Authenticated Diffie-Hellman <i>Joshua D. Guttman</i> . . . . .	59
Formal Specification and Analysis of Security Policies <i>Helene Kirchner</i> . . . . .	60
Transforming Password Protocols to Compose <i>Steve Kremer</i> . . . . .	61
A procedure for verifying equivalence-based properties of cryptographic protocols <i>Steve Kremer</i> . . . . .	61
Asymmetric Unification: A New Unification Paradigm for Cryptographic Protocol Analysis <i>Christopher Lynch</i> . . . . .	62
My Own Little Hilbert's Program <i>Sebastian Moedersheim</i> . . . . .	62
On the Complexity of Linear Authorization Logics (Preliminary Results) <i>Vivek Nigam</i> . . . . .	62
Timed Collaborative Systems <i>Vivek Nigam</i> . . . . .	63
Unbounded Verification and Falsification of Protocols that use Diffie-Hellman Exponentiation <i>Benedikt Schmidt</i> . . . . .	63
Intruder Deduction in Sequent Calculus <i>Alwen Tiu</i> . . . . .	64
Automated Validation of Trust and Security in the Internet of Services <i>Luca Vigano</i> . . . . .	64


**56**      **11332 – Security and Rewriting**

An Environmental Paradigm for Defending Security Protocols	
<i>Luca Vigano</i> . . . . .	65
<b>Participants</b> . . . . .	<b>66</b>

## 3 Overview of Talks

### 3.1 Automated Analysis of Access Control Policies

*Alessandro Armando (University of Genova, IT)*

**License**  Creative Commons BY-NC-ND 3.0 Unported license  
© Alessandro Armando

**Joint work of** Armando, Alessandro; Ranise Silvio


**Main reference** F. Alberti, A. Armando, and S. Ranise, “Efficient Symbolic Automated Analysis of Administrative Role Based Access Control Policies,” Proc. of the 6th ACM Symposium on Information, Computer, and Communications Security (ASIACCS), Hong Kong, March 22–24, 2011.

**URL** <http://dx.doi.org/10.1145/1966913.1966935>

Automated techniques for the security analysis of Role-Based Access Control (RBAC) access control policies are crucial for their design and maintenance. In this talk, we describe an automated symbolic security analysis technique for Administrative RBAC policies. A class of formulae of first-order logic is used to symbolically encode both the policies and the administrative actions upon them. State-of-the-art automated theorem proving techniques are used (off-the-shelf) to mechanize the security analysis procedure. Besides discussing the assumptions for the effectiveness and termination of the procedure, we demonstrate its efficiency through an extensive empirical evaluation.

### 3.2 Model Checking of Browser-based Single Sign-On Protocols: an Experience Report

*Alessandro Armando (University of Genova, IT)*

**License**  Creative Commons BY-NC-ND 3.0 Unported license  
© Alessandro Armando

**Joint work of** Armando, Alessandro; Carbone, Roberto; Compagna, Luca; Cuellar, Jorge; Giancarlo Pellegrino; Sorniotti, Alessandro


**Main reference** A. Armando, R. Carbone, L. Compagna, J. Cuellar, G. Pellegrino, and A. Sorniotti, “From Multiple Credentials to Browser-based Single Sign-On: Are We More Secure?” Proceedings of the 26th IFIP TC-11 International Information Security Conference (SEC 2011), pp. 68–79Luzern, Switzerland, June 7–9, 2011.

**URL** [http://dx.doi.org/10.1007/978-3-642-21424-0\\_6](http://dx.doi.org/10.1007/978-3-642-21424-0_6)

I will report on my experience in formal modeling and model checking one of the most popular web-based SSO protocols, the SAML 2.0 Web Browser SSO Profile. I will outline the challenges posed to model checkers by this type of security protocols. I will then discuss our findings: the discovery of a serious man-in-the-middle attack on the SAML-based SSO for Google Apps and, more recently, the discovery of an authentication flaw in the prototypical use case described in the SAML standard.

### 3.3 Real-world Key Exchange versus Symbolic Analysis - Where do we stand?

*Cas Cremers (ETH Zürich, CH)*


License  Creative Commons BY-NC-ND 3.0 Unported license  
© Cas Cremers

Joint work of Basin, David, Cremers, Cas; Feltz, Michele; Meier, Simon, Schmidt, Benedikt

Real-world applications that require key exchange often use protocols from international standards, such as IEEE P1363, NIST SP800-56, ANSI, or ISO. The design of these protocols is driven by cryptographers; choosing among the proposed protocols also involves engineering considerations, such as efficiency. We study the relation between the desired properties of such protocols, and cryptographic security notions for key exchange, such as the CK and eCK models. We provide symbolic formalizations of the majority of these properties with corresponding automatic tool support. Our symbolic methods have lead to several new results in the cryptographic domain. Although our methods are sufficiently mature to be useful to the designers of key exchange protocols, there are also some types of attack on relevant security properties that are outside of the scope of our symbolic methods.

### 3.4 Security Analysis in Geometric Logic: To Models via Rewriting

*Dan Dougherty (Worcester Polytechnic Institute, US)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Dan Dougherty


Starting from the observations that strand spaces—embodying protocol executions—are models for a certain first-order language and that security goals can be captured by first-order sentences, we present an approach to protocol analysis based on model-finding.

A central role is played by “geometric logic, a logic of finite observations previously studied in the context of denotational semantics.

An important strategic aspect of our approach is the interplay between (i) certain canonical theories incorporating inductive definitions and well-foundedness assumptions and (ii) purely first-order companion theories supporting a model-finding method based on The Chase. The latter is a model-finding method jointly inspired by database theory and rewriting in quasi-equational theories.

### 3.5 The Margrave policy-analysis tool

*Dan Dougherty (Worcester Polytechnic Institute, US)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Dan Dougherty


Joint work of Dougherty, Dan; Fislser, Kathi; Krishnamurthi, Shriram; Nelson, Timothy

Margrave is a policy-analysis tool providing query-based verification and query-based views of policies. It supports "change-impact analysis", allowing a user to compare the effects of multiple policies. It supports reasoning about the combined effects of policies written in different configuration languages, such as a firewall filter and a static router, or a firewall combined with an access-control policy (perhaps on a different component).

In this talk we will focus on the foundations of Margrave: model-finding in order-sorted first-order logic, and describe how Margrave relies on a finite-model theorem, whose proof is based on tree automata.

### 3.6 Rewrite Specifications of Access Control Policies in Distributed Environments

*Maribel Fernandez (King's College – London, GB)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Maribel Fernandez

Joint work of Fernandez, Maribel; Bertolissi, Clara


We present a meta-model for access control that takes into account the requirements of distributed environments, where the resources and the access control policies may be distributed across several sites. This distributed meta-model is an extension of the category-based meta-model studied in [1], from which standard centralised access control models such as MAC, DAC, RBAC, Bell-Lapadula can be derived. We use term rewriting to give an operational semantics to the distributed meta-model, and then show how various distributed access control models can be derived as instances.

#### References

- 1 Clara Bertolissi and Maribel Fernández. *Category-Based Authorisation Models: Operational Semantics and Expressive Power*. In Proc. of 2nd Int'l Symposium on Engineering Secure Software and Systems (ESSoS), 2010, Pisa, Italy, February 3-4, 2010. Lecture Notes in Computer Science, vol. 5965, pp. 140–156, Springer.

### 3.7 Logical Protocol Analysis for Authenticated Diffie-Hellman

*Joshua D. Guttman (Worcester Polytechnic Institute, US)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Joshua D. Guttman

Joint work of Guttman, Joshua D.; Dougherty, Daniel J.

Main reference unpublished

Diffie-Hellman protocols for authenticated key agreement construct a shared secret with a peer using a minimum of communication and using limited cryptographic operations. However, their analysis has been challenging in computational models and especially in symbolic models.

In this paper, we develop a framework for protocol analysis that combines algebraic and strand space ideas. We show that it identifies exact assumptions on the behavior of a certifying authority. These assumptions establish the confidentiality and authentication properties for two protocols, the Unified Model and Menezes-Qu-Vanstone (MQV). For MQV, we establish a stronger authentication property than previously claimed, using a stronger (but realistic) assumption on the certifying authority.

Verification within our framework implies that the adversary has no strategy that works uniformly, independent of the choice of the cyclic group in which the protocol operates. Indeed, we provide an equational theory which constitutes an analysis of these uniform

strategies. We provide an abstraction, the notion of indicator, which leads to easy proofs of protocol correctness assertions.

Computational soundness awaits further investigation.

### 3.8 Formal Specification and Analysis of Security Policies

*Helene Kirchner (INRIA, FR)*

**License** © © © Creative Commons BY-NC-ND 3.0 Unported license  
© Helene Kirchner

**Joint work of** Bourdier, Tony; Cirstea, Horatiu; Jaume, Mathieu

**Main reference** T. Bourdier, H. Cirstea, M. Jaume, H. Kirchner, “Formal Specification and Validation of Security Policies,” 4th Canada-France MITACS Workshop on Foundations & Practice of Security (FPS 2011), Paris (France), May 12–13, 2011. Lecture Notes in Computer Science, vol. 6888.

**URL** <http://hal.inria.fr/inria-00507300/PDF/FormalValidation2010.pdf>

A general approach to model a secured system is to consider a transition system whose transitions are guarded by a security policy.

More precisely the evolution of security information in the system is described by transitions triggered by authorization requests and the policy is given by a set of rules describing the way the corresponding decisions are taken.

Policy rules are constrained rewrite rules whose constraints are first-order formulas on finite domains, which provides enhanced expressive power compared to classical security policy specification approaches like the ones using Datalog, for example.

Such specifications have an operational semantics based on transition and rewriting systems and are thus executable.

Non-termination, conflicts or under-specification of policies are easy to detect. Syntactic conditions over the policy rules, satisfied by a large class of policies, can be given for ensuring consistency and completeness.

The presented framework provides ability to

- Specify a security system and an associated security policy: this clear separation is useful for reusability and composition.
- Execute the specification of a secured system, since it can be compiled into term rewriting rules.
- Analyse the specification related properties: experiments can be performed with existing tools, like model-checkers or invariant verifiers.
- Check security requirements, even when they are expressed in a different specification.

More details can be found in [1].

#### References

- 1 Bourdier, T., Cirstea, H., Jaume, M., Kirchner, H.: *Formal Specification and Validation of Security Policies*, 4th Canada-France MITACS Workshop on Foundations & Practice of Security (FPS 2011), Paris (France), May 12-13, 2011. Lecture Notes in Computer Science, vol. 6888.



### 3.9 Transforming Password Protocols to Compose

*Steve Kremer (ENS - Cachan, FR)*

**License** © ⓘ ⊖ Creative Commons BY-NC-ND 3.0 Unported license  
© Steve Kremer

**Joint work of** Chevalier, Céline; Delaune Stéphanie; Kremer, Steve;

**Main reference** Céline Chevalier, Stéphanie Delaune, and Steve Kremer, “Transforming Password Protocols to Compose,” Proceedings of the 31st Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS’11), Mumbai, India, December 2011, Leibniz International Proceedings in Informatics (LIPIcs), Leibniz-Zentrum für Informatik. To appear.

Formal, symbolic techniques are extremely useful for modelling and analyzing security protocols. They improved our understanding of security protocols, allowed to discover flaws, and also provide support for protocol design.

However, such analyses usually consider that the protocol is executed in isolation or assume a bounded number of protocol sessions. Hence, no security guarantee is provided when the protocol is executed in a more complex environment.

In this paper, we study whether password protocols can be safely composed, even when a same password is reused. More precisely, we present a transformation which maps a password protocol that is secure for a single protocol session (a decidable problem) to a protocol that is secure for an unbounded number of sessions. Our result provides an effective strategy to design secure password protocols: (i) design a protocol intended to be secure for one protocol session; (ii) apply our transformation and obtain a protocol which is secure for an unbounded number of sessions. Our technique also applies to compose different password protocols allowing us to obtain both inter-protocol and inter-session composition.

### 3.10 A procedure for verifying equivalence-based properties of cryptographic protocols

*Steve Kremer (ENS – Cachan, FR)*

**License** © ⓘ ⊖ Creative Commons BY-NC-ND 3.0 Unported license  
© Steve Kremer

**Joint work of** Chadha, Stefan; Ciobaca, Stefan; Kremer, Steve


Indistinguishability properties are essential in formal verification of cryptographic protocols. They are needed to model anonymity properties, strong versions of confidentiality and resistance against offline guessing attacks. We present a procedure for verifying observational equivalence for determinate cryptographic protocols when the number of sessions is bounded. For determinate cryptographic protocols, observational equivalence coincides with trace equivalence. The cryptographic protocols are formalized in a fragment of applied pi-calculus without replication and all communication is over public channels.

As in applied pi-calculus, this fragment is parametrized by a first-order sorted term signature and an equational theory which allows formalization of algebraic properties of cryptographic primitives. Our procedure is sound and complete for subterm convergent theory which can model several used cryptographic primitives.

The procedure is based on a fully abstract modelling of the traces of a bounded number of sessions of the protocols in first-order Horn clauses on which a dedicated resolution procedure is used to decide both reachability properties and observational equivalence. Currently we were unable to prove termination of the procedure which is conjectured. The procedure has been implemented and tested in the KiSs tool.

### 3.11 Asymmetric Unification: A New Unification Paradigm for Cryptographic Protocol Analysis

*Christopher Lynch (Clarkson University – Potsdam, US)*

**License**  Creative Commons BY-NC-ND 3.0 Unported license  
© Christopher Lynch


A new extension of equational unification, called *asymmetric unification*, is introduced.

In asymmetric unification, the equational theory is divided into a set  $R$  of rewrite rules and a set  $E$  of equations. A substitution  $\sigma$  is an asymmetric unifier of a set of equations  $P$  iff for every  $s = t \in P$ ,  $s\sigma$  is equivalent to  $t\sigma$  modulo  $R \cup E$ , and furthermore  $t\sigma$  is in  $E \setminus R$  normal form.

This problem is at least as hard as the unification problem modulo  $R \cup E$  and sometimes harder. The problem is motivated from cryptographic protocol analysis using unification techniques for handling equational properties of operators such as XOR.

### 3.12 My Own Little Hilbert's Program

*Sebastian Moedersheim (Technical University of Denmark – Lyngby, DK)*


**License**  Creative Commons BY-NC-ND 3.0 Unported license  
© Sebastian Moedersheim

**Main reference** Sebastian Moedersheim, “Diffie-Hellman without Difficulty,” FAST 2011, to appear  
**URL** <http://www.imm.dtu.dk/~samo/dh-d.pdf>

There have been a number of relative soundness results that make verification of protocols easier, basically showing that certain restrictive models are without loss of generality. The first of these results concerns only the use of certain typing restrictions in protocol analysis, but it turns out that very similar concepts are helpful for compositional reasoning as well. Another application is to reduce the amount of algebraic reasoning in protocols such as those based on Diffie-Hellman: allowing for the use of pattern matching when receiving Diffie-Hellman half-keys even though actually in reality the agent could not check for such patterns. What these results have in common is to exploit good protocol engineering practice for protocol verification: a good protocol suite should be designed such that every message and non-atomic message part has a unique interpretation or type. My own Hilbert's program tries to recognize all protocols as *samt und sonders wohlgetypt* (completely well-typed); I present some examples where this typing is sound and set out the challenge to find interesting counter-examples.

### 3.13 On the Complexity of Linear Authorization Logics (Preliminary Results)

*Vivek Nigam (LMU München, DE)*

**License**  Creative Commons BY-NC-ND 3.0 Unported license  
© Vivek Nigam


Linear Authorization Logics have been used in the Proof-Authentication Framework (PCA) to specify effect-based policies, such as policies involving consumable resources. A key requirement of PCA is the need to construct proof-objects, which requires proof search. We

demonstrate that the propositional multiplicative fragment of linear authorization logics is undecidable.

Therefore, PCA using simple linear policies might already not be feasible. However, we also identify a first-order fragment for which the provability problem is decidable. In particular, we capitalize on the recent work on the decidability of the reachability problem for MSR systems with balanced actions to identify a fragment of linear authorization logics that is PSPACE-complete, namely the fragment of balanced bipolars. This is accomplished by first formalizing a (sound and complete) correspondence between linear authorization logic provability and MSR reachability and then showing that MSR reachability is PSPACE-complete.

### 3.14 Timed Collaborative Systems

*Vivek Nigam (LMU München, DE)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Vivek Nigam

Time is often a key component used in specifying the rules and the requirements of a collaboration. In this talk, we report on our initial steps in extending with explicit time our previous work on models for collaborative systems with confidentiality. In particular, we discuss conditions for PSPACE-completeness of previous compliance problems extended with explicit time. Finally, we identify and discuss in detail a possible application of our model, namely for clinical investigations.

### 3.15 Unbounded Verification and Falsification of Protocols that use Diffie-Hellman Exponentiation


*Benedikt Schmidt (ETH Zürich, CH)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Benedikt Schmidt  
Joint work of Schmidt, Benedikt; Meier, Simon; Cremers, Cas; Basin, David

We present a method for the automatic analysis of protocols specified as multiset rewriting rules. Our approach accounts for algebraic properties of Diffie-Hellman Exponentiation. We support an expressive fragment of two-sorted first-order logic to formalize security properties. Given a protocol and a property such that our method terminates, it either returns a counterexample or proves that all traces of the protocol satisfy the security property. To illustrate the applicability of the method, we sketch the analysis of the NAXOS authenticated key exchange protocol.

### 3.16 Intruder Deduction in Sequent Calculus

*Alwen Tiu (Australian National University - Canberra, AU)*

**License**  Creative Commons BY-NC-ND 3.0 Unported license  
© Alwen Tiu

**Main reference** Alwen Tiu, Rajeev Gore and Jeremy Dawson, “A proof theoretic analysis of intruder theories,” Logical Methods in Computer Science, 6(3), 2010.


**URL** [http://dx.doi.org/10.2168/LMCS-6\(3:12\)2010](http://dx.doi.org/10.2168/LMCS-6(3:12)2010)

An approach to modeling the intruder in analysing security protocols is to formalise the capabilities of the intruder via a natural deduction calculus, or equivalently, via a rewrite system capturing the proof normalisation processes of the natural deduction system. In proof theory, it is well known that natural deduction systems can be equivalently presented in Gentzen’s sequent calculus.

Sequent calculus enjoys the so-called subformula property, which in many cases entail bounded proof search. Some preliminary results in using sequent calculus as a framework to structure proof search for intruder deduction problems, under a range of intruder models involving extensions of Dolev-Yao model with AC-convergent theories, are presented. Extensions of these sequent-calculus-based techniques to solve deducibility constraints and symbolic trace equivalence problems are also discussed.

### 3.17 Automated Validation of Trust and Security in the Internet of Services

*Luca Vigano (Università di Verona, IT)*

**License**  Creative Commons BY-NC-ND 3.0 Unported license  
© Luca Vigano




**Joint work of** AVANTSSAR

**URL** <http://www.avantssar.eu>

The AVANTSSAR Project ([www.avantssar.eu](http://www.avantssar.eu)) has developed an automated platform that provides a rigorous technology for the formal specification and Automated VALIDatioN of Trust and Security of Service-oriented ARchitectures. This technology, which is being tuned on a number of relevant industrial case studies so to allow for the migration into the development process for software solutions for the Internet of Services, aims at speeding up the development of new network and service infrastructures, enhance their security and robustness, and increase the public acceptance of emerging IT systems and applications based on them. I will present some of the main techniques and technologies that are part of the AVANTSSAR Platform and some of the case studies it has been applied on. In particular, to illustrate the platform on the field, I will discuss some of our industrial case studies, including a brief account of our formal analysis of a SAML Web Browser Single Sign-On Protocol. I will also present the first results of the SPaCIoS Project ([www.spacios.eu](http://www.spacios.eu)) that has been combining the AVANTSSAR Platform with techniques and tools for penetration and vulnerability testing to allow for the automated validation of services at provision and consumption time.

### 3.18 An Environmental Paradigm for Defending Security Protocols

*Luca Vigano (Università di Verona, IT)*

**License**    Creative Commons BY-NC-ND 3.0 Unported license  
© Luca Vigano

**Joint work of** Fiazza, Maria-Camilla; Peroli, Michele; Vigano, Luca

**Main reference** Maria-Camilla Fiazza and Michele Peroli and Luca Vigano, Attack Interference in Non-Collaborative Scenarios for Security Protocol Analysis, Proceedings of SECURE 2011, 144–156, SciTePress, 2011

Although computer security typically revolves around threats, attacks and defenses, the sub-field of security protocol analysis (SPA) has so far focused almost exclusively on the notion of attack. We wish to show that such focus on attacks depends on few critical assumptions that have been characteristic of the field and have governed its mindset, approach and developed tools. We motivate that indeed there is room in SPA for a fruitful notion of defense and that the conceptual bridge lies in the notion of multiple non-collaborating attackers. To support SPA for defense-identification, we propose a paradigm shift that brings security closer to the conceptual tools of fields that have a rich notion of agent, such as robotics and AI — in contrast to the weak notion of agent that is typical of SPA. These fields, however, lack the required understanding of how to instantiate their tools in a manner that is informative for security analysis. Hence, our main contribution is a novel paradigm for defending security protocols, based on importing into SPA well-established techniques and tools from robotics and AI. At the conceptual and methodological level these techniques form a cohesive picture, which can prompt a parallel development in our understanding of protocols as environments.

## Participants

- Myrto Arapinis  
University of Birmingham, GB
- Alessandro Armando  
University of Genova, IT
- Yannick Chevalier  
Université Paul Sabatier –  
Toulouse, FR
- Hubert Comon-Lundh  
ENS – Cachan, FR
- Cas Cremers  
ETH Zürich, CH
- Stéphanie Delaune  
ENS – Cachan, FR
- Dan Dougherty  
Worcester Polytechnic Inst., US
- Santiago Escobar  
Universidad Politécnica –  
Valencia, ES
- Maribel Fernandez  
King's College – London, GB
- Cédric Fournet  
Microsoft Research UK –  
Cambridge, GB
- Joshua D. Guttman  
Worcester Polytechnic Inst., US
- Hélène Kirchner  
INRIA, FR
- Steve Kremer  
ENS – Cachan, FR
- Ralf Küsters  
Universität Trier, DE
- Christopher Lynch  
Clarkson Univ. – Potsdam, US
- Catherine Meadows  
Naval Res. – Washington, US
- José Meseguer  
Univ. of Illinois – Urbana, US
- Sebastian Mödersheim  
Technical University of Denmark  
– Lyngby, DK
- Paliath Narendran  
Univ. of Albany – SUNY, US
- Vivek Nigam  
LMU München, DE
- Michaël Rusinowitch  
INRIA Lorraine, FR
- Mark D. Ryan  
University of Birmingham, GB
- Ralf Sasse  
Univ. of Illinois – Urbana, US
- Benedikt Schmidt  
ETH Zürich, CH
- Helmut Seidl  
TU München, DE
- Slawomir Staworko  
University of Lille III, FR
- Carolyn L. Talcott  
SRI – Menlo Park, US
- Sophie Tison  
Université de Lille I, FR
- Alwen Tiu  
Australian National University –  
Canberra, AU
- Tomasz Truderung  
University of Wrocław, PL
- Luca Vigano  
Università di Verona, IT
- Christoph Weidenbach  
MPI für Informatik –  
Saarbrücken, DE

