07421 Abstracts Collection
Formal Protocol Verification Applied
— Dagstuhl Seminar —

Liqun Chen[1], Steve Kremer[2] and Mark D. Ryan[3]

[1] HP Labs - Bristol, UK
liqun.chen@hp.com
[2] LSV, ENS Cachan, CNRS, INRIA, FR
kremer@lsv.ens-cachan.fr
[3] Univ. of Birmingham, UK
M.D.Ryan@cs.bham.ac.uk

Abstract. From 14/10/2007 to 19/10/2007, the Dagstuhl Seminar 07421 "Formal Protocol Verification Applied" was held in the International Conference and Research Center (IBFI), Schloss Dagstuhl. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

Keywords. Security protocols, formal verification, trusted computing, biometrics, security of mobile computing, electronic voting, payment systems

07421 Executive Summary – Formal Protocol Verification Applied

Security protocols are a core part of distributed computing systems, and are part of our everyday life since they are used in web servers, email, mobile phones, bank transactions, etc. However, security protocols are notoriously difficult to get right. There are many cases of protocols which are proposed and considered secure for many years, but later found to have security flaws. Formal methods offer a promising way for automated security analysis of protocols. While there have been considerable advances in this area, most techniques have only been applied to academic case studies and security properties such as secrecy and authentication. The seminar brought together researchers deploying security protocols in new application areas, cryptographers, and researchers from formal methods who analyse security protocols. The interaction between researchers from these different communities aims to open new research topics, e.g., identify new security properties that need verification and refine abstractions of the abstract models of crytpographic primitives.

Dagstuhl Seminar Proceedings 07421
Formal Protocol Verification Applied
http://drops.dagstuhl.de/opus/volltexte/2008/1419

Keywords: Security protocols, formal verification, trusted computing, biometrics, security of mobile computing, electronic voting, payment systems

Joint work of: Chen, Liqun ; Kremer, Steve ; Ryan, Mark D.

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2008/1418

Secure Group Key Exchange

Frederik Armknecht (Ruhr-Universität Bochum, D)

This talk is on some of our recent work on group key exchange (GKE) protocols. After an introduction into the subject of GKE protocols, our recently proposed GKE protocol is described. The protocol requires two broadcast rounds and is provably secure within the universal composability (UC) framework. The second property ensures that the protocol can be securely combined with other protocols secure within the UC framework. Moreover, it can be shown that any UC-secure GKE protocol requires at least two communication rounds, that is, our protocol is optimal in that sense.

The talk concludes by discussing some unsolved problems and pointing out future work.

Verifying Implementations of the Information Card Federated Identity-Management Protocol

Karthik Bhargavan (Microsoft Research UK - Cambridge, GB)

I will describe reference implementations for selected configurations of the card-based user authentication protocol ("InfoCard") implemented within Windows Vista. I will show how we prove authentication and privacy properties of these protocol implementations using our tool FS2PV, relying on the theorem prover ProVerif.

Keywords: Protocol verification, verified implementations, federated identity management

Joint work of: Bhargavan, Karthik; Fournet, Cedric; Gordon, Andy; Swamy, Nikhil

CryptoVerif: A Computationally Sound Mechanized Prover for Cryptographic Protocols

Bruno Blanchet (Ecole Normale Supérieure - Paris, F)

We present CryptoVerif, a mechanized prover for secrecy and correspondence properties of security protocols.

In contrast to most previous provers, CryptoVerif does not rely on the Dolev-Yao model, but on the computational model. It produces proofs presented as sequences of games, as used by cryptographers; these games are formalized in a probabilistic polynomial-time process calculus.

CryptoVerif provides a generic method for specifying security assumptions on cryptographic primitives, which can handle shared-key and public-key encryption, signatures, message authentication codes, and hash functions. It produces proofs valid for a number of sessions polynomial in the security parameter, in the presence of an active adversary.

Keywords: Cryptographic protocols, computationally sound, automatic verification

Full Paper:
http://www.cryptoverif.ens.fr

See also: Bruno Blanchet. A Computationally Sound Mechanized Prover for Security Protocols. In IEEE Symposium on Security and Privacy, pages 140-154, Oakland, California, May 2006.

Modular Preservation of Safety Properties by Cookie-Based DoS-Protection Wrappers

Rohit Chadha (Univ. of Illinois - Urbana, USA)

Current research on verifying security properties of communication protocols has focused on proving integrity and confidentiality using models that include a strong Man-in-the-Middle (MitM) threat. By contrast, protection measures against Denial-of-Service (DoS) must assume a weaker model in which an adversary has only limited ability to interfere with network communications. In this paper we demonstrate a modular reasoning framework in which a protocol that satisfies certain security properties can be assured to retain these properties after it is “wrapped” in a protocol that adds DoS protection. This modular wrapping is based on the “onion skin" model of actor reflection. In particular, we show how a common DoS protection mechanism based on cookies can be applied to a protocol while provably preserving safety properties (including confidentiality and integrity) that it was shown to have in an MitM threat model.

Joint work of: Chadha, Rohit; Gunter Carl A.; Meseguer, Jose; Shankesi, Ravinder; Viswanathan, Mahesh

Making Random Choices Invisible to the Scheduler

Kostas Chatzikokolakis (Ecole Polytechnique - Palaiseau, F)

When dealing with process calculi and automata which express both nondeterministic and probabilistic behavior, it is customary to introduce the notion of scheduler to resolve the nondeterminism.

It has been observed that for certain applications, notably those in security, the scheduler needs to be restricted so not to reveal the outcome of the protocol's random choices, or otherwise the model of adversary would be too strong even for "obviously correct" protocols. In this talk I present a process-algebraic framework in which the control on the scheduler can be specified in syntactic terms, and I show how to apply it to solve the problem mentioned above. I also consider the definition of (probabilistic) may and must preorders, and show that they are precongruences with respect to the restricted schedulers. Furthermore, I show that all the operators of the language, except replication, distribute over probabilistic summation, which is a useful property for verification. This framework is applied to the dining cryptographers problem, where the scheduler problem comes into play.

Joint work of: Chatzikokolakis, Kostas; Palamidessi, Catuscia

Full Paper:
http://www.lix.polytechnique.fr/∼catuscia/papers/Scheduler/report.pdf

Simplified Security Notions of Direct Anonymous Attestation

Liqun Chen (HP Lab - Bristol, GB)

Direct Anonymous Attestation (DAA) is a special signature scheme that enables remote authentication of a user while preserving privacy under the user's control.

In this talk, a new formal specification and security model of DAA will be introduced.

It is intended to address the same concept of a DAA scheme and to cover the same security properties that the DAA scheme should hold, as introduced by Brickell, Camenisch and Chen in ACMCCS 2004. However, hopefully, this new interpretation would be easier to read than the relative content in the original DAA paper, and would be helpful for readers to understand and accept the concept of DAA and its security properties.

The security model of a DAA scheme is specified with two new security notions, namely user-controlled-anonymity and user-controlled-traceability. The talk will focus on the formal definition of the two notions, and will also compare them with the full-anonymity and full-traceability notions of group signatures, as defined by Bellare, Micciancio and Warinschi in EUROCRYPT 2003.

As a case study, the talk will briefly cover the security proof of a new DAA scheme from bilinear maps. The scheme makes use of the Camenisch and Lysyanskaya pairing-based signature scheme.

This talk is based on the results of a joint work with Ernie Brickell and Jiangtao Li.

Soundness of symbolic equivalence

Hubert Comon-Lundh (AIST - Tokyo, J)

We revisit some of the soundness/completeness results of abstract cryptography, after defining a general notion of symbolic equivalence.

We emphasize some pending questions, which may be subject to discussion.

Keywords: Security protocols, cryptography

Secure Implementations for Typed Session Abstractions : Secrecy and Integrity

Ricardo Corin (INRIA-MSR - Orsay, F)

I will present ongoing work on compiling high level session types specifications into secure cryptographic protocols.

Complete Characterization of Security Protocols by Pattern Refinement

Cas Cremers (ETH Zürich, CH)

Recently, the notion of complete characterizations of security protocols was introduced by Guttman and Thayer. We provide an alternative definition of this concept, and extend an existing protocol verification tool (Scyther) to compute our notion of complete characterization.

We present both notions of complete characterization, discuss their relative merits, and provide preliminary empirical results using an extended version of the Scyther tool.

Keywords: Security protocols, formal analysis, verification tools

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1417

Secure Pairing with Biometrics: the SAfE protocol

Sandro Etalle (University of Twente, NL)

Alice and Bob want to exchange a secret, but all the knowledge they have of each other is a vague picture (no public keys). They have found a protocol based on fuzzy extractors they believe secure. But will the protocol withstand Dagstuhl verification? And how do you verify a protocol that uses guessing and fuzzy extractors?

Keywords: Authentication, biometrics, secure pairing

Joint work of: Buhan, Ileana; Doumen, Jeroen; Hartel, Pieter; Veldhuis, Raymond; Etalle, Sandro

Full Paper:
http://eprints.eemcs.utwente.nl/10783/

Cryptographically Sound Implementations for Typed Information-Flow Security

Cédric Fournet (Microsoft Research UK - Cambridge, GB)

In language-based security, confidentiality and integrity policies conveniently specify the permitted flows of information between different parts of a program with diverse levels of trust.

These policies enable a simple treatment of security, and they can often be verified by typing. However, their enforcement in concrete systems involves delicate compilation issues.

We consider cryptographic enforcement mechanisms for imperative programs with untrusted components.

Such programs may represent, for instance, distributed systems connected by some untrusted network.

In source programs, security depends on an abstract information-flow policy for accessing the shared memory.

In their implementations, shared memory is unprotected and security depends instead on encryption and signing.

We build a translation from well-typed source programs and policies to cryptographic implementations. To establish its correctness, we develop a cryptographic type system for a target probabilistic language. Our typing rules enforce the correct usage of cryptographic primitives against active adversaries; from an information-flow viewpoint, they capture controlled forms of robust declassification and endorsement.

We show type soundness for a variant of the non-interference property, then show that our translation preserves typability.

We rely on concrete primitives and hypotheses for cryptography, stated in terms of probabilistic polynomial-time algorithms and games. We model these primitives as commands in our target language.

Thus, we develop a uniform language-based model of security, ranging from computational non-interference for probabilistic programs down to standard cryptographic hypotheses.

Joint work of: Fournet, Cédric; Rezk, Tamara

Full Paper:
http://www.msr-inria.inria.fr/projects/sec/cflow

Security Types for Implementations of Cryptographic Protocols

Andrew Gordon (Microsoft Research UK - Cambridge, GB)

We implement a logic-based type checker to support verification of security protocols and authorization decisions expressed as executable ML programs.

Joint work of: Bengtson, Jesper; Bhargavan, Karthikeyan; Fournet, Cédric; Gordon, Andrew; Maffeis, Sergio

FT Electronic Purse, a small but challenging protocol

Francis Klay (France Telecom - Lannion, F)

In this talk we present partial results and perspectives for an electronic purse protocol issued from France Telecom. The goal was to prove that the protocol is secure or that there is an attack. Modeling this protocol requires algebraic properties of a fragment of arithmetic, typically containing modular exponentiation. The usual equational theories described in papers on security protocols are too weak: this small and simple protocol cannot even be executed in these models.

Keywords: Cryptographic protocols, verification, electronic purse

Composition of Password-based Protocols

Steve Kremer (ENS - Cachan, F)

We investigate the composition of protocols that share a common secret. This situation arises when users employ the same password on different services. More precisely we study whether resistance against guessing attacks composes when a same password is used. We model guessing attacks using a common definition based on static equivalence in a cryptographic process calculus close to the applied pi calculus. We show that resistance against guessing attacks composes in the presence of a passive attacker. However, composition does not preserve resistance against guessing attacks for an active attacker. We therefore propose a simple syntactic criterion under which we show this composition to hold. Finally, we present a protocol transformation that ensures this syntactic criterion and preserves resistance against guessing attacks.

Cryptographic and Formal Analysis of Contract Signing Protocols

Ralf Küsters (ETH Zürich, CH)

Some cryptographic tasks, such as contract signing and other related tasks, need to ensure complex, branching time security properties.

When defining such properties one needs to deal with subtle problems regarding the scheduling of non-deterministic decisions, the delivery of messages sent on resilient (non-adversarially controlled) channels, fair executions (executions where no party, both honest and dishonest, is unreasonably precluded to perform its actions), and defining strategies of adversaries against all possible non-deterministic choices of parties and arbitrary delivery of messages via resilient channels. Unlike formal models, these problems are typically not, or not all, addressed in cryptographic models and these models therefore do not suffice to formalize branching time properties, such as those required of contract signing protocols.

In this talk, a cryptographic model that deals with all of the above problems is proposed. One central feature of this model is a general definition of fair scheduling which not only formalizes fair scheduling of resilient channels but also fair scheduling of actions of honest and dishonest principals. Based on this model and the notion of fair scheduling, a definition of a prominent branching time property of contract signing protocols, namely balance, is provided, along with the first cryptographic proof that the Asokan-Shoup-Waidner two-party contract signing protocol is balanced. In the talk, recent work on the formal analysis of contract signing and related protocols in a Dolev-Yao style model will also be discussed.

The talk is based on the following publications: ESORICS 2007 (with Veronique Cortier and Bogdan Warinschi), ICALP 2006 (with Detlef Kaehler and Thomas Wilke), and LICS 2007 (with Detlef Kaehler and Tomasz Truderung).

A Federated Unsplittable Privacy-Protecting Multi-Coupon Scheme

Hans Löhr (Ruhr-Universität Bochum, D)

A multi-coupon represents a collection of k coupons that a user can redeem to a vendor in exchange for some goods or services. In FC 2007, a privacy-protecting multicoupon scheme with protection against splitting was presented. However, in this scheme, the coupons in a multi-coupon have to be redeemed in a sequential order that has to be fixed when the multi-coupon is issued. This imposes limitations on the use of the multi-coupon scheme when different types of coupons are used in one multi-coupon.

In this paper, we overcome this limitation and propose a scheme where the coupons can be redeemed in an arbitrary order. The communication and computation complexity of issuing a multi-coupon is O(k), the complexity for redeeming a single coupon is constant. If different types of coupons do not have to be supported, the complexity of issuing could be reduced to O(log k). Moreover, we generalize the scheme to support a federation of vendors, which requires a generalized formal framework, new security requirements and proofs.

Keywords: Coupon, privacy, unsplittability, unlinkability, loyalty, federation

Zero-Knowledge in the Applied Pi-calculus and Automated Verification of the Direct Anonymous Attestation Protocol

Matteo Maffei (Saarland University, D)

We devise an abstraction of zero-knowledge protocols that is accessible to a fully mechanized analysis. The abstraction is formalized within the applied pi-calculus using a novel equational theory that abstractly characterizes the cryptographic semantics of zero-knowledge proofs. We present an encoding from the equational theory into a convergent rewriting system that is suitable for the automated protocol verifier ProVerif. The encoding is sound and fully automated. We successfully used ProVerif to obtain the first mechanized analysis of the Direct Anonymous Attestation (DAA) protocol. The analysis in particular required us to devise novel abstractions of sophisticated cryptographic security definitions based on interactive games.

Keywords: Language-based security, zero-knowledge proofs, applied pi-calculus, direct anonymous attestation

Joint work of: Backes, Michael; Maffei, Matteo; Unruh, Dominique

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1415

OFMC: Models and Methods for the Automated Analysis of Security Protocols

Sebastian Mödersheim (IBM Research - Zürich, CH)

OFMC (On-the-Fly Model-Checker for Security Protocols) is one of the analysis tools of the AVISPA toolset. The talk will focus on the two most recent extensions of OFMC. The first is the integration of algebraic reasoning in a generic way, namely that the user can specify an algebraic theory as part of the problem to check; we will discuss what restrictions are necessary for decidability. The second is the integration of techniques based on over-approximation and abstract interpretation. These techniques can help to overcome the bound to a finite number of sessions in the verification, and also may speed up verification. We give a formal comparison of several models at different levels of over-approximation, and show that the reasoning is sound for secrecy and a certain specification of authentication goals.

Formal approaches to Information-hiding - An overview -

Catuscia Palamidessi (Ecole Polytechnique - Palaiseau, F)

We give an overview of various formal approaches from literature to information-hiding: The possibilistic approaches, the probabilistic approaches, the information-theoretic approaches, and the one based on statistical inference.

We compare the various frameworks and point out the relations. Finally, we show how to specify information-hiding protocols and verify them (in the various approaches) using language-based techniques.

Keywords: Anonymity, probability, information theory, hypothesis testing, model checking

Full Paper:
http://www.lix.polytechnique.fr/∼catuscia/papers/Anonymity/Channels/full.pdf
http://www.lix.polytechnique.fr/∼catuscia/papers/ProbabilityError/full.pdf

Provable security - an introduction

Kenny Paterson (Royal Holloway Univ. - London, GB)

In this talk, I will give a general introduction to provable security, with an emphasis on:
* the basic formalism of the approach,
* the scope of its application, and
* its strengths and weaknesses.

Keywords: Provable security

Towards Characterising Observational Equivalence in the Applied Pi-Calculus

Eike Ritter (University of Birmingham, GB)

Proverif does not always allow automatic verification of static equivalence in the Applied Pi-calculus. In this talk I present characterisations of static equivalence for a class of substitutions and establish some compositionality results.

Security evaluation of scenarios based on the TCG's TPM Specification

Carsten Rudolph (Fraunhofer SIT - Darmstadt, D)

The Trusted Platform Module TPM is a basic but nevertheless very complex security component that can provide the foundations and the root of security for a variety of applications. In contrast to the TPM, other basic security mechanisms like cryptographic algorithms or security protocols have been subject to thorough security analysis and formal verification. This paper presents a first methodic security analysis of a large part of the TPM specification. A formal automata model based on asynchronous product automata APA and a finite state verification tool SHVT are used to emulate a TPM within an executable model. On this basis four different generic scenarios were analysed with respect to security and practicability: secure boot, secure storage, remote attestation and data migration. A variety of security problems and inconsistencies was adapted to overecome the problems identified. In this paper, the analysis of the remote attestation scenario and some of the problems found are explained in more detail.

Joint work of: Gürdens, Sigrid; Rudolph, Carsten; Scheuermann, Dirk; Atts, Marion; Plaga, Rainer

Verifying privacy-type properties of electronic voting protocols

Mark D. Ryan (University of Birmingham, GB)

Electronic voting promises the possibility of a convenient, efficient and secure facility for recording and tallying votes in an election. Recently highlighted inadequacies of implemented systems have demonstrated the importance of formally verifying the underlying voting protocols. We study three privacy-type properties of electronic voting protocols: in increasing order of strength, they are vote-privacy, receipt-freeness, and coercion-resistance.

We use the applied pi calculus, a formalism well adapted to modelling such protocols, which has the advantages of being based on well-understood concepts.

The privacy-type properties are expressed using observational equivalence and we show in accordance with intuition that coercion-resistance implies receipt-freeness, which implies vote-privacy.

We illustrate our definitions on three electronic voting protocols from the literature. Ideally, these three properties should hold even if the election officials are corrupt. However, protocols that were designed to satisfy receipt-freeness or coercion-resistance may not do so in the presence of corrupt officials. Our model and definitions allow us to specify and easily change which authorities are supposed to be trustworthy.

Keywords: Electronic voting, vote privacy, coercion resistance, property verification

Joint work of: Delaune, Stephanie; Kremer, Steve; Ryan, Mark D.

Full Paper:
http://www.cs.bham.ac.uk/∼mdr/research/papers/index.html

See also: To appear in Journal of Computer Security. Expected 2008.

Security Protocols on Trusted Platforms: Tutorial

Ahmad-Reza Sadeghi (Ruhr-Universität Bochum, D)

The advent of e-commerce, e-government, and the rapid expansion of world-wide connectivity demands end-user systems that adhere to well-defined security policies. In this context Trusted Computing (TC) aims at providing a framework and effective mechanisms that allow computing platforms and processes in a distributed IT system to ain assurance about each other's integrity/trustworthiness. An industrial attempt towards realization of TC is the initiative of the Trusted Computing Group (TCG), an alliance of a large number of IT enterprises. The TCG has published a set of specifications for extending conventional computer architectures with a variety of security-related features and cryptographic mechanisms. The TCG approach has not only been subject of research but also public debates and concerns. Currently, several prominent academic and industrial research projects are investigating trustworthy IT systems based on TC, virtualization technology, and secure operating system design.

In this tutorial we highlight some special aspects of Trusted Computing and give a short overview of the TCG approach and associated shortcomings and present some current research challenges.

Automatic verification of privacy properties in the applied pi calculus

Ben Smyth (University of Birmingham, GB)

Abstract: We develop a formal method verification technique for cryptographic protocols. We focus on proving equivalences of the kind P Q, where the processes P and Q have the same structure and differ only in the choice of terms. The calculus of ProVerif, a variant of the applied pi calculus, makes some progress in this direction. We expand the scope of ProVerif, to provide reasoning about further equivalences. We also provide an extension which allows modelling of protocols which require global synchronisation. Finally we develop an algorithm to enable automated reasoning. We demonstrate the practicality of our work with two case studies.

Keywords: Security, formal verification, automated verification, equivalence, ProVerif, applied pi calculus.

Computationally Sound Mechanized Proofs of Basic and Public-key Kerberos

Joe-Kai Tsay (University of Pennsylvania, USA)

In this talk, we present a computationally sound mechanized analysis of Kerberos 5, both with and without its public-key extension PKINIT.

We prove authentication and key secrecy properties using the prover CryptoVerif, which works directly in the computational model; these are the first mechanical proofs of a full industrial protocol at the computational level. We also generalize the notion of key usability and use CryptoVerif to prove that this definition is satisfied by keys in Kerberos.

Towards an Automatic Analysis of Web Services Security

Laurent Vigneron (LORIA & Nancy University, F)

Web services send and receive messages in XML syntax with some parts hashed, encrypted or signed, according to the WS-Security standard. In this paper we introduce a model to formally describe the protocols that underly these services, their security properties and the rewriting attacks they might be subject to. Unlike other protocol models (in symbolic analysis) ours can handle non-deterministic receive/send actions and unordered sequence of XML nodes. Then to detect the attacks we have to consider the services as combining multiset operators and cryptographic ones and we have to solve specific satisfiability problems in the combined theory. By non-trivial extension of the combination techniques of [3] we obtain a decision procedure for insecurity of Web services with messages built using encryption, signature, and other cryptographic primitives. This combination technique allows one to decide insecurity in a modular way by reducing the associated constraint solving problems to problems in simpler theories.

Keywords: Security, web services, verification, cryptographic protocols, combination of decision procedures, equational theories, rewriting

See also: Yannick Chevalier, Denis Lugiez, and Michaël Rusinowitch. Towards an Automatic Analysis of Web Service Security. In Franck Wolter, editor, Proceedings of the 6th International Symposium on Frontiers of Combining Systems (FroCoS'07), volume 4720 of Lecture Notes in Artificial Intelligence, pages 133-147, Liverpool, UK, September 2007. Springer.