Report on DIMACS* Workshop on Security Analysis of Protocols

Date of workshop: June 7 – 9, 2004

Workshop Organizers:

John Mitchell, Stanford University
Ran Canetti, IBM Watson

Report Author:

Zhiqiang Yang
Department of Computer Science, Stevens Institute of Technology

Date of Report: July 27, 2005

*DIMACS was founded as a National Science Foundation Science and Technology Center. It is a joint project of Rutgers University, Princeton University, AT&T Labs-Research, Bell Labs, NEC Laboratories America, and Telcordia Technologies, with affiliated partners Avaya Labs, HP Labs, IBM Research, Microsoft Research, and Stevens Institute of Technology.

1 Workshop Focus

The analysis of cryptographic protocols is a fundamental and challenging area of network security research. Traditionally, there have been two main approaches. One is the logic approach aimed at developing automated tools for the formal verification of protocols. The other is the computational or complexity-theoretic approach that characterizes protocol security as a set of computational tasks and proves protocol security via reduction to the strength of the underlying cryptographic functions. The challenge in security analysis is whether the two approaches have similar properties and whether they can be linked together by some methods. This workshop explored the current techniques addressing the compatibility problem between the computational approach and the logic approach for the analysis of security protocols. This workshop provided tutorials on security analysis of both approaches and the research on both approaches were presented by researchers from the two communities. The commonality between the two approaches was explored and some results in that area were presented and discussed. The topics discussed in this workshop include: analysis methods involving computational complexity, probabilistic methods, model checking and symbolic search, formal proof systems, and decision procedures and lower bounds.

2 Summary of Presentations

2.1 Tutorial: Formal Methods and Protocol Analysis

Speaker: Peter Ryan, University of Newcastle Upon Tyne

This talk briefly reviewed the history of security protocol analysis and listed current formal methods (FM). The speaker introduced several formal methods, e.g. BAN logic (Burrows, Abadi, Needham), Dolev-Yao approach, CSP (Communicating Sequential Processes) approach. BAN logic can be used to reason about security properties of protocols. For BAN logic, the basic notations were given and the drawbacks of BAN logic were also discussed. The problem of authentication was discussed by giving the example of the Lowe attack on Needham-Schroeder public key protocol. The basic ideas and the adversary model in the Dolev-Yao approach were introduced briefly. The CSP approach was discussed in detail. First the syntax, semantics and specifications of CSP were introduced. Then examples of the representations of trustworthy agents, adversaries and systems were given.

Properties of CSP, such as authentication, non-repudiation, and secrecy were also discussed thoroughly. Richer adversary models beyond Dolev-Yao were demonstrated, e.g. computation/complexity and capacity of monitoring and intercepting limitations. The speaker listed the analogies between crypto folk and FM folk. One of the speaker's recommendations is to turn FMs into an engineering discipline.

2.2 Modeling and Analyzing Security Protocols Using I/O Automata

Speaker: Nancy Lynch, MIT

Within the I/O (Input/Output) automata framework, the speaker described formal models and proofs for the composition of two security protocols: a simple shared-key communication protocol and the Diffie-Hellman key distribution protocol. The speaker introduced the basic concepts of I/O automata and the standard I/O techniques including invariant assertions, forward simulation relations, and compositional reasoning. Some basic automata for security protocols was also introduced, e.g. environment, insecure channel, and eavesdropper. The abstract service specifications and implementations of private communication (PC) and key distribution (KD) were modelled and proved by standard I/O automata techniques in this talk. The composition of the two systems of PC and KD was discussed by using the ordinary I/O automata composition. The speaker also commented that possible future work would extend to complex protocols with active adversaries by using timed I/O and probabilistic I/O automata.

2.3 Automata-based Analysis of Recursive Cryptographic Protocols

Speaker: Thomas Wilke, Kiel University

This talk proved decidability of security for a class of recursive protocols and undecidability for several extensions. A recursive authentication protocol was discussed as an example of protocols that need recursive actions. The message model, the action model (tree transducer), the intruder models (w.r.t. Dolev-Yao intruder), and the protocol model in its proof were discussed. The key ingredient of the protocol model is specifically designed tree transducers that work over infinite signatures and have the ability to generate new constants. The speaker gave the proof of the main theorem

that *it is decidable whether a protocol is secure*. The decidability result is based on an automata-theoretic construction. The speaker concluded that group protocols and web services would be the potential area of application.

2.4 Formal Analysis of Availability

Speaker: Carl A. Gunter, University of Pennsylvania

First the speaker observed that there was excellent progress on formal analysis of integrity and confidentiality, e.g. algebraic and complexity-theoretic techniques, but modest progress on formal analysis on availability. The problems of analysis on availability are limited to formal models, not automation and there are few case studies. The speaker introduced some progress towards formal analysis of DoS (Denial of Services) by giving corresponding case studies. Three key concepts in this talk are: (1) shared channel model (2) selective processing countermeasures and (3) asymmetry paradigm. Shared channel model is realistic and is a four-tuple(W_0, W_1, A, p) where W_0 and W_1 denote the minimum and maximum of the sender's bandwidth, A denotes the attacker's maximum bandwidth, and p denotes the loss rate of the sender. Experimental results show that selective verification is very effective. The idea of the asymmetry paradigm is to inflate the cost of a resource that the attacker consumes at a greater rate, so that it becomes a bottleneck for the attacker before being able to deny service. The TCP (Transmission Control Protocol) case was studied with its corresponding experimental results. From this talk, it can be seen that progress is possible on formal analysis of availability.

2.5 Tutorial: Towards Cryptographically Sound Formal Analysis

Speaker: Daniele Micciancio, UCSD

The tutorial presented a brief overview of the work bridging the gap between the symbolic and computational approaches to the modelling and analysis of security protocols. A detailed case study (secure multicast) exemplified how symbolic methods can be profitably used by cryptographers to prove computational security properties. The example was also used to pinpoint limitations of current cryptographic techniques and illustrate how to cope with these limitations within the symbolic setting. Some open problems in cryptography and formal methods were described in this talk. In

cryptography, the research direction and goals are to find encryption schemes such that soundness of encrypted expressions holds without the acyclicity restriction and to find encryption schemes such that adaptive soundness of encrypted expressions holds without any syntactic restriction. In formal methods, the research direction and goals are to extend with other cryptographic primitives and to universal composability settings.

2.6 A Reactively Secure Dolev-Yao-Style Cryptographic Library

Speaker: Birgit Pfitzmann, IBM Research

This talk presented a reactively secure cryptographic library like the Dolev-Yao model for automated proofs. The speaker first gave a brief introduction to the Dolev-Yao approach and other related variants, then a new approach was presented. A new notion called reactive simulatability was explained: everything that can happen to users of the real system in the presence of an arbitrary adversary A can also happen to the users in the ideal system, where attack capabilities are usually much more restricted, in the presence of an adversary A'. The ideal cryptographic library was presented in detail. In this talk, it was observed that the main differences from the Dolev-Yao model are tolerable imperfections, i.e., imperfections that must be allowed. Examples include: the lengths of encrypted messages cannot be kept secret; the adversary may include incorrect messages inside encryptions; and signature schemes can have memory. The real cryptographic library was presented following the ideal one. In the real one the main additions to given cryptosystems are Type tags-Tagging with keys and additional randomization.

2.7 Towards Automated Computationally Faithful Verification of Cryptoprotocols

Speaker: Jan Jürjens, TU Munich

This speaker presented his ongoing work of automated verification using first-order logic ATP's (automated theorem prover) of the Dolev-Yao style. This talk also introduced one European project named "VeriSoft" whose goal is the practical application of formal methods. Briefly, the idea of security analysis in first-order logic is to predict whether the adversary gets to know some secret if a set of control flow diagrams (of C-programs) and an

approximate set of possible values are known to the adversary. A proposed variant of TLS (Transport Layer Security) as an example was discussed in detail. In this talk, it was proven that work towards automated verification is efficient, simple, and computationally faithful, but it gives up theoretical completeness, and complexity theory is still just a theoretical model.

2.8 Computational and Information-Theoretic Soundness and Completeness of the Expanded Logics of Formal Encryption

Speaker: Gergei Bana, University of Pennsylvania

In the expanded formalism of the Abadi-Rogaway logic of indistinguishability of formal cryptographic expressions, the speaker demonstrated how to establish soundness and completeness for a variety of interpretations. Two such interpretations were discussed in detail: a purely probabilistic one that interprets formal expressions in One-Time Pad, and another one in the type 2 (which-key revealing) cryptosystems based on computational complexity. A new, general technique for proving completeness was presented by the speaker. Future research will include new primitives, extend the formalism to include adaptive adversaries, and relate their work with information-theoretic models.

2.9 Universally Composable Symbolic Analysis of Cryptographic Protocols

Speaker: Jonathan Herzog, MIT

The speaker demonstrated how Dolev-Yao style symbolic analysis can guarantee universally composable (UC) security. The speaker first introduced the UC framework and the Dolev-Yao model extended with local outputs. Then the speaker gave two examples, mutual authentication and key exchange protocols, to show how to translate a protocol in the UC framework to a symbolic protocol. Meanwhile, the speaker demonstrated that if the symbolic protocol satisfies a certain symbolic condition then the original protocol is UC-secure. Future work will include how to prove Dolev-Yao real-or-random, symbolic representations for other types of tasks, and whether similar results can be achieved for protocols using symmetric encryption, signatures, or Diffie-Hellman.

2.10 Tutorial - Secure Composition of Multiparty Protocols

Speaker: Yehuda Lindell, IBM Research

The speaker first gave a brief review of results in security computation. In summary, any distributed task can be carried out securely in a stand-alone model of computation. But it has been shown that security in the stand-alone setting does not imply security under protocol composition. In modern network settings, secure protocols are run concurrently (or "composed") with other arbitrary protocols. The interaction of different protocols with each other can be exploited by malicious parties to mount successful attacks on protocols that are secure when considered in isolation. In order to ensure security in modern network settings like the Internet, these "new" adversarial threats must be explicitly considered. A survey was given of what is known regarding the feasibility of obtaining security in this general adversarial setting. In this tutorial, a number of different models were considered and both positive and negative results that provide a rather comprehensive picture of feasibility were presented. Finally this tutorial discussed future work, including the continuing study of the feasibility in (realistic) restricted networks and considering weaker notions of security definitions.

2.11 New Notions of Security: Achieving Universal Composability without Trusted Setup

Speaker: Manoj Prabhakaran, Princeton University

The speaker demonstrated a modification to the framework of Universally Composable (UC) security, which gives secure protocols for tasks for which no secure protocol is possible in the original UC framework (except with trusted setup). The new notion introduced in this talk involves comparing the protocol executions with an ideal execution involving ideal functionalities (just as in UC-security), but allowing the environment and adversary access to some super-polynomial computational power. The new notion in particular subsumes many of the traditional notions of security. The speaker generalized the Universal Composition theorem to the new setting. Then under new computational assumptions, the speaker demonstrated the realization of secure multiparty computation (for static adversaries), without a common reference string or any other setup assumptions. Future work will include investigating/simplifying the assumptions, extending to adaptive adversaries, and getting simpler/more efficient protocols and an even

more realistic environmental security model.

2.12 Documented Ideal Protocols: A Flexible Notion of Universal Composability for Simple Protocols and no Trusted Setup

Speaker: Dominic Mayers, CalTech

The speaker generalized the universally composable (UC) security definition to use a new kind of ideal protocol, the documented ideal protocol. A documented ideal protocol uses ideal channels and an incorruptible party just as an ordinary ideal protocol. The main difference between this proposed approach and the standard case is that the simulator in this approach can execute special operations that must be specified in the documented ideal protocol and taken into account when the security of the higher level application protocol is considered. In this talk, two simple bit commitment protocols were proven universally composable with respect to this new definition. The speaker also used these composable bit commitments in some simple application protocols that do not realize any standard ideal protocol to illustrate a generalized UC framework that includes a much larger class of protocols.

2.13 A Probabilistic Polynomial-time Calculus for the Analysis of Cryptographic Protocols

Speaker: Andre Scedrov, University of Pennsylvania

The speaker described properties of a process calculus that has been developed for the purpose of analyzing security protocols. The process calculus is a restricted form of CCS (Calculus of Communicating Systems), with bounded replication and probabilistic polynomial-time expressions allowed in messages and boolean tests. This talk also introduced the properties of a form of asymptotic protocol equivalence that allows security to be specified using observational equivalence. Using a form of probabilistic bisimulation, the speaker gave an equational proof system for reasoning about process equivalence. Two examples, computational indistinguishability and Decision Diffie-Hellman & ElGamal encryption were discussed in detail. Future work is to simplify semantics, weaken bisimulation technique to generate asymptotic equivalences, and apply the technique to more complex protocols.

2.14 Sequential Process Calculus and Machine Models for Simulation-based Security

Speaker: Ralf Kuesters, University of Kiel

The speaker presented a sequential probabilistic polynomial-time process calculus (SPPC) that served as a basis for comparing related work on simulation-based security. The speaker introduced SPPC as a general computational model for simulation-based security notions that allows one to embed other models. First, different variants of security notions were reviewed. Then SPPC was discussed including its important features and advantages. By using representations of communicating Turing machines and I/O Automata in SPPC, one is able to compare three related simulation-based security notions: universal composability, black-box-simulatability, and process observational equivalence. The relationships and differences between different security notions were proved in the results section. In future work, the speaker will try to find whether there are realistic attacks in a concurrent (non-sequential) framework that can not be captured by a sequential framework.

2.15 Tutorial: Security Protocols and Trust

Speaker: Joshua D. Guttman, MITRE

The speaker described how to use the strand space formalism to study cryptographic protocols. In this tutorial, the speaker introduced a widely applicable method called the authentication test method, to determine exactly what authentication and secrecy goals a protocol achieves. Needham-Schroeder, Needham-Schroeder-Lowe and Yahalom protocols were used to illustrate how to use that kind of method. The speaker demonstrated how to use the same ideas as a heuristic to create new (demonstrably correct) protocols by developing a new electronic commerce protocol–electronic purchase with a money order.

2.16 Machine-Checked Formalization of the Generic Model and the Random Oracle Model

Speaker: Sabrina Tarento, INRIA

By using the proof assistant Coq, the speaker provided a machine-checker account of the Generic Model (GM) and the Random Oracle Model (ROM)

and some of its applications, e.g. ElGamal. Briefly speaking, Coq is a general purpose proof assistant based on the Calculus of Inductive Constructions and allows the development and checking of mathematical proofs in a high order logic. The speaker presented the formalization of a generic algorithm and an interactive generic algorithm in this talk. Future work discussed by the speaker included reasoning about attacks and the extension of Paulson's Model by using the ideas from GM and ROM.

2.17 Monte-Carlo Analysis of Protocols

Speaker: Radu Grosu, SUNY Stony Brook

The speaker presented the Monte-Carlo Analysis of security protocols with the example of Needham-Schroeder (NS) protocol. The LTL (Linear Temporal Logic) model checking and Monte-Carlo model checking (MC^2) were introduced with other related concepts. The speaker then presented the experimental results from the implementations of DDFS (Double Depth-First Search) and MC^2 in jMocha model checker for synchronous systems specified using Reactive Modules, where NS was specified as a reactive module and all communications went through an intruder who obeyed the Dolev-Yao model. The experimental results indicated that Monto-Carlo model checking may be more effective than traditional approaches in discovering attacks. But further experimentation is required to draw definitive conclusions.

2.18 A Framework for Security Analysis with Team Automata

Speaker: Marinella Petrocchi, IIT-CNR, Italy

The speaker showed a framework based on team automata (TA) that can be effectively used for formal security analysis. The origins and foundations of TA and an example of TA over component automata were presented. This talk gave the definition of an insecure communication scenario for team automata, which is general enough to encompass various communication protocols. Then this talk reformulated the Generalized Non-Deducibility on Compositions schema—originally introduced in the context of process algebras—in terms of team automata. Based on the new framework, the speaker subsequently presented a compositional analysis strategy that can be used for the verification of security properties in a variety of communication protocols. The integrity of EMSS (Efficient Multi-chained Stream Signature)

protocol was illustrated as a case study.

2.19 Tutorial: Formal Representations of Polynomial-time Algorithms and Security

Speaker: Bruce Kapron, University of Victoria

In this tutorial, the speaker showed the methodologies of formalizing polynomial time function(al)s. The importance of the formalization of PPT (Probabilistic Polynomial Time) was discussed first. Then the speaker presented several function algebras which characterize poly-time functions. Recursion on notation (RN) was introduced. Briefly, it uses primitive recursion on binary notation of the recursion parameter to capture polynomial time. While discussing the drawbacks of RN, bounded recursion on notation, safe composition and recursion on notation, and full concatenation recursion on notation were presented. Finally, a methodology for reduction proofs was given by presenting an example of stretching the output of PRG (Pseudorandom Generator). From this tutorial, it can be derived that formal reasoning about PPT functions in cryptographic settings is doable in a fairly direct way, but it still seems far from practical application. What is needed is to extend this methodology to more complex notions (e.g. pseudorandom functions, zero knowledge) and arguments and extensions of function algebras.

2.20 Collusion-Free Protocols

Speaker: Silvio Micali, MIT

The speaker put forward a new notion of secure protocols, namely, collusion-free protocols, in which malicious parties are prevented from colluding during run time. Those kinds of protocols prevent the traditional problem that secure protocols just minimize the damage inflictable by malicious colluding parties, but do not prevent the collusion. The speaker also showed how to implement Collusion-Free protocols under general complexity assumptions. The key feature of collusion-free protocols is that they make steganography provably impossible.

2.21 A Framework for Fair (Multi-Party) Computation

Speaker: Juan Garay, Bell Labs

The speaker presented the problem of constructing fair secure multi-party computation (FMPC) protocols. The speaker first discussed the drawbacks of the previous security definitions for fairness. With the secure and fair definitions, the speaker proposed a new approach to construct FMPC protocols. The proposed approach allows protocols to depend on the running time of adversaries. This approach admits constructions that tolerate up to $(n-1)$ corruptions and avoids the impossibility result for FMPC in corrupted majority ($t \geq n/2$), where n is the total number of parties and t is the number of corrupted parities. With the proposed "commit-proved-fair-open" functionality in this talk, the speaker showed that some of the existing secure MPC protocols can be easily transformed into fair protocols while preserving their security. The speaker also demonstrated that the FMPC framework is a variation of the Universal Composability framework, but with modifications so that the ideal process in it is fair. Determining the adversary's time dynamically rather than fixing the time in advance is the speaker's future work.

2.22 Dolev-Yao-type Abstraction of Modular Exponentiation - the Cliques Case Study

Speakers: Olivier Pereira and Jean-Jacques Quisquater, UCL

By using Cliques authenticated group key agreement protocols as a case study, the speaker presented a new message algebra based on a Dolev-Yao abstraction of modular exponentiation: atomic elements are elements of a freely generated abelian group G. By systematic reasoning with this algebra on the case study of the Cliques authenticated group key agreement protocols, the speaker showed that these protocols do not achieve the expected security properties and that it is impossible to define a scalable Cliques-type authenticated group key agreement protocol guaranteeing implicit key authentication. The speaker also observed that this is the first such generic insecurity result reported in the literature of authentication protocols. Some open questions in this area include transposing the impossible result to other classes of protocols and proving other protocols secure when considering an infinite number of sessions.

2.23 Message Equivalence and Imperfect Cryptography in a Formal Model

Speaker: Angelo Troina, Univerity of Pisa

The speaker presented the compatibility problem between the computational approach and the Dolev-Yao model for the analysis of security protocols. In particular, the speaker presented a novel equivalence for cryptographic expressions that overcomes the two limitations of classical security models: perfect cryptography and a nondeterministic adversary. Their framework takes into account the probability of a polynomial time adversary attacking with success a message encrypted with a secret key. In their framework, equivalence among formal cryptographic expressions is parameterized by a computational adversary that may exploit weaknesses of the cryptosystem to analyze ciphertexts with a certain probability of success. The speaker introduced a new compatibility relation– ε-probabilistic similarity that approximates the equivalence by introducing a tolerance to small differences and also allows for equating those ciphertexts that can be decrypted with small probabilities. By presenting the novel framework, the speaker offered the means for defining a formal cryptographic language where information leakage due to cryptanalysis can be estimated by employing "probabilistic equivalence" and conditional statements, and probabilistic covert channels can be studied by verifying non-interference security properties. Future work will use the proposed similarity relation in combination with an approximated definition of non-interference to verify whether the privacy of cryptographic protocols can be guaranteed at a reasonable level.

2.24 Tutorial: Constraint-based Methods: Adding Computational Properties to Symbolic Models

Speaker: Vitaly Shmatikov, SRI

The speaker proposed a symbolic analysis method for cryptographic protocols, and presented recent decidability results for formal protocol analysis in the presence of XOR, Abelian group operator, and modular exponentiation from an arbitrary base. The speaker first gave a brief review of current protocol analysis techniques. Then A-GDH.2 Protocol was discussed and analyzed as an example to demonstrate this new method. The speaker showed that this new method can be extended with algebraic theories for XOR, modular multiplication, and Diffie-Hellman push-button procedure

for finding both Dolev-Yao and algebraic attacks within a finite number of sessions. Current and future research in this area is to construct axiomatic models of various cryptographic primitives.

2.25 Towards a Hierarchy of Cryptographic Protocol Models

Speaker: Cathy Meadows, NRL

The speaker outlined a theory for cryptographic protocol analysis based on a hierarchy of models and also showed how different work by different people in different areas took a common approach. The speaker showed that it is not always necessary to restrict ourselves to two models. Instead, this talk proposed a hierarchy of models, so that models at one level of the hierarchy can be shown sound with respect to models at a lower level of the hierarchy if certain conditions are satisfied. The speaker also discussed what kinds of statements can be guaranteed to be sound in the hierarchy, and what kinds of conditions can be put into the system. The speaker gave an example of an intermediate model to demonstrate that using an intermediate model might make sense sometimes. One of the open questions is what the best way is to give a usable hierarchy.

2.26 Sound Approximations to Diffie-Hellman Using Rewrite Rules

Speaker: Christopher Lynch, Clarkson University

The commutative property (C) of exponentiation is necessary to model the Diffie-Hellman (DH) protocol. The speaker presented an efficient theory H to approximate the commutativity soundly. The speaker derived simple properties for a DH protocol to satisfy, and the speaker showed that if a protocol has these properties then a C-attack can be converted to an H-attack. Future work includes converting H-attack to C-attack, and considering group DH protocols.

2.27 Fine-Grained MSR Specifications for Quantitative Security Analysis

Speaker: Iliano Cervesato, NRL

The speaker outlined a methodology for assigning a precise measure of cost to protocol actions and computing it over traces. In this methodol-

ogy, the protocol actions includes both the Dolev-Yao kind as well as non traditional forms. This allows cost-conscious tools to extend the operations available to an intruder beyond the Dolev-Yao model. This quantitative methodology enables the evaluation of protocol resilience to various forms of denial of service, guessing attacks, and resource limitation. The speaker used a low-level variant of the security protocol specification language MSR (MultiSet Rewriting)–Fine-Grained MSR to illustrate this methodology. Future work will include reporting on preliminary experiments with WEP and pursue experimentation on resource-conscious protocols designed with denial-of service in mind, such as JFK. Costs expressed as complexity bounds will be further investigated.

2.28 Summary of Open Problems and Future Research Challenges

In this workshop, researchers pointed out a variety of open problems and future challenges that deserve further investigation. Those open problems and challenges apply to both the cryptography and formal methods communities. One of the key challenges is the compatibility problem between the two communities, and there is still a big gap between the two communities. Many of the open problems and future challenges are listed as follows:

- Turn formal methods into an engineering discipline.
- Apply formal reasoning about PPT functions to practical applications.
- Determine whether there are realistic attacks in a concurrent (non-sequential) framework that can not be captured by a sequential framework.
- Determine whether Paulson's model can be formalized by using the similar ideas that are used to formalize the random oracle model and generic model.
- Promote team automata for security analysis.
- In secure composition of security protocols, feasibility in (realistic) restricted networks or under weaker notions of security definitions needs to be further explored.
- Investigate an even more realistic environmental security model towards the goal of universal composability without trust setup or simplified assumptions, and extend to adaptive adversaries.

- Explore fairness in secure multiparty protocols, e.g., without the limited power of adversaries. Is it possible to determinate the adversaries' power dynamically?
- Extend formal methods with other cryptographic primitives and extend to a universal composability setting.
- Cryptographers should find an encryption scheme such that soundness of encrypted expressions holds without the acyclicity restriction, and adaptive soundness of encryptions holds without any syntactic restriction.
- Further investigate more complex protocols with active adversaries by using probabilistic and timed IO automata.
- Find a usable hierarchy of cryptographic protocols models.

3 Acknowledgement

The author and the DIMACS Center acknowledge the support of the National Science Foundation under grant number CCR 03-14161 to Rutgers University.