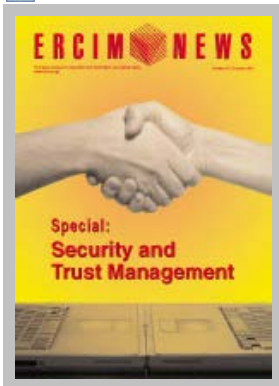


This issue in pdf
(64 pages; 30Mb)

Subscription

Archive:

previous issue:
Number 62
July 2005:
Special theme:
Multimedia Informatics

previous issues online

Next issue:
January 2006

Next Special theme:
Emergent Computing

Call for the next issue

About ERCIM News

Using Probabilistic I/O Automata to Improve the Analysis of Cryptographic Protocols

by Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira and Roberto Segala

Modelling cryptographic protocols and analysing their security is a tricky business. On the one hand, valid modelling and analysis must address the concurrency aspects of asynchronous distributed systems, with potentially adversarial scheduling of events. On the other hand, realistic analysis must accommodate the fact that, in most interesting cases, it is impossible to completely prevent successful attacks against the protocol. Instead, we can only bound the success probability of attacks that use a bounded amount of computational resources, based on underlying computational hardness assumptions.

Cryptographic modelling and analysis is typically complex, involving many subtleties and details, even when the analysed protocols are simple. Furthermore, analysis is handwritten and often tedious to verify. These factors make the security analysis of cryptographic protocols susceptible to errors and omissions.

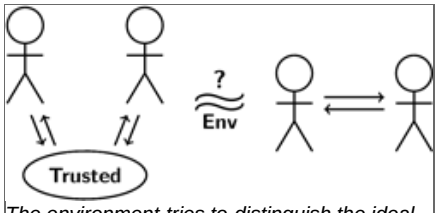
This project demonstrates how to cast cryptographic security analysis of distributed protocols within the Probabilistic I/O Automata (PIOA) framework of Lynch, Segala and Vaandrager. This framework provides standard tools for arguing rigorously about the concurrency and scheduling aspects of protocols. It supports reasoning with multiple levels of abstraction and has a well-defined notion of composition. Consequently, using the PIOA framework can help in making cryptographic analysis more precise and less susceptible to errors.

In the context of this project, we aim to develop general techniques applicable to the analysis of a wide range of security protocols that exhibit various levels of complexity in terms of adversarial behavior or the use of cryptographic primitives. As a first step, we are currently analysing a relatively simple protocol, the two-party Oblivious Transfer (OT) protocol, in the presence of a semi-honest adversary (essentially, an eavesdropper). The particular OT protocol we are studying is the classic protocol by Even, Goldreich and Lempel, which uses trapdoor permutations (and hard-core predicates for them) as the underlying cryptographic primitive. For the underlying cryptographic notion of security, we start from Canetti's Universally Composable Security.

In spite of the relative simplicity of the investigated case, the exercise is non-trivial and requires addressing a number of fundamental issues. These include modelling resource-bounded computations, resource-bounded adversarial behaviour and scheduling, combining non-deterministic and probabilistic choices, and modelling computational hardness assumptions. Some of these are beyond the reach of the existing semantic theory of probabilistic I/O automata. This project therefore involves using not only probabilistic I/O automata in security protocol analysis but also extending the basic theory to address the requirements of such analysis.

Approach

One common approach to simplifying cryptographic protocol analysis and improving its correctness is to model cryptographic primitives as 'symbolic operations', or 'ideal boxes', which represent the security properties of the primitives in an idealized way that involves no error probabilities or computational issues. This approach is quite promising; however, it does not completely remove the need for cryptographic analysis of protocols. Rather, it only proves the security of the overall protocol by assuming the security of the cryptographic primitives in use. One still has to prove the security of these primitives in a fully fledged cryptographic model with all its subtleties. Our project proposes an alternative (in fact, complementary) approach to making cryptographic protocol analysis more systematic and rigorous, and thus less susceptible to errors.



The environment tries to distinguish the ideal-world system, representing the specification of the protocol, from the real-world system running the actual protocol.

We benefit from the powerful proof techniques that have traditionally been used within I/O automaton

frameworks. In particular, we express the system at multiple levels of abstraction, where the highest level in the abstraction hierarchy represents the specification of the protocol and the lowest represents the real-world system running the protocol. We demonstrate simulation relations between these levels that allow us to conclude that the real-world system implements the abstract specification. The composition operation for PIOAs makes it possible to separate the specification of correctness and security requirements of the protocol, and to express the real-world system naturally, as a composition of logically separate units interacting with another.

Future Work

We would like to assess the techniques we have developed so far in the analysis of more complex protocols. This complexity arise through more powerful adversaries, more complex interaction patterns between the components of the protocol, or more subtle uses of cryptographic primitives.

One limitation of our current approach is that the existing scheduling mechanism is oblivious to execution histories and hence significantly limits the capabilities of the adversarial components. We will investigate how our assumptions about task-PIOAs and scheduling mechanisms can be relaxed to enable the analysis of a larger class of protocols.

Once our modelling and proof techniques become more general and established, we can focus on mechanizing our proofs with interactive theorem-provers, or even automate some or all of the proof steps.

Please contact:

Olivier Pereira, Université catholique de Louvain (FNRS), Belgium
Tel: +32 10 47 91 63
E-mail: pereira@dice.ucl.ac.be