

4th Cisca-Loria workshop – Formal Methods 28 Avril 2022

09:00 – 09:30

Welcome coffee

09:30 – 09:40

Opening words by Antoine Joux and Marine Minier

09:40 – 10:10

That nagging thing in the back of your mind:

Rethinking how symbolic analysis tools model cryptographic primitives

Cas Cremers, CISPA (<https://people.cispa.io/cas.cremers/>)

The Dolev-Yao symbolic, black-box model of cryptographic primitives has proven to be very effective during the last 30 years to develop automated tools that can prove the correctness of, or find attacks on, security protocols. During this time, there have been many developments that have made these tools more effective and scalable, enabling the analysis of large real-world protocols using automated tools such as Tamarin and ProVerif.

During all this time, the basic modeling of cryptographic primitives barely changed, until very recently. In this talk, we will talk about how nagging ideas in the back of one's head and scientific conferences lead us to revisit the foundations of the symbolic modeling approach and show how this work had many implications within symbolic approaches, computational analyses, and beyond.

10:10 – 10:40

Formal verification in action: an in-depth case study of LAKE-EDHOC

Steve Kremer, PESTO Team-LORIA/INRIA (<https://members.loria.fr/SKremer/>)

The IETF is working on a Lightweight Authenticated Key Exchange (LAKE) protocol called EDHOC (EphemeralDiffie-Hellman Over COSE) suitable for constrained devices. Following a call by the IETF working group for formal verification we started an in-depth analysis of the current version of EDHOC. Our analysis uses the recent SAPIC+ platform which allows to use the Tamarin, ProVerif and DeepSec provers, while starting from a same specification. We also exploit several recent results in formal verification that allow to relax the perfect cryptography assumptions on Diffie-Hellman groups, digital signatures and hash functions. While we mainly confirmed security, we also identified several weaknesses and possibilities to strengthen the protocol which is currently in discussion with IETF.

This is joint work with Charlie Jacomme (CISPA), Elise Klein and Maïwenn Racouchot (Inria Nancy & LORIA).

10:40 – 11:10 **Time break**

11:10 – 11:40

DY*: A Modular Symbolic Verification Framework for Executable Cryptographic Protocol Code

Tim Würtele, University of Stuttgart (<https://www.sec.uni-stuttgart.de/institute/team/Wuertele/>)

DY* is a recent formal verification framework for the symbolic security analysis of cryptographic protocol code written in the F* programming language. Unlike automated symbolic provers, DY* accounts for advanced protocol features like unbounded loops and mutable recursive data structures, as well as low-level implementation details like protocol state machines and message formats, which are often at the root of real-world attacks.

As such, DY* extends a long line of research on using dependent type systems for this task, but takes a fundamentally new approach by explicitly modeling the global trace-based semantics within the framework, hence bridging the gap between trace-based and type-based protocol analyses. This approach enables us to uniformly, precisely, and soundly model, for the first time using dependent types, long-lived mutable protocol state, equational theories, fine-grained dynamic corruption, and trace-based security properties like forward secrecy and post-compromise security. DY* is built as a library of F* modules that includes a model of low-level protocol execution, a Dolev-Yao symbolic attacker, and generic security abstractions and lemmas, all verified using F*. The library exposes a high-level API that facilitates succinct security proofs for protocol code.

DY* has been used to analyze - in addition to several standard protocols such as Needham-Schroeder-Lowe - the Signal protocol with the first mechanized proof of Signal to account for forward and post-compromise security over an unbounded number of protocol rounds, as well as the ACME certificate issuance and management protocol with a level of detail that lets the ACME client model interoperate with other ACME servers. This talk will introduce DY*, present the ACME analysis, and discuss current work done on DY*.

11:40 – 12:10

Prophecy Made Simple

Stephan Merz, Veridis team-LORIA/INRIA (<https://members.loria.fr/Stephan.Merz/>)

Although refinement mappings are the standard technique for showing that one specification implements another, it is well known that there are cases where no refinement mapping exists. Abadi and Lamport (AL) therefore proposed adding auxiliary variables to a specification, and they proved that refinement mappings can be found by adding history and prophecy variables for specifications satisfying certain conditions. While AL's prophecy variables were elegant in theory, they turned out to be difficult to use in practice. We describe a new kind of prophecy variables that we find easier to understand and to use, and we prove the completeness of the technique, without requiring AL's conditions.

12:30 – 14:00 **Lunchtime**

14:00 – 14:30

Logics for the Specification of Hyperproperties

Jana Hofmann, CISP A (<https://www.react.uni-saarland.de/people/hofmann.html>)

Hyperproperties relate multiple execution traces of a system. They occur in various areas of computer science: examples are information flow policies like noninterference and observational determinism, but also robustness properties, symmetry, and optimality. To understand the similarities and differences between different hyperproperties, we need to study hyperproperties on a logical level. In this talk, I will present different logics for the specification of hyperproperties, ranging from temporal logics to first-order and second-order logics. I will discuss which logics are best suited for which classes of hyperproperties and compare their expressiveness, resulting in a hierarchy of hyperlogics. Finally, I present a hyperlogic for reasoning about infinite-state systems and showcase its expressiveness on the example of smart contracts.

14:30 – 15:00

Probabilistic Hyperproperties of Markov Decision Processes

Rayna Dimitrova, CISPÀ (<https://raynadimitrova.github.io/>)

Hyperproperties describe the correctness of a system as a relation between multiple executions. They generalize trace properties and include information-flow security requirements, like noninterference, as well as requirements like symmetry, partial observation, robustness, and fault tolerance.

In this talk I will present a recently introduced temporal logic for the specification of hyperproperties of Markov decision processes (MDPs), called Probabilistic Hyper Logic (PHL). PHL extends classic probabilistic logics with quantification over schedulers and traces. It can express a wide range of hyperproperties for probabilistic systems, including both classical applications, such as probabilistic noninterference and differential privacy, as well as novel applications in areas such as planning. A consequence of the generality of the logic is that the model checking problem for PHL is undecidable. I will present methods both for proving and for refuting formulas from a fragment of the logic that includes many probabilistic hyperproperties of interest.

15:00 – 16:30 **Coffee time and brainstorming time**

16:30 – 17:15 **LORIA visit**

17:15 – 17:30 **Conclusion by Antoine Joux and Marine Minier**