INRIA Grant for a PhD

Title: The SAPIC/Tamarin Security Protocol Verification Toolchain

Keywords: Security protocols, automated verification, formal methods.

Location: Inria Nancy Grand Est Research Centre, 615 rue du Jardin Botanique, 54600 Villers les Nancy, France.

Research theme: Automated verification of security protocols.

Inria Project-team : PESTO (`https://www.inria.fr/en/teams/pesto`)

Environment:

Established in 1967, Inria is the only public research body fully dedicated to computational sciences. Combining computer sciences with mathematics, Inria's 3,500 researchers strive to invent the digital technologies of the future. Educated at leading international universities, they creatively integrate basic research with applied research and dedicate themselves to solving real problems, collaborating with the main players in public and private research in France and abroad and transferring the fruits of their work to innovative companies. The researchers at Inria published over 4,500 articles in 2013. They are behind over 300 active patents and 120 start-ups. The 172 project teams are distributed in eight research centers located throughout France.

Inria Nancy - Grand-Est Centre has 430 researchers, engineers and technicians in its project teams and departments. It conducts most of its scientific activities in partnership with the French National Centre for Scientific Research, the University of Lorraine, the University of Strasbourg and the University of Franche Comté. We also maintain close ties with research institutes and universities from the wider region, notably in Saarbrücken and Luxembourg.

The Inria research team PESTO aims at building formal models and techniques, for computer-aided analysis and design of security protocols. The proposed PhD thesis will be carried out in the context of the ERC SPOOC project.

Missions and activities :

General Context. Security protocols are distributed programs that aim at ensuring security properties, such as confidentiality, authentication or anonymity, by the means of cryptography. Such protocols are widely deployed, e.g., for electronic commerce on the Internet, in banking networks, mobile phones and more recently electronic elections. As properties need to be ensured, even if the protocol is executed over untrusted networks (such as the Internet), these protocols have shown extremely difficult to get right. Formal methods have shown very useful to detect errors and ensure their correctness.

We generally distinguish two families of security properties : trace properties and observational equivalence properties. Trace properties verify a predicate on a given trace and are typically used to express authentication properties. Observational equivalence expresses that an adversary cannot distinguish two situations and is used to model anonymity and strong confidentiality properties.

The Tamarin prover [SMCB12] is a state-of-the art protocol verification tool which has recently been extended to verify equivalence properties in addition to trace properties [BDS15]. SAPIC [KK14] allows protocols to be specified in a high-level protocol specification language, an extension of the applied pi-calculus, and uses the Tamarin prover as a backend by compiling the language into multi-set rewrite rules, the input format of Tamarin.

The objective of this thesis is to contribute to the development of the work SAPIC/Tamarin toolchain, work on extensions and use the tool to analyse particular classes of protocols. We give here a (non-exhaustive) list of possible extensions/case cases.

Support for exclusive or in tamarin. Many protocols, in particular low-level protocols such as RFID protocols, use exclusive or (XOR) operations as they are cheap to implement. Although there exist protocol verification tools supporting precise models of XOR (e.g., extensions of ProVerif [KT08]), as well as tools supporting observational equivalence (e.g., ProVerif [BAF08], APTE [Che14], Tamarin [SMCB12]), none of these supports both. An exception is a recent extension of AKISS [CCK12], but it can only analyse a bounded number of protocol sessions.

The goal is to extend the Tamarin prover [SMCB12, BDS15], with support for XOR operators. Tamarin already deals with Diffie-Hellman-type equational theories, which have similar properties to XOR (notably the finite variant property [CD05] and an associative commutative operator). The idea is to leverage as much of the existing theory and implementation as possible, in particular the computation of the variants and the intruder's computations. Then, suitable heuristics need to be developed to make the approach efficient in practice.

Observational equivalence properties in SAPIC. As mentioned above, SAPIC [KK14] compiles an extension of the applied pi calculus into multi-set rewrite rules which can be analysed using Tamarin. This compilation has been proven correct for any property written in a first-order logic, allowing to express trace properties. The goal of the internship is to extend SAPIC to observational equivalences in order to take advantage of the recent extensions of Tamarin [BDS15].

The work will require to adapt the current translation and the correctness proof to show the translation preserves observational equivalence properties.

If-then-else terms. To verify observational equivalence Tamarin uses bi-systems, i.e. multiset rewrite systems that only differ in certain terms, but otherwise keep the same execution structure. This has some limitations for protocols with branching, notably when one branch needs to be simulated by a different one to prove observational equivalence. One solution to improve handling of branches is to extend terms with an "if-then-else" operator, as done by ProVerif [CB13]. This operator can express multiple branches inside a single branch by pushing differing terms inside the "if-then-else" operator, and thus helps to prove more complex equivalences.

The goal is to adapt the theory developed for ProVerif to Tamarin and implement a correct treatment of "if-then-else terms". In a first step, only the treatment of the terms will be implemented. Automated identification and merging of suitable branches similar to ProVerif can be done in a second step, but is not required.

Towards symbolic verification of smart contracts. Blockchain based smart contracts, such as for instance those supported by the Ethereum platform, are a promising alternative to traditional contracts. However, as witnessed by the attack on the DAO funds [Pop16], security holes may have serious economic consequences. The SAPIC/tamarin toolchain is nowadays among the most expressive protocol verification tools. As shown in recent work [BDKK17], it is even possible to verify complex liveness properties which also arise in smart contracts.

The aim is to first analyse a concrete case study, the blockchain based fair exchange protocol "Zero-Knowledge Contingent Payment" (ZKCP) [ZKC]. The insights from this case study will then pave the road towards a more general framework for analysing the security of smart contracts in (an extension of) SAPIC.

Skills and profile: The working language can be either French or English. The candidate should have good knowledge of logic (deduction, trees, proofs), and should not be afraid of writing proofs. For the implementation, a good command of Haskell, OCaml, or a similar functional language is necessary. Security knowledge is not mandatory, but a plus.

References

[BAF08] B. Blanchet, M. Abadi, C. Fournet. Automated verification of selected equivalences for security protocols. *Journal of Logic and Algebraic Programming*, 75(1):3–51, 2008.

[BDKK17] M. Backes, J. Dreier, S. Kremer, R. Künnemann. A novel approach for reasoning about liveness in cryptographic protocols and its application to fair exchange. In *Proc. 2nd IEEE European Symposium on Security and Privacy (EuroS&P'17)*. IEEE Computer Society, 2017. To appear.

[BDS15] D. A. Basin, J. Dreier, R. Sasse. Automated symbolic proofs of observational equivalence. In *22nd ACM Conference on Computer and Communications Security (CCS'15)*, 1144–1155. ACM Press, 2015.

[CB13] V. Cheval, B. Blanchet. Proving more observational equivalences with proverif. In *2nd Conference on Principles of Security and Trust (POST'13)*, vol. 7796 of *Lecture Notes in Computer Science*, 226–246. Springer, 2013.

[CCK12] R. Chadha, Ş. Ciobâcă, S. Kremer. Automated verification of equivalence properties of cryptographic protocols. In *Programming Languages and Systems — Proceedings of the 21th European Symposium on Programming (ESOP'12)*, vol. 7211 of *Lecture Notes in Computer Science*, 108–127. Springer, 2012.

[CD05] H. Comon-Lundh, S. Delaune. The finite variant property: How to get rid of some algebraic properties. In *16th International Conference on Rewriting Techniques and Applications (RTA'05)*, vol. 3467 of *Lecture Notes in Computer Science*, 294–307. Springer, 2005.

[Che14] V. Cheval. Apte: an algorithm for proving trace equivalence. In *20th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'14)*, vol. 8413 of *Lecture Notes in Computer Science*, 587–592. Springer, 2014.

[KK14] S. Kremer, R. Künnemann. Automated analysis of security protocols with global state. In *35th IEEE Symposium on Security and Privacy (S&P'14)*, 163–178. IEEE Comp. Soc., 2014.

[KT08] R. Küsters, T. Truderung. Reducing Protocol Analysis with XOR to the XOR-free Case in the Horn Theory Based Approach. In *ACM Conference on Computer and Communications Security (CCS'08)*, 129–138. ACM Press, 2008.

[Pop16] N. Popper. Hacker may have taken $50 million from cybercurrency project. *The New York Times*, 2016.

[SMCB12] B. Schmidt, S. Meier, C. Cremers, D. Basin. Automated analysis of Diffie-Hellman protocols and advanced security properties. In *25th IEEE Computer Security Foundations Symposium (CSF'12)*, 78–94. IEEE Comp. Soc., 2012.

[ZKC] Zero knowledge contingent payment. `https://en.bitcoin.it/wiki/Zero_Knowledge_Contingent_Payment`.

Starting date: The thesis is scheduled to start on September 1, 2017. The thesis may be preceded by a research internship.

Duration: 3 years

Monthly salary: 1.580 € net (medical insurance included) for the first two years, 1 661 € net the third year

Help and benefits:

- Possibility of free French courses
- Help for finding housing
- Contribution in part to the costs of transport (French public transport company)
- Help for the resident card procedure and for husband/wife visa
- Lunch cost at Inria is 2,72 € per day
- Complementary health insurance with competitive price

For further information: Please contact : Jannik Dreier, `Jannik.Dreier@loria.fr` and Steve Kremer, `Steve.Kremer@inria.fr`

The required documents for applying are the following :

- CV
- a motivation letter
- your degree certificates and transcripts for Bachelor and Master (or the last 5 years if not applicable).

- Master thesis (or equivalent) if it is already completed, or a description of the work in progress, otherwise;
- all your publications, if any (it is not expected that you have any);
- At least one recommendation letter from the person who supervises(d) your Master thesis (or research project or internship).

Application deadline : March 1, 2017.

Security and defence procedure: In the interests of protecting its scientific and technological assets, Inria is a restricted-access establishment. Consequently, it follows special regulations for welcoming any person who wishes to work with the institute. The final acceptance of each candidate thus depends on applying this security and defence procedure.