Improving Cryptographic Protocols Verification: The Best of Two Worlds

City and country Nancy, France.

Team or project in the lab
Team PESTO at LORIA lab (Inria Nancy, CNRS and Université de Lorraine).

Name and email address of the advisor
Vincent Cheval, `vincent.cheval@inria.fr` & Lucca Hirschi, `lucca.hirschi@inria.fr`

Name and mail of the head of the laboratory
Jean-Yves Marion, `jean-yves.marion@loria.fr`

Indemnisation
The internship is supported by the ERC Consolidator grant SPOOC.

General Context. Security protocols aim at exchanging information securely leveraging *cryptographic primitives* (*e.g.,* encryption, signature). Their goals are diverse (*e.g.,* keeping information confidential, authenticate agents) but recently *privacy* protection is becoming increasingly important. Unfortunately, designing secure and privacy-preserving protocols is extremely complex as witnessed by attacks regularly disclosed on protocols of utmost importance (*e.g.,* Wi-Fi Protected Access [10], TLS [1, 4], mobile telephony protocols [3, 6]). In order to improve the security of such protocols and increase the confidence we can put in them, it is now recommended to use *formal methods* based on the *symbolic model* providing rigorous, mathematical frameworks and techniques to analyze cryptographic protocols. This approach has lead to mature tools and industrial successes, *e.g.,* with the verification tools ProVerif [5], Tamarin [9], and DeepSec [7, 8]

Unfortunately, the state of the art techniques dedicated to privacy have not reached such maturity, which can be explained by the recentness of this line of work and the more complex nature of privacy properties often modeled through *behavioral equivalences* instead of *reachability properties.* On the one hand, we have tools like ProVerif and Tamarin that are very efficient yet imprecise in their equivalence verification. On the other hand, we have tools such as DeepSec that are exact, in that they decide equivalence, but that scale very badly due to the so-called *states space explosion problem.*

Objective of the internship. The *states space explosion problem* has been partially mitigated by recent *Partial Order Reduction* techniques [2] that aim at reducing the search space that the tool has to explore. However such techniques are limited by the restricted amount of information provided by DeepSec about the states that are explored on the fly.

This internship aims at reconciling the two approaches by using ProVerif to speed up DeepSec. More precisely, the internship goal is to identify simple reachability properties: (i) that can be quickly verified by ProVerif and (ii) that can be leveraged by the POR techniques to further reduce the search space. A strong form of secrecy is an example of such a property. It both meets (i) and (ii) and will be used as a first example.

The intern will:

- become familiar with the POR techniques that are implemented in DeepSec and with the ProVerif tool,
- study, as a first example, the strong form of secrecy we suggested above: investigate its verification in ProVerif and its relevance to the POR techniques,
- explore other properties meeting the two conditions (i) and (ii), and
- implement and evaluate on a couple of case studies the pre-processing and the enhanced POR techniques (benchmarks).

We do not necessarily expect that the intern will complete all of these objectives. According to the wishes and skills of the intern, priority can be given to theoretical aspects (*e.g.,* identifying properties and showing how they are helpful to the POR) or to practical aspects (*e.g.,* implementation of the pre-processing and of the enhanced POR techniques, evaluation on case studies) of this project.

Expected ability of the student We expect mathematical maturity, knowledge in logic, theoretical computer science. Knowledge in security and cryptography is not mandatory. For the implementation, a good command of OCaml, or a similar functional language, is necessary. If the candidate is interested, continuation towards a PhD on related topics is possible.

References

[1] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, et al. Imperfect forward secrecy: How diffie-hellman fails in practice. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 5–17. ACM, 2015.

[2] David Baelde, Stéphanie Delaune, and Lucca Hirschi. Partial order reduction for security protocols. In *26th International Conference on Concurrency Theory, CONCUR 2015, Madrid, Spain, September 1.4, 2015*, pages 497–510, 2015.

[3] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. A formal analysis of 5g authentication. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1383–1396. ACM, 2018.

[4] Karthikeyan Bhargavan, Antoine Delignat Lavaud, Cédric Fournet, Alfredo Pironti, and Pierre Yves Strub. Triple handshakes and cookie cutters: Breaking and fixing authentication over TLS. In *2014 IEEE Symposium on Security and Privacy*, pages 98–113. IEEE, 2014.

[5] Bruno Blanchet. Proverif manual. `http://prosecco.gforge.inria.fr/personal/bblanche/proverif/manual.pdf`.

[6] Ravishankar Borgaonkar, Lucca Hirschi, Shinjo Park, and Altaf Shaik. New privacy threat on 3g, 4g, and upcoming 5g aka protocols. *Proceedings on Privacy Enhancing Technologies*, 2019(3):108–127, 2019.

[7] Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. DEEPSEC: Deciding Equivalence Properties in Security Protocols – Theory and Practice. In *IEEE Symposium on Security and Privacy (S&P)*, 2018.

[8] Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. The DEEPSEC prover. In *International Conference on Computer Aided Verification (CAV)*, 2018.

[9] Simon Meier, Benedikt Schmidt, Cas J. F. Cremers, and David Basin. The TAMARIN Prover for the Symbolic Analysis of Security Protocols. In *CAV*, volume 8044, pages 696–701, 2013.

[10] Mathy Vanhoef and Frank Piessens. Key reinstallation attacks: Forcing nonce reuse in WPA2. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 1313–1328, 2017.