Formally Verifying Privacy in Cryptographic Protocols through Trace Properties

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 advisors
Lucca Hirschi, `lucca.hirschi@inria.fr` & Steve Kremer, `steve.kremer@inria.fr`

Name and email of the head of the laboratory
Yannick Toussaint, `yannick.toussaint@loria.fr`

Indemnisation
The internship is supported by PEPR "Cyberseécuriteé" (France 2030 program managed by the French National Research Agency under grant agreement No. ANR-22-PECY-0006).

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 [13], TLS [1, 5], mobile telephony protocols [4, 7]). 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.

Objective of the internship. This approach has lead to mature tools and successful real-world case studies, e.g., [12, 6, 3, 9], TLS 1.3 whose the design process has been guided by such techniques. 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* (e.g., bisimulation) instead of *trace properties*, which are reachability properties (e.g., is there a reachable state where the attacker learns a supposedly secret key). To mitigate this and obtain precise and complete automated analyses for privacy, we have developed a privacy verification framework [10, 11] based on *sufficient conditions* that are easier to check, and successfully applied this approach to some RFID protocols and e-voting protocols (later extended to stateful protocols [2]). This verification framework has been mechanized in the UKano tool [10]. The two conditions that we have proven to be sound with respect to privacy properties (unlinkability and anonymity) are (i) *well-authentication*, a *trace property*, and (ii) *frame-opacity*, an *behavioral equivalence property* for a semi-passive adversary, which is still challenging to verify, compared to trace properties.

The aim of this internship is to develop sufficient conditions for frame-opacity that can be verified trough trace properties only. Combined with the result [10], this would show, for the first time, that privacy can be soundly reduced to trace properties in the symbolic model. Completeness of these conditions is unachievable by design but we seek for tightness in practice: interesting case studies, such as the ones from [10], should be deemed secure when they are.

Intern's Tasks. The intern will not start from scratch as we already have preliminary results that the intern can build on. The intern will:

1. become familiar with the symbolic model [8] and in particular with static equivalence, as well as with the verification framework [10],
2. study, as a first example, the (supposedly) sufficient conditions for frame-opacity that we have already found and prove that they indeed imply frame-opacity,
3. explore weaker, yet sufficient, conditions, and adapt the soundness proof,
4. implement the verification of the designed conditions in the tool UKano,
5. evaluate the conditions tightness and the verification efficiency on some case studies, including the RFID properties presented in [10].

If time allows, various open problems around this methodology can then be studied.

Expected ability of the student. We expect mathematical maturity, basic knowledge in logic, basic theoretical computer science. Knowledge in security and cryptography is not mandatory. For the implementation, a reasonable command of OCaml, or a similar functional language, is necessary.

If the candidate is interested, continuation towards a PhD, for which we already have funding, 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 Solène Moreau. A Method for Proving Unlinkability of Stateful Protocols. Research Report, Irisa, January 2020.

[3] David Basin, Cas Cremers, and Simon Meier. Provably repairing the iso/iec 9798 standard for entity authentication. *Journal of Computer Security*, 21(6):817–846, 2013.

[4] 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.

[5] 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.

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

[7] 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.

[8] Véronique Cortier and Steve Kremer. *Formal Models and Techniques for Analyzing Security Protocols: A Tutorial*. Now, 2014.

[9] Cas Cremers, Marko Horvat, Sam Scott, and Thyla van der Merwe. Automated analysis and verification of TLS 1.3: 0-RTT, resumption and delayed authentication. In *IEEE Symposium on Security and Privacy*, 2016.

[10] Lucca Hirschi, David Baelde, and Stéphanie Delaune. A method for unbounded verification of privacy-type properties. *Journal of Computer Security*, pages 1–66, 2017.

[11] Lucca Hirschi and Cas Cremers. Improving Automated Symbolic Analysis of Ballot Secrecy for E-Voting Protocols: A Method Based on Sufficient Conditions. In *2019 IEEE European Symposium on Security and Privacy (EuroS P)*, pages 635–650, June 2019.

[12] 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.

[13] 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.