Formalizing and Verifying the Privacy Guarantees of Cryptographic Protocols from the NOISE Framework

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
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. The NOISE Protocol Framework [9] is a description language for Authenticated Key Exchange (AKE) cryptographic protocols using Diffie-Hellman exponentiation. The official specification [10] defines a language based on *patterns* whose combination forms a specific NOISE *protocol* with a *handshake phase*, establishing a shared key, and a *transport phase*, that protects exchanged messages using the previously established shared key. A very large number of protocols can be written within this framework (actually infinitely many). In practice, it is currently used by WHATSAPP, WIREGUARD, and LIGHTNING.

The main benefits of such a generic framework are twofold. First, given some security requirements, one can quickly write patterns that (supposedly) meet those requirements. Second, such an unified framework reduces the implementation efforts since one can build modular compilers (e.g., first compiling patterns, and on top of that, compiling NOISE protocols). This is also supported by the numerous implementations of NOISE in C, Go, Haskell, Java, Javascript, Python, and Rust.

However, not all NOISE protocols provide the same level of security, and choosing the right instantiation, given some security requirements, is highly error-prone. Prior work[1] [4] partly addresses this critical issue by leveraging *formal methods* and the TAMARIN [8] security protocol verification tool to generically find the *security* properties satisfied by any NOISE pattern. Unfortunately, [4] focuses on *security* and the *privacy* analysis it provides is very limited in that only a few privacy properties were analyzed and only partial results were obtained due to fundamental limitations of the chosen analyzing framework and tool.

[1] I was a co-tutor of this master thesis, which has lead to an academic paper under submission of which I am a co-author.

Objective of the internship. More generally, formal methods based on the symbolic model have proved their usefulness by providing rigorous, mathematical frameworks to analyze security protocols. Such methods, and notably TAMARIN and PROVERIF [2], have been used to analyze, break, and fix large-scale real-life protocols such as TLS [3] and 5G AKA [1]. Privacy properties can also be formalized in such a model, but automated analyses thereof are notoriously much harder to obtain due to precision and efficiency issues. To mitigate this and obtain precise and complete results for privacy on NOISE protocols, we plan to leverage a recent privacy verification framework we developed [6] and successfully applied to RFID protocols [5] and e-voting protocols [7].

The aim of this internship is to develop a privacy verification framework based on this technique. The intern will investigate relevant privacy guarantees one expects from NOISE protocols (e.g., anonymity, untraceability) and (standard) formalization thereof. Next, the technique from [6] shall be combined with the existing verification framework for NOISE [4] in order to extend it to relevant privacy properties. Finally, the resulting framework will be evaluated on the Noise protocols listed in the specification [9] in order to derive precise privacy guarantees.

The NOISE framework would benefit tremendously from such a formal treatment and analysis of privacy. The underlying practically relevant, yet scientifically challenging long-term objective is the following:

> Develop a tool and theoretical foundations that allows the NOISE framework users to automatically obtain a security evaluation of the NOISE protocol studied.

This internship will contribute to this goal.

Expected ability of the student We expect mathematical maturity, knowledge in logic, basic theoretical computer science. Knowledge in security and cryptography is not mandatory. If the candidate is interested, continuation towards a PhD on related topics is possible.

References

[1] 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.

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

[3] 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.

[4] Guillaume Girol. Formalizing and verifying the security protocols from the noise framework. Master's thesis, ETH Zurich, 2019.

[5] Lucca Hirschi, David Baelde, and Stéphanie Delaune. A method for verifying privacy-type properties: the unbounded case. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 564–581. IEEE, 2016.

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

[7] 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. IEEE, 2019.

[8] S. Meier, B. Schmidt, C. Cremers, and D. Basin. The Tamarin Prover for the Symbolic Analysis of Security Protocols. In *Proc. 25th International Conference on Computer Aided Verification*, volume 8044 of *LNCS*, pages 696–701. Springer, 2013.

[9] Trevor Perrin. Webpage of the the Noise protocol framework. `http://noiseprotocol.org/`.

[10] Trevor Perrin. The Noise protocol framework. `http://noiseprotocol.org/noise.html`, 2016.