Formally Comparing and Evaluating Privacy 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 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. 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 [26], TLS [3, 8], mobile telephony protocols [6, 10]). 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.,* [23, 9, 5, 16]. 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*. One of the main current limitations is our poor understanding of how to formally model privacy.

Objective of the internship. Numerous regulations and normative requirements informally specify some privacy expectations [15, 2, 1, 22]. Unfortunately, such informal requirements fall short of precisely defining what security protocols must protect from. This internship aims at finding and devising formal security goals which match best privacy expectations. The intern will first focus on the untraceability property.

Intuitively, untraceability ensures that unauthorized parties are unable to link different uses based on the fact that they were initiated by the same user (ISO 15408 [22]). However, normative requirements for untraceability found in international standards are sometimes rather weak [2] or ambigious [1, 19]. We

believe that formally defining such notions would have notably allowed formal comparisons between them and clearly revealed such shortcomings.

However, finding the appropriate definition is not an easy task and heavily depends on the considered threat model and the usage context. Numerous definitions of untraceability have been proposed in the literature [12, 11, 4, 25, 20, 18, 21, 17]. The question then arises:

> How do those notions compare to each other for realistic security protocols? Do the differences in their formulations translate to meaningful differences on real world systems? Most importantly, given a threat model and a use case, how can one choose the most appropriate untraceability notion?

In addition to formally comparing those notions, the intern will use various case studies for evaluating the practical relevance of (potential) attacks captured by the different notions to answer the previous questions.

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.,* formally comparing definitions) or to practical aspects (*e.g.,* evaluation on case studies, review of normative specifications) of this project.

Expected ability of the student We expect mathematical maturity, knowledge in logic, and 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] 3GPP. LTE; Service requirements for V2X services. TS 122.185, 3rd Generation Partnership Project (3GPP).

[2] 3GPP. Study on subscriber privacy impact in 3GPP. TS 33.849, 3rd Generation Partnership Project (3GPP).

[3] 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.

[4] Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. Analysing unlinkability and anonymity using the applied pi calculus. In *Proceedings of the IEEE Computer Security Foundations Symposium*. IEEE Comp. Soc. Press, 2010.

[5] 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.

[6] 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.

[7] David Bernhard, Véronique Cortier, David Galindo, Olivier Pereira, and Bogdan Warinschi. Sok: A comprehensive analysis of game-based ballot privacy definitions. In *Security and Privacy (SP), 2015 IEEE Symposium on*, pages 499–516. IEEE, 2015.

[8] 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.

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

[10] 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.

[11] Mayla Brusó, Konstantinos Chatzikokolakis, and Jerry Den Hartog. Formal verification of privacy for RFID systems. In *Proc. 23rd Computer Security Foundations Symposium*, pages 75–88. IEEE Computer Society Press, 2010.

[12] Mayla Brusó, Konstantinos Chatzikokolakis, Sandro Etalle, and Jerry Den Hartog. Linking unlinkability. In *International Symposium on Trustworthy Global Computing*, pages 129–144. Springer, 2012.

[13] Katriel Cohn-Gordon, Cas Cremers, and Luke Garratt. On post-compromise security. In *Computer Security Foundations Symposium (CSF), 2016 IEEE 29th*, pages 164–178. IEEE, 2016.

[14] Alissa Cooper, Hannes Tschofenig, Dr. Bernard D. Aboba Ph.D., Jon Peterson, John B. Morris, Marit Hansen, and Rhys Smith. Privacy Considerations for Internet Protocols. RFC 6973, July 2013.

[15] Council of the European Union and the European Commission. GDPR: General data protection regulation. `http://ec.europa.eu/justice/data-protection/reform/index_en.htm`. [Last accessed: 3 January 2018].

[16] 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.

[17] Ihor Filimonov, Ross Horne, Sjouke Mauw, and Zach Smith. Breaking unlinkability of the icao 9303 standard for e-passports using bisimilarity. In *European Symposium on Research in Computer Security*, pages 577–594. Springer, 2019.

[18] Ivan Gazeau and Steve Kremer. Automated analysis of equivalence properties for security protocols using else branches. In *European Symposium on Research in Computer Security*, pages 1–20. Springer, 2017.

[19] John Harding, Gregory Powell, Rebecca Yoon, Joshua Fikentscher, Charlene Doyle, Dana Sade, Mike Lukuc, Jim Simons, and Jing Wang. Vehicle-to-vehicle communications: Readiness of v2v technology for application. Technical report, 2014.

[20] 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.

[21] Lucca Hirschi, David Baelde, and Stéphanie Delaune. A method for unbounded verification of privacy-type properties. *CoRR*, abs/1710.02049, 2017. Under submission at Journal of Computer Security.

[22] ISO. ISO 15408-2: Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, July 2009.

[23] 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.

[24] Altaf Shaik, Jean-Pierre Seifert, Ravishankar Borgaonkar, N. Asokan, and Valtteri Niemi. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. In *23nd Annual Network and Distributed System Security Symposium*, 2016.

[25] Ton Van Deursen, Sjouke Mauw, and Saša Radomirović. Untraceability of RFID protocols. In *Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks*, pages 1–15. Springer, 2008.

[26] 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.