Security ceremonies

Master thesis within the SPICY team, at IRISA in Rennes, France

Under the supervision of **Barbara FILA**

Keywords

Protocols, cermonies, formal modeling, verification, security.

Context and motivation

Cryptographic protocols are used to guarantee a secure exchange of data, such as credentials and sensitive information, between agents (e.g., computers, electronic devices, servers) connected in a network. Classical protocols rely principally on two events – sending and receiving of cryptographic messages – and on inference rules allowing agents and potential attackers to infer new information from the set of data that they already know.

Protocols have been extensively studied from the security perspective [10, 13, 9, 4, 14]. Numerous tools supporting specification and automated verification of protocols have been developed [3, 2, 5]. Furthermore, dedicated scientific events where researchers and practitioners working in the domain present their results and share their experience exist [1].

Nevertheless, ensuring a secure exchange goes way beyond designing an appropriate sequence of sending and receiving events. In the context of protocols, we usually consider a deterministic setting: fixed inference rules are defined and the agents (usually machines) can apply them at any time and in any conditions. In practice however, these machines are managed by humans who may fail, forget or refuse to execute some actions. Taking such non-deterministic behavior of humans into account is thus necessary while analyzing the security of exchanges involving digital agents (machines and devices) and users (people) manipulating them.

To analyze networks where both machines and humans communicate, Ellison proposed the concept of **security ceremonies** [11]. In a nutshell, ceremonies augment protocols in two aspects:

- the set of agents (machines for protocols) is augmented with humans,
- exchanges are no longer restricted to passing cryptographic messages, but can involve physical objects, goods, documents, legal rights (like ownership), etc.

Researchers have already worked on formalizing security ceremonies, but the existing methods are usually ad-hoc or limited to a specific application context [16, 6, 15, 12, 8, 7].

Objective

The objective of this project is to create a solid formal basis of a mathematical model for specification and verification of security ceremonies.

Work description

In the first phase of the project, the student will perform a thorough literature study on security ceremonies with the objective of writing a comparative analysis between protocols and ceremonies. This phase will help us to identify aspects and elements that will need to be included in the future formal model of ceremonies to make it as complete as possible. Examples of such aspects are: adding humans to the set of agents, augmenting the set of messages with physical objects, legal rights, etc., enlarging inference rules with those modeling non-deterministic human behavior, including external aspects (like emotions, health condition, etc.) to the inference rules, and many more.

Next, a theoretical formal model for ceremonies will be developed. This includes designing a specification language for ceremonies, including all the aspects previously identified, and defining a formal semantics allowing to parse this language and to automatically verify ceremony executions. An important and challenging aspect to keep in mind while developing the formal model will be its universality: the proposed model will need to be as general and open as possible, so that it can accommodate future (and thus yet unknown) technological evolution.

Finally, if time permits, we will also investigate the problem of automated verification of ceremonies. This problem is already well known to be undecidable in the case of protocols that rely on simpler setting than ceremonies. This implies that, in the case of ceremonies, a special effort will need to be put on the optimization aspects. Suitability of existing tools for protocols' verification in the context of ceremonies will be studied, and if the results show that these tools do not scale up sufficiently well, a design of a dedicated tool for security ceremonies will be considered. The work on the verification tool will then be continued in a follow-up PhD project.

Candidate's profile

This is a strongly formal and theoretical project. We are seeking for ambitious students enthusiastic about research and having interest in formal modeling, logical reasoning (e.g., inference, rewriting), verification, etc. The domain of security ceremonies being young, it is important that the selected student is keen on brainstorming, open to innovative solutions, and eager to investigate new directions. The scope of this project is not rigidly fixed, and the explored paths will depend on the candidate's interests and strengths. If the results of this master project are satisfactory, a follow-up PhD thesis is foreseen (funding already guaranteed).

Contact and application

For all inquiries please contact Barbara Fila (barbara.fila@irisa.fr). Informal inquiries are welcome.

To apply, please send us

- your detailed CV,
- a short letter explaining your motivation for working on this project,
- the grade transcript of all university-level courses taken.

References

[1] Cambridge International Workshop on Security Protocols. https://link.springer.com/conference/spw.

[2] ProVerif: Cryptographic protocol verifier in the formal model. https://bblanche.gitlabpages.inria.fr/proverif/.

[3] Tamarin Prover. https://tamarin-prover.github.io/.

[4] The AVISPA Project: Automated Validation of Internet Security Protocols and Applications. `https://www.avispa-project.org/`.

[5] The Scyther Tool. `https://people.cispa.io/cas.cremers/scyther/`.

[6] Giampaolo Bella and Lizzie Coles-Kemp. Layered analysis of security ceremonies. In *Information Security and Privacy Research*, volume 376 of *IFIP AICT*, pages 273–286. Springer Berlin Heidelberg, 2012.

[7] Giampaolo Bella, Rosario Giustolisi, and Carsten Schürmann. Modelling human threats in security ceremonies. *Journal of Computer Security*, Pre-press:1–23, 2022.

[8] Marcelo Carlomagno Carlos, Jean Everson Martina, Geraint Price, and Ricardo Felipe Custódio. An updated threat model for security ceremonies. In Sung Y. Shin and José Carlos Maldonado, editors, *SAC'13*, pages 1836–1843. ACM, 2013.

[9] Véronique Cortier. Research projects. `https://members.loria.fr/VCortier/projects/`.

[10] Stéphanie Delaune. ERC Project POPSTAR: Reasoning about Physical properties Of security Protocols with an Application To contactless Systems. `https://popstar.irisa.fr/`.

[11] Carl M. Ellison. Ceremony design and analysis. *IACR Cryptol. ePrint Arch.*, page 399, 2007.

[12] Rosario Giustolisi. Free rides in denmark: Lessons from improperly generated mobile transport tickets. In Helger Lipmaa, Aikaterini Mitrokotsa, and Raimundas Matulevicius, editors, *NordSec 2017*, volume 10674 of *LNCS*, pages 159–174. Springer, 2017.

[13] Steve Kremer. ERC Project Automated Security Proofs of Cryptographic Protocols: Privacy, Untrusted Platforms and Applications to E-voting Protocols (SPOOC). `https://members.loria.fr/skremer/files/spooc/index.html`.

[14] Simon Meier, Benedikt Schmidt, Cas Cremers, and David A. Basin. The TAMARIN prover for the symbolic analysis of security protocols. In Natasha Sharygina and Helmut Veith, editors, *CAV 2013*, volume 8044 of *LNCS*, pages 696–701. Springer, 2013.

[15] Kenneth Radke, Colin Boyd, Juan Manuel González Nieto, and Margot Brereton. Ceremony analysis: Strengths and weaknesses. In *IFIP SEC*, pages 104–115, 2011.

[16] Diego Sempreboni and Luca Viganò. X-men: A mutation-based approach for the formal analysis of security ceremonies. In *EuroS&P*, pages 87–104. IEEE, 2020.