Master thesis proposal
with a potential follow-up PhD position

Title: ***Formal modeling of ceremonies***

Supervisor: **Barbara FILA**

Location: IRISA, Rennes, France

Context and motivation

Security ceremonies have been introduced by Ellison in [1] to reason about interactions within distributed socio-technical systems. Such systems are composed of computing entities (computers, servers), physical objects (IoT devices, smartphones, chips), interactive sensors, and humans (users, clients). An electronic voting procedure is an example of a ceremony. It involves the voters, an electronic infrastructure with voting terminals and trusted servers, the voting authority and the humans who prepare, run and manage (from a physical, a technical and a legal perspective) the voting sessions. To analyze the security of a voting process, it is not sufficient to focus solely on the protocol responsible for transmitting an encrypted vote between the voter's computer and the voting server. What if the cryptographic keys used for the election are compromised? What if the voter is constraint by its environment to vote for a certain candidate? What if the voting server is run by one of the political parties? What if the power outage occurs on the election day? To answer these questions, features characterizing the system technical, physical and human components as well as their weaknesses must be modeled and taken into account during the security analysis of the overall system.

Technical background

In 2024, Fila and Radomirović introduced an abstract formal framework for specification and verification of ceremonies [2]. It relies on simple mathematical components: a typed language, n-ary relations, substitutions, and transition systems. The framework is fully generic, i.e., it is suitable to reason about various types of agents (e.g., machines, humans, physical objects, legal rights) and supports the modeling of synchronous interactions between any finite number of agents. Abstract n-ary relations are used to model atomic steps within the ceremonies, and a labeled transition system provides a formal model for execution of sequences of such steps.

Objective and research challenges

We are interested in analyzing the security of interactions within a socio-technical system modeled using the framework developed in [2]. Intuitively speaking, we aim at verifying whether the system's behavior is compatible with desired security properties. Security properties have been extensively studied in the context of cryptographic protocols [3, 4]. Existing definitions, however, do not take the intentions of humans nor the properties of physical objects or the environment into account. Since the user is a central part of socio-technical systems, defining the security requirements for ceremonies cannot be dissociated from considering their functional requirements.

The work of the master student will consist on analyzing numerous real-life ceremonies, focusing on their functional and non-functional requirements, in order to exhibit security properties relevant within the context of socio-technical systems. The objective will be to evaluate the expressiveness of these properties and select a suitable logic for their formal modeling. We will also be interested in finding out whether it is possible to define generic security properties for ceremonies, i.e., properties applicable to any type of ceremony, or whether such properties must be customized for each ceremony or tailored to every application domain.

Supervision and scientific environment

This master project is proposed by the IRISA institute in Rennes, France. IRISA is the largest French research laboratory (more than 850 people) in the field of computer science and information technologies. It provides an excellent environment where French and international researchers perform cutting edge scientific activities in all domains of the computer science.

The master thesis will be supervised by Barbara FILA (PhD, HDR, dr hab), associate professor at INSA Rennes and researcher at IRISA. Fila's research work focuses on formal models for security and risk analysis. Her interests include formal modeling and analysis of security protocols and security ceremonies.

In accordance with French legislation, the student working on this project will get the internship bonus of approximately 660€ per month. The duration of this project will be around 5–6 months (to be defined with the prospective candidate). The work can start at any time in 2024/2025 and will begin as soon as a suitable candidate is found.

Finally, funding for a follow-up doctoral project has already been secured. If the master thesis results are promising, the student will have an opportunity to continue on a PhD position at IRISA with the aim of obtaining a PhD degree in computer science within three years.

Candidate profile and applications

We are looking for a candidate

- interested in theoretical research in mathematics and/or computer science,
- enthusiastic about formal modeling (logic, verification, formal languages),
- curious and open-minded,
- speaking English or French (knowledge of French is not mandatory).

To apply, please send the following documents to `barbara.fila@irisa.fr`:

- your CV,
- the grade transcript of all university-level courses taken.

Informal inquiries are welcome. Do not hesitate to contact `barbara.fila@irisa.fr` if you have questions.

References

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

[2] Barbara Fila and Sasa Radomirovic. Nothing is out-of-band: formal modeling of ceremonies. In *CSF'24*, pages 464–478. IEEE Computer Society, 2024. Available at `https://people.irisa.fr/Barbara.Fila/papers/CSF24.pdf`.

[3] Gavin Lowe. A hierarchy of authentication specification. In *CSFW*, pages 31–44. IEEE Computer Society, 1997.

[4] Stéphanie Delaune, Steve Kremer, and Mark Ryan. Verifying privacy-type properties of electronic voting protocols. *J. Comput. Secur.*, 17(4):435–487, 2009.