PhD Thesis Proposal

Cryptographic Communication Protocols

Contact: Gildas AVOINE (gildas.avoine@irisa.fr)

IRISA, Rennes, France

The research group EMSEC from the research institute IRISA in France has an open PhD thesis position in the field of cryptographic protocols, starting in September 2019. The candidate is expected to:

- Have followed a master program in computer science;
- Be strongly interested in both theoretical and applied aspects of computer science;
- Be fluent in English.

Keywords

Security, cryptography, protocols, attacks, proofs.

Context

Exchanging information is today digitally performed. It is consequently of the utmost importance to guarantee security properties on the exchanges, including confidentiality, authenticity, and integrity. Cybersecurity aims to guarantee these properties using cryptographic protocols. Every one uses such protocols everyday, e.g., WPA2 for WiFi connection either at home or at the office place ; A5.1 for GSM communications ; TLS to check his/her mailbox or purchase items on Internet ; EMV-CAP to authenticate on a bank account, etc. All the mentioned protocols, without any exception, were broken at some point, then repaired. This is the common life cycle of a cryptographic protocol. The weakness can for example be due to a wrong design, an implementation issue, or a misuse of the protocol.

It is worth noting that the data of the users are threatened as long as the protocol is vulnerable. When a flaw is revealed, it is usually easy to know how long the weakness has been existing, and so how long an adversary has been able to exploit it. In the most common cases, it takes two to three years before a flaw is revealed. The protocol must then be repaired, and the fixed version deployed, which can be complicated in case of large-scale systems, or embedded systems that have not been planned to be updated.

The scientific challenge of this thesis is to break the unacceptable life cycle of cryptographic protocols, where a protocol can be periodically vulnerable for several years without anyone noticing.

The research work performed in this thesis will define a methodology to analyze the security of a deployed protocol. It will take into account the design of the protocol, its implementation, and its use. The work will also focus on the tools to be put in place to ensure the security of a protocol throughout its life. It will study the main existing protocols in order to build a portfolio of secure protocols (under certain conditions) that can be used by any individual or company. Finally, this thesis will help identifying protocols widely deployed today that suffer from flaws. In particular, protocols used in the Internet of Things, on social networks and for secure messaging will be considered.

The thesis will be supervised by Gildas Avoine, Mohamed Sabt, and Pierre-Alain Fouque, all from the research group EMSEC.

Examples of work previously achieved by the team on the considered topic

[1] Stéphanie Alt, Pierre-Alain Fouque, Gilles Macario-Rat, Cristina Onete, and Benjamin Richard. A cryptographic analysis of UMTS/LTE AKA. In *ACNS 2016, Guildford, UK*, pages 18–35, 2016.

[2] Gildas Avoine, Antonin Beaujeant, Julio Hernandez-Castro, Louis Demay, and Philippe Teuwen. A survey of security and privacy issues in ePassport protocols. *ACM Comput. Surv.*, 48(3), 2016.

[3] Gildas Avoine and Loïc Ferreira. Attacking GlobalPlatform SCP02-compliant smart cards using a padding oracle attack. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(2):149–170, 2018.

[4] Gildas Avoine and Loïc Ferreira. Rescuing lorawan 1.0. In *Financial Cryptography and Data Security – FC'18*, Lecture Notes in Computer Science, 2018.

[5] Olivier Blazy, Angèle Bossuat, Xavier Bultel, Pierre-Alain Fouque, Cristina Onete, and Elena Pagnin. SAID: Reshaping signal into an identity-based asynchronous messaging protocol with authenticated ratcheting. In *2019 IEEE Symposium on S&P*, 2019.

[6] Pierre-Alain Fouque, Cristina Onete, and Benjamin Richard. Achieving better privacy for the 3GPP AKA protocol. *PoPETs*, 2016(4):255–275, 2016.

[7] Mohamed Sabt and Jacques Traoré. Cryptanalysis of GlobalPlatform secure channel protocols. In *Security Standardisation Research - Third International Conference, SSR 2016, Gaithersburg*, 2016.

Research Institute

IRISA (*Institut de Recherche en Informatique et Systèmes Aléatoires*), founded in 1975, is a research center for IT, image, signal processing, and robotics, located in Rennes, France. The institute hosts 800 researchers distributed in 40 research groups, and is funded by 7 entities, namely CNRS, ENS Rennes, Inria, INSA Rennes, Institut-Mines-Télécom, CentraleSupélec, Université de Bretagne Sud (UBS), and Université de Rennes 1. IRISA so "forms a research cluster for excellence within the ICTS, with scientific priorities that include bioinformatics, system security, new software architecture (many-cores, cloud computing), and virtual reality". IRISA is well-known for its research activities in computer security and cryptography (more than 100 researchers work full-time on this topic) and many neighboring companies are actively involved in this field. Rennes is located in the West part of France, about 45 minutes by car from the sea, and a fast train connects Rennes to Paris in less than 1h30.

Research Group

Embedded Security and Cryptography (EMSEC) is a research group within the IRISA computer science institute located in Rennes, France. EMSEC was created in February 2016 and is headed by Prof. Gildas Avoine and Prof. Pierre-Alain Fouque. The group hosts more than 35 researchers, including 8 permanent members. EMSEC's activities are organized along three axes: cryptography, formal methods, and system security.

Link: `https://www.irisa.fr/emsec`

Contact and Applications

Applications should contain a curriculum vitæ (including the grades obtained so far during the Master), and a motivation letter explaining why you are excited by this PhD thesis proposal. Applications should be sent by email to Gildas Avoine (`gildas.avoine@irisa.fr`).