Analysing security protocols based on low-entropy secrets in the symbolic model

Laboratory, institution and university The internship will be located at IRISA - EMSEC team (Rennes) and/or at LORIA - Pesto team (Nancy) depending on the choice of the candidate.

Advisors Stéphanie Delaune, `Stephanie.Delaune@irisa.fr`, and Steve Kremer, `Steve.Kremer@inria.fr`

Indemnisation The internship is supported by **POPSTAR** (ERC Starting Grant) and/or the ANR **Sequoia**.

Keywords security protocols, formal verification, symbolic model, dictionary attacks

Summary. The use of formal methods to verify the security of cryptographic protocols is essential to avoid security breaches. In this internship we propose to analyse protocols that rely on low-entropy secrets, i.e., protocols that rely on human passwords or use short secrets to be sent on out-of-band channels (such as short messages sent by sms), and add the human into the loop.

Context. Security protocols are distributed programs that aim at ensuring security properties, such as confidentiality, authentication or anonymity, by the means of cryptography. Such protocols are widely deployed, e.g., for electronic commerce on the Internet, in banking networks, mobile phones and more recently electronic elections. As properties need to be ensured, even if the protocol is executed over untrusted networks (such as the Internet), these protocols have shown extremely difficult to get right. Formal methods, and especially symbolic models that are amenable to automation, have shown very useful to detect errors and ensure their correctness.

Low entropy secrets arise in password-based protocols and also when human copiable strings are sent through an out-of-band channel, e.g. an sms to confirm an authentication [4]. In both cases an adversary may be able to perform brute force attacks, and dedicated models have been designed to take these vulnerabilities into account. In the symbolic approach, a popular definition to capture the so-called guessing attacks is the one presented in [2] and that has been used in subsequent work. This definition is generic in the sense that it is parametrized by an equational theory which is the usual way (in the symbolic model) to represent cryptographic primitives and their properties. This definition has been extended to consider the case where

multiple low-entropy secrets are used [3]. However, it happens that this definition is not suitable in presence of the exlusive-or operator: some low-entropy secrets will be declared guessable whereas they are not.

Objectives of the internship. The aim of the internship is to propose a new definition more suitable to capture brute-force attacks in presence of the exclusive-or operator. Once the definition will be settled, the intern will start by designing a procedure for checking resistance against guessing attacks in this new setting. A good starting point will be to consider the verification problem in presence of the so-called passive attacker as done e.g. in [1].

Expected skills. We are looking for candidates with good skills in Foundations of Computer Science (logic, automated deduction,...). Some knowledge in security is an asset but is not mandatory. The candidate will assimilate this knowledge during the internship.

References

[1] M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. *Theor. Comput. Sci.*, 367(1-2):2–32, 2006.

[2] R. Corin, J. Doumen, and S. Etalle. Analysing password protocol security against off-line dictionary attacks. *Electr. Notes Theor. Comput. Sci.*, 121:47–63, 2005.

[3] S. Delaune, S. Kremer, and M. D. Ryan. Composition of password-based protocols. In *Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF'08)*, pages 239–251, Pittsburgh, Pennsylvania, USA, June 2008. IEEE Computer Society Press.

[4] L. H. Nguyen and A. W. Roscoe. Authentication protocols based on low-bandwidth unspoofable channels: A comparative survey. *Journal of Computer Security*, 19(1):139–201, 2011.