Formalizing some combinatorial attacks in security protocols

Laboratory, institution and university LSV, ENS Cachan and LORIA, Nancy universités. The internship will be located at Nancy or at ENS Cachan depending on the choice of the candidate.

Team or project of the Lab Team SecSI at LSV and team Cassis at Loria.

Name and email address of the advisor Stéphanie Delaune, `delaune@lsv.ens-cachan.fr` and Steve Kremer, `Steve.Kremer@inria.fr`

Indemnisation The internship is supported by the European grant ProSecure (ERC Starting Grant) and the ANR grant VIP (Programme JCJC).

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 have shown very useful to detect errors and ensure their correctness.

Many results exist in literature for analyzing reachability properties, such as confidentiality and authentication. These results generally rely on the assumption that cryptographic primitives work perfectly and there is essentially no chance of guessing any data. However, these assumptions are unrealistic in some situations. Indeed, recent protocols attempt to achieve authentication by using an *out of band channel* (e.g. SMS) and require comparison of strings which are short enough for humans to compare or retype them easily. This novel sort of authentication protocols is used in many daily life applications (e.g. bank transfer) and it is important to ensure their security [NR11]. However, the use of weak data and/or weak primitives means that new types of attacks can be achieved by guessing the weak data or by discovering an alternative way to produce it. As a consequence, the standard attacker model used by most of the existing protocol analysis tools is not suitable for analyzing these protocols.

Objectives of the internship. The aim of the internship is to propose formal definitions of security for this class of protocols that use in particular hashing on short values which is too weak to resist combinatorial attacks. The applied pi calculus [AF01] allows the modeling of cryptography by the

means of equational theories, and allows to express indistinguishability properties. It seems to be a well-suited framework for this work as well. Once a suitable attacker model and security properties have been formally defined, a procedure for analysing those protocols could be developed and possibly implemented. As a starting point, the intern can read [RSN11] where a first attempt for analyzing this new type of protocols is presented.

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

This internship may also lead to a PhD thesis on similar topics with funding available through the ProSecure and VIP projects.

References

[AF01] Martín Abadi and Cédric Fournet. Mobile values, new names, and secure communication. In *Principles of Programming Languages*, pages 104–115, 2001.

[NR11] Long Hoang 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.

[RSN11] A.W. Roscoe, Toby Smyth, and Long Nguyen. Model checking cryptographic protocols subject to combinatorial attack. Technical report, Oxford University, 2011. Available at `http://www.cs.ox.ac.uk/files/4157/guess.pdf`.