LICS: Logic In Computer Security
Some attacker's models and related decision problems

Hubert Comon-Lundh
LSV, École Normale Supérieure de Cachan
comon@lsv.ens-cachan.fr

Logic plays an important role in formal aspects of computer security, for instance in access control, security of communications or even intrusion detection.

The peculiarity of security problems is the presence of an attacker, whose goal is to break the intended properties of a system/database/protocol...

In this tutorial, we will consider several attacker's models and study how to find attacks (or to get security guarantees) on communication protocols in these different models.

One of the most popular attacker's model, sometimes called the "Dolev-Yao model" after [8], consists in assuming that messages are first-order terms and the attacker is an inference system that formalizes the attacker's computations on these messages. In this context, whether an attacker can forge (or not) a message from the available messages, is the classical Entscheidungsproblem. When the attacker may send some forged messages, in order to trigger new actions, and therefore to get additional information, the possible sequences of messages (traces) can be represented using *deducibility constraints* [7], [6]. The first part of the tutorial will present the deducibility constraints, how to solve them and how to apply the results to security analysis.

Abstracting messages by terms might not be faithful: messages are actually bitstrings and some operations on bitstrings might not be adequately represented at the term level. An attacker is not necessarily limited to the computations that are represented by the function symbols. A more realistic model consists in considering that the attacker is an arbitrary probabilistic polynomial time Turing machine (PPT). The *computational soundness* results [1], [2] show that, under some assumptions, the only useful attacker's computations are the computations represented by the function symbols. These results may be seen as a full abstraction of the Dolev-Yao model. Such soundness results require however strong hypotheses, some of which are often not realistic. In the second part of the tutorial, we discuss two ways to overcome this problem. The first one consists in formalizing the PPT attacker's capabilities within the logic (following [4], [5]) and the second one consists in specifying within first-order logic, what an attacker cannot do (following [3]). This amounts to consider yet another model of attacker, which is more powerful than the PPT model.

References

[1] Martín Abadi and Phillip Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). *J. Cryptology*, 15(2):103–127, 2002.

[2] M. Backes, B. Pfitzmann, and M. Waidner. A composable cryptographic library with nested operations. In *Proc. 10th ACM Concerence on Computer and Communications Security (CCS'03)*, 2003.

[3] Gergei Bana and Hubert Comon-Lundh. Towards unconditional soundness: Computationally complete symbolic attacker. In *Proceedings of the 1st International Conference on Principles of Security and Trust (POST'12)*, volume 7215 of *Lecture Notes in Computer Science*. Springer, 2012.

[4] Gilles Barthe, Benjamin Grégoire, and Santiago Zanella-Béguelin. Formal certification of code-based cryptographic proofs, 2010. Submitted manuscript under review.

[5] Bruno Blanchet. A computationally sound mechanized prover for security protocols. *IEEE Transactions on Dependable and Secure Computing*, 5(4):193–207, October–December 2008. Special issue IEEE Symposium on Security and Privacy 2006. Electronic version available at http://doi.ieeecomputersociety.org/10.1109/TDSC.2007.1005.

[6] Hubert Comon-Lundh, Véronique Cortier, and Eugen Zlinescu. Deciding security properties of cryptographic protocols. application to key cycles. *ACM Transaction on Computational Logic*, 11, 2010.

[7] Hubert Comon-Lundh, Stéphanie Delaune, and Jonathan Millen. Constraint solving techniques and enriching the model with equational theories. In *Formal Models and Techniques for Analyzing Security Protocols*, volume 5 of *Cryptology and Information Security Series*, pages 35–61. IOS Press, 2011.

[8] D. Dolev and A.C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2), 1983.