On Well-founded Security Protocols (Extended Abstract)

Sibylle Fröschle
OFFIS & University of Oldenburg, Germany
Email: froeschle@informatik.uni-oldenburg.de

Consider the decidability problem that stands behind classical protocol verification: Given a protocol P and an attack goal G, is there a run of protocol P controlled by the Dolev-Yao intruder that obtains G? The problem is well-known to be undecidable, in general. Moreover, it is well-investigated what computational power remains when restricting the problem with respect to the three sources of infinity the Dolev-Yao intruder can make use of: an attack may involve messages of unbounded size, an unbounded number of freshly generated data, and an unbounded number of sessions. A recent survey can be found in [2]

Another way to obtain positive results is to impose restrictions on the message format of protocols. A summary of such results can be found in [1]. In one group of such results decidability is obtained by imposing conditions that make encrypted messages context-explicit. The first such result is the completeness result of Lowe in [3]. His condition requires that encrypted components are textually distinct, and that each encrypted component includes all protocol roles. Together this ensures that every encryption that occurs in a protocol run can be uniquely assigned to a protocol position and the set of agents involved in the run. The *structured* protocols of [4] introduce a condition that is similar to the first of [3]: between any two terms that occur in distinct communications, no encrypted subterm of one can be unified with a subterm of the other. This yields decidability for a particular notion of secrecy, called *leakiness* here. Moreover, there are results for richer, dynamic schemes that require that encryptions are tagged with freshly generated nonces while composed during a protocol run (c.f. [5])

All these results are based on ad hoc protocol models, which introduce additional restrictions such as that the protocol must have an honest run (i.e. there must be a protocol run without intruder interaction), or subtle constraints on the typing. Altogether this makes it difficult to obtain a systematic understanding.

In this talk we will present the class of *well-founded protocols*. They are defined to directly exclude what is common to all undecidability results: that the message format allows the intruder to build unbounded chains of causally connected 'honest' encryptions, i.e. encryptions that he could have neither analysed nor synthesized himself. The protocol class is defined by first defining a relation over protocol positions that expresses that information might be passed in a protected manner from one position to the other, and then requiring that this relation must be acyclic. The definition does not require further constraints such as the existence of an honest run.

Moreover, we will explain why leakiness is decidable for well-founded protocols. The main insight is that the well-foundedness condition translates into a boundedness condition for particular protocol runs. We hope that this proof will help us to unify the other results and give a more systematic understanding of context-explicit protocols. Finally, we motivate why such protocols could play an important role in the protocols that are currently designed and standardized for embedded security applications such as in the automotive domain.

References

[1] V. Cortier, S. Delaune, and P. Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1):1–43, 2006.

[2] S. Fröschle. *From Security Protocols to Security APIS: Foundations and Verification*. To appear in the Information Security and Cryptography series of Springer.

[3] G. Lowe. Towards a completeness result for model checking of security protocols. *Journal of Computer Security*, 7(1):89–146, 1999.

[4] R. Ramanujam and S. P. Suresh. A decidable subclass of unbounded security protocols. In *WITS'03*, pages 11–20, 2003.

[5] R. Ramanujam and S. P. Suresh. Tagging makes secrecy decidable with unbounded nonces as well. In *FSTTCS'03*, volume 2914 of *LNCS*, pages 363–374. Springer, 2003.