Intruder Theories (Ongoing Work)

Hubert Comon-Lundh*

Laboratoire Spécification et Vérification, CNRS
Ecole Normale Supérieure de Cachan,
comon@lsv.ens-cachan.fr

1 Context

The specification of security protocols usually comes in two parts:

- A finite number of processes called *roles*, each of which is parametrized by agent identities and consists of a sequence of name generation, the *nonces* and a finite sequence of rules $u \Rightarrow v$, which should be read as "upon receiving a message matching u, send the corresponding message v."
- A description of intruder capabilities, sometimes given as a proof system, which we call hereafter the *offline intruder theory*.

The roles can be replicated and instanciated by agent names any number of times. Each such instance is called a *session*. The roles and the offline intruder theory define a transition system whose states are, for each agent name a local state and a set of messages called the *intruder knowledge*. The peculiarity of security protocols is the synchronization mechanism: the only effect of sending a message m is to increase the intruder knowledge with m, while any message that can be forged, i.e. deduced, by the intruder using his knowledge and the offline theory can be received. This models the fact that the intruder controls the public network: he can intercept messages, forge new messages and send them through the network. In addition, dishonest (or compromised) agents communicate all their private data, increasing the intruder knowledge.

As far as confidentiality is concerned, there is an *attack* on the security protocol if there is a reachable state in which the intruder knowledge contains a message which is supposed to remain a secret shared by honest agents.

One of the most well-known offline intruder theory is now called the *Dolev-Yao model*, and relies on the *perfect cryptography assumption*, which roughly states that nothing can be learned on a plain text from its encrypted version, without knowing the decryption key. The verification of such protocols is undecidable in this model. This remains undecidable when there is no name generation (see e.g. [3]) or when the size of messages is bounded [6]. It becomes decidable (and co-NP-complete) when the number of sessions is bounded [10].

* This work is partly supported by the RNTL project PROUVÉ and the ACI Rossignol

The perfect cryptography assumption is only an idealization of cryptographic primitives, which is not relevant in many cases. Two typical cases are the use of exclusive or (denoted $\oplus$) and modular exponentiation, since several protocol use, on purpose, their algebraic properties. That is why a third component in the protocol specification is now considered: the equational theory describing the (supposedly relevant) algebraic properties of cryptographic primitives. In this context, the offline intruder theory is slightly modified. The result of [10] was recently extended to a number of other models, including exclusive or [1, 4] and some properties of modular exponentiation [2, 9, 7].

Another generalization of the offline intruder theory consists in modeling for instance guessing attacks [5]. This roughly consists in guessing a value and comparing it with the result of an independent computation, checking that the guess is correct. Again, the results of [10] are generalized in a non trivial way. Other offline intruder theories are relevant, depending on typing assumptions, typically the ability to recognized whether a given message is a cyphertext or not. Finally, one can think of modeling some online deductions, such as the so-called chosen plaintext attacks.

2 Online Intruder Theories

Our main contribution will be the introduction of "online intruder theories". We claim that most existing results can be restated in a nice way in this framework, which is moreover amenable to several extensions.

If we take the intruder point of view, besides his offline deduction capabilities, he also has the possibility to send messages and get replies increasing his knowledge. This can also be modeled as deduction rules: we get what we call the *online intruder theory*. An attack is then simply a proof of some supposed secret in such a formal system. The advantages of such a viewpoint are many-fold.

Uniformization. Most of the decidability results for a bounded number of sessions [10, 1, 2, 5] rely on two main properties:

- The *locality* of the offline intruder theory: if s is deducible from T, then there is a proof using subterms of s, T only
- A bound on the size of substitutions: if there is an attack, then there is an attack in which the intruder only forges messages that are built by stacking subterms of distinct protocol rules.

The locality of the offline theory implies its decidability in linear time. The second property implies an NP decision procedure, by guessing the adequate substitution.

In the framework of online intruder theories, these two properties are consequences of a single property of the form "if there is a proof, then there is a simple proof".

Strategies. A proof normalization result for the online intruder capabilities can be used to restrict the search space in the case of an unbounded number of sessions; we only have to search for normal proofs.

Generality. The results for a bounded number of sessions [10, 1, 2, 5, 4, 9] rely on similar proof schemes, but cannot be deduced from each other. Each of the results uses different hypotheses on the protocol or on the offline theory and the proofs are non-trivial.

In [1, 2], the authors give properties of the offline deduction system, called "oracle rules", which are sufficient for their decidability result. We will state a proof normalization result, which abstracts out not only the offline deduction system but also the equational theory.

Though this has not been proved yet, all above-cited results should be corollaries of our normal proof results. In particular, it should encompass both results for the exclusive or [4, 1].

Extendability With a general result allowing one to lift offline theories to online theories, we may apply it to new models, deriving decision results for a bounded number of sessions. We may also include deductions which are typically "online". For instance, the chosen plaintext attack can be written as a simple rule:

$$\frac{x, T \vdash \{x\}_k}{T \vdash k} \text{ If } x \text{ does not occur free in } T$$

in other words, if, for any message x, it is possible to get the encrypted message in which x is encrypted by k, then we can compute k. Depending on the encryption algorithm, we may (or may not) include such a rule in the online intruder theory.

3 Conclusion

We believe that studying the proof systems for online intruder theories can be very fruitful in deriving both theorem proving strategies and decision results for a large variety of models.

References

1. Y. Chevalier, R. Kuester, M. Rusinowitch, and M. Turuani. An NP decision procedure for protocol insecurity with xor. In Kolaitis [8].
2. Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. Deciding the security of protocols with Diffie-Hellman exponentiation and products in exponents. In J. Radhakrishnan and P. Pandya, editors, *Proc. FST/TCS, Mumbai*, volume 2914 of *Lecture Notes in Computer Science*, 2003.
3. H. Comon and V. Cortier. Tree automata with one memory, set constraints and cryptographic protocols. *Theoretical Comput. Sci.*, 2004. To appear. Also available as LSV research report LSV-01-13.

4. H. Comon-Lundh and V. Shmatikov. Intruder deductions, constraint solving and insecurity decision in preence of exclusive or. In Kolaitis [8].
5. S. Delaune and F. Jacquemard. A theory of guessing attacks and its complexity. Research Report LSV-04-1, Lab. Specification and Verification, ENS de Cachan, Cachan, France, 2004.
6. N. Durgin, P. Lincoln, J. Mitchell, and A. Scedrov. Undecidability of bounded security protocols. In *Proc. Workshop on formal methods in security protocols*, Trento, Italy, 1999.
7. J. Goubault-Larrecq, M. Roger, and K. N. Verma. Abstraction and resolution modulo AC: How to verify diffie-hellman-like protocols automatically. *Journal of Logic and Algebraic Programming*, 2004. Submitted to the special issue on processes and security, 40 pages.
8. P. Kolaitis, editor. *Eighteenth Annual IEEE Symposium on Logic in Computer Science*, Ottawa, Canada, June 2003. IEEE Computer Society.
9. J. Millen and V. Shmatikov. Symbolic protocol analysis with products and diffie-hellman exponentiation. nvited submission to Journal of Computer Security (selected papers of CSFW-16), 2004.
10. M. Rusinowitch and M. Turuani. Protocol insecurity with finite number of sessions is NP-complete. In *Proc.14th IEEE Computer Security Foundations Workshop*, Cape Breton, Nova Scotia, June 2001.