Composition results for equivalence-based security properties

Stéphanie Delaune and Steve Kremer

[1] LSV, CNRS & ENS Cachan
[2] LORIA, Inria Nancy Grand Est

The results presented in this report are based on results that have been published in [11, 3, 4]– works that have been supported by the VIP project and that are available on the website of the VIP project.

Abstract. This deliverable concerns the Task 4 of the VIP project: *Modularity issues.* This report aims to sum up the results that have been obtained during the project and that are related to composition issues.

1 Introduction

Security protocols are used in many of our daily-life applications, and our privacy largely depends on their design. Since security protocols are notoriously difficult to design and analyse, formal verification techniques are important. These techniques have become mature and have achieved success. For instance, a flaw has been discovered in the Single- Sign-On protocol used by Google Apps [5], and several verification tools are nowadays available (*e.g.* ProVerif [9], the AVANTSSAR platform [6]).

However, security protocols used in practice are more and more complex and it is difficult to analyse them altogether. For example, the UMTS standard [1] specifies tens of sub-protocols running concurrently in 3G phone systems. While one may hope to verify each protocol in isolation, it is however unrealistic to expect that the whole application will be checked relying on a unique automatic tool. Existing tools have their own specificities that prevent them to be used in some cases. Furthermore, most of the techniques do not scale up well on large systems, and sometimes the ultimate solution is to rely on a manual proof. It is therefore important that the protocol under study is as small as possible.

Unfortunately, security proofs of network services or protocols considered in isolation, do not carry over when they share keys or passwords. Consider for example the two naive protocols:

$$P : A \to S : \{A\}^r_{pk(S)} \qquad Q : A \to S : \{N_a\}^r_{pk(S)}$$
$$S \to A : N_a$$

In protocol P, the agent A simply identifies himself to the server S by sending him his identity encrypted under S's public key (using a probabilistic encryption

scheme). In protocol Q, the agent sends some fresh nonce N_a encrypted under S's public key. The server S acknowledges A's message by forwarding A's nonce. While P executed alone guarantees A's anonymity, it is not the case when the protocol Q is run in parallel. Indeed, an adversary may use Q as an oracle to decrypt any message. More realistic examples illustrating interactions between protocols can be found in *e.g.* [16].

State of the art at the beginning of the VIP *project.* There are a number of papers studying the secure composition of security protocols in the symbolic model (*e.g.* [14, 12]) and in the computational model (*e.g.* [10, 17]). Our result clearly belongs to the first approach. However, all the existing results have been established for trace-based security property such as secrecy and authentication. Here, we propose composition results to analyse privacy-type security properties expressed using the notion of equivalence.

Contributions. First, we study the case of password-based protocol. Security of password-based protocols can be expressed using the notion of equivalence. However, for this purpose, we may restrict our attention to consider equivalences between very similar processes, which simplifies our work. Our goal is to study whether password protocols can be safely composed, even when a same password is reused. More precisely, we present a transformation which maps a password protocol that is secure for a single protocol session (a decidable problem) to a protocol that is secure for an unbounded number of sessions. Our result provides an effective strategy to design secure password protocols: *(i)* design a protocol intended to be secure for one protocol session; *(ii)* apply our transformation and obtain a protocol which is secure for an unbounded number of sessions. Moreover, our technique also applies to compose different password protocols that use the same password, allowing us to obtain both inter-protocol and inter-session composition.

Second, we study the notion of trace equivalence and we show how to establish such an equivalence relation in a modular way. It is well-known that composition works well when the processes do not share secrets. However, there is no result allowing us to compose processes that rely on some shared secrets such as long term keys. We show that parallel and sequential compositions work even when the processes share secrets provided that they satisfy some reasonable conditions In particular, we deal with the case where a protocol uses a sub-protocol to establish some keys. To achieve this, we propose several theorems that state the conditions that need to be satisfied so that the security of the whole protocol can be derived from the security analysis performed on each sub-protocol in isolation. Our composition results allows us to prove various equivalence-based properties in a modular way, and works in a quite general setting. In particular, we consider arbitrary cryptographic primitives and processes that use non-trivial else branches.

2 The case of password-based protocols

Password-based cryptographic protocols are a prominent means to achieve authentication or to establish authenticated, shared session keys, *e.g.* EKE [8], or J-PAKE [15]. However, such passwords are generally *weak* and may be subject to dictionary attacks (also called guessing attacks). In an *online* dictionary attack an adversary tries to execute the protocol for each possible password. While online attacks are difficult to avoid they can be made impracticable by limiting the number of password trials or adding a time-out of few seconds after a wrong password. In an *offline* guessing attack an adversary interacts with one or more sessions in a first phase. In a second, offline phase the attacker uses the collected data to verify each potential password. Thus, we concentrate on offline guessing attacks.

Several attempts have been made, based on the initial work of Lowe [18], to characterize guessing attacks. In [13], Corin *et al.* proposed an elegant definition of resistance to passive guessing attacks, based on static equivalence in the applied pi calculus. A similar definition has also been used by Baudet [7] who uses constraint solving techniques to decide resistance against guessing attacks for an active attacker and a bounded number of sessions. Moreover, Abadi *et al.* further increase the confidence in this definition by showing its computational soundness for a given equational theory in the case of a passive attacker [2].

In this work, we study whether resistance against guessing attacks composes when the same password is used for different protocols. Protocols are modelled in a cryptographic process calculus inspired by the applied pi calculus. We use the definition introduced by Corin *et al.* (see [13]). This allows us to provide results for protocols involving a variety of cryptographic primitives represented by means of an arbitrary equational theory.

First we show that in the case of a passive attacker, resistance against guessing attacks composes. In the case of an active attacker we prove that as expected, resistance against guessing attacks does compose when no secrets are shared. However, resistance against active guessing attacks does *not* compose in general when the same password is shared between different protocols. In this work we propose a simple protocol transformation which ensures that a same password can safely be shared between different protocols. More precisely, our results can be summarized as follows. We use a safe transformation which replaces a weak password w by $\mathsf{h}(t, w)$ where t is some *tag* and h a hash function. Then, we show how to use this tagging technique to compose different protocols. Consider n password protocols such that each protocol resists separately against guessing attacks on w. When we instantiate the tag t to a unique protocol identifier pid, one for each of the n protocols, we show that the parallel composition of these tagged protocols resists against guessing attacks on w, where w is the password shared by each of these protocols. Next we show how to dynamically establish a session identifier sid. Instantiating the tag t by this session identifier allows us to compose different sessions of a same protocol. Hence it is sufficient to prove resistance against guessing attacks on a single session of a protocol to conclude that the transformed protocol resists against guessing attacks for an unbounded

number of sessions. These techniques can also be combined into a tag which consists of both the protocol and session identifier obtaining both inter-protocol and inter-session composition.

One may note that resistance against guessing attack is generally not the main goal of a protocol, which may be authentication or key exchange. Therefore we additionally show that secrecy and authentication properties are also preserved when composing transformed protocols.

These results have been obtained by Stéphanie Delaune and Steve Kremer in collaboration with Céline Chevalier and Mark Ryan. They have been published in the journal Formal Methods in System Design.

3 More general privacy-type properties

This work tackles the compositionality problem with respect to privacy-type properties which are usually expressed as equivalences between processes. Roughly, two processes P and Q are equivalent ($P \approx Q$) if no process O can observe any difference between the processes P and Q.

We identify sufficient conditions of *disjointness* under which protocols can "safely" be executed in parallel. In particular, we require protocols run in parallel not to use the same primitives. Our theorems hold for arbitrary primitives that can be modelled by a set of equations, and can thus handle composition of protocols relying on symmetric and asymmetric encryption schemes, hash functions, signatures, zero knowledge proofs, message authentication codes, designated verifier proofs, exclusive or, *etc.*

We first state a composition result that also allows the protocols considered to share the usual cryptographic primitives of symmetric and asymmetric encryption, hashing, and signing, provided that these primitives are tagged and that public and verification keys are not derivable. In this setting, we are able to establish a strong result that basically says that the disjoint scenario is equivalent to the shared one. This allows us to go back to the disjoint case (with no shared keys) for which composition works unsurprisingly well. We show that whenever processes P and Q (*resp.* P' and Q') satisfy the corresponding disjointness property, we can derive that P and Q running in parallel under the *composition context* $C[\_]$ are equivalent to P' and Q' running in parallel under the *composition context* $C'[\_]$, *i.e.*

$$C[P \mid Q] \;\approx\; C'[P' \mid Q']$$

from the equivalences $C[P] \approx C'[P']$ and $C[Q] \approx C'[Q']$. The composition context under which two processes are composed contains the shared keys possibly under some replications.

We also go beyond parallel composition. In particular, we study the case where a protocol uses a sub-protocol to establish some keys.

We illustrate the usefulness of our composition results on protocols from the 3G phone application, as well as on protocols from the e-passport application.

We show how to derive some privacy guarantees from the analysis performed on each sub-protocol in isolation.

These results have been obtained by Stéphanie Delaune in collaboration with Myrto Arapinis and Vincent Cheval, and have been published in the proceedings of CSF'12 and POST'15.

4 Conclusion

We now have several composition results to analyse privacy-type properties in a modular way. We note that our results on password-based protocols hold in a general setting, and are independent of the equational theory. The result suggests a design strategy through a transformation which enforces a tagging discipline.

The results on more general privacy-type properties also hold in a quite general setting, *e.g.* processes may have non trivial else branches, we consider arbitrary primitives expressed using an equational theory, and processes may even share some standard primitives as long as they are tagged in different ways. We illustrate the usefulness of our results through the mobile phone and e-passport applications.

These composition results are all derived from a generic result, and we believe that this generic result could be used to derive further composition results. For example, we may want to consider situations where sub-protocols sharing some data are arbitrarily interleaved.

References

1. 3GPP. Technical specification group services and system aspects; 3G security; security architecture (release 9). Technical report, 3rd Generation Partnership Project, 2010.
2. M. Abadi, M. Baudet, and B. Warinschi. Guessing attacks and the computational soundness of static equivalence. In L. Aceto and A. Ingólfsdóttir, editors, *Proc. 9th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'06)*, volume 3921, pages 398–412. Springer, Mar. 2006.
3. M. Arapinis, V. Cheval, and S. Delaune. Verifying privacy-type properties in a modular way. In *Proceedings of the 25th IEEE Computer Security Foundations Symposium (CSF'12)*, pages 95–109, Cambridge Massachusetts, USA, June 2012. IEEE Computer Society Press.
4. M. Arapinis, V. Cheval, and S. Delaune. Composing security protocols: from confidentiality to privacy. In R. Focardi and A. Myers, editors, *Proceedings of the 4th International Conference on Principles of Security and Trust (POST'15)*, volume 9036 of *Lecture Notes in Computer Science*, pages 324–343, London, UK, Apr. 2015. Springer.
5. A. Armando, R. Carbone, L. Compagna, J. Cuéllar, and M. L. Tobarra. Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for google apps. In *Proc. 6th ACM Workshop on Formal Methods in Security Engineering (FMSE 2008)*, pages 1–10. ACM Press, 2008.

6. A. Armando et al. The AVANTSSAR Platform for the Automated Validation of Trust and Security of Service-Oriented Architectures. In *Proc. 18th Int. Conference on Tools and Algorithms for the Construction and Analysis of Systems*, 2012.
7. M. Baudet. Deciding security of protocols against off-line guessing attacks. In *Proc. 12th ACM Conference on Computer and Communications Security (CCS'05)*, pages 16–25. ACM Press, Nov. 2005.
8. S. M. Bellovin and M. Merritt. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In *Proc. Symposium on Security and Privacy (SP'92)*, pages 72–84. IEEE Comp. Soc., 1992.
9. B. Blanchet. An Efficient Cryptographic Protocol Verifier Based on Prolog Rules. In *Proc. 14th Computer Security Foundations Workshop (CSFW'01)*, pages 82–96. IEEE Comp. Soc. Press, 2001.
10. R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proc. 42nd Annual Symposium on Foundations of Computer Science (FOCS'01)*, pages 136–145, Las Vegas (Nevada, USA), 2001. IEEE Computer Society Press.
11. C. Chevalier, S. Delaune, S. Kremer, and M. D. Ryan. Composition of password-based protocols. *Formal Methods in System Design*, 43(3):369–413, Dec. 2013.
12. Ş. Ciobâcă and V. Cortier. Protocol composition for arbitrary primitives. In *Proc. of the 23rd IEEE Computer Security Foundations Symposium (CSF'10)*, pages 322–336. IEEE Computer Society Press, 2010.
13. R. Corin, J. Doumen, and S. Etalle. Analysing password protocol security against off-line dictionary attacks. *ENTCS*, 121:47–63, 2005.
14. J. D. Guttman and F. J. Thayer. Protocol independence through disjoint encryption. In *Proc. 13th Computer Security Foundations Workshop (CSFW'00)*, pages 24–34. IEEE Comp. Soc. Press, 2000.
15. F. Hao and P. Y. A. Ryan. Password authenticated key exchange by juggling. In *Proc. 16th International Security Protocols Workshop*, volume 6615 of *Lecture Notes in Computer Science*, pages 159–171. Springer, 2008.
16. J. Kelsey, B. Schneier, and D. Wagner. Protocol interactions and the chosen protocol attack. In *Proc. 5th Inter. Workshop on Security Protocols*, volume 1361 of *LNCS*, pages 91–104. Springer, 1997.
17. R. Küsters and M. Tuengerthal. Composition Theorems Without Pre-Established Session Identifiers. In *Proc. 18th Conference on Computer and Communications Security (CCS 2011)*, pages 41–50. ACM Press, 2011.
18. G. Lowe. Analysing protocols subject to guessing attacks. *Journal of Computer Security*, 12(1):83–98, 2004.