Freshness Analysis in Security Protocols [1]

Chiara Braghin Agostino Cortesi Riccardo Focardi

Dipartimento di Informatica,
Università Ca' Foscari di Venezia,
Via Torino 155, 30173 Venezia – Mestre (Italy)
{braghin,cortesi,focardi}@dsi.unive.it

Abstract

Guaranteeing freshness of messages is a key issue in entity authentication within security protocols, to prevent replay attacks. In this paper we show how to model cryptographic protocols by Mobile Ambients, and how a suitable Control Flow Analysis of Mobile Ambients can be defined for message freshness verification.

Keywords: Mobile Ambients, Security, Static Analysis.

The growing need for distributed systems development and the increasing load of network functionalities ask for the design of formal methods that properly model and face both mobility and security issues, leading to sophisticated analysis and verification tools. So, mobility and security can be seen as a very challenging and demanding workbench for any analysis and verification technique.

This paper originates from a couple of quite naive questions:

- As Mobile Ambient Calculus [7] seems to be one of the best high-level approaches to mobility issues, what is needed to properly model also cryptographic protocols in that Calculus?
- Is it possible to specialize existing abstract-interpretation based analyses of Mobile Ambients to verify specific properties of cryptographic protocols, thus preventing malicious attacks?

The results we present can be seen as a first attempt to properly address the questions above. We restrict our attention to a particular set of common attacks to cryptographic protocols, the so called "replay attacks", where an adversary records a communication session and replays the entire session, or a portion thereof, at some later point in time. In order to avoid this kind of attacks, a crucial role in cryptographic protocols is played by message *freshness*, that guarantees against replication of messages. So we focus on a specific goal: designing a freshness verifier for cryptographic protocols within Mobile Ambient Calculus.

[1] Partially supported by MURST Projects "Interpretazione Astratta, Type Systems e Analisi Control-Flow", and "Modelli formali per la sicurezza" and the EU Contract IST-2001-32617 "Models and Types for Security in Mobile Distributed Systems".

In the scenario above, the contribution of the paper can be summarized as follows:

- We show that the notion of boundary, recently introduced to model information leakage in (pure) Mobile Ambient Calculus [5,6], allows to model cryptographic primitives and cryptographic protocols, in a quite natural way. Intuitively, in a multilevel security setting, where any entity can be either confidential or public, ambients labelled as boundaries represent locations where confidential information is confined and cannot be blabbed.
- We show how the common methods used to assure freshness (nonces and sequence numbers) can also be expressed within Mobile Ambients.
- We show how freshness can be expressed in terms of information flow. Intuitively, a leakage of confidential information is generated as soon a principal receives the same nonce or sequence number more than once. Therefore, suitable ambient nesting analyses [5,11] (that may in fact detect information leakage) can be applied, thus enforcing freshness verification.
- We report on the preliminary results of applying the occurrence counting of Nielson et al. [11], enhanced with security boundaries, to a suite of classical protocol drawn from the literature.

As far as we know, this is the first attempt to address the issue of verifying freshness either within the Mobile Ambient Calculus or by a Control Flow Analysis approach. This can be seen as an alternative approach to the type and effect system approaches for proving properties in security protocols [1,2], and to the introduction of more sophisticated language primitives (like in Safe Ambients [12] or spi-calculus [4] that may more or less directly model cryptography.

This work can be seen as a preliminary step towards the design of a more general analysis and verification framework of security properties by a control-flow analysis/abstract interpretation approach. These seminal results seem to hint at a promising impact of static analysis techniques to security protocols verification.

References

[1] Martín Abadi. Secrecy by typing in security protocols. In *TACS: 3rd International Conference on Theoretical Aspects of Computer Software*, 1997.

[2] Martín Abadi and Bruno Blanchet. Analyzing Security Protocols with Secrecy Types and Logic Programs. In *Proc. of the 29th ACM Symposium on Principles of Programming Languages*, pages33–44, January 2002.

[3] Martín Abadi and Andrew D. Gordon. A bisimulation method for cryptographic protocols. *Nordic Journal of Computing*, 5(4):267–303, Winter 1998.

[4] Martín Abadi and Andrew D. Gordon. A Calculus for Cryptographic Protocols: The Spi Calculus. *Proc. of Fourth ACM Conference on Computer and Communications Security*, ACM Press, pages 36–47, 1997.

[5] Chiara Braghin, Agostino Cortesi, and Riccardo Focardi. Control Flow Analysis of Mobile Ambients with Security Boundaries. In Bart Jacobs and Arend Rensink, editors, *Proc. of Fifth IFIP International Conference on Formal Methods for Open Object-Based Distributed Systems (FMOODS'02)*, pages 197–212. Kluwer Academic Publisher, 2002.

[6] C. Braghin, A. Cortesi, R. Focardi, and S. van Bakel. Boundary Inference for Enforcing Security Policies in Mobile Ambients. In *Proc. of The 2nd IFIP International Conference on Theoretical Computer Science (TCS'02)*, pages 383–396. Kluwer Academic Publisher, to appear.

[7] L. Cardelli and A. Gordon. Mobile Ambients. In *Proc. FoSSaCS'98*, volume 1378 of *Lecture Notes in Computer Science*, pages 140–155, Springer-Verlag, 1998.

[8] A. Cortesi, and R. Focardi. Information Flow Security in Mobile Ambients. In *Proc. of International Workshop on Cuncurrency and Coordination* CONCOORD'01, Lipari Island, July 2001, volume 54 of *Electronic Notes in Theoretical Computer Science*, Elsevier, 2001.

[9] D. Dolev and A.C. Yao. On the Security of Public Key Protocols. *IEEE Transactions on Information Theory*, 29(2), pages 198–208, 1983.

[10] Riccardo Focardi and Fabio Martinelli. A Uniform Approach for the Analysis of Cryptographic Protocols. In *Second Conference on Security in Communication Networks (SCN'99)*, G. Persiano ed., September 16-17, 1999, Amalfi, Italy.

[11] R. R. Hansen, J. G. Jensen, F. Nielson, and H. R. Nielson. Abstract Interpretation of Mobile Ambients. In *Proc. Static Analysis Symposium* SAS'99, volume 1694 of *Lecture Notes in Computer Science*, pages 134–148, Springer-Verlag, 1999.

[12] Francesca Levi and Davide Sangiorgi. Controlling Interference in Ambients. In *Proc. 28th ACM Symposium on Principles of Programming Languages (POPL'01)*, pages 352–364, 2000.

[13] F. Nielson, H. Riis Nielson, C.L. Hankin. Principles of Program Analysis. Springer, 1999.