Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 242 (2009) 99–112
www.elsevier.com/locate/entcs

Security Abstractions and Intruder Models (Extended Abstract)

Michele Bugliesi [1] and Riccardo Focardi [2]

Dipartimento di Informatica
Università Ca' Foscari di Venezia

Abstract

Process algebraic specifications of distributed systems are increasingly being targeted at identifying security primitives well-suited as high-level programming abstractions, and at the same time adequate for security analysis and verification. Drawing on our earlier work along these lines [5], we investigate the expressive power of a core set of security and network abstractions that provide high-level primitives for the specifications of the honest principals in a network as well as the lower-level adversarial primitives that must be assumed available to an attacker.
We analyze various bisimulation equivalences for security, arising from endowing the intruder with (*i*) different adversarial capabilities and (*ii*) increasingly powerful control on the interaction among the distributed principals of a network. By comparing the relative strength of the bimimulation equivalences we obtain a direct measure of the discriminating power of the intruders, hence of the expressiveness of the corresponding models.

Keywords: Process algebras, bisimulation for security, intruder model

1 Introduction

The challenges in achieving security in distributed systems often create a tension between two conflicting requirements. On the one side, security concerns call for detailed formal specifications of the safeguards built against the threats to which the systems are exposed. On the other side, programming the systems needs techniques and reasoning methods that abstract away from such details to focus on the expected functional properties.

In the literature on process calculi, this tension has generated a range of approaches, with two extremes. At one end, we find specifications that draw on low-level cryptographic primitives as in the spi calculus [3] or in the applied-pi calculus [1]. At the other end lie specifications based on the pi calculus [11], which assume

[1] Email: michele@dsi.unive.it
[2] Email: focardi@dsi.unive.it

doi:10.1016/j.entcs.2009.06.015

very abstract, and hard-to-implement, mechanisms to secure communications by hiding them on private channels. A more recent line of research [2,9,4,6,7] follows a different approach, aimed at identifying security primitives well-suited as high-level programming abstractions, and at the same time adequate for security analysis and verification in adversarial setting.

Drawing on our initial ideas in [5], in the present paper we further assess the adequacy of our approach by investigating the expressive power of our security and network abstractions. In particular, we analyze various bisimulation equivalences for security, associated with a variety of intruder models. The models arise from endowing the intruders with (i) different adversarial capabilities and (ii) increasingly powerful control on the interaction among the distributed principals of a network. The bisimulation equivalences, in turn, provide a direct measure of the discriminating power of the intruders, hence of the expressiveness of the corresponding models.

The starting point is the asynchronous pi-calculus with security abstractions we defined in [5]. In this model, the intruder has the capability to interfere in all network interactions: it can forge its own traffic, intercept all messages and forward them back to the network, possibly replicating them. However, similarly to what happens in the Dolev-Yao model for cryptographic protocols, it cannot learn any secret message and cannot forge any authenticated transmission. For this intruder, we give a sound characterization of strong barbed equivalence in terms of strong asynchronous bisimulation. Also, we show that asynchronous and synchronous bisimilarity coincide.

We then extend our network abstractions with a new primitive that enables the intruder to silently eavesdrop on network traffic (without necessarily intercepting it). We show that the new capability adds no discriminating power to the intruder, in that it does not affect the security equivalences (either synchronous or asynchronous). On the other hand, eavesdropping turns out to be strictly less powerful than intercepting.

As a further, and final step, we look at the notion of intruder adopted in [4], that corresponds to what is sometimes referred to as the *man-in-the-middle* intruder. In this new model two principals may never engage in a synchronization directly as it is customary for the semantics of traditional process calculi (and as we assume in the initial model). Instead, all exchanges take place with the intruder's intervention. We show, somewhat surprisingly, that this additional control on the interactions on the network does not change the notion of equivalence, hence does not add discriminating power to the intruder.

Plan. Sections 2 and 3 review the calculus from [5]. Sections 4 and 5 discuss the results for the Dolev-Yao intruder of [5]. Section 6 contrasts this model with the man-in-the-middle intruder of [4]. Section 7 concludes the presentation.