# Modelling and Verification of Layered Security Protocols: A Bank Application

Johannes Grünbauer[1], Helia Hollmann[2], Jan Jürjens[1], and Guido Wimmel[1]

[1] Department of Computer Science, Munich University of Technology
Boltzmannstr. 3, D-85748 Garching, Germany
{gruenbau|juerjens|wimmel}@in.tum.de
[2] Secaron AG, Ludwigstrasse 55, D-85399 Hallbergmoos, Germany
hollmann@secaron.de

**Abstract.** Designing security-critical systems correctly is very difficult and there are many examples of weaknesses arising in practice. A particular challenge lies in the development of layered security protocols motivated by the need to combine existing or specifically designed protocols that each enforce a particular security requirement. Although appealing from a practical point of view, this approach raises the difficult question of the security properties guaranteed by the combined layered protocols, as opposed to each protocol in isolation. In this work, we apply a method for facilitating the development of trustworthy security-critical systems using the computer-aided systems engineering tool AutoFocus to the particular problem of layered security protocols. We explain our method at the example of a banking application which is currently under development by a major German bank and is about to be put to commercial use.

## 1 Introduction

Security aspects have become an increasingly important issue in developing distributed systems, especially in the electronic business sector. Because of the fact that failures of security mechanisms may cause very high potential damage (e.g., loss of money through fraud), the correctness of such systems is crucial.

Designing security critical systems correctly is difficult. Also, it is easy to misunderstand assumptions on the environment in which e.g. protocols are to be used and what their secure functioning may rely on. Security violations often occur at the boundaries between security mechanisms and the general system [11,1].

Therefore, the consideration of security aspects has to be integrated into general systems development [20,1] and also take into account aspects of security management [7]. Common modelling techniques used in industry, such as collaboration diagrams, state charts and message sequence charts (MSCs) have to be tailored for that purpose.

A particular challenge lies in the development of layered security protocols motivated by the need to combine existing or specifically designed protocols

S. Anderson et al. (Eds.): SAFECOMP 2003, LNCS 2788, pp. 116–129, 2003.

that each enforce a particular security requirement. Although appealing from a practical point of view, this approach raises the difficult question of the security properties guaranteed by the combined layered protocols, as opposed to each protocol in isolation.

In this work, we apply a method for facilitating the development of trustworthy security-critical systems using the computer-aided systems engineering tool AutoFocus [14,15] to the particular problem of layered security protocols. Cryptographic protocols are specified with state charts. Together with a suitable attacker model, they are examined for security weaknesses using model checking.

We explain our method at the example of a banking application which is currently under development by a major German bank and is about to be put to commercial use.

We specify cryptographic protocols using state transition diagrams (STDs, similar to UML state charts). Together with the modelled adversary, this system is checked for security weaknesses automatically using the model checker SMV connected to AutoFocus to verify the desired security properties of the protocol.

The approach has the benefits of combining intuitive graphical modelling, simulation and model checking in one user-friendly CASE-tool, and allows to represent possible attacks as MSCs. Since the AutoFocus tool builds on the formal development method Focus [4], our approach also supports formal proofs in this framework. The intruder model used is rather flexible, e.g. the adversary can switch between acting as one or another party, intercept only certain messages or learn certain keys etc. Also, the AutoFocus tool integrates several formal tools, which in [3] was identified as a major obstacle to widespread adoption of formal methods.

To put our work into context, we give some background information and related work. There has been extensive research in using formal methods to verify security protocols, following an abstract way to describe protocols in [8]. A few examples are [6,22,25]. [28] considers refinement of security-critical systems. Aspects of security engineering have been considered in [1,27,21,10]. As an example for the treatment of security in the context of general systems engineering, [17,18] presents work towards using the UML notation in security engineering. AutoFocus has been used for security e.g. in [31].

This paper is structured as follows. In Section 2 we introduce the notation of AutoFocus. In Section 3, we give an overview over the banking application under consideration, specify a critical part (a layered authentication protocol) and carry out a security analysis.

We end with a conclusion and indicate further planned work.

## 2 The Tool AutoFocus

For modelling and verification of the layered protocol, we use the tool AutoFocus [14,29]. AutoFocus is a CASE tool for graphically specifying distributed systems. It is based on the formal method Focus [5], and its models have a simple,