Chapter 8

Alfredo Pironti
Politecnico di Torino, Italy

Davide Pozza
Politecnico di Torino, Italy

Riccardo Sisto
Politecnico di Torino, Italy

ABSTRACT

Designing and implementing security protocols are known to be error-prone tasks. Recent research progress in the field of formal methods applied to security protocols has enabled the use of these techniques in practice. The objective of this chapter is to give a circumstantial account of the state-of-the-art reached in this field, showing how formal methods can help in improving quality. Since automation is a key factor for the acceptability of these techniques in the engineering practice, the chapter focuses on automated techniques and illustrates in particular how high-level protocol models in the Dolev-Yao style can be automatically analyzed and how it is possible to automatically enforce formal correspondence between an abstract high-level model and an implementation.

DOI: 10.4018/978-1-60960-851-4.ch008
INTRODUCTION

Security protocols enable distributed interactions to occur securely even over insecure networks. Well known examples are the protocols for secure authentication or key exchange that we use daily. With the growth of connectivity over the Internet, there is an increasing demand for secure distributed ICT systems, which in turn is rapidly widening the spread and scope of security protocols. Web services, grid computing, electronic commerce and SCADA systems for remote control are just few examples of the many emerging distributed applications that need security. In addition to the bare data secrecy and authenticity goals, which characterize the most classical protocols, new different goals such as non-repudiation or secure transactions in electronic commerce systems have recently started to be considered as desirable, with several new protocols being proposed. The role of standards is fundamental in this field, because distributed applications rely on interoperability. However, the variegated needs of applications may sometimes call for proprietary solutions as well, when standards do not (yet) cover needs adequately. So, tasks such as designing and implementing security protocols are becoming less esoteric and more common, either as part of new standards development or as part of new products development.

These tasks are generally quite critical, because of the delicate role security protocols normally play in protecting valuable assets. Furthermore, despite their apparent simplicity, security protocols are very difficult to get right, even when developed and reviewed by experts, because they add the difficulty of taking into account all the possible operations of malicious parties to the ones of concurrent operation in a distributed environment. It is then widely recognized that the rigorous approach of formal methods plays a key role in developing security protocol designs and implementations at the desired quality level.

Although using formal methods is still considered difficult and requires expertise, research on formal methods in general, and on their application to security protocols in particular, has recently made much progress. Therefore, difficulty is progressively mitigated by the greater automation level and user friendliness that can be achieved. This progress is also being acknowledged by development process standards and evaluation standards, such as the Common Criteria for Information Technology Security Evaluation (2009), which prescribe the use of formal methods for attaining the highest assurance level, required for the most critical system components. It can be expected that in the near future the role of these more rigorous practices will further increase, as the demand for critical components increases.

The objective of this chapter is to give a circumstantial account of the state-of-the-art formal techniques that can help in improving the quality of security protocol designs and implementations in practice. The chapter aims to show what can still be done in practice, using the most promising available research results that do not require excessive expertise from users, thus being affordable. The intended focus is then on those techniques that have already been studied in depth and that can offer acceptable user-friendly automated tool support, demonstrated by research prototype tools. The newest theoretical research trends will just be mentioned, in order to show how the research in this field is moving on.

BACKGROUND

A security protocol can be defined as a communication protocol aimed at reaching a goal in a distributed environment even in the presence of hostile agents that have access to the network. Examples of security goals are user authentication (that is, proving a user’s identity to another remote user) and secrecy in data exchange (that