Chapter XIV
A Formal Verification Centred Development Process for Security Protocols

Tom Coffey
University of Limerick, Ireland

Reiner Dojen
University of Limerick, Ireland

ABSTRACT

This chapter concerns the correct and reliable design of modern security protocols. It discusses the importance of formal verification of security protocols prior to their release by publication or implementation. A discussion on logic-based verification of security protocols and its automation provides the reader with an overview of the current state-of-the-art of formal verification of security protocols. The authors propose a formal verification centred development process for security protocols. This process provides strong confidence in the correctness and reliability of the designed protocols. Thus, the usage of weak security protocols in communication systems is prevented. A case-study on the development of a security protocol demonstrates the advantages of the proposed approach. The case-study concludes with remarks on the performance of automated logic-based verification and presents an overview of formal verification results of a range of modern security protocols.

INTRODUCTION

The security of electronic networks and information systems is a critical issue for the use of new technologies in all fields of life. Mobile and fixed networks are trusted with highly sensitive information. Thus, security protocols (also called cryptographic protocols) are required to ensure the security of both the infrastructure itself and the information that runs through it. These security protocols can be thought of as the keystones of a secure architecture. Basic cryptographic protocols allow agents to authenticate each other, to establish fresh session keys for confidential communication and to ensure the authenticity of data and services. Building on such basic cryptographic protocols, more advanced services like nonrepudiation, fairness, electronic payment, and electronic contract signing are achieved.

The massive growth in communications technologies—in particular in the wireless sector—causes an ever-changing environment for today’s communication services. The pervasive nature of emerging Information and Communications Technologies has added new areas of concern to information security. For example, the increased virtual and physical mobility of users enhances their possibilities for interaction,
but leads to an increasing demand for reliable trust relationships. To address new security risks and threats arising from such changes in the communication environment, a constant supply of novel security protocols is required.

However, security protocols are vulnerable to a host of subtle attacks, and designing protocols to be impervious to such attacks has been proven to be extremely challenging and error-prone. This is evident from the surprisingly large number of published protocols, which have later been found to contain various flaws, in many cases, several years after the original publication (Brackin, 2000; Coffey, Dojen, & Flanagan, 2003a, 2003b, 2003c, 2003d; Huima, 1999; Gürgens & Rudolph, 2002; Newe & Coffey, 2002; Ventuneac, Coffey, & Newe, 2004; Ventuneac, Dojen, & Coffey, 2006; Zhang & Fang, 2005; Zhang & Varadharajan, 2001).

**Motivation**

The importance of formal verification of cryptographic protocols during the development process cannot be overstated (Coffey et al., 2003a), as the absence of formal verification of these protocols can lead to flaws and security errors remaining undetected. However, an ad-hoc survey carried out at the Data Communication Security Laboratory, UL in 2005 on over 200 recent papers on cryptographic protocols revealed that only 15% of these publications contained formal verifications.

The BCY protocol (Beller, Chang, & Yacobi, 1993) provides a very interesting case study to highlight the problems with the correct design of security protocols. Published in 1993, the BCY protocol demonstrated the feasibility of public-key cryptography in mobile communications. Subsequently, Carlsen (1994) discovered weaknesses in the protocol and published an amended protocol. Weaknesses in Carlsen’s amended protocol were discovered by Mu and Varadharajan (1996), and another modified protocol was published. Horn, Martin, and Mitchell (2002) identified a weakness in the Mu and Varadharajan version of the BCY protocol, but did not publish a corrected version. Coffey et al. (2003a) published formal verifications of the BCY protocol and its derivatives. In addition to all previously identified weaknesses, a hitherto unknown flaw in the BCY protocol and its derivatives was detected. A corrected protocol was proposed and also formally verified. This case study highlights that the design of security protocols is a highly complex and error-prone process. It also shows that formal verification is an imperative step in the design of security protocols.

This chapter advocates the use of formal verification during the development of modern security protocols. It discusses the importance of formal verification of security protocols prior to their release by publication or implementation. A discussion on logic-based verification of security protocols and its automation provides the reader with an insight into the current state-of-the-art of formal verification of security protocols. The authors propose a formal verification centred development process for security protocols. This approach results in a strong confidence in the correctness and reliability of the designed protocols and prevents the usage of weak security protocols in communication systems. Further, a case-study demonstrates the advantages of the proposed approach to the design of security protocols. This case study provides a discussion on the difficulties involved in designing correct and reliable security protocols. As an example, the authentication and key-agreement protocol by Beller, Chang, and Yacobi (1993) is taken. The BCY protocol contains a number of well-known weaknesses and, thus, the ability of the proposed process to detect these weaknesses is demonstrated. The case-study concludes with remarks on the performance of automated logic-based verification and presents an overview of formal verification results of a range of modern security protocols.

**FORMAL VERIFICATION OF SECURITY PROTOCOLS**

Needham and Schroeder (1978) are generally credited with the introduction of formal methods as a possible tool for cryptographic protocol analysis. However, the first experimental work in this area was done by Dolev, Even, and Karp (1982) and by Dolev and Yao (1983), who developed a set of polynomial-time algorithms for deciding the security of a restricted class of protocols. It was soon found that relaxing the restrictions on the protocols made the security problem undecidable (Even & Goldreich, 1983). However, Dolev and Yao’s work was significant in that it was the first to develop a formal model that provided:

1. The possibility of multiple executions of the protocol running concurrently.
2. Cryptographic algorithms behaving like black boxes, obeying a set of algebraic properties.