Chapter XV
The Provably Secure Formal Methods for Authentication and Key Agreement Protocols

Jianfeng Ma
Xidian University, China

Xinghua Li
Xidian University, China

ABSTRACT

In the design and analysis of authentication and key agreement protocols, provably secure formal methods play a very important role, among which the Canetti-Krawczyk (CK) model and universal composable (UC) security model are very popular at present. This chapter focuses on these two models and consists mainly of three parts: (1) an introduction to CK model and UC models; (2) A study of these two models, which includes an analysis of CK model and an extension of UC security model. The analysis of CK model presents its security analysis, advantages, and disadvantages, and a bridge between this formal method and the informal method (heuristic method) is established; an extension of UC security model gives a universally composable anonymous hash certification model. (3) The applications of these two models. With these two models, the four-way handshake protocols in 802.11i and Chinese wireless LAN (WLAN) security standard WLAN authentication and privacy infrastructure (WAPI) are analyzed.

INTRODUCTION

Key agreement protocols are mechanisms by which two parties that communicate over an adversarially controlled network can generate a common secret key. Key agreement protocols are essential for enabling the use of shared-key cryptography to protect transmitted data over insecure networks. As such they are a central piece for building secure communications and are among the most commonly used cryptographic protocols.

The design and analysis of secure key agreements protocols has proved to be a non-trivial task, with a large body of work written on the topic. Among the methods for the design and analysis of key agreement protocols, formal methods have always been a focused problem in the international investigation of cryptography. Over the years, two distinct views of formal methods, symbolic logic method and computational complexity method, have developed in two mostly separate communities (Martin & Phillip, 2002). The symbolic logic method relies on a simple but effective symbolic formal expression approach, in which cryptographic operations are seen as functions on a space of symbolic formal expressions (e.g., BAN, communicating sequential processes [CSP], NRL) (Wenbo, 2004). The other one, computational complexity method, relies on a detailed computational model that considers issues of complexity and probability of successful attacks, in which cryptographic operations are seen as functions on strings of bits.

Provably secure formal method, which is based on the computational complexity method, is a very hot research point at present. Its salient property is that the security protocols designed by them are provably secure. Among the provably secure formal methods, CK model and UC security model are very popular.

In 2001, Canetti and Krawczyk presented the CK model for the formal analysis of key-exchange (KE) protocols. A session-key security definition and a simple modular methodology to prove a KE protocol with this definition are introduced in this model. One central goal of the CK model is to simplify the usability of the definition via a modular approach to the design and analysis of KE protocols. It adopts the indistinguishability approach (Bellare, Canetti, & Krawczyk, 1998) to define security: A KE protocol is called secure if under the allowed adversarial actions it is infeasible for the attacker to distinguish the value of a key generated by the protocol from an independent random value. The security guarantees that result from the proof by the CK model are substantial as they capture many of the security concerns in the real communications setting.

Concurrent composition is a fact of life of real network settings. Protocols that are proven secure in the stand-alone model are not necessarily secure under composition. Therefore, it does not suffice to prove that a protocol is secure in the stand-alone model. UC security model proposed by Canetti in 2001 (Birgit & Michael, 2001) is for representing and analyzing cryptographic protocols under concurrent circumstance (Yeluda, 2003). The salient property of definitions of security in this framework is that they guarantee security even when the given protocol is running in an arbitrary and unknown multi-party environment. An approach taken in this framework is to use definitions that treat the protocol as stand-alone but guarantee secure composition. Security in complex settings (where a protocol instance may run concurrently with many other protocol instances, or arbitrary inputs and in an adversary controlled way) is guaranteed via a general composition theorem. On top of simplifying the process of formulating a definition and analyzing protocols, this approach guarantees security in arbitrary protocol environments, even unpredictable ones that have not been explicitly considered. The abstract level of UC security goes far beyond other security models, therefore, it tends to be more restrictive than other definitions of security. The most outstanding nature of UC framework is its modular design concept: may alone design a protocol, so long as the protocol satisfies the UC security, it can be guaranteed secure while runs concurrently with other protocols.

This chapter focuses mainly on the introduction, analysis, and applications of these two provably secure formal methods. The rest of this chapter is organized as follows. The next section, the CK model and the UC security model are introduced. In the third section, we analyze the security of the CK model. A bridge between this formal method and the informal method (heuristic method) is established. What is more, the advantages and disadvantages of the CK model are given. In the *Universally Composable Anonymous Hash Certification Model* section, an extension of the UC security model is presented. The UC security model fails to characterize the special security requirements of anonymous authentication with