Abstract

Cryptographic protocols are a critical element of the infrastructure for secure communication. They can be used to provide security guarantees for the exchanged data when multiple parties are communicating in an insecure or untrusted environment. The core of cryptographic protocols such as SSL, TLS, SSH, or IPSec is the key exchange protocol, which allows two parties to generate a shared secret key used for establishing a secure channel. Authenticated key exchange (AKE) and authenticated and confidential channel establishment (ACCE) protocols are the most important building blocks in secure communication. Intuitively, they allow a party “Alice” to authenticate a communication partner “Bob” and securely establish a common session key (used for establishing a secure communication channel) with Bob, and vice versa. The communication between Alice and Bob is then protected with this secret session key.

This thesis is concerned with the approach to design and analysis of cryptographic protocols based around the most widely used security models. In particular, we show how to systematically construct and analyze security protocols in realistic models. This work splits into two parts.

In the first part of this thesis we give an overview of the most widely used security models for AKE/ACCE protocols. Then, we extend existing security models to capture relevant attacks that were originally outside the scope of these models. Finally, we discuss the differences between the proposed security models and show the relationship between the existing models and our models.

In the second part of this thesis we first analyze the security of all three TLS-PSK ciphersuites in our extended ACCE model. It is the first detailed security analysis for the symmetric-key based TLS-PSK protocols. Then, we construct the first tightly-secure AKE protocol in an enhanced Bellare-Rogaway security model under standard assumptions. In contrast to other AKE protocols, its security does not degrade with an increasing number of participating parties and protocol sessions. Moreover, we present new efficient compilers that generically turn passively secure key exchange protocols into efficient AKE protocols where the security properties hold in the realistic setting of communication channels controlled by an active adversary. Finally, we introduce a new theoretical attack for AKE protocols, named no-match attack, and show that proving security under the matching conversations (MC) as session IDs (MC-based sID) is a delicate issue. In particular, we provide several examples of AKE protocols that claim to be secure under a security definition based on MC-based session identifier but where the security proof is actually flawed. Additionally, we give several generic ways to thwart our no-match attacks.