Case studies: Needham–Schroeder, Kerberos, TLS, 802.11 WiFi

The authentication protocols originally published by Needham and Schroeder [1978] are

at the heart of many security techniques. We present them in detail in Section 11.6.1.

One of the most important applications of their secret-key authentication protocol is the

Kerberos system [Neuman and Ts’o 1994], which is the subject of our second case study

(Section 11.6.2). Kerberos was designed to provide authentication between clients and

servers in networks that form a single management domain (intranets).

Our third case study (Section 11.6.3) deals with the Transport Layer Security

(TLS) protocol. This was designed specifically to meet the need for secure electronic

transactions. It is now supported by most web browsers and servers and is employed in

most of the commercial transactions that take place via the Web.

Our final case study (Section 11.6.4) illustrates the difficulty of engineering

secure systems. The IEEE 802.11 WiFi standard was published in 1999 with a security

specification included. But subsequent analysis and attacks have shown the

specification to be severely inadequate. We identify the weaknesses and relate them to

the cryptographic principles covered in this chapter.

The Needham–Schroeder authentication protocol

The protocols described here were developed in response to the need for a secure means

to manage keys (and passwords) in a network. At the time the work was published

[Needham and Schroeder 1978], network file services were just emerging and there was

an urgent need for better ways to manage security in local networks.

In networks that are integrated for management purposes, this need can be met by

a secure key service that issues session keys in the form of challenges (see Section

11.2.2). That is the purpose of the secret-key protocol developed by Needham and

Schroeder. In the same paper, Needham and Schroeder also set out a protocol based on

the use of public keys for authentication and key distribution that does not depend upon

the existence of secure key servers and is hence more suitable for use in networks with

many independent management domains, such as the Internet. We do not describe the

public-key version here, but the TLS protocol described in Section 11.6.3 is a variation

of it.

Needham and Schroeder proposed a solution to authentication and key

distribution based on an *authentication server* that supplies secret keys to clients. The

job of the authentication server is to provide a secure way for pairs of processes to obtain

shared keys. To do this, it must communicate with its clients using encrypted messages.

**Needham and Schroeder with secret keys •** In their model, a process acting on behalf of

a principal A that wishes to initiate secure communication with another process acting

on behalf of a principal B can obtain a key for this purpose. The protocol is described

for two arbitrary processes A and B, but in client-server systems, A is likely to be a client

initiating a sequence of requests to some server B. The key is supplied to A in two forms:

one that A can use to encrypt the messages that it sends to B and one that it can transmit

securely to B. (The latter is encrypted in a key that is known to B but not to A, so that B

can decrypt it and the key is not compromised during transmission.)

The authentication server S maintains a table containing a name and a secret key

for each principal known to the system. The secret key is used only to authenticate client

processes to the authentication server and to transmit messages securely between client

processes and the authentication server. It is never disclosed to third parties and it is

transmitted across the network at most once, when it is generated. (Ideally, a key should

always be transmitted by some other means, such as on paper or in a verbal message,

avoiding any exposure on the network.) A secret key is the equivalent of the password

used to authenticate users in centralized systems. For human principals, the name held

by the authentication service is their username and the secret key is their password. Both

are supplied by the user on request to client processes acting on the user’s behalf.

The protocol is based on the generation and transmission of tickets by the

authentication server. A ticket is an encrypted message containing a secret key for use

in communication between A and B. We tabulate the messages in the Needham and

Schroeder secret-key protocol in Figure 11.14. The authentication server is S.

*NA* and *NB* are *nonces*. A nonce is an integer value that is added to a message to

demonstrate its freshness. Nonces are used only once and are generated on demand. For

example, the nonces may be generated as a sequence of integer values or by reading the

clock at the sending machine.

If the protocol is successfully completed, both A and B can be sure that any

message encrypted in *KAB* that they receive comes from the other, and that any message

