# Exercises accompanying 'The Modelling and Analysis of Security Protocols'

## Chapter 5

**Exercise 5.1** In the first version of the Yahalom protocol above, investigate the effect of moving $b$'s identity outside of the encrypted component of Message 3a: adapt the Casper script to model this change, and then use FDR to analyse the protocol. △

**Exercise 5.2** Consider the Needham Schroeder Public Key Protocol:

$$\begin{array}{lll} \text{Message 1.} & a \rightarrow b & : \{na.a\}_{PK(b)} \\ \text{Message 2.} & b \rightarrow a & : \{na.nb\}_{PK(a)} \\ \text{Message 3.} & a \rightarrow b & : \{nb\}_{PK(b)} \end{array}$$

It is assumed that each agent knows all the public keys. Analyse this protocol using Casper and FDR. △

**Exercise 5.3** In some protocols, nonces are considered to be *predictable*: that is, an intruder may be able to predict which nonces other agents are about to use. How can we model predictable nonces within Casper? △

**Exercise 5.4** Produce a Casper script to model the Yahalom-BAN protocol:

$$\begin{array}{lll} \text{Message 1.} & a \rightarrow b & : na \\ \text{Message 2.} & b \rightarrow s & : nb.\{a.na\}_{ServerKey(b)} \\ \text{Message 3.} & s \rightarrow a & : nb.\{b.kab.na\}_{ServerKey(a)}.\{a.kab.nb\}_{ServerKey(b)} \\ \text{Message 4.} & a \rightarrow b & : \{a.kab.nb\}_{ServerKey(b)}.\{nb\}_{kab} \ , \end{array}$$

for example, by adapting the script from Section 5.1. △

**Exercise 5.5** Adapt the script for the seven message adapted Needham Schroeder Public Key Protocol to remove the identities from within the encrypted components of the key delivery messages, messages 3 and 6:

$$\begin{array}{lll} \text{Message 1.} & a \rightarrow s & : b \\ \text{Message 2.} & s \rightarrow a & : \{PK(b)\}_{SSK(s)} \\ \text{Message 3.} & a \rightarrow b & : a, b, \{na, a\}_{PK(b)} \\ \text{Message 4.} & b \rightarrow s & : a \\ \text{Message 5.} & s \rightarrow b & : \{PK(a)\}_{SSK(a)} \\ \text{Message 6.} & b \rightarrow a & : b, a, \{na, nb, b\}_{PK(a)} \\ \text{Message 7.} & a \rightarrow b & : a, b, \{nb\}_{PK(b)} \ . \end{array}$$

Analyze this protocol using Casper and FDR. △

**Exercise 5.6** Consider the following protocol, based upon one suggested by Denning and Sacco:

$$\begin{array}{lll} \text{Message 1.} & a \rightarrow b & : cert_A \\ \text{Message 2.} & b \rightarrow a & : cert_B.\{\{kab\}_{SK(b)}\}_{PK(a)} \end{array}$$

Here $cert_A$ and $cert_B$ are public key certificates for $a$ and $b$, respectively, of the following form:

$$\begin{array}{lcl} cert_A & = & \{a, PK(a)\}_{CASK(ca)}, \\ cert_B & = & \{b, PK(b)\}_{CASK(ca)}, \end{array}$$

where $CASK(ca)$ is the secret key of trusted certification authority $ca$.

Analyse this protocol using Casper and FDR. Hint: use environment messages to model the agents retrieving their key certificates; you should include the intruder's key certificate in his initial knowledge. △

**Exercise 5.7** Investigate which, if any, authentication specifications are satisfied by the Needham-Schroeder Public Key Protocol from [1]; also investigate whether the corrected version in [1] satisfies the `StrongSecret` specification for the nonces. △

**Exercise 5.8** Code up the Needham Schroeder Signature Protocol from Section 5.5 of the book (Hash Functions) as a Casper script. Compile the script into CSP, and analyse it using FDR. △

**Exercise 5.9** Consider the TMN protocol:

$$\begin{array}{lll} \text{Message 1.} & A \rightarrow S & : B.\{ka\}_{pks} \\ \text{Message 2.} & S \rightarrow B & : A \\ \text{Message 3.} & B \rightarrow S & : A.\{kb\}_{pks} \\ \text{Message 4.} & S \rightarrow A & : ka \oplus kb \end{array}$$

where $pks$ is the public key of server $s$, $ka$ and $kb$ are session keys, and the intention is to establish a new session key $kb$ shared between $A$ and $B$. Use Casper and FDR to analyze this protocol; you should discover an attack. Suggest how to adapt the protocol to prevent this attack, and then investigate whether the adapted protocol is secure. △

# Bibliography

[1] M. Burrows, M. Abadi, and R. Needham, *A Logic of Authentication*, Digital Equipment Corporation Systems Research Center report No. 39, 1989.