CSSE4603/7032 Models of Software Systems Semester 1, 2016

Assignment 1: Needham-Schroeder Protocol

Course coordinator: Graeme Smith **Due: 5pm, Mon 4 April**

The purpose of this assignment is to give you experience formalising requirements in the Z notation. The case study is a simplified version of the Needham-Schroeder protocol in which agents send each other encrypted messages, where the messages are encrypted (and decrypted) using keys supplied by a trusted server. The widely used Kerberos computer network authentication protocol is based on the Needham-Schroeder protocol.

Informal description

- The system consists of agents, a server, keys and encrypted messages.
- Initially each agent A has a key k_{AS} for encrypting messages (in either direction) between it and the server S, but at this stage no other keys.
- The server S has the key k_{AS} for each agent A in the system. Furthermore, the server has access to each of the keys k_{AB} needed by agents A and B if they wish to send each other encrypted messages.
- If an agent A wishes to obtain a key for encrypting messages (in either direction) between it and some other agent B, it initiates the protocol by sending a (non-encrypted) message to the server S. This message identifies the participating agents. Symbolically,

  $$A \rightarrow S : A, B$$

- The server S responds to this protocol initiation by extracting an encryption key k_{AB} for encrypting messages between the agents A and B involved. The server S sends back to the initiating agent A two messages each encrypted with the key k_{AS}. The first encrypted message contains the new key k_{AB} and the identity of the other agent B. The second encrypted message contains an encrypted message. This 'inner' message is encrypted with the key k_{BS} and hence can only be decrypted by B. It contains the new key k_{AB} and the identity of the initiating agent A. Symbolically,

  $$S \rightarrow A : \{k_{AB}, B\}_{k_{AS}}, \{\{k_{AB}, A\}_{k_{BS}}\}_{k_{AS}}$$

- When the initiating agent A receives these two messages, the inner message of the second message is sent as-is (i.e., not decrypted) to the agent B. Symbolically,

  $$A \rightarrow B : \{k_{AB}, A\}_{k_{BS}}$$

Task description

Your task is to complete the missing declarations and predicates in the following partial Z specification of the Needham-Schroeder protocol. A template LaTeX document of this partial specification is available on the Blackboard site. A demonstration of using TeXstudio to produce LaTeX documents, and CZT to type-check Z specifications in LaTeX will be given in the first lecture slot of Week 4.

A pdf file of your completed assignment must be submitted via Blackboard by the due date.

Partial Z specification

Let the given set

$$[Comm]$$

denote the set of all possible communications.

Let *Message* and *EncryptedMessage* denote the sets of messages and encrypted messages, respectively.

$$Message, EncryptedMessage : \mathbb{P}\, Comm$$

The actual way a message or encrypted message is internally structured is of no concern. Then a key can be thought of as an injective (one-to-one) function that takes an element of type communication and converts it into an encrypted message. Hence we can define the set of all keys by

$$Key == Comm \rightarrowtail EncryptedMessage$$

Suppose the agents and server are identified via their names, and we have the given set

$$[Name]$$

of all possible names.

The following functions allow us to extract information from messages. For a request message sent to a server, *this* returns the name of the agent which sent the message, and *other* returns the name of the agent with which it wants to communicate. For a message with a key, *key* returns the key, and *other* returns the agent that can be communicated with using that key.

$$\begin{array}{l} this : Message \pfun Name \\ key : Message \pfun Key \\ other : Message \fun Name \\ \hline \mathrm{dom}\, this \cap \mathrm{dom}\, key = \varnothing \\ \mathrm{dom}\, this \cup \mathrm{dom}\, key = Message \end{array}$$

The predicate states that no message is both a request message (in the domain of *this*) and a key message (in the domain of *key*). Also, all messages are either request or key messages.

An agent is modelled as having a name, the name of the server (which is not an agent), and a table whose entries map names of other agents and the server to the key used to communicate with them.

Agent

$$\begin{array}{l} name, serverName : Name \\ table : Name \pfun Key \\ \hline name \neq serverName \end{array}$$

Initially, the table contains a single key for communication between the agent and the server.

Init

$$\begin{array}{l} Agent \\ \hline \ldots \end{array}$$

An agent may request a key for communication with another agent for which it does not already have a key. This request is sent to the server via a non-encrypted message containing the agent's name and that of the other agent.

RequestKey

. . .

. . .

An agent may receive a key via an encrypted message from the server and add it to its table. This message also contains the name of the other agent with which the agent can communicate using the received key. A second encrypted message is also received from the server, decrypted and its further encrypted content is sent to the other agent.

ReceiveKeyFromServer

. . .

. . .

An agent may receive a key via an encrypted message from another agent (but encrypted with the agent's key for communication with the server) and add it to its table. The message also contains the name of the other agent with which the agent can communicate using the received key.

ReceiveKeyFromAgent

. . .

. . .

Assessment Criteria

The assignment is worth 10% of your final grade. You will be given a mark out of 10 based on the percentage of the required declarations and predicates which are both syntactially and semantically correct. For example, your mark will be 8.5 if you get 85% of the required declarations and predicates correct.

A mark of zero will be given for work with little or no academic merit.

School Policy on Student Misconduct:

You are required to read and understand the School Statement on Misconduct, available on the School's website at:

http://www.itee.uq.edu.au/itee-student-misconduct-including-plagiarism