CS259 - Security Analysis of Network Protocols

Winter Quarter, 2004
Homework #1 (Due: 01/29/04)

January 14, 2004

Overview

The purpose of this assignment is to get you started with the Murφ verifier. You are required to extend the provided Murφ model of the Needham-Schroeder protocol with new rules and invariants. You are also required to run the verifier and interpret the results of the verification.

Technical

Murφ is available on Leland System computers in the following directory: `/usr/class/cs259/Murphi3.1/`
Murφ models relevant to this assignment are available in the following directory: `/usr/class/cs259/hw1/`
Consult the `Readme` file in the `hw1` directory for information on running Murφ. If you wish to run Murφ on a different machine, check the class website for instructions.

Submission

You should compile your answers into a single text file and submit by email at `aderek@cs.stanford.edu`.

General

In this assignment we will look at two similar protocols, the Needham-Schroeder protocol (NS), and its fixed version – the Needham-Schroeder-Lowe (NSL) protocol. Using the informal arrows-and-messages diagrams, they can be described as follows:

$A \rightarrow B : \{\|A, N_A\|\}_{K_B}$	$A \rightarrow B : \{\|A, N_A\|\}_{K_B}$
$B \rightarrow A : \{\|N_A, N_B\|\}_{K_A}$	$B \rightarrow A : \{\|B, N_A, N_B\|\}_{K_A}$
$A \rightarrow B : \{\|N_B\|\}_{K_B}$	$A \rightarrow B : \{\|N_B\|\}_{K_B}$
Needham-Schroeder protocol	Needham-Schroeder-Lowe protocol

Murφ model of both protocols is given in the file `ns.m` in the assignment directory. Boolean variable `FIXED` is used to switch between the two. The model also contains the actions of the intruder who can intercept messages and generate new messages, using observed data and initial knowledge.

In each of the problems you are asked to check if some protocol invariant is satisfied in the Murφ model. If an invariant fails, you are required to write down the sequence of rules fired in the violating trace and a corresponding message-and-arrows diagram describing the attack. If an invariant is satisfied, write down the information about the number of states explored and the time needed for verification.

For the purpose of this assignment, you can use the default parameters in the model (one initiator, one responder, one intruder), but you are encouraged to run the verifier with larger parameters. Extra credit will be given for finding a previously undiscovered bug in the protocol.

Problem 1

Two invariants in the model specify the mutual authentication property we are interested in verifying. When translated to English, `"initiator correctly authenticated"` invariant states that whenever a responder i completes a session, apparently with some initiator j, then it must be that j has completed a session, apparently with i. The meaning of the other invariant is analogous.

For both invariants (independently), determine if they are satisfied in the provided Murφ model of the NS protocol.

Problem 2

In this problem we investigate whether NS or NSL can be used as key-exchange protocols. Specifically, we want to check if the nonces exchanged in the protocol remain secret.

(a) Write down the Murφ invariant `"initiator secrecy"` modelling the following property: if some initiator i completes a session with an honest responder then the intruder does not know the initiator's nonce. Also, write down the analogous invariant `"responder secrecy"`.

(b) For both NS and NSL protocol, test if these invariants are satisfied.

Problem 3

In this problem we look at the scenario when a malleable encryption scheme is used in the NSL protocol. We say than an encryption scheme is *malleable* if, under some circumstances, an intruder can predictably modify the contents of an encrypted message without knowing the corresponding decryption key.

(a) Assume that, if the intruder knows a message of the form $\{|Y, \text{data}|\}_{K_X}$, where X and Y are agent names, then he can generate a message of the form $\{|Z, \text{data}|\}_{K_X}$ where Z is an arbitrary agent name. Write down a Murφ rule which models this new capability of the intruder in the NSL protocol.

(b) Test if the authentication and secrecy invariants hold in the NSL protocol with the improved intruder.