Homework 1

CS259 - Security Analysis of Network Protocols

Out: Thursday, January 10, 2008
Due: Thursday, January 24, 2008

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 arnab@cs.stanford.edu. Please use "CS259 Homework 1 *your name*" as the subject line when submitting. Also, mention your name in the text file itself.

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 interpret the sequence

of rules fired in the violating trace and write down the 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, the "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.

1. 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 initiators nonce. Also, write down the analogous invariant "responder secrecy".

2. For both NS and NSL protocol, test if these invariants are satisfied.

Problem 3 Consider the following variant(s) of the Needham-Schroeder(-Lowe) protocol(s) where the last message is sent unencrypted:

$A \to B : \{\|A, N_A\|\}_{K_B}$	$A \to B : \{\|A, N_A\|\}_{K_B}$
$B \to A : \{\|N_A, N_B\|\}_{K_A}$	$B \to A : \{\|B, N_A, N_B\|\}_{K_A}$
$A \to B : N_B$	$A \to B : N_B$
NS Variant	NSL Variant

1. Modify the existing Murphi code to model the variant protocols. Check if the initiator and responder authentication properties hold. If not, describe the attack(s) found.

2. As you can see, the secrecy of the nonce N_B no longer holds at the end of the protocol. Confirm if Murphi comes up with the expected attack on secrecy in both protocols. What about the secrecy of N_A?

3. Though the secrecy of N_B does not hold at the end, it might hold at intermediate points. Check and describe upto what state, for both initiator and responder, there is no attack found on secrecy of N_B.