CS259 - Security Analysis of Network Protocols

Winter Quarter, 2006
Homework #2 (Due: 01/31/06)

January 22, 2006

Overview

The purpose of this assignment is to get you acquainted with the AVISPA model checker .

Technical

AVISPA is available on Leland System computers in the following directory: `/usr/class/cs259/Avispa-1.0/` AVISPA models relevant to this assignment are available in the following directory: `/usr/class/cs259/hw2a/`. Follow instructions listed in the Readme file in this directory to run AVISPA.

Submission

You should compile your answers into a single text file and submit by email at `mukunds@stanford.edu`. Please submit one file per group. Please use `"CS259 Homework 2a"` as the subject line when submitting. Also, mention the names of the group members in the file.

General

In this assignment, we shall continue looking at the two protocols we saw in Homework 1. 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 → B : $\{\!|A, N_A|\!\}_{K_B}$	A → B : $\{\!|A, N_A|\!\}_{K_B}$
B → A : $\{\!|N_A, N_B|\!\}_{K_A}$	B → A : $\{\!|B, N_A, N_B|\!\}_{K_A}$
A → B : $\{\!|N_B|\!\}_{K_B}$	A → B : $\{\!|N_B|\!\}_{K_B}$
Needham-Schroeder protocol	Needham-Schroeder-Lowe protocol

Murφ model of the Needham-Schroeder protocol is given in the file `ns.hlspl` in the assignment directory.

Problem 1

Run AVISPA on the given model for the Needham-Schroeder protocol. AVISPA should say that the given model is 'safe', though we know that the Needham-Schroeder protocol is flawed. Submit the number of nodes visited by the model checker (The value of the visitedNodes field).

Since AVISPA does not find the flaw, discounting any errors in the implementation of the tool, one of two things may be a problem: We modeled the protocol with its environment incorrectly, or we modeled one of the properties incorrectly. Which is the problem?

Modify the given model by adding a line to fix the modeling bug. Run AVISPA on the new model and verify the error trace. Submit the modification to the code. Also, list the number of nodes visited by the model checker when run on the modified file. *Hint: Think of how the Needham-Schroeder attack starts.*

Problem 2

Modify the model to implement Lowe's fix. Indicate which lines of code you needed to modify and what the modification was. Run the model checker on the modified code. The result should be that the model checks out safely. List the number of nodes visited by the model checker.