Homework 2

CS259 - Security Analysis of Network Protocols

Out: Friday, February 1, 2008

Due: Tuesday, February 12, 2008

Overview The purpose of this assignment is to get you started with the PRISM model checker.

Technical PRISM is available here:
http://www.prismmodelchecker.org/download.php.
Manual:
http://www.prismmodelchecker.org/manual/.

Go through this tutorial: http://www.prismmodelchecker.org/tutorial/die.php and probably that's all you will need to know for this assignment.

Those of you who find PRISM way too fun for doing only one assignment can look up these case studies including security protocols:
http://www.prismmodelchecker.org/casestudies/index.php

Submission You should compile your answers into a single text file and submit by email to arnab@cs.stanford.edu. Please use "CS259 Homework 2 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 network topologies with probabilistic attackers. In the network topologies analyzed in problems 1 and 2, we make the simplifying assumption that all honest nodes send out packets received by them on exactly one outgoing edge, each having equal probability of usage.

The files *nw.pm* and *nw.pctl*, available at the course website, model the network in figure 1 and specify a property to verify respectively. You will use these files as starting points in this assignment.

Problem 1. Consider the network topology in figure 1, modeled in the file *nw.pm*. *s = 0* models the source node and *s = 3* models the destination node. Load the property file *nw.pctl* and do verify. The temporal logic formula *x* U *y* holds true on a path in which *y* is eventually true and *x* is true on all the nodes till you hit a node where *y* is true - whatever happens after is immaterial. In particular, (*true* U (*s = 3*)) holds on a path in which *s = 3* occurs eventually. Confirm for this network that the destination is always reached.

1. Suppose node 1 is a malicious agent who drops half of the packets received. Compute manually the probability of a packet sent by the source arriving at the destination.
2. Modify *nw.pm* to reflect this scenario. Describe the modifications. Confirm your answer to the last question using PRISM.

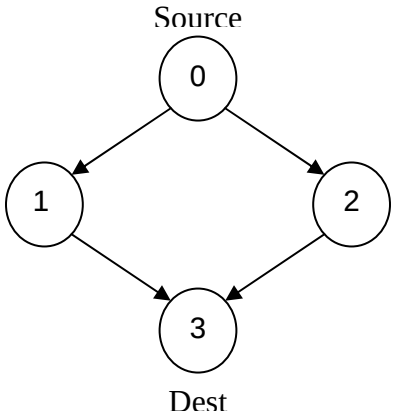

Figure 1

Problem 2. Model the network in Figure 2 in PRISM. Again confirm that all the packets from source eventually reach destination.

1. Which node would you, as an attacker, compromise to cause maximum damage in communication, node 1, 2, 3 or 4? The compromised node drops packets received with probability 50% and transmits the rest with each outgoing node having equal probability of usage. Describe the modifications in code and justify your answer, stating the results from PRISM.
2. Suppose node 3 modifies packets with 50% probability before sending out and node 2 drops packets with 50% probability. When the destination node receives a packet, we will say the source is *authenticated* to the destination if the packet is unmodified. Compute the probability that authentication holds, using PRISM. More precisely, compute:

   Pr[*packet received by dest is unmodified* | *packet is received by dest*]

   Describe the modifications to the code.

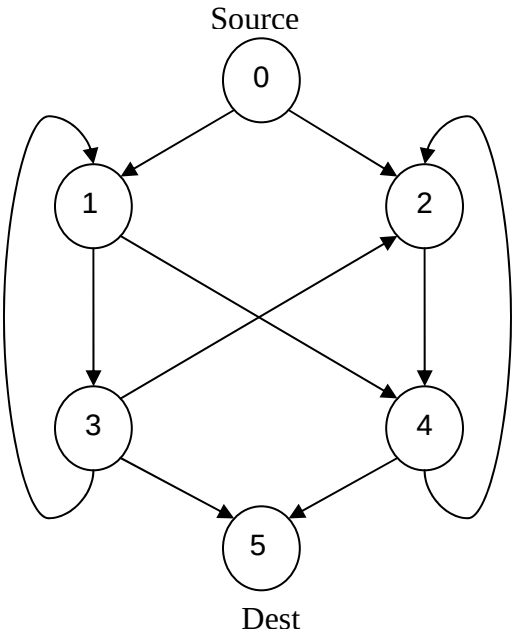

Figure 2