Technische Universität München
Fakultät für Informatik

Dr. K. N. Verma
verma@in.tum.de
Room: MI 02.07.041

Language Based Security

Summer Semester 2006

8. Homework *05 July 2006*

Exercise 1:

Given the set of statements produced for Java stack inspection, give an algorithm which examines them and decides whether a checkPrivilege(T) operation should succeed.

Exercise 2:

Consider the following modified version of the Needham-Schroeder public key protocol where both nonces N_a and N_b are sent in the third message.

1. $A \longrightarrow B : \{A, N_a\}_{K_b}$
2. $B \longrightarrow A : \{N_a, N_b\}_{K_a}$
3. $A \longrightarrow B : \{Na, N_b\}_{K_b}$

What are the security properties of this protocol ?