CSE543/Fall 2006 - Homework Questions - BAN Logic

Due: Tuesday, September 26, 2006 — Professor Trent Jaeger

Please read the instructions and questions carefully. You will be graded for clarity and correctness.
Short Answer - some will be one or two words – no more than 3 sentences

1. (*3pts*) What is the goal of authentication protocol analysis?

   answer: To show that the two legitimate parties in an authentication protocol believe that only the other party shares a secret with them as the result of executing the protocol. The threat model is that of a powerful attacker.

2. (*3pts*) Use the logical postulates in BAN Logic (name them as they are used) to show that "B believes A believes N_b" based on the following input knowledge:

   (i) B believes $fresh(N_b)$

   (ii) B sees $\{N_b\}_{K^{-1}}$

   (iii) B believes $\underset{\rightarrow}{K} A$

   answer: (ii),(iii) implies (4) B believes A said N_b by Message Meaning Rule.

   (i),(4) implies (5) B believes A believes N_b by Nonce Verification Rule.

Long Answer - no more than 2 paragraphs

4. (*7pts*) Why is modeling attacker behavior one of the biggest challenges in protocol analysis? How well does BAN Logic address this challenge? Support your argument with BAN Logic concepts.

   answer: A powerful attacker can eavesdrop, add any message, or modify any message. Thus, an attacker's impact may be seen anywhere in protocol analysis.

   While the BAN Logic enables specification of messages seen (sees) and sent (said) among principals, it does not explicitly model attacker behavior nor search the space of attacker steps.

5. (*7pts*) How does BAN Logic enable us to state our trust in an authentication server in Kerberos shared key? How does BAN Logic distinguish between trust in principals and the current state of the protocol?

   answer: In BAN Logic, we use the *believes* statement to specify our trust in what the participants have at the start. However, trust that these cannot be leaked to attackers somehow is implicit.

   Distinguishing between trust and the protocol execution is implicit. Some state changes occur due to rules in the logic, and some to the introduction of new facts during protocol execution. For example, when a subject chooses a nonce as part of the protocol, *believes* statements are used to indicate this. This could be considered as trust in the choice of the nonce or a protocol state change.

Constructions - take your time and answer clearly and completely.

6. (*10pts*) Gavin Lowe found a vulnerability in the Needham-Schroeder Public Key Protocol that was (supposedly) proven correct using the BAN logic in Section 6.

   The flaw enables an intruder I to trick principal B into believing that it shares a secret with A only when it also shares this secret with I.

   The attack involves the intruder interleaving two sessions X (A authenticates to I correctly) and Y (I authenticates to B as A) in the manner below (using the notation in the paper where K_X is the public key of X).

X.1	$A \rightarrow I$	$\{N_a, A\}_{K_I}$
Y.1	$I \rightarrow B$	$\{N_a, A\}_{K_B}$
Y.2	$B \rightarrow I$	$\{N_b, N_a\}_{K_A}$
X.2	$I \rightarrow A$	$\{N_b, N_a\}_{K_A}$
X.3	$A \rightarrow I$	$\{N_b\}_{K_I}$
Y.3	$I \rightarrow B$	$\{N_b\}_{K_B}$

(a) Which of the final beliefs in the BAN logic proof (in the paper) is incorrect?

(b) What rule is used to prove this belief (i.e., the one the generates these kinds of statements)?

(c) Which precondition clause in that rule is not actually true?

(d) How did the conclusion that only A and B know N_a and N_b get proven when it is also possible for I to know these values?

answer: (a) B believes A believes N_a (B believes that I has N_a)

(b) nonce-verification rule

(c) B believes that A said N_a (B thinks I said it)

(d) Use of public keys is different than expected. Q encrypting a statement for P does not indicate the source is Q. Thus, I can forward messages from A and B implying that they are from I.

This results in a number of the initial beliefs being incorrect, so the resulting reasoning is also incorrect. For example, A believes that it shares N_b only with B, but it provides it for I as well.