CSEP590SG Winter 2004
Prof. Steve Gribble

CSEP590SG - Assignment #4

This assignment is due in class (before class begins) on Wednesday, March 9, 2004. Please do not turn in a late assignment.

BAN logic puzzle

In the BAN logic paper (“A Logic of Authentication”), the authors show a complete analysis of the Kerberos protocol in section 4.1. The analysis starts with the initial assumptions, then derives a proof of the final conclusions using a series of rule applications.

1. In section 6.1, the authors give an abridged analysis of the Needham-Schroeder public key protocol. Your first job is to convert their abridged analysis into a full analysis, by showing the set of proof steps you need to take in order to go from the initial assumptions they state to the final conclusions they reached.

2. In class, I showed a man-in-the-middle attack against Needham-Schroeder public key protocol, and I suggested a simple fix. Your next job is to apply this fix to the protocol, adjust the initial assumptions as appropriate, and construct a proof to take you to appropriate final conclusions.

   As a reminder, here is the man-in-the-middle attack:

   “I” is undergoing instance of protocol with A, and “I” pretends to be A with B:

(i)	A → I:	$\{Na, A\}^{PKI}$
(ii)	I(A) → B:	$\{Na, A\}^{PKB}$
(iii)	B → I(A):	$\{Na, Nb\}^{PKA}$
(iv)	I → A:	$\{Na, Nb\}^{PKA}$
(v)	A → I:	$\{Nb\}^{PKI}$
(vi)	I(A) → B:	$\{Nb\}^{PKB}$

   Suggested fix…in full Needham-Schroeder protocol as described in class, change:

   (vi) B → A $\{Na, Nb\}^{PKA}$

   to:

   (vi) B → A $\{Na, Nb, B\}^{PKA}$

3. In class, I showed a naïve authentication protocol with plenty of flaws:

(i)	A → KDC:	A, B
(ii)	KDC → A:	$\{CK, \{CK\}^{KB}\}^{KA}$
(iii)	A → B:	$\{CK\}^{KB}$

As a reminder, this is a symmetric key protocol. KA is a symmetric key known only to A and KDC, and KB is a symmetric key known only to B and KDC. CK is the symmetric conversation key that A and B should use to communicate with each other at the end of the protocol.

Your final job is to use the BAN logic to analyze this protocol.

First, you must convert this protocol into "ideal form". Next, you either need to start with a set of reasonable assumptions and derive conclusions, or you must start with a set of reasonable conclusions and derive the assumptions you would need to get there. Take whichever approach you believe is most illuminative.