Computer Security

Practical Exercise P2

Analysing security protocols with BAN

Division of Informatics
University of Edinburgh
http://www.dcs.ed.ac.uk/home/compsec

This is an **individual assessed practical exercise**. It will be awarded a mark out of 25. It is one of four exercises in the Computer Security module. Each exercise is worth 5% of the final result for the module, when combined with the exam mark. You can expect to spend 2–4 hours on this exercise, plus any time required for reading. The deadline for completing this practical is **20th February 2002**. You should submit your answers in hard-copy to the Informatics Teaching Office, JCMB Room 1502. Please write your answers clearly and make sure that your name and matriculation number are on every sheet of paper. Mark the first page with **Computer Security Practical P2**.

A Write the following statements in BAN logic:

1. "Alice believes that Bob believes they share a secret key. Bob has told Alice the key."

   Can we conclude that Alice and Bob share a secret key? Why or why not? [*2 marks*]

2. "Bob believes everything a trusted server says. Alice also trusts the server but only to make keys for her. The server sends a fresh shared key to Alice and Bob."

   [*2 marks*]

B Answer the following questions concerning the use of BAN.

1. The BAN jurisdiction rule is:

$$\frac{P \models Q \Rightarrow X \qquad P \models Q \models X}{P \models X} \qquad \text{(JURISDICTION)}$$

   We've seen that this rule can be used for trusted servers that do key generation. Give another example of how this might be used in real-life computing. [*1 mark*]

2. BAN logic assumes that all parties communicating are honest. This is an unrealistic assumption for the real-life use of protocols. Does it limit the effectiveness of BAN logic? [*2 marks*]

3. If in the BAN system of logic everyone is always honest, why is it possible for one party to see another say something and not automatically believe them? [*1 mark*]

C The Kerberos protocol is a key exchange protocol that uses a trusted server. It has the steps:

$$
\begin{array}{l}
A \rightarrow S \ : \ A, B \\
S \rightarrow A \ : \ \{T_s, L, K_{ab}, B, \{T_s, L, K_{ab}, A\}_{K_{bs}}\}_{K_{ab}} \\
A \rightarrow B \ : \ \{T_s, L, K_{ab}, A\}_{K_{bs}}, \{A, T_a\}_{K_{ab}} \\
B \rightarrow A \ : \ \{T_a + 1\}_{K_{ab}}
\end{array}
$$

We can rewrite this in *idealized protocol* as:

$$
\begin{array}{l}
S \rightarrow A \ : \ \{T_s, (A \overset{K_{ab}}{\leftrightarrow} B), \{T_s, (A \overset{K_{ab}}{\leftrightarrow} B)\}_{K_{bs}}\}_{K_{ab}} \\
A \rightarrow B \ : \ \{T_s, (A \overset{K_{ab}}{\leftrightarrow} B)\}_{K_{bs}}, \{T_a, (A \overset{K_{ab}}{\leftrightarrow} B)\}_{K_{ab}} \quad \text{from } A \\
B \rightarrow A \ : \ \{T_a, (A \overset{K_{ab}}{\leftrightarrow} B)\}_{K_{ab}} \quad \text{from } B
\end{array}
$$

1. What are the key differences between the normal way in which security protocols are written and idealized protocol? Give short reasons for leaving out the parts of the Kerberos protocol that are left out of the idealized version. [*2 marks*]

2. The assumptions made by the Kerberos protocol can be summarized in BAN logic as:

$$
\begin{array}{ll}
A \models A \overset{K_{as}}{\longleftrightarrow} S & B \models B \overset{K_{bs}}{\longleftrightarrow} S \\
S \models A \overset{K_{as}}{\longleftrightarrow} S & S \models B \overset{K_{bs}}{\longleftrightarrow} S \\
S \models A \overset{K_{ab}}{\longleftrightarrow} B &
\end{array}
$$

$$
\begin{array}{ll}
A \models (S \Rightarrow A \overset{K}{\longleftrightarrow} B) & B \models (S \Rightarrow A \overset{K}{\longleftrightarrow} B)
\end{array}
$$

$$
\begin{array}{ll}
A \models \sharp(T_s) & B \models \sharp(T_s) \\
B \models \sharp(T_a) &
\end{array}
$$

   Briefly, explain in English what the assumptions are (do this by breaking the assumptions down into 3 groups). [*2 marks*]

3. Give a correctness proof for the Kerberos protocol using the Jape proof system. You should prove that at the end of the protocol run, A knows that A and B share a key (i.e., $A \models A \overset{K_{ab}}{\longleftrightarrow} B$) and each knows that the other knows they share that key ($A \models B \models A \overset{K_{ab}}{\longleftrightarrow} B$ and $B \models A \models A \overset{K_{ab}}{\longleftrightarrow} B$). Each part is proved after a message is seen.

   You will find that the theorems you need to prove are already programmed into the `BAN.jt` Jape file. Hints on how to do the proof are on pages 22–24 of the paper *A Logic of Authentication* which is available from the course homepage. (NB: Jape uses the notation $(A, B) \longleftrightarrow K_{ab}$ instead of $A \overset{K_{ab}}{\longleftrightarrow} B$. See "Jape for Dummies" for more details).

   Print out your three Jape proofs and submit these as your answer. [*9 marks*]

4. Examine your proofs carefully. Were all the assumptions used? If not, why not? Can you see any ways to simplify the protocol? [*2 marks*]

5. What exactly does this proof tell us about the practical use of this protocol? Does it mean that the protocol is secure? Discuss briefly. [*2 marks*]

Practical prepared by Tom Chothia and David Aspinall.
7th February 2002
2002/02/07 11:42:52.