Notes on BAN Logic

CSG 399

March 7, 2006

The wide-mouthed frog protocol, in a slightly different form, with only the first two messages, and time stamps:

$$A \longrightarrow S: \ A, \{T_a, B, K_{ab}\}_{K_{as}}$$
$$S \longrightarrow B: \ \{T_s, A, K_{ab}\}_{K_{bs}}$$

Initial assumptions:

- A and B trust server S
- A and B share keys K_{ab} and K_{bs} (respectively) with server S
- Their clocks are loosely synchronized with S
- B trusts A to generate good cryptographic keys

The goals:

- For K_{ab} to be a good cryptographic key
- For K_{ab} to be a secret known only to A and B (and S)
- For A and B to believe these facts (so they are willing to use the key)

We will use a logic to derive the goals from the initial assumptions and the messages exchanged by the protocol. The logic will take as primitives notions such as

- belief
- encryption
- freshness, that is that some messages have been created recently
- jurisdiction, that is, who controls what aspects of the protocol

How we are going to use the logic:

1. Write initial assumptions in the language of the logic
2. Write goals in the language of the logic
3. Express the protocol in the language of the logic
4. Attempt to derive the goals using inference rules

Formulas in the logic (X is a formula, P, Q are principals, K is a key)

- P **believes** X: P may act as though X is true
- P **sees** X: P has received a message containing X (and can read it)
- P **said** X: P at some time in the past sent a message containing X (and could read it)
- P **controls** X: P has jurisdiction (or authority, or controls the truth) over X—P can make X true
- **fresh**(X): Formula X has been created recently
- $P \overset{K}{\leftrightarrow} Q$: K is a shared key between P and Q

(There are other formulas to deal with public keys and secrets, but I will not refer to them in this lecture.)

As usual, the encryption of X with key K is written $\{X\}_K$. Note that we can encrypt formulas.

The initial assumptions for WMF in BAN:

- A **believes** $A \overset{K_{as}}{\leftrightarrow} S$
- B **believes** $B \overset{K_{bs}}{\leftrightarrow} S$
- S **believes** $A \overset{K_{as}}{\leftrightarrow} S$
- S **believes** $B \overset{K_{bs}}{\leftrightarrow} S$
- A **believes** $A \overset{K_{ab}}{\leftrightarrow} B$
- B **believes** A **controls** $A \overset{K}{\leftrightarrow} B$
- B **believes** S **controls** A **believes** $A \overset{K}{\leftrightarrow} B$
- S **believes fresh**(T_a)
- B **believes fresh**(T_s)

The goals for WMF in BAN:

- B **believes** $A \overset{K_{ab}}{\leftrightarrow} B$

- B **believes** A **believes** $A \overset{K_{ab}}{\leftrightarrow} B$

To deal with the protocol, we need to re-express the protocol using formulas of the logic. BAN proposes to analyze an "idealized" version of the protocol. Roughly, an idealized protocol is a protocol where the messages exchanged by the protocol are replaced by formulas expressing the "meaning" of the messages exchanged. This depends very much on context, and a particular message in a given protocol might be idealized differently than the same message in another protocol.

For example, a message

$$A \longrightarrow B : \ \{A, K_{ab}\}_{K_{bs}},$$

where the key K_{ab} is meant to be a good key to communicate between A and B, might be idealized as

$$A \longrightarrow B : \ \{A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}.$$

Idealization is tricky and difficult to get right. There is no formal way to idealize. It is up to the skill of the designer.

One idealization for WMF:

$$A \longrightarrow S : \ \{T_a, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{as}}$$
$$S \longrightarrow B : \ \{T_s, A \textbf{ believes } A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}$$

Details of analyzing protocols:

1. Let Z be the initial assumptions of the protocol
2. For every message
$$A \longrightarrow B : \ X$$
in the idealized protocol, add formula B **sees** X to Z
3. Check whether all goals can be derived from formulas in Z using the inference rules presently described

A sample of the BAN inference rules:

$$\frac{P \textbf{ believes } Q \overset{K}{\leftrightarrow} P \quad P \textbf{ sees } \{X\}_K}{P \textbf{ believes } Q \textbf{ said } X}$$

$$\frac{P \textbf{ believes fresh}(X) \quad P \textbf{ believes } Q \textbf{ said } X}{P \textbf{ believes } Q \textbf{ believes } X}$$

$$\frac{P \textbf{ believes fresh}(X)}{P \textbf{ believes fresh}(X, Y)}$$

$$\frac{P \textbf{ believes } Q \textbf{ controls } X \quad P \textbf{ believes } Q \textbf{ believes } X}{P \textbf{ believes } X}$$

$$\frac{P \textbf{ believes } P \overset{K}{\leftrightarrow} Q \quad P \textbf{ sees } X_K}{P \textbf{ sees } X}$$

$$\frac{P \textbf{ sees } (X, Y)}{P \textbf{ sees } X}$$

We first show that B **believes** S **believes** A **believes** $A \overset{K_{ab}}{\leftrightarrow} B$:

$$\frac{\dfrac{B \textbf{ believes } \textbf{fresh}(T_s)}{B \textbf{ believes } \textbf{fresh}(T_s, A \textbf{ believes } A \overset{K_{ab}}{\leftrightarrow} B)} \quad \dfrac{B \textbf{ believes } S \overset{K_{bs}}{\leftrightarrow} B \quad B \textbf{ sees } \{T_s, A \textbf{ believes } A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}}{B \textbf{ believes } S \textbf{ said } (T_s, A \textbf{ believes } A \overset{K_{ab}}{\leftrightarrow} B)}}{\dfrac{B \textbf{ believes } S \textbf{ believes } (T_s, A \textbf{ believes } A \overset{K_{ab}}{\leftrightarrow} B)}{B \textbf{ believes } S \textbf{ believes } A \textbf{ believes } A \overset{K_{ab}}{\leftrightarrow} B}}$$

From this, we get the second goal by an application of the jurisdiction rule:

$$\frac{B \textbf{ believes } S \textbf{ controls } A \textbf{ believes } A \overset{K_{ab}}{\leftrightarrow} B \quad B \textbf{ believes } S \textbf{ believes } A \textbf{ believes } A \overset{K_{ab}}{\leftrightarrow} B}{B \textbf{ believes } A \textbf{ believes } A \overset{K_{ab}}{\leftrightarrow} B}$$

From the second goal we get the first goal by an application of the jurisdiction rule again:

$$\frac{B \textbf{ believes } A \textbf{ controls } A \overset{K_{ab}}{\leftrightarrow} B \quad B \textbf{ believes } A \textbf{ believes } A \overset{K_{ab}}{\leftrightarrow} B}{B \textbf{ believes } A \overset{K_{ab}}{\leftrightarrow} B}$$

Implicit in the BAN approach is the fact that agents can only say what they believe. Thus, in the second idealized protocol message, we need to ensure that the server believes A **believes** $A \overset{K_{ab}}{\leftrightarrow} B$ at that point of the protocol exchange. This is easy to derive from the initial assumptions and the first message of the protocol:

$$\frac{\dfrac{S \textbf{ believes } \textbf{fresh}(T_a)}{S \textbf{ believes } \textbf{fresh}(T_a, A \overset{K_{ab}}{\leftrightarrow} B)} \quad \dfrac{S \textbf{ believes } A \overset{K_{as}}{\leftrightarrow} S \quad S \textbf{ sees } \{T_a, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{as}}}{S \textbf{ believes } A \textbf{ said } (T_a, A \overset{K_{ab}B}{\leftrightarrow})}}{\dfrac{S \textbf{ believes } A \textbf{ believes } (T_a, A \overset{K_{ab}}{\leftrightarrow} B)}{S \textbf{ believes } A \textbf{ believes } A \overset{K_{ab}}{\leftrightarrow} B}}$$

Similarly, before the first message exchanged, we need to ensure that A believes that $A \overset{K_{ab}}{\leftrightarrow} B$—fortunately, this is exactly one of the assumptions.

Some implicit assumptions of the BAN approach:

- Analyzes an idealized protocol, not the original protocol.
- All agents are honest—thus, cannot catch the Lowe man-in-the-middle attack for NS protocol.
- Dolev-Yao adversary is implicit—it is very hard to make explicit.
- Beliefs do not change during a protocol interaction.

The approach advocated by BAN for verification is vastly different from what we have seen until now. We said that properties were properties of systems generated from protocols. This does not seem to be what is happening here. We can recover this view by giving a suitable semantics to BAN.

A semantics specifies when a formula of BAN logic is true. We will actually describe the semantics by giving conditions under which a formula is true in a system generated from a protocol. We can then check whether or not a protocol goal as expressed in BAN is true at all the states corresponding to the end of the protocol. (We can then examine whether or not proving a protocol correct using the inference rules of BAN means that the formulas derived are true of the generated system.)

Abadi and Tuttle give a semantics for BAN along the above lines. They slightly modify the definition of the logic to make it more suitable for semantic analysis, and also because they discovered that some additional primitives (such as **has** and **says**) are useful.

A system for Abadi and Tuttle is given by a set of runs, where each run describe a possible execution of the protocol. Runs are infinite sequences of global states, and we allow the first time step corresponding to the run to be negative. (Intuitively, the run can start in the past; the global states corresponding to times before time 0 refer to messages exchanged before the current protocol interaction, which starts at time 0.) A global state is a tuple $(s_e, s_1, \ldots, s_n)$, where s_e is the local state of the environment, and s_i is the local state of agent i. The local state of each agent holds a set of keys initially known to the agent, as well the sequence of events (messages received and sent) performed by the agent.

A *point* of a system is a pair (r, k) of run r and time k; this is the global state in run r at time k.

The truth of a formula in a system is given by a relation $(r, k) \models X$, saying that formula X is true at point (r, k) of the system. The definition is by induction on the structure of formulas.

- $(r, k) \models P$ **sees** X iff for some message M, message M was received by agent P by time k in run r, and $\{M\} \cup \mathcal{K}_i \vdash X$, where $\mathcal{K}_i$ is the set of keys initially known to agent i.
- $(r, k) \models P$ **said** X iff for some message M, P sends message M at some time $k' \leq k$, and X is a message that the agent can construct from the messages that he has received (see definition in the paper). The semantics for P **says** X is similar, except we require that the message sent was sent at time $k' \geq 0$.
- $(r, k) \models P$ **controls** X iff for all $k' \geq 0$, $(r, k') \models P$ **says** X implies $(r, k') \models X$.
- $(r, k) \models$ **fresh**(X) iff X does not appear in any message exchanged up to time 0 in run r.
- $(r, k) \models P \overset{K}{\leftrightarrow} Q$ iff, intuitively, only P or Q ever send messages encrypted with key k (see paper for formal definition).

- $(r, k) \models P$ **believes** X iff for every point (r', k') that agent i cannot distinguish from (r, k), then $(r', k') \models X$.

The last clause is the central one, as far as BAN is concerned, since BAN is really a logic about the belief of agents in a cryptographic setting. We say agent i cannot distinguish points (r, k) and (r', k') is i can see the same things at both points. We assume that the only things that the agent can see is what is in his local state, so (r, k) and (r', k') are indistinguishable to agent i if the local state of i in (r, k) and the local state of i in (r', k') are the same, *after ensuring that all messages encrypted with keys unknown to agent i are replaced by some arbitrary but fixed symbol.* (This last bit is to ensure that the agents cannot distinguish states based on messages that they cannot decrypt.)

There are additional details to get right before having a suitable semantics for BAN, and that is to ensure that the system satisfies (i.e., makes true) the initial assumptions of the BAN analysis. I will point to the paper for the details of how to do this.