Notes on Formal Methods (Logics)

Lecturer: Jeannette Wing
Scribe: Derek R. Dreyer

October 15, 1997

1 Jeannette Wing's View of the Security World

At the bottom of the security world (though not at all the least important) are the number theorists and crypto researchers who provide us with all the actual cryptography and cryptanalysis, the algorithms on which anything and everything in the security world depends. Above them sit the cryptographic protocol designers, who develop protocols based on intuition, an intuition formed from years and years of experience breaking other people's protocols. But, there is something missing from this dichotomy: namely, a way of looking at protocols formally and systematically in order to gain a logically sound understanding of their properties. And this is where the formal methods researchers come in, encroaching upon the workspace of theorists and hackers alike (or better yet, broadening it), in an attempt to reason about the behavior of protocols and their susceptibility to attacks through techniques from logic, algebra and automata theory.

2 The BAN Logic

A formal logical approach to reasoning about protocols was first set out in 1989 by Burrows, Abadi and Needham in their paper "A Logic of Authentication." In this paper, which was distributed in class and serves as one of the foundational papers in the area of formal methods, a logic is presented, subsequently dubbed the BAN logic, that introduces the concept of belief as a logical construct. For example, if party A *believes* that it shares a secret key K_{ab} with party B, then it should also *believe* that any message it receives encrypted with K_{ab} comes originally from B. The details of the BAN logic are omitted here and we refer you to the paper itself.

3 Strengths and Weaknesses of BAN

The strengths of the BAN logic are rather apparent. It allows us to analyze protocols, to find subtle security holes and redundancies, through systematic application of simple logical rules. In fact, it has discovered protocol flaws previously unknown, as well as several previously exposed by informal methods. However, it is not guaranteed to find all flaws, even in simple protocols like Wide-Mouthed Frog, and it has shown to be secure some protocols that were later determined to be otherwise. One problem is that, in order to submit a protocol for analysis under the BAN logic, one must first perform an "idealization step" in which the messages of the protocol are transformed to BAN logic form, and it is possible for some of the details that might be useful to an intruder to be discarded. This step also allows for human error in the translation. In addition, the BAN logic makes some assumptions about the nature of cryptographic systems that are at best highly optimistic. It assumes that protocols use perfect encryption, that trusted parties are indeed trustworthy, and that there are no failures in the distributed systems sense.

4 BAN Analysis of Otway-Rees

The following is an analysis of the Otway-Rees protocol using the BAN logic. We begin with the idealization step, which produces the following set of messages representing Otway-Rees in BAN form:

- $\mathbf{A} \rightarrow \mathbf{B}:\quad \{N_a, N_c\}_{K_{as}}$
- $\mathbf{B} \rightarrow \mathbf{S}:\quad \{N_a, N_c\}_{K_{as}}, \quad \{N_b, N_c\}_{K_{bs}}$
- $\mathbf{S} \rightarrow \mathbf{B}:\quad \{N_a, (A \overset{K_{ab}}{\longleftrightarrow} B), (B \mid\!\sim N_c)\}_{K_{as}},$
  $\{N_b, (A \overset{K_{ab}}{\longleftrightarrow} B), (A \mid\!\sim N_c)\}_{K_{bs}}$
- $\mathbf{B} \rightarrow \mathbf{A}:\quad \{N_a, (A \overset{K_{ab}}{\longleftrightarrow} B), (B \mid\!\sim N_c)\}_{K_{as}}$

One thing to note about the idealization is that all the unencrypted parts of messages were discarded because the BAN logic insists that no party can *believe* things about statements that could have been forged.

The authentication goals are then for A to believe that K_{ab} is the key it shares with B and vice versa, written formally as $A \models A \overset{K_{ab}}{\longleftrightarrow} B$ and $B \models A \overset{K_{ab}}{\longleftrightarrow} B$. We may also want to have A and B believe something about what each other believes, but we will see what the analysis produces (see Appendix for summary of notation).

Assumptions:

`(* A and B believe their keys with S are secret *)`

$A \models A \stackrel{K_{as}}{\longleftrightarrow} S \quad B \models B \stackrel{K_{bs}}{\longleftrightarrow} S$

`(* as does S, which also knows` K_{ab} `*)`

$S \models A \stackrel{K_{as}}{\longleftrightarrow} S \quad S \models B \stackrel{K_{bs}}{\longleftrightarrow} S$

$S \models A \stackrel{K_{ab}}{\longleftrightarrow} B$

`(* A and B trust S *)`

$A \models (S \Rightarrow A \stackrel{K}{\longleftrightarrow} B) \quad B \models (S \Rightarrow A \stackrel{K}{\longleftrightarrow} B)$

$A \models (S \Rightarrow B \mid\sim X) \quad B \models (S \Rightarrow B \mid\sim X)$

`(* A and B believe their nonces are fresh *)`

$A \models \#(N_a) \quad B \models \#(N_b)$

$A \models \#(N_c)$

$\mathbf{A} \rightarrow \mathbf{B}: \quad \{N_a, N_c\}_{K_{as}}$

$B \triangleleft \{N_a, N_c\}_{K_{as}}$

$\mathbf{B} \rightarrow \mathbf{S}: \quad \{N_a, N_c\}_{K_{as}}, \quad \{N_b, N_c\}_{K_{bs}}$

$S \triangleleft \{N_a, N_c\}_{K_{as}}, \quad \{N_b, N_c\}_{K_{bs}}$

$S \triangleleft \{N_a, N_c\}_{K_{as}} \quad S \triangleleft \{N_b, N_c\}_{K_{bs}}$

`(* Since` $S \models A \stackrel{K_{as}}{\longleftrightarrow} S$`, message-meaning rule gives us *)`

$S \models A \mid\sim (N_a, N_c)$

`(* and since` $S \models B \stackrel{K_{bs}}{\longleftrightarrow} S$`, the same rule gives us *)`

$S \models B \mid\sim (N_b, N_c)$

$\mathbf{S} \rightarrow \mathbf{B}: \quad \{N_a, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (B \mid\sim N_c)\}_{K_{as}},$
$\quad \{N_b, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (A \mid\sim N_c)\}_{K_{bs}}$

$B \triangleleft \{N_a, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (B \mid\sim N_c)\}_{K_{as}}$

$B \triangleleft \{N_b, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (A \mid\sim N_c)\}_{K_{bs}}$

`(* Since` $S \models B \stackrel{K_{bs}}{\longleftrightarrow} S$`, we have by message-meaning *)`

$B \models S \mid\sim (N_b, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (A \mid\sim N_c))$

`(* and since` $B \models \#(N_b)$`, nonce-verification gives *)`

$B \models S \models (N_b, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (A \mid\sim N_c))$

`(* Then, B opens up the message ... *)`

$B \models S \models N_b$

$B \models S \models A \stackrel{K_{ab}}{\longleftrightarrow} B$

$B \mid\equiv S \mid\equiv A \mid\sim N_c$

(* Since $B \mid\equiv S \mid\Rightarrow A \stackrel{K}{\longleftrightarrow} B$, jurisdiction gives *)

$\boxed{B \mid\equiv A \stackrel{K_{ab}}{\longleftrightarrow} B}$

(* and since $B \mid\equiv S \mid\Rightarrow A \mid\sim X$, jurisdiction gives *)

$\boxed{B \mid\equiv A \mid\sim N_c}$

$\mathbf{B} \rightarrow \mathbf{A}:\quad \{N_a, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (B \mid\sim N_c)\}_{K_{as}}$

$A \triangleleft \{N_a, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (B \mid\sim N_c)\}_{K_{as}}$

(* Since $A \mid\equiv A \stackrel{K_{as}}{\longleftrightarrow} S$, message-meaning gives *)

$A \mid\equiv S \mid\sim (N_a, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (B \mid\sim N_c))$

(* and since $A \mid\equiv \#(N_a)$, nonce-verification gives *)

$A \mid\equiv S \mid\equiv (N_a, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (B \mid\sim N_c))$

$A \mid\equiv S \mid\equiv N_a$

$A \mid\equiv S \mid\equiv A \stackrel{K_{ab}}{\longleftrightarrow} B$

$A \mid\equiv S \mid\equiv B \mid\sim N_c$

(* $A \mid\equiv S \mid\Rightarrow A \stackrel{K}{\longleftrightarrow} B$, so jurisdiction gives *)

$\boxed{A \mid\equiv A \stackrel{K_{ab}}{\longleftrightarrow} B}$

(* $A \mid\equiv S \mid\Rightarrow B \mid\sim X$, so jurisdiction gives *)

$A \mid\equiv B \mid\sim N_c$

(* and since $A \mid\equiv \#(N_c)$, nonce-verification gives *)

$\boxed{A \mid\equiv B \mid\equiv N_c}$

5 What We Learn From the Analysis

By doing BAN analyses such as the one above, one may discover flaws and/or redundancies in protocols. In the case of Otway-Rees, careful inspection of the analysis will reveal several things:

1. In the end, since K_{ab} is never actually used as an encryption key, neither A nor B can have any belief about whether the other believes it is the secret key they share.

2. One redundancy: there is no need for N_a, we can just use N_c.

3. Another redundancy: N_b need not be encrypted in the second message.

That eliminating the redundancies will not affect what we were able to prove about Otway-Rees is shown in the following analysis.

6 Trimming Otway-Rees

The idealized version of Otway-Rees with the elimination of the above-mentioned redundancies is as follows:

- $\mathbf{A} \to \mathbf{B}: \quad \{N_c\}_{K_{as}}$
- $\mathbf{B} \to \mathbf{S}: \quad \{N_c\}_{K_{as}}, \quad \{N_c\}_{K_{bs}}$
- $\mathbf{S} \to \mathbf{B}: \quad \{N_c, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (B \mid\!\sim N_c)\}_{K_{as}},$
  $\{N_b, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (A \mid\!\sim N_c)\}_{K_{bs}}$
- $\mathbf{B} \to \mathbf{A}: \quad \{N_c, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (B \mid\!\sim N_c)\}_{K_{as}}$

Then, the analysis, with the same assumptions as before, works out similarly:

$\mathbf{A} \to \mathbf{B}: \quad \{N_c\}_{K_{as}}$

$B \triangleleft \{N_c\}_{K_{as}}$

$\mathbf{B} \to \mathbf{S}: \quad \{N_c\}_{K_{as}}, \quad \{N_c\}_{K_{bs}}$

$S \triangleleft \{N_c\}_{K_{as}}, \quad \{N_c\}_{K_{bs}}$
$S \triangleleft \{N_c\}_{K_{as}} \quad S \triangleleft \{N_c\}_{K_{bs}}$
`(* Since` $S \mid\equiv A \stackrel{K_{as}}{\longleftrightarrow} S$`, message-meaning rule gives us *)`
$S \mid\equiv A \mid\!\sim N_c$
`(* and since` $S \mid\equiv B \stackrel{K_{bs}}{\longleftrightarrow} S$`, the same rule gives us *)`
$S \mid\equiv B \mid\!\sim N_c$

$\mathbf{S} \to \mathbf{B}: \quad \{N_c, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (B \mid\!\sim N_c)\}_{K_{as}},$
$\{N_b, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (A \mid\!\sim N_c)\}_{K_{bs}}$

`(* the analysis follows as before to get` B`'s belief *)`

$\mathbf{B} \to \mathbf{A}: \quad \{N_c, (A \stackrel{K_{ab}}{\longleftrightarrow} B), (B \mid\!\sim N_c)\}_{K_{as}}$

`(* the analysis follows as before to get` A`'s belief *)`

7 Appendix: Notation

The BAN paper itself does not use the symbols I have used here, but rather uses the words these symbols represent. The following is a summary of how to translate my (and Jeannette's) symbols:

$$
\begin{array}{rcl}
P \mid\equiv X & \equiv & P \texttt{ believes } X \\
P \lhd X & \equiv & P \texttt{ sees } X \\
P \mid\sim X & \equiv & P \texttt{ said } X \\
P \mid\Rightarrow X & \equiv & P \texttt{ controls } X \\
\#(X) & \equiv & \texttt{fresh}(X) \\
P \stackrel{K}{\longleftrightarrow} Q & \equiv & P \text{ and } Q \text{ share key } K
\end{array}
$$