BAN Logic
A Logic of Authentication

Sape J. Mullender

Huygens Systems Research Laboratory
Universiteit Twente
Enschede

BAN Logic

The BAN logic was named after its inventors, Mike Burrows, Martín Abadí, and Roger Needham.

The logic is, as they stated, a *logic of belief and action*. It contains no logical inversions; therefore it cannot be used to prove a protocol flawed.

But when proof that a protocol is correct cannot be obtained, that protocol deserves to be treated with grave suspicion.

Notation

The logic reasons about beliefs. If Alice believes a proposition P, we write $A \mid\equiv\ P$ and say 'A *believes* P'.

Alice believes that K_{AT} is a good key for communicating with Trent. This is expressed as $A \mid\equiv\ A \overset{K_{AT}}{\longleftrightarrow} T$; we say A *believes* K_{AT} *is a good key for* A *and* T.

Trent acts as *authentication server* or *certification authority* in many of the protocols analyzed by BAN logic. If Alice believes that Trent can be trusted to create a 'good key' for communication with Bob, we write $A \mid\equiv\ T \Rightarrow A \overset{K}{\longleftrightarrow} B$; we say '$A$ *believes* T *has jurisdiction over* or *speaks for* *good keys for* A *and* B'.

Messages

When Alice receives a message (which, in our logic, always contains a proposition), we write $A \triangleleft P$ and say A *sees* P.

Seeing is not believing unless you know who said it. Note that, in this logic, nobody says anything he or she does not believe. If Alice sent a message containing the statement P, we may write $A \mid\!\sim P$ and say A *once said* P.

But, Alice may have said it so long ago that we can no longer trust the contents of her message. We need to know that Alice's statement is *fresh*. When a statement P is fresh we write $\#(P)$ and say P *is fresh*.

Notation Summary

$P \mid\equiv X$	P *believes* X
$P \triangleleft X$	P *sees* X
$P \mid\sim X$	P *once said* X
$\#(P)$	P is *fresh*
$P \Rightarrow X$	P has *jurisdiction over* X
$P \overset{K}{\longleftrightarrow} Q$	K is a *good key* for communicating between P and Q
$\overset{K}{\mapsto} P$	P has K as a *public key*
$P \overset{X}{\rightleftharpoons} Q$	X is a *secret* known only to P and Q
$\langle X\rangle_Y$	X *combined with* (secret) Y

Axioms

We adopt the notation in the BAN papers: $\frac{P}{Q}$ means *if* P *is true then* Q *is true*.

We assume that participants in protocols are good logicians: if Alice believes a proposition X and $\frac{X}{Y}$, then she believes Y too. This is true for the axioms also.

Message meaning rules

$$\frac{P \mid\equiv P \overset{K}{\longleftrightarrow} Q, P \triangleleft \{X\}_K}{P \mid\equiv Q \mid\sim X}$$

$$\frac{P \mid\equiv \overset{K}{\rightarrow} Q, P \triangleleft \{X\}_{K^{-1}}}{P \mid\equiv Q \mid\sim X}$$

$$\frac{P \mid\equiv P \overset{Y}{\rightleftharpoons} Q, P \triangleleft \langle X \rangle_Y}{P \mid\equiv Q \mid\sim X}$$

Nonce Verification

$$\frac{P \mid\equiv \#(X),\; P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$$

Jurisdiction Rule

$$\frac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$$

More Rules

$$\frac{P \mid\equiv X, P \mid\equiv Y}{P \mid\equiv (X, Y)}$$

$$\frac{P \mid\equiv (X, Y)}{P \mid\equiv X}$$

$$\frac{P \mid\equiv Q \mid\equiv (X, Y)}{P \mid\equiv Q \mid\equiv X}$$

$$\frac{P \mid\equiv Q \mid\sim (X, Y)}{P \mid\equiv Q \mid\sim X}$$

And More

$$\frac{P \lhd (X, Y)}{P \lhd X}$$

$$\frac{P \lhd \langle X \rangle_Y)}{P \lhd X}$$

$$\frac{P \mid\equiv P \stackrel{K}{\longleftrightarrow} Q, P \lhd \{X\}_K}{P \lhd X}$$

And More

$$\frac{P \mid\equiv \stackrel{K}{\rightarrow} P,\ P \lhd \{X\}_K}{P \lhd X}$$

$$\frac{P \mid\equiv \stackrel{K}{\rightarrow} Q,\ P \lhd \{X\}_{K^{-1}}}{P \lhd X}$$

$$\frac{P \mid\equiv \#(X)}{A \mid\equiv \#((X, Y))}$$

Most analyses start with assumptions such as

$$A \mid\equiv A \stackrel{K_{AT}}{\longleftrightarrow} T \qquad B \mid\equiv B \stackrel{K_{BT}}{\longleftrightarrow} T$$

$$A \mid\equiv T \Rightarrow A \stackrel{K_{AB}}{\longleftrightarrow} B \qquad B \mid\equiv T \Rightarrow B \stackrel{K_{AB}}{\longleftrightarrow} B$$

$$A \mid\equiv \#(N_A) \qquad B \mid\equiv \#(N_B)$$

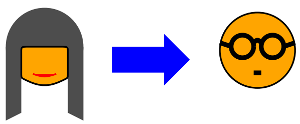
$$T \mid\equiv A \stackrel{K_{AB}}{\longleftrightarrow} B$$

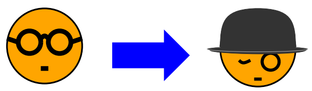
and need to conclude with

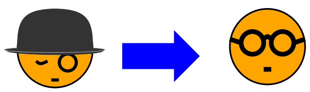
$$A \mid\equiv A \stackrel{K_{AB}}{\longleftrightarrow} B \qquad B \mid\equiv A \stackrel{K_{AB}}{\longleftrightarrow} B$$

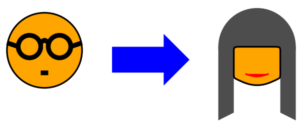
$$A \mid\equiv B \mid\equiv A \stackrel{K_{AB}}{\longleftrightarrow} B \qquad B \mid\equiv A \mid\equiv A \stackrel{K_{AB}}{\longleftrightarrow} B$$

The Ottway-Rees Authentication Protocol

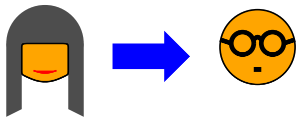
1.  $M, A, B, \{N_A, M, A, B\}_{K_{AT}}$

2.  $M, A, B, \{N_A, M, A, B\}_{K_{AT}}, \{N_B, M, A, B\}_{K_{BT}}$

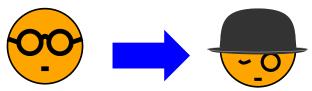
3.  $M, \{N_A, K_{AB}\}_{K_{AT}}, \{N_B, K_{AB}\}_{K_{BT}}$

4.  $M, \{N_A, K_{AB}\}_{K_{AT}}$

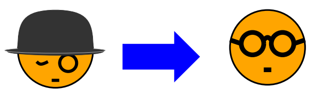
Analysis — The Protocol

1.  $M, A, B, \{N_A, M, A, B\}_{K_{AT}}$

   $\{N_A, N_C\}_{K_{AS}}$

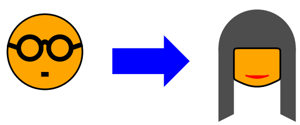
2.  $M, A, B, \{N_A, M, A, B\}_{K_{AT}}, \{N_B, M, A, B\}_{K_{BT}}$

   $\{N_A, N_C\}_{K_{AS}}, \{N_B, N_C\}_{K_{BS}}$

3.  $M, \{N_A, K_{AB}\}_{K_{AT}}, \{N_B, K_{AB}\}_{K_{BT}}$

   $\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B, B \mid\!\sim\ N_C\}_{K_{AT}},$

   $\{N_B, A \overset{K_{AB}}{\longleftrightarrow} B, A \mid\!\sim\ N_C\}_{K_{BT}}$

4.  $M, \{N_A, K_{AB}\}_{K_{AT}}$

   $\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B, B \mid\!\sim\ N_C\}_{K_{AT}}$

Analysis — Assumptions

$$A \mid\equiv A \stackrel{K_{AT}}{\longleftrightarrow} T \qquad B \mid\equiv B \stackrel{K_{BT}}{\longleftrightarrow} T$$

$$T \mid\equiv A \stackrel{K_{AT}}{\longleftrightarrow} T \qquad T \mid\equiv B \stackrel{K_{BT}}{\longleftrightarrow} T$$

$$T \mid\equiv A \stackrel{K_{AB}}{\longleftrightarrow} B$$

$$A \mid\equiv T \Rightarrow A \stackrel{K_{AB}}{\longleftrightarrow} B \qquad B \mid\equiv T \Rightarrow B \stackrel{K_{AB}}{\longleftrightarrow} B$$

$$A \mid\equiv T \Rightarrow B \mid\sim X \qquad B \mid\equiv T \Rightarrow A \mid\sim X$$

$$A \mid\equiv \#(N_A) \qquad B \mid\equiv \#(N_B)$$

$$A \mid\equiv \#(N_C)$$

$$\frac{B \triangleleft \{N_B, A \stackrel{K_{AB}}{\longleftrightarrow} B\}_{K_{BT}}, B \mid\equiv B \stackrel{K_{BT}}{\longleftrightarrow} T}{B \mid\equiv T \mid\sim N_B, A \stackrel{K_{AB}}{\longleftrightarrow} B}$$

$$\frac{B \triangleleft \{N_B, A \stackrel{K_{AB}}{\longleftrightarrow} B\}_{K_{BT}}, B \mid\equiv \#(N_B)}{B \mid\equiv \#(A \stackrel{K_{AB}}{\longleftrightarrow} B)}$$

$$\frac{B \mid\equiv T \mid\sim A \stackrel{K_{AB}}{\longleftrightarrow} B, B \mid\equiv \#(A \stackrel{K_{AB}}{\longleftrightarrow} B)}{B \mid\equiv T \mid\equiv A \stackrel{K_{AB}}{\longleftrightarrow} B}$$

$$\frac{B \mid\equiv T \mid\equiv A \stackrel{K_{AB}}{\longleftrightarrow} B, B \mid\equiv T \Rightarrow A \stackrel{K_{AB}}{\longleftrightarrow} B}{B \mid\equiv A \stackrel{K_{AB}}{\longleftrightarrow} B}$$

Analysis — Conclusion

Similarly, we derive $A \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B$.

We can also derive

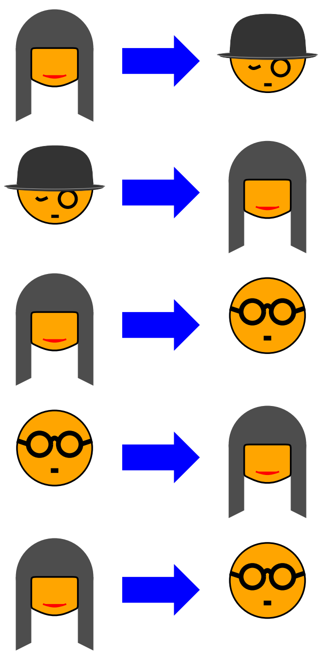
$$A \mid\equiv B \mid\equiv N_C,$$

but we can only prove

$$B \mid\equiv A \mid\sim N_C.$$

N_A is not needed, N_C can be used instead.

the Needham-Schroeder Protocol



1. A, B, N_A

2. $\{N_A, B, K_{AB}, \{A, K_{AB}\}_{K_{BT}}\}_{K_{AT}}$

3. $\{A, K_{AB}\}_{K_{BT}}$

4. $\{N_B\}_{K_{AB}}$

5. $\{N_B - 1\}_{K_{AB}}$

Needham-Schroeder Analysed

Assumptions:

$$T \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B$$

$$A \mid\equiv A \overset{K_{AT}}{\longleftrightarrow} T \qquad B \mid\equiv B \overset{K_{BT}}{\longleftrightarrow} T$$

$$T \mid\equiv A \overset{K_{AT}}{\longleftrightarrow} T \qquad T \mid\equiv B \overset{K_{BT}}{\longleftrightarrow} T$$

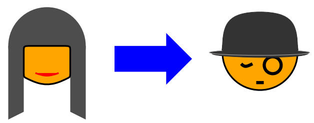
$$A \mid\equiv T \Rightarrow A \overset{K_{AB}}{\longleftrightarrow} B \qquad B \mid\equiv T \Rightarrow B \overset{K_{AB}}{\longleftrightarrow} B$$

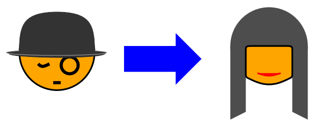
$$A \mid\equiv T \Rightarrow \#(K_{AB})$$

$$A \mid\equiv \#(N_A) \qquad B \mid\equiv \#(N_B)$$

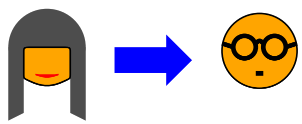
$$T \mid\equiv \#(K_{AB}) \qquad B \mid\equiv \#(A \overset{K}{\longleftrightarrow} B)$$

Messages

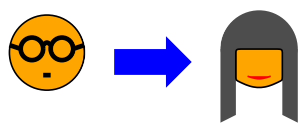
1.  A, B, N_A

2.  $\{N_A, B, K_{AB}, \{A, K_{AB}\}_{K_{BT}}\}_{K_{AT}}$

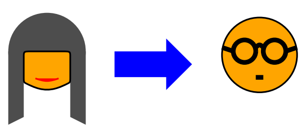
$$\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B,\ \#(A \overset{K_{AB}}{\longleftrightarrow} B)\ , \{A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{BT}}\}_{K_{AT}}$$

3.  $\{A, K_{AB}\}_{K_{BT}}$

$$\{A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{BT}}$$

4.  $\{N_B\}_{K_{AB}}$

$$\{N_B, A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{AB}} from B$$

5.  $\{N_B - 1\}_{K_{AB}}$

$$\{N_B, A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{AB}} from A$$

Analysis

As in the Ottway-Rees protocol, we have the message for Alice saying $\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B\}_{K_{AT}}$, so we can prove in an identical manner $A \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B$.

But Bob gets no message linking Trent's statement $A \overset{K_{AB}}{\longleftrightarrow} B$ to something he knows to be fresh. We cannot get beyond $B \mid\equiv T \mid\sim A \overset{K_{AB}}{\longleftrightarrow} B$.

Needham-Schroeder Exposed

This exactly puts the finger on the weakness in the Needham-Schroeder protocol: Mallory could record Alice and Bob's key exchange and trick Bob into accepting the key in Message 3 any time he chooses.

Mallory will be thwarted, however, when he cannot respond to Bob's Message 4.

But if he can afford to spend a year of CPU time cracking K_{AB}, he can get Bob to accept *and use* a year-old key.