A Logic of Authentication
by Burrows, Abadi, and Needham

Presented by
Adam Schuchart, Kathryn Watkins, Michael Brotzman, Steve Bono, and Sam Small

Agenda
• The problem
• Some formalism
• The goals of authentication, formalized
• The Needham-Schroeder Protocol
  • with shared keys
  • with asymmetric keys
Introduction

Hi, I am Adam →

← Hi, I am Dr. Masson

Let’s speak privately, use key $K$ →

← {¿Whud up f00?}$^K$

• Pairs of principals seek mutual authentication

• Pairs of principals want to share a secret

• Specifically, principals want assurance of their beliefs

• A variety of authentication protocols have been proposed
How can we be sure these protocols are secure?

The Plan

• We will define a logic of authentication in order to explain protocols step-by-step
• Initial assumptions will be made explicit
• The protocol goal will be clearly defined
In their own words...

“Our goal is not to provide a logic that would explain every authentication method, but rather a logic that would explain most of the central concepts of authentication.”

BAN Logic

• Attempts to validate solutions under the following framework using formal logic:
  • There exists a goal (e.g. authentication) that we want to achieve by using a certain message protocol
  • We are aware of the properties we want and need our protocol to exhibit
• We want to be satisfied that our protocol meets our goals

• We *do not* want to depend on trial by fire for this satisfaction

The BAN logic uses formal methods to answer the following:

• What does our protocol *really* achieve?

• What assumptions does our protocol make?

• Does the protocol use any redundant or unnecessary information?

• Does our protocol needlessly encrypt information?
The BAN logic does not attempt to answer:

- Are our assumptions reasonable?
- Do problems exist in particular implementations of the protocol?
- Do we use an inappropriate crypto-system?

Typically, we present protocols by symbolically denoting which principal sends what to whom.

E.g., $A \rightarrow B : (msg)_{K_{AB}}$
• This style is inconvenient for manipulation in logic

• We must transform our traditional protocol syntax into a logic syntax

• The transformations are will not be perfect, they produce messages of an idealized form

• This is OK if we annotate these new messages with assertions
$K \xrightarrow{\rightarrow} \{X\}_K$

$F \triangleleft X$
$G \sim X$

$\#(X)$
OK, enough hand-holding

Basic Notation

- A, B, and S denote specific principals (think, Alice, Bob, Server)
- $K_{AB}$, $K_{AS}$, $K_{BS}$ denote specific shared keys
- $K_A$, $K_B$, $K_S$ denote specific public keys
- $K_A^{-1}$, $K_B^{-1}$, $K_S^{-1}$ denote specific private keys
More Basic Notation

- $N_A, N_B, N_C$ denote specific statements
- $P, Q, R$ refer to a generic instance of a principal
- $X, Y$ refer to a generic instance of a statement
- $K$ is generic and ranges over encryption keys

Constructs

| $P \equiv X$ | principal $P$ believes statement $X$ |
| $P \triangledown X$ | principal $P$ sees statement $X$ |
| $P \rightrightarrows X$ | principal $P$ said statement $X$ |
| $P \Rightarrow X$ | principal $P$ controls statement $X$ |
| $\#(X)$ | fresh(statement $X$) |
More Constructs

<table>
<thead>
<tr>
<th>$P \leftrightarrow^K Q$</th>
<th>$P$ and $Q$ use the <em>shared</em> key $K$ to communicate</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K \leftrightarrow P$</td>
<td>$P$ has $K$ as a <em>public</em> key</td>
</tr>
<tr>
<td>${X}^K$</td>
<td>Statement $X$ encrypted under key $K$</td>
</tr>
</tbody>
</table>

- If two separate encrypted sections are included in one message, treat them as if they arrived in separate messages.
- A message cannot be understood by a principal who does not know the key.
- The key cannot be deduced from an encrypted message.
- Principals can tell whether or not they have used the correct key after decryption.
- Principals can detect (and ignore) their own messages.
Rules of Inference

- *Message meaning rules* concern the interpretation of messages.
- When using shared keys, we assert:

\[
P \text{ believes } Q \leftrightarrow P, \quad P \text{ sees } \{X\}_K \quad \Rightarrow \quad P \text{ believes } Q \text{ said } X
\]

Something of the form:

\[
\begin{align*}
X \\
\hline
Y
\end{align*}
\]

simply means:

if \(X\) is true, then \(Y\) is true
$P$ believes $Q \leftrightarrow^n P$, $P$ sees $\{X\}_K$

$P$ believes $Q$ said $X$

If $P$ believes that the key $K$ is shared with $Q$ and itself
If P believes that the key $K$ is shared with $Q$ and itself

and P sees $X$ encrypted under $K$,

then P believes that $Q$ once said $X$.
\[ P \text{ believes } Q \leftrightarrow K \rightarrow P, \quad P \text{ sees } \{X\}_K \]

\[ P \text{ believes } Q \text{ said } X \]

If P believes that the key K is shared with Q and itself and P sees X encrypted under K, then P believes that Q once said X.

---

For public keys:

\[ P \text{ believes } K \rightarrow Q, \quad P \text{ sees } \{X\}_{K^{-1}} \]

\[ P \text{ believes } Q \text{ said } X \]

If P believes that K is Q’s public key, and P receives a message encoded with Q’s secret key, then P believes Q once said X.
Rules of Inference

- The **nonce-verification** rule shows us how to assert that a message is fresh, and that the sender believes it is fresh.

\[
\begin{align*}
P \text{ believes fresh } (X), & \quad P \text{ believes } Q \text{ said } X \\
\hline
P \text{ believes } Q \text{ believes } X
\end{align*}
\]

If \( P \) believes that \( X \) could have been uttered only recently and that \( Q \) once said \( X \), then \( P \) believes that \( Q \) believes \( X \).

Rules of Inference

- The **jurisdiction** rule states that a principal \( P \) will trust the beliefs that \( Q \) has jurisdiction (or control) over.

\[
\begin{align*}
P \text{ believes } Q \text{ controls } X, & \quad P \text{ believes } Q \text{ believes } X \\
\hline
P \text{ believes } X
\end{align*}
\]
Rules of Inference

- If a principal sees a formula, he also sees its components, given he knows the necessary keys.

\[
\frac{P \text{ sees } (X, Y)}{P \text{ sees } X}, \quad \frac{P \text{ believes } Q \leftrightarrow P, P \text{ sees } \{X\}_K}{P \text{ sees } X},
\]

\[
\frac{P \text{ believes } K \rightarrow P, P \text{ sees } \{X\}_K}{P \text{ sees } X}, \quad \frac{P \text{ believes } K \rightarrow Q, P \text{ sees } \{X\}_{K-1}}{P \text{ sees } X}.
\]

Note that if P sees X and P sees Y, it does NOT follow that P sees (X, Y) since X and Y were not uttered at the same time.

Rules of Inference

- If one part of the formula is fresh, then the entire formula must be fresh:

\[
\frac{P \text{ believes } \text{fresh}(X)}{P \text{ believes } \text{fresh}((X, Y))}.
\]
Given the previous inference rules, we can construct proofs in the logic.

Protocol Analysis in the BAN Logic

- Create an idealized form of the protocol
- Assumptions about the initial state are written
- Logical formulas are attached to the statements of the protocol
- Logical postulates (inference rules) are applied to the assumptions and assertions
The Goals of Authentication, Formalized

A believes $A \leftrightarrow B$

B believes $A \leftrightarrow B$
\( A \) believes \( B \) believes \( A \overset{K}{\leftrightarrow} B \)

\( B \) believes \( A \) believes \( A \overset{K}{\leftrightarrow} B \)

\( A \) believes \( B \) believes \( X \)

or

\( A \) believes \( \overset{K}{\rightarrow} B \)
Needham-Schroeder Protocol (w/ shared keys)

Goals

- A believes $A \leftrightarrow B$
- B believes $A \leftrightarrow B$
- A believes $\text{fresh}(A \leftrightarrow B)$
- B believes $\text{fresh}(A \leftrightarrow B)$
- A believes B believes $A \leftrightarrow B$
- B believes A believes $A \leftrightarrow B$

Diagram:

![Diagram of the Needham-Schroeder Protocol]
Weeks Later, Mallory has discovered key $K_{AB}$. Mallory can then impersonate Alice to Bob.

Assumptions

$A$ believes $A \xleftrightarrow{K_{ab}} S$

$B$ believes $B \xleftrightarrow{K_{bs}} S$

$S$ believes $A \xleftrightarrow{K_{as}} S$

$S$ believes $B \xleftrightarrow{K_{bs}} S$

$S$ believes $A \xleftrightarrow{K_{ab}} B$
A believes $S$ controls $A \overset{K_{ab}}{\leftrightarrow} B$

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

$A$ believes $S$ controls fresh($A \overset{K_{ab}}{\leftrightarrow} B$)

$A$ believes fresh($N_a$) $B$ believes fresh($N_b$)

$S$ believes fresh($A \overset{K_{ab}}{\leftrightarrow} B$) $B$ believes fresh($A \overset{K_{ab}}{\leftrightarrow} B$)
Message 2

A sees \( \{N_a, A \xleftarrow{K_{ab}} B, \text{ fresh}(A \xleftarrow{K_{ab}} B), \{A \xleftarrow{K_{ab}} B\}_K_{bs}\}_K_{as} \)

\[\begin{align*}
A &\text{ believes fresh}(N_a) \\
&\text{ A believes fresh}(N_a, A \xleftarrow{K_{ab}} B, \text{ fresh}(A \xleftarrow{K_{ab}} B))
\end{align*}\]

By the *nonce-verification* rule:

\[\begin{align*}
A &\text{ believes fresh}(A \xleftarrow{K_{ab}} B), \quad A \text{ believes S said } A \xleftarrow{K_{ab}} B \\
&\text{ A believes S believes } A \xleftarrow{K_{ab}} B
\end{align*}\]

By the *jurisdiction* rule:

\[\begin{align*}
A &\text{ believes S controls } A \xleftarrow{K_{ab}} B, \quad A \text{ believes S believes } A \xleftarrow{K_{ab}} B \\
&\text{ A believes } A \xleftarrow{K_{ab}} B
\end{align*}\]
Message 3

\[ B \text{ sees } \{A \leftrightarrow B\}_{K_{bs}} \]

By decrypting the message: \( B \) believes \( S \) once said \( A \leftrightarrow B \)

But is \( A \leftrightarrow B \) fresh?

Let’s just ASSUME \( B \) believes fresh(\( A \leftrightarrow B \)) (so says the paper)

\[
\begin{align*}
\text{B believes fresh(} A \leftrightarrow B \text{),} & \quad \text{B believes S said } A \leftrightarrow B \\
\text{B believes S believes } A \leftrightarrow B \\
\text{B believes S controls } A \leftrightarrow B , & \quad \text{B believes S believes } A \leftrightarrow B \\
& \quad \text{B believes } A \leftrightarrow B
\end{align*}
\]

Message 4

\[ A \text{ sees } \{N_b, A \leftrightarrow B\}_{K_{ab}} \]

\[
\begin{align*}
\text{A believes fresh(} A \leftrightarrow B \text{),} & \quad \text{A believes B said } A \leftrightarrow B \\
\text{A believes B believes } A \leftrightarrow B
\end{align*}
\]

Message 5

\[ B \text{ sees } \{N_b, A \leftrightarrow B\}_{K_{ab}} \]

\[
\begin{align*}
\text{B believes fresh(} N_b \text{),} & \quad \text{B believes A said } (N_b, A \leftrightarrow B) \\
\text{B believes A believes } A \leftrightarrow B
\end{align*}
\]
Finally

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

$A$ believes $\text{fresh}(A \overset{K_{ab}}{\leftrightarrow} B)$
$B$ believes $\text{fresh}(A \overset{K_{ab}}{\leftrightarrow} B)$

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

Next Week...