

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:

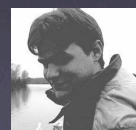
- Are our assumptions reasonable?
- Do problems exist in particular implementations of the protocol?
- Do we use an inappropriate crypto-system?

BAN Logic Formalism

- Typically, we present protocols by symbolically denoting which principal sends what to whom
- E.g., $A \rightarrow B : (msg)_{K_{AB}}$



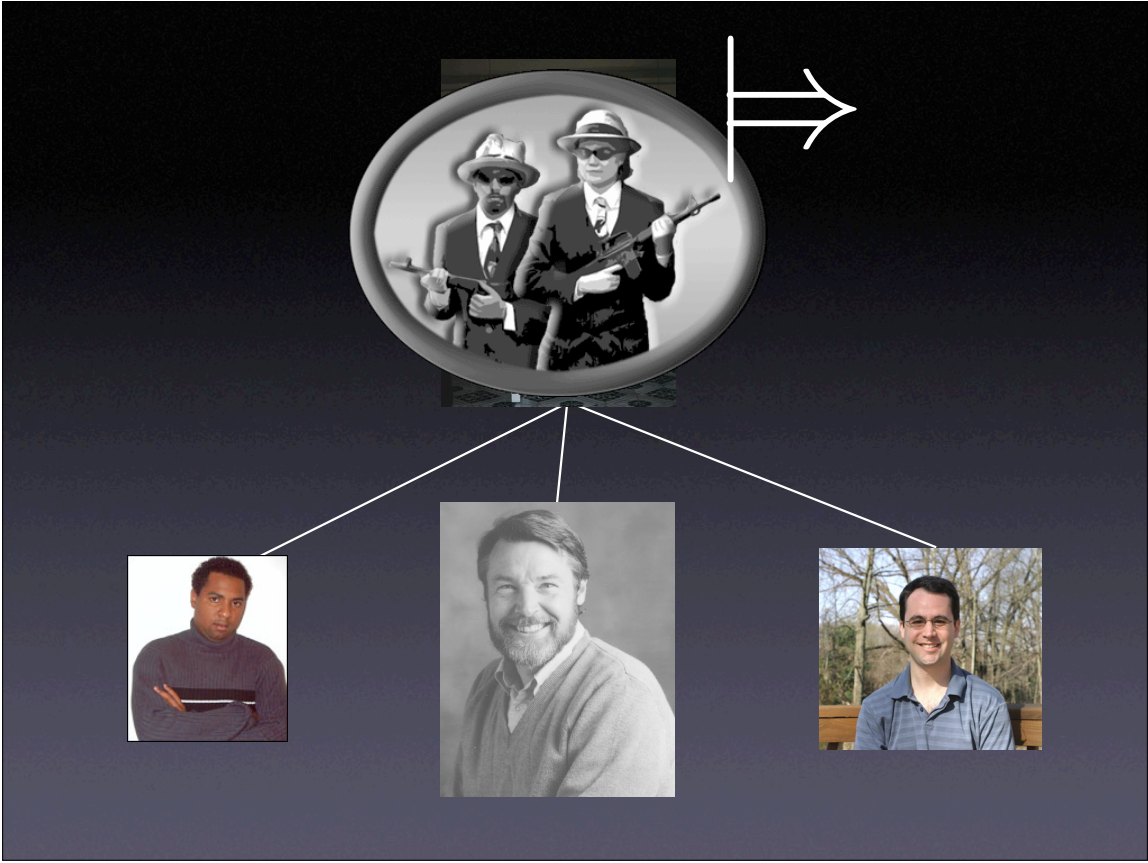
{“you got served”}_K

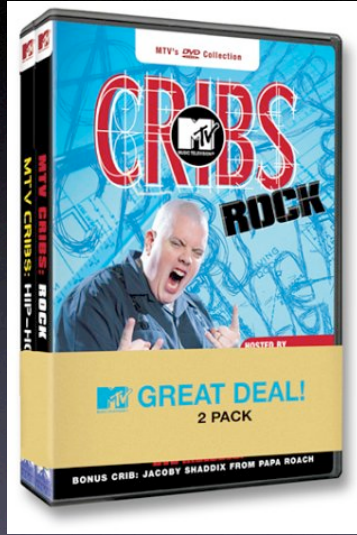


- This style is inconvenient for manipulation in logic
- We must transform our traditional protocol syntax into a logic syntax
 - The transformations are *will not be perfect*, they produce messages of an *idealized form*
 - This is OK if we annotate these new messages with *assertions*

The Heist







$\{X\}_K$

K
→



Carnegie Mellon



$F \triangleleft X$





$G \sim X$

$\#(X)$



Carnegie Mellon



~~CNN.com~~

Avi

~~FOX NEWS channel~~

~~Avi Jr.~~ Adam



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

$P \models X$	principal P <i>believes</i> statement X
$P \triangleleft X$	principal P <i>sees</i> statement X
$P \sim X$	principal P <i>said</i> statement X
$P \models\Rightarrow X$	principal P <i>controls</i> statement X
$\#(X)$	<i>fresh</i> (statement X)

More Constructs

$P \stackrel{K}{\leftrightarrow} Q$	P and Q use the <i>shared key</i> K to communicate
$K \stackrel{\vdash}{\rightarrow} P$	P has K as a <i>public key</i>
$\{X\}_K$	Statement X encrypted under key K

- 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:

$$\frac{P \text{ believes } Q \stackrel{K}{\leftrightarrow} P, \quad P \text{ sees } \{X\}_K}{P \text{ believes } Q \text{ said } X} \quad ?!?$$

Something of the form:

$$\frac{X}{Y}$$

simply means:
if X is true, then Y is true

$$\frac{P \text{ believes } Q \stackrel{K}{\leftrightarrow} P, \quad P \text{ sees } \{X\}_K}{P \text{ believes } Q \text{ said } X}$$
$$\frac{P \text{ believes } Q \stackrel{K}{\leftrightarrow} P,}{\phantom{P \text{ believes } Q \text{ said } X}}$$

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

P sees $\{X\}_K$

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

P believes Q 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

$$\frac{P \text{ believes } Q \stackrel{K}{\leftrightarrow} P, \quad P \text{ sees } \{X\}_K}{P \text{ believes } Q \text{ said } X}$$

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:

$$\frac{P \text{ believes } \stackrel{K}{\mapsto} Q, P \text{ sees } \{X\}_{K^{-1}}}{P \text{ believes } Q \text{ said } X}$$

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

$$\frac{P \text{ believes fresh } (X), P \text{ believes } Q \text{ said } X}{P \text{ believes } Q \text{ believes } X}$$

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

$$\frac{P \text{ believes } Q \text{ controls } X, P \text{ believes } Q \text{ believes } X}{P \text{ believes } X}$$

Rules of Inference

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

$$\frac{P \text{ sees } (X, Y)}{P \text{ sees } X}, \frac{P \text{ believes } Q \stackrel{K}{\leftrightarrow} P, P \text{ sees } \{X\}_K}{P \text{ sees } X},$$

$$\frac{P \text{ believes } \stackrel{K}{\mapsto} P, P \text{ sees } \{X\}_K}{P \text{ sees } X}, \frac{P \text{ believes } \stackrel{K}{\mapsto} Q, P \text{ sees } \{X\}_{K-1}}{P \text{ sees } X}.$$

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:

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

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 $A \stackrel{K}{\leftrightarrow} B$
 B believes $A \stackrel{K}{\leftrightarrow} B$

A believes B believes $A \stackrel{K}{\leftrightarrow} B$
 B believes A believes $A \stackrel{K}{\leftrightarrow} B$

A believes B believes X
or
 A believes $\stackrel{K}{\mapsto} B$

Needham-Schroeder Protocol (w/ shared keys)

Goals

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

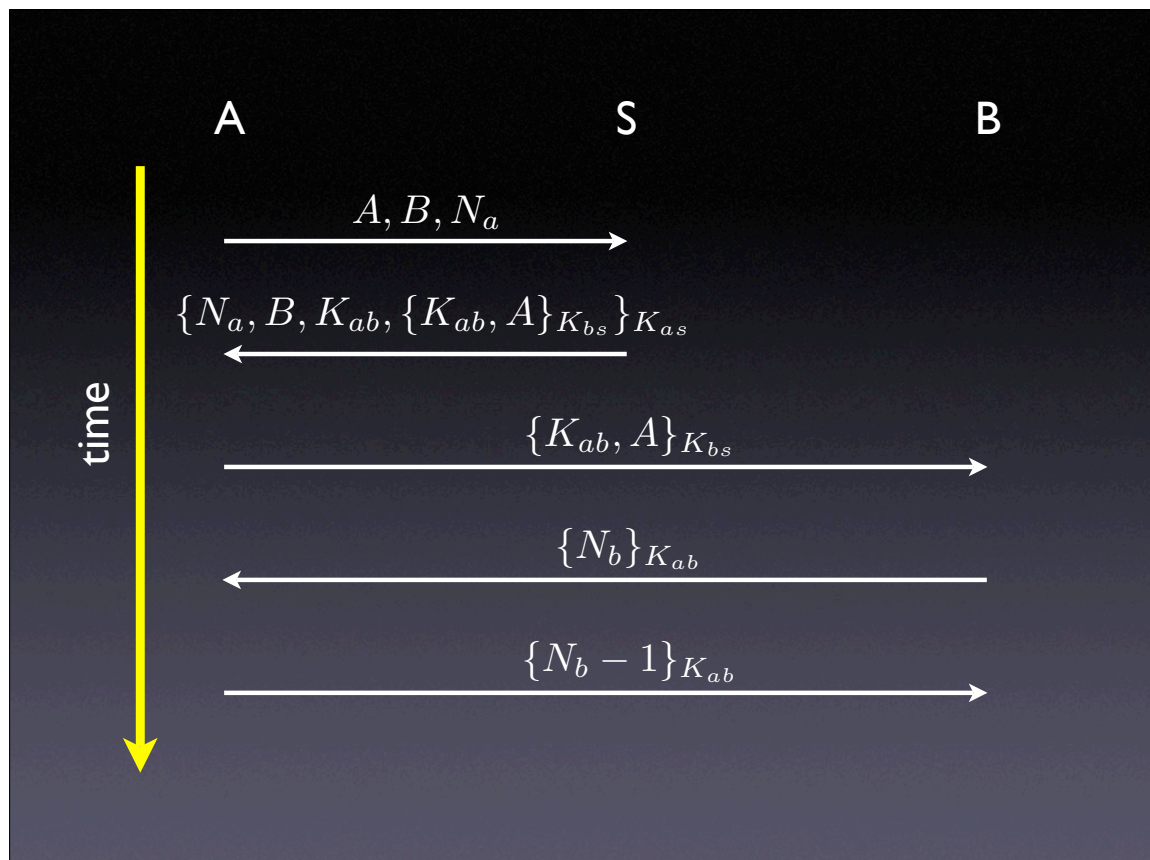
B believes $A \stackrel{K_{ab}}{\leftrightarrow} B$,

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

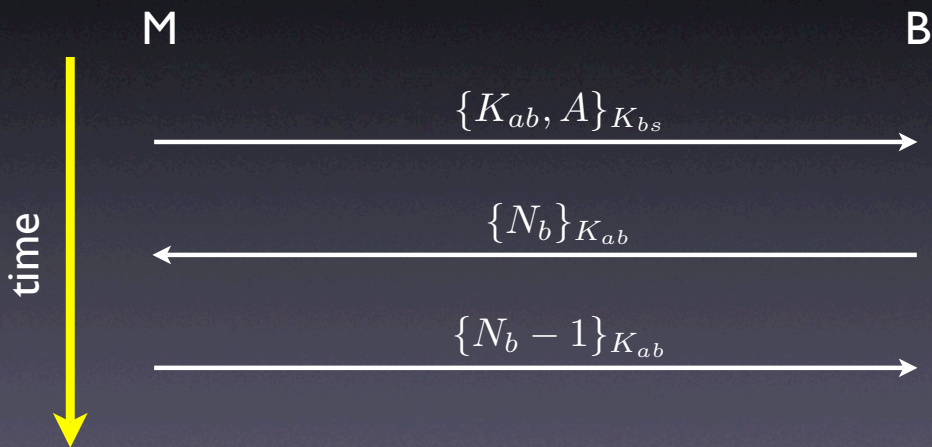
B believes $\text{fresh}(A \stackrel{K_{ab}}{\leftrightarrow} B)$,

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

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



Weeks Later, Mallory has discovered key K_{AB} .
Mallory can then impersonate Alice to Bob.



Assumptions

A believes $A \stackrel{K_{as}}{\leftrightarrow} S$

B believes $B \stackrel{K_{bs}}{\leftrightarrow} S$

S believes $A \stackrel{K_{as}}{\leftrightarrow} S$

S believes $B \stackrel{K_{bs}}{\leftrightarrow} S$

S believes $A \stackrel{K_{ab}}{\leftrightarrow} B$

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

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

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

A believes $\text{fresh}(N_a)$

B believes $\text{fresh}(N_b)$

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

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

Message 3

B sees $\{A \stackrel{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}$

By decrypting the message: B believes S once said $A \stackrel{K_{ab}}{\leftrightarrow} B$

But is $A \stackrel{K_{ab}}{\leftrightarrow} B$ fresh?

Let's just ASSUME B believes $\text{fresh}(A \stackrel{K_{ab}}{\leftrightarrow} B)$ (so says the paper)

B believes $\text{fresh}(A \stackrel{K_{ab}}{\leftrightarrow} B)$, B believes S said $A \stackrel{K_{ab}}{\leftrightarrow} B$

B believes S believes $A \stackrel{K_{ab}}{\leftrightarrow} B$

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

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

Message 4

A sees $\{N_b, A \stackrel{K_{ab}}{\leftrightarrow} B\}_{K_{ab}}$

A believes $\text{fresh}(A \stackrel{K_{ab}}{\leftrightarrow} B)$, A believes B said $A \stackrel{K_{ab}}{\leftrightarrow} B$

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

Message 5

B sees $\{N_b, A \stackrel{K_{ab}}{\leftrightarrow} B\}_{K_{ab}}$

B believes $\text{fresh}(N_b)$, B believes A said $(N_b, A \stackrel{K_{ab}}{\leftrightarrow} B)$

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

Finally

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

B believes $A \stackrel{K_{ab}}{\leftrightarrow} B$,

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

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

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

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

Next Week...