CSE 552
BAN logic

Steve Gribble
Department of Computer Science & Engineering
University of Washington

Why BAN logic?

Authentication protocols seem simple, but are very subtle

- long history of busted protocols littering the side of the road
- until this paper, there was no good systematic way for evaluating the correctness of a protocol

BAN constructs

P **believes** X

P **sees** X

P **said** X

P **controls** X

fresh(X)

$P \overset{K}{\leftrightarrow} Q$

$\overset{K}{\mapsto} P$

$P \overset{X}{\rightleftharpoons} Q$

$\{X\}_K$

$\langle X \rangle_Y$

BAN postulate #1

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

$$\frac{P \textbf{ believes } \overset{K}{\mapsto} Q, \quad P \textbf{ sees } \{X\}_{K^{-1}}}{P \textbf{ believes } Q \textbf{ said } X}$$

$$\frac{P \textbf{ believes } Q \overset{Y}{\rightleftharpoons} P, \quad P \textbf{ sees } \langle X \rangle_Y}{P \textbf{ believes } Q \textbf{ said } X}$$

message-meaning

BAN postulate #2

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

nonce-verification

BAN postulate #3

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

jurisdiction

BAN postulate #4

$$\frac{P \text{ sees } (X, Y)}{P \text{ sees } X}, \quad \frac{P \text{ sees } \langle X \rangle_Y}{P \text{ sees } X}, \quad \frac{P \text{ believes } Q \overset{K}{\leftrightarrow} P,\ P \text{ sees } \{X\}_K}{P \text{ sees } X},$$

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

(components)

BAN postulate #5

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

(freshness)

Kerberos (messages, ideal)

Message 1. $A \rightarrow S: A, B.$

Message 2. $S \rightarrow A: \{T_s, L, K_{ab}, B, \{T_s, L, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}.$

Message 3. $A \rightarrow B: \{T_s, L, K_{ab}, A\}_{K_{bs}}, \{A, T_a\}_{K_{ab}}.$

Message 4. $B \rightarrow A: \{T_a + 1\}_{K_{ab}}.$

Message 2. $S \rightarrow A: \{T_s, A \overset{K_{ab}}{\leftrightarrow} B, \{T_s, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}\}_{K_{as}}.$

Message 3. $A \rightarrow B: \{T_s, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}, \{T_a, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{ab}}$ *from* $A.$

Message 4. $B \rightarrow A: \{T_a, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{ab}}$ *from* $B.$

Kerberos (assumptions)

Message 2. $S \rightarrow A: \{T_s, A \overset{K_{ab}}{\leftrightarrow} B, \{T_s, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}\}_{K_{as}}$.

Message 3. $A \rightarrow B: \{T_s, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}, \{T_a, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{ab}}$ *from* A.

Message 4. $B \rightarrow A: \{T_a, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{ab}}$ *from* B.

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

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

Proof

Message 2. $S \to A$: $\{T_s, A \overset{K_{ab}}{\leftrightarrow} B, \{T_s, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}\}_{K_{as}}$.

A receives Message 2. The annotation rules yield that

$$A \textbf{ sees } \{T_s, (A \overset{K_{ab}}{\leftrightarrow} B), \{T_s, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}\}_{K_{as}}$$

holds afterward. Since we have the hypothesis

$$A \textbf{ believes } A \overset{K_{as}}{\leftrightarrow} S$$

the message-meaning rule for shared keys applies and yields the following:

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

One of our rules to break conjunctions (omitted here) then produces

$$A \textbf{ believes } S \textbf{ said } (T_s, (A \overset{K_{ab}}{\leftrightarrow} B))$$

Proof (continued)

Moreover, we have the following hypothesis:

$$A \textbf{ believes fresh}(T_s)$$

The nonce-verification rule applies and yields

$$A \textbf{ believes } S \textbf{ believes } (T_s, A \overset{K_{ab}}{\leftrightarrow} B)$$

Again, we break a conjunction, to obtain the following:

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

Then, we instantiate K to K_{ab} in the hypothesis

$$A \textbf{ believes } S \textbf{ controls } A \overset{K}{\leftrightarrow} B$$

deriving the more concrete

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

Finally, the jurisdiction rule applies, and yields the following:

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

Proof (continued)

Message 3. $A \rightarrow B$: $\{T_s, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}, \{T_a, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{ab}}$ *from* A.

same proof yields:

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

message meaning and nonce verification yield:

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

Final result

Message 4. $B \rightarrow A$: $\{T_a, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{ab}}$ *from* B.

message meaning and nonce verification yield:

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

So, in the end, our beliefs are:

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

Needham-Schroeder

Two principals A, B that don't know each other wish to communicate securely with each other

- get "introduced" to each other through a mutually trusted server S
- S delivers / verifies public keys to A, B

Needham-Schroeder

Messages

$$\begin{aligned}
&\textit{Message 1.}\ A \rightarrow S: A, B.\\
&\textit{Message 2.}\ S \rightarrow A: \{K_b, B\}_{K_s^{-1}}.\\
&\textit{Message 3.}\ A \rightarrow B: \{N_a, A\}_{K_b}.\\
&\textit{Message 4.}\ B \rightarrow S: B, A.\\
&\textit{Message 5.}\ S \rightarrow B: \{K_a, A\}_{K_s^{-1}}.\\
&\textit{Message 6.}\ B \rightarrow A: \{N_a, N_b\}_{K_a}.\\
&\textit{Message 7.}\ A \rightarrow B: \{N_b\}_{K_b}.
\end{aligned}$$

Idealized protocol

$$\begin{aligned}
&\textit{Message 2.}\ S \rightarrow A: \{\overset{K_b}{\mapsto} B\}_{K_s^{-1}}.\\
&\textit{Message 3.}\ A \rightarrow B: \{N_a\}_{K_b}.\\
&\textit{Message 5.}\ S \rightarrow B: \{\overset{K_a}{\mapsto} A\}_{K_s^{-1}}.\\
&\textit{Message 6.}\ B \rightarrow A: \{\langle A \overset{N_b}{\rightleftharpoons} B \rangle_{N_a}\}_{K_a}.\\
&\textit{Message 7.}\ A \rightarrow B: \{\langle A \overset{N_a}{\rightleftharpoons} B \rangle_{N_b}\}_{K_b}.
\end{aligned}$$

Assumptions

A **believes** $\overset{K_a}{\mapsto} A$

A **believes** $\overset{K_s}{\mapsto} S$

S **believes** $\overset{K_a}{\mapsto} A$

S **believes** $\overset{K_s}{\mapsto} S$

A **believes** (S **controls** $\overset{K}{\mapsto} B$)

A **believes fresh**(N_a)

A **believes** $A \overset{N_a}{\rightleftharpoons} B$

A **believes fresh**$(\overset{K_b}{\mapsto} B)$

B **believes** $\overset{K_b}{\mapsto} B$

B **believes** $\overset{K_s}{\mapsto} S$

S **believes** $\overset{K_b}{\mapsto} B$

B **believes** (S **controls** $\overset{K}{\mapsto} A$)

B **believes fresh**(N_b)

B **believes** $A \overset{N_b}{\rightleftharpoons} B$

B **believes fresh**$(\overset{K_a}{\mapsto} A)$

Conclusions

$$A \textbf{ believes } \overset{K_b}{\mapsto} B \qquad B \textbf{ believes } \overset{K_a}{\mapsto} A$$

$$A \textbf{ believes } B \textbf{ believes } A \overset{N_b}{\rightleftharpoons} B \qquad B \textbf{ believes } A \textbf{ believes } A \overset{N_a}{\rightleftharpoons} B$$

A surprising weakness

If an imposter I can convince A to communicate with I, then I can impersonate A to B

The attack

$$A \rightarrow I : \{N_A, A\}_{K_{PI}}$$

A sends N_A to I, who decrypts the message with K_{SI}

$$I \rightarrow B : \{N_A, A\}_{K_{PB}}$$

I relays the message to B, pretending that A is communicating

$$B \rightarrow I : \{N_A, N_B\}_{K_{PA}}$$

B sends N_B

$$I \rightarrow A : \{N_A, N_B\}_{K_{PA}}$$

I relays it to A

$$A \rightarrow I : \{N_B\}_{K_{PI}}$$

A decrypts N_B and confirms it to I, who learns it

$$I \rightarrow B : \{N_B\}_{K_{PB}}$$

I re-encrypts N_B, and convinces B that he's decrypted it

Why didn't BAN catch this?

A broken assumption:

$$B \text{ believes } A \overset{N_b}{\rightleftharpoons} B$$

- need to modify a message to really achieve this. We replace:

$$B \rightarrow A : \{N_A, N_B\}_{K_{PA}}$$

- with the fixed version:

$$B \rightarrow A : \{N_A, N_B, B\}_{K_{PA}}$$