Logic of Authentication
1. BAN Logic
Ravi Sandhu

Source
These lectures are primarily based on:

Protocol 1 (Needham-Schroeder Shared-Key) [NS78]

Message 1 $A \rightarrow S : A, B, n_A$
Message 2 $S \rightarrow A : \langle n_B, B, k_{AB}, (k_{AB}, A)k_{AS} \rangle k_{AS}$
Message 3 $A \rightarrow B : \langle k_{AB}, A \rangle k_{BS}$
Message 4 $B \rightarrow A : \langle n_B \rangle k_{AB}$
Message 5 $A \rightarrow B : \langle n_B - 1 \rangle k_{AB}$

Nonces are random unpredictable values generated by a principal and included in messages so that she can tell any messages later received and containing her nonce must have been produced after she generated and sent the nonce.

BAN Logic
- BAN is a logic of belief.
- In an analysis, the protocol is first idealized into messages containing assertions, then assumptions are stated, and finally conclusions are inferred based on the assertions in the idealized messages and those assumptions.

The language of BAN
- In all of these expressions, $X$ is either a message or a formula.
- As we will see, every formula can be a message, but not every message is a formula.

The language of BAN
- $P$ believes $X$:
- $P$ received $X$: message; this may require decryption.
- $P$ said $X$:
- $P$ controls $X$:
- $\text{fresh}(X)$: (Read ‘$X$ is fresh’.) $X$ has not been sent in any message prior to current protocol run.
The language of BAN

- \( P \leftrightarrow Q \): (Read 'k is a good key for \( P \) and \( Q \).')
  - \( k \) will never be discovered by any principal but \( P \) or a principal trusted by \( P \) or \( Q \).
- \( PK(P, k) \): (Read 'k is a public key of \( P \).')
  - The secret key, \( k^{-1} \), corresponding to \( k \) will never be discovered by any principal but \( P \) or a principal trusted by \( P \).
- \( [[X]]^k \): Short for \( \{X\}^k \) (from \( P \)). (Read 'X encrypted with \( k \) (from \( P \)').)
  - This is the notation for encryption. Principals can recognize their own messages. Encrypted messages are uniquely readable and verifiable as such by holders of the right keys.

BAN Rules: Message Meaning

\[
P \text{ believes } P \leftrightarrow Q \quad P \text{ received } [X]^k \quad P \text{ believes } Q \text{ said } X
\]

"If \( P \) receives \( X \) encrypted with \( k \) and if \( P \) believes \( k \) is a good key for talking with \( Q \), then \( P \) believes \( Q \) once said \( X \)."

In applying symmetric keys, there is no explicit distinction between signing and encryption.

BAN Rules: Nonce Verification

\[
P \text{ believes } \text{fresh}(X) \quad P \text{ believes } Q \text{ said } X
\]

This rule allows promotion from the past to the present (something said some time in the past to a present belief).

In order to be applied, \( X \) should not contain any encrypted text.

BAN Rules: Jurisdiction

\[
P \text{ believes } Q \text{ controls } X \quad P \text{ believes } Q \text{ believes } X \quad P \text{ believes } X
\]

The jurisdiction rule allows inferences that a principal believes a key is good, even though it is a random string that he has never seen before.

BAN Rules: Message Meaning

\[
P \text{ believes } PK(Q, k) \quad P \text{ received } [X]k^{-1} \quad P \text{ believes } Q \text{ said } X
\]

There is no explicit distinction between signing and encryption. Both are represented by \( [X]^k \) or \( [X]k^{-1} \). The distinction is implicit in the notation for the key used: \( k \) or \( k^{-1} \).

BAN Rules: Belief Conjunction

\[
P \text{ believes } X \quad P \text{ believes } Y \quad P \text{ believes } (X, Y)
\]

The obvious rules apply to beliefs concerning concatenations of messages/conjunctions of formulae.

Concatenations of messages and conjunctions of formulae are both represented as \( (X, Y) \) in the above rules.
BAN Rules: Belief Conjunctatenation

\[
P \text{ believes } Q \text{ believes } (X, Y) \quad P \text{ believes } Q \text{ said } (X, Y) \\
P \text{ believes } Q \text{ believes } X \quad P \text{ believes } Q \text{ said } X
\]

We do not list all of the rules; we give only a representative sampling.

BAN Protocol Analysis

1. Idealize the protocol.
2. Write assumptions about the initial state.
3. Annotate the protocol: For each message transmission \( P \rightarrow Q : M \) in the protocol, assert \( Q \) received \( M \).
4. Use the logic to derive the beliefs held by protocol principals.

BAN Rules: Freshness Conjunctatenation

\[
P \text{ believes fresh}(X) \\
P \text{ believes fresh}(X, Y)
\]

For some inexplicable reason, this is a commonly misunderstood BAN rule. Some try to deny it; others try to assert the converse rule. Be wary of these mistakes.

Protocol 1 (Needham-Schroeder Shared-Key) [NS78]

Message 1 \( A \rightarrow S : A, B, n_A \)
Message 2 \( S \rightarrow A : (n_A, B, k_{AB}, (k_{AB} A) k_{AS}), k_{AS}, A ) \)
Message 3 \( A \rightarrow B : (k_{AB} A) k_{AS} \)
Message 4 \( B \rightarrow A : (n_B) k_{AB} \)
Message 5 \( A \rightarrow B : (n_B - 1) k_{AB} \)

Idealized Needham-Schroeder Shared-Key [BAN89a]

Message 2 \( S \rightarrow A : (n_A, A, k_{AB} B, \text{fresh}(k_{AB}), (4 \oplus^{k_{AB}} B) k_{AS}, k_{AS} \) from \( S \))
Message 3 \( A \rightarrow B : (4 \oplus^{k_{AB}} B) k_{AS} \) from \( S \)
Message 4 \( B \rightarrow A : (n_B, A, k_{AB} B) k_{AS} \) from \( B \)
Message 5 \( A \rightarrow B : (n_B, 4 \oplus^{k_{AB}} B) k_{AS} \) from \( A \)

BAN Rules: Receiving Rules: Seeing is Receiving

\[
P \text{ believes } P \leftrightarrow Q \\
P \text{ received } (X)k \quad P \text{ received } (X, Y) \\
P \text{ received } X \quad P \text{ received } X
\]

A principal receiving a message also receives submessages he can uncover.
1. A believes S said (nA, A ↔kAB B, fresh(kAB)kAS) from S
   By Message Meaning using P1, P8.
2. A believes fresh (nA, A ↔kAB B, fresh(kAB)kAS) from S
   By Freshness Conjunction using 1, P6.
3. A believes S believes (nA, A ↔kAB B, fresh(kAB)kAS) from S
   By Nonce Verification using 2, 1.
4. A believes S believes (A ↔kAB B)
   By Belief Conjunction using 3.
5. A believes S believes (fresh(A ↔kAB B))
   By Belief Conjunction using 3.
6. A believes (A ↔kAB B)
   By Jurisdiction using 4, P3.
7. A believes fresh(A ↔kAB B)
   By Jurisdiction using 4, P5.

We have derived Alice's belief in the goodness and in the freshness of kAB. How about Bob?
NSSK Derivations

8. B believes S said \( A \leftrightarrow k_{AB} B \)
   This gives us Bob’s belief in the goodness of \( k_{AB} \). Unlike Alice, Bob has sent no nonce at this point in the protocol. To get Bob’s belief in freshness we need the following assumption.

P12. B believes fresh\( (A \leftrightarrow k_{AB} B) \) [Dubious]
   This is different than P6, P7 which were based on nonces that the believing principal generates. Here Bob believes that a random value generated by someone else is fresh.

9. B believes S believes \( A \leftrightarrow k_{AB} B \)
   By Nonce Verification using P12, 8.

10. B believes \( A \leftrightarrow k_{AB} B \)
    By Jurisdiction using P4, 9.

11. A believes B said \( (n_B, A \leftrightarrow k_{AB} B) \)
    By Message Meaning using 6, P10.

12. A believes fresh\( (n_B, A \leftrightarrow k_{AB} B) \)
    By Freshness Conjunction using 7.

13. A believes B believes \( (n_B, A \leftrightarrow k_{AB} B) \)
    By Nonce Verification using 12, 11.

14. A believes B believes \( A \leftrightarrow k_{AB} B \)
    By Belief Conjunction using 13.

Similarly we can get A believes B believes \( A \leftrightarrow k_{AB} B \)
By Belief Conjunction using P12, 8.

NSSK Derivations

15. A believes B believes A believes S says \( A \leftrightarrow k_{AB} B \)
    By Belief Conjunction using 13, 14.

16. A believes B believes A
    By Belief Conjunction using 13.

An obviously insecure protocol, yet proved "secure" using BAN
The Nessett Protocol [Nes90]

Idealized Nessett Protocol
Message 1: \( A \rightarrow B : \{ n_A, A \leftrightarrow k_{AB} B \} k_A^{-1} \)
Message 2: \( B \rightarrow A : \{ A \leftrightarrow k_{AB} B \} k_B^{-1} \)

Annotation Premises
P1. B received \( \{ n_A, A \leftrightarrow k_{AB} B \} k_A^{-1} \)
P2. A received \( \{ A \leftrightarrow k_{AB} B \} k_B^{-1} \)

Nessett Protocol Derivations for Bob

1. B believes A said \( \{ n_A, A \leftrightarrow k_{AB} B \} \)
   By Message Meaning using P3, P1.
2. B believes fresh(\( n_A, A \leftrightarrow k_{AB} B \))
   By Freshness Conjunction using P6.
3. B believes A believes fresh(\( n_A, A \leftrightarrow k_{AB} B \))
   By Nonce Verification using P5, 6.
4. B believes A believes A \( \leftrightarrow k_{AB} B \)
   By Belief Conjunction using 3.
5. B believes A \( \leftrightarrow k_{AB} B \)
   By Jurisdiction using P7, 4.

The Nessett Protocol [Nes90]

Initial State Assumptions
P3. B believes PK(\( k_A, A \))
P4. A believes A \( \leftrightarrow k_{AB} B \)
P5. A believes fresh(\( A \leftrightarrow k_{AB} B \))
P6. B believes fresh(\( n_A \))
P7. B believes A controls (\( A \leftrightarrow k_{AB} B \))

Note P6 whereby \( n_A \) is more naturally thought of as a timestamp rather than a nonce

Nessett Protocol Derivations for Alice

6. A believes B said A \( \leftrightarrow k_{AB} B \)
   By Message Meaning using P4, P2.
7. A believes B believes A \( \leftrightarrow k_{AB} B \)
   By Nonce Verification using P5, 5.

These are Alice's second order beliefs in the goodness of \( k_{AB} \)
(her first order belief was assumed.)

Beyond BAN

- GNY90
- AT91
- vO93
- And others
- SvO94, SvO96 unifies these