Logic of Authentication
1. BAN Logic

Ravi Sandhu

Source

These lectures are primarily based on:

- Paul Syverson and Iliano Cervesato, *The Logic of Authentication Protocols*, in R. Focardi, R. Gorrieri (Eds.): Foundations of Security Analysis and Design, Lecture Notes in Computer Science, LNCS 2171, Springer-Verlag 2001.

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

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

Message 2 $S \rightarrow A : \{n_A, B, k_{AB}, \{k_{AB}, A\}k_{BS}\}k_{AS}$

Message 3 $A \rightarrow B : \{k_{AB}, A\}k_{BS}$

Message 4 $B \rightarrow A : \{n_B\}k_{AB}$

Message 5 $A \rightarrow B : \{n_B - 1\}k_{AB}$

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*** :
- ***fresh*(*X*)** : (Read '*X* is fresh'.)

  X has not been sent in any message prior to current protocol run

The language of BAN

- $P \leftrightarrow^k Q$: (Read '*k* is a good key for *P* and *Q*'.)

  k will never be discovered by any principal but *P*, *Q*, or a principal trusted by *P* or *Q*. (The last case is necessary, since the server often sees, indeed generates, *k*.)

- ***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

$$\frac{P \text{ believes } P \leftrightarrow^k Q \qquad P \text{ received } \{X\}k}{P \text{ believes } Q \text{ said } X}$$

"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: Message Meaning

$$\frac{P \text{ believes } PK(Q, k) \qquad P \text{ received } \{X\}k^{-1}}{P \text{ believes } Q \text{ said } X}$$

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: Nonce Verification

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

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

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

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: Belief Conjuncatenation

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

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 Conjuncatenation

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

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

BAN Rules: Freshness Conjuncatenation

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

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.

BAN Rules: Receiving Rules: Seeing is Receiving

$$\frac{P \text{ believes } P \overset{k}{\leftrightarrow} Q \quad P \text{ received } \{X\}k}{P \text{ received } X} \qquad \frac{P \text{ received } (X, Y)}{P \text{ received } X}$$

A principal receiving a message also receives submessages he can uncover.

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.

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

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

Message 2 $S \rightarrow A : \{n_A, B, k_{AB}, \{k_{AB}, A\}k_{BS}\}k_{AS}$

Message 3 $A \rightarrow B : \{k_{AB}, A\}k_{BS}$

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 $S \rightarrow A : \{n_A, A \overset{k_{AB}}{\leftrightarrow} B, fresh(k_{AB}), \{A \overset{k_{AB}}{\leftrightarrow} B\}k_{BS}\}k_{AS}$ *from S*

Message 3 $A \rightarrow B : \{A \overset{k_{AB}}{\leftrightarrow} B\}k_{BS}$ *from S*

Message 4 $B \rightarrow A : \{n_B\ A \overset{k_{AB}}{\leftrightarrow} B\}k_{AB}$ *from B*

Message 5 $A \rightarrow B : \{n_B, A \overset{k_{AB}}{\leftrightarrow} B\}k_{AB}$ *from A*

NSKK Idealization

- First message is omitted
  - Plaintext is omitted
- It is assumed that principals recognize their own messages. Thus, with a shared key, if a recipient can decrypt a message, she can tell who it is from. As this is often implicitly clear, the *from* field is often omitted.
- What is inside the encrypted messages is also altered. Specifically, the key k_{AB} is replaced by assertions about it.
- Also in the last message n_B - 1 is changed to just n_B.

NSSK Initial State Assumptions

P1. ***A believes*** $A \leftrightarrow^{kAS} S$

P2. ***B believes*** $B \leftrightarrow^{kBS} S$

P3. ***A believes S controls*** $A \leftrightarrow^{k} B$

P4. ***B believes S controls*** $A \leftrightarrow^{k} B$

P5. ***A believes S controls fresh***$(A \leftrightarrow^{k} B)$

P6. ***A believes fresh***(n_A)

P7. ***B believes fresh***(n_B)

NSSK Initial State Assumptions

- P1, P2 are beliefs in quality of long-term keys
  - S has similar beliefs but are not relevant
- P3, P4, P5 are jurisdiction beliefs
- P6, P7 are beliefs in freshness of each principal's nonces

NSSK Annotated Protocol

P8. *A received* $\{n_A, A \overset{k_{AB}}{\leftrightarrow} B, fresh(k_{AB}), \{A \overset{k_{AB}}{\leftrightarrow} B\}k_{BS}\}k_{AS}$ *from S*

P9. *B received* $\{A \overset{k_{AB}}{\leftrightarrow} B\}k_{BS}$ *from S*

P10. *A received* $\{n_B, A \overset{k_{AB}}{\leftrightarrow} B\}k_{AB}$ *from B*

P11. *B received* $\{nB, A \overset{k_{AB}}{\leftrightarrow} B\}k_{AB}$ *from A*

Basically read directly from idealized protocol

NSSK Derivations

1. ***A believes S said*** $(n_A, A \leftrightarrow^{kAB} B, fresh(A \leftrightarrow^{kAB} B), \{A \leftrightarrow^{kAB} B\}k_{BS})$

   By Message Meaning using P1, P8.

2. ***A believes fresh***$(n_A, A \leftrightarrow^{kAB} B, fresh(A \leftrightarrow^{kAB} B), \{A \leftrightarrow^{kAB} B\}k_{BS})$

   By Freshness Conjuncatenation using 1, P6.

3. ***A believes S believes*** $(n_A, A \leftrightarrow^{kAB} B, fresh(A \leftrightarrow^{kAB} B), \{A \leftrightarrow^{kAB} B\}k_{BS})$

   By Nonce Verification using 2, 1.

4. ***A believes S believes*** $(A \leftrightarrow^{kAB} B)$

   By Belief Conjuncatenation using 3.

5. ***A believes S believes*** $(fresh(A \leftrightarrow^{kAB} B))$

   By Belief Conjuncatenation using 3.

NSSK Derivations

6. ***A believes*** $(A \leftrightarrow^{kAB} B)$

   By Jurisdiction using 4, P3.

7. ***A believes fresh***$(A \leftrightarrow^{kAB} B)$

   By Jurisdiction using 4, P5.

We have derived Alice's belief in the goodness and in the freshness of k_{AB}.
How about Bob?

NSSK Derivations

8. B believes S said ($A \leftrightarrow^{kAB} B$)

By Message Meaning using P2, P9.

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*($A \leftrightarrow^{kAB} B$) **[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.

NSSK Derivations

9. B believes S believes $A \leftrightarrow^{kAB} B$

By Nonce Verification using P12, 8.

10. B believes $A \leftrightarrow^{kAB} B$

By Jurisdiction using P4, 9.

NSSK Derivations

11. A believes B said (n_B, A $\leftrightarrow^{kAB}$ B)

By Message Meaning using 6, P10.

12. A believes fresh(n_B, A $\leftrightarrow^{kAB}$ B)

By Freshness Conjuncatenation using 7.

13. A believes B believes (n_B, A $\leftrightarrow^{kAB}$ B)

By Nonce Verification using 12, 11.

14. A believes B believes A $\leftrightarrow^{kAB}$ B

By Belief Conjuncatenation using 13.

NSSK Derivations

Similarly we can get A believes B believes A $\leftrightarrow^{kAB}$ B

By Belief Conjuncatenation using 13.

See page 73, need clarification about use of nB

NSSK: Denning-Sacco Attack [DS81]

Message 3 $E_A \rightarrow B : \{k_{AB}, A\}k_{BS}$

Message 4 $B \rightarrow E_A : \{n_B\}k_{AB}$

Message 5 $E_A \rightarrow B : \{n_B - 1\}k_{AB}$

E_A is the attacker masquerading as *A* using an old compromised session key k_{AB} within the lifetime of the long-term key k_{BS}

The attack is not directly uncovered by BAN but BAN analysis shows the desired beliefs of *B* cannot be derived without the dubious assumption P12 *B believes fresh*($A \leftrightarrow^{kAB} B$) that underlies this attack.

The Nessett Protocol [Nes90]

Message 1 $A \rightarrow B : \{n_A, k_{AB}\}k_A^{-1}$

Message 2 $B \rightarrow A : \{n_B\}k_{AB}$

An obviously insecure protocol, yet proved “secure” using BAN

The Nessett Protocol [Nes90]

Idealized Nessett Protocol

Message 1 $A \rightarrow B : \{n_A, A \leftrightarrow^{kAB} B\}k_A^{-1}$

Message 2 $B \rightarrow A : \{A \leftrightarrow^{kAB} B\}_{kAB}$

Annotation Premises

P1. B *received* $\{n_A, A \leftrightarrow^{kAB} B\}k_A^{-1}$

P2. A *received* $\{A \leftrightarrow^{kAB} B\}_{kAB}$

The Nessett Protocol [Nes90]

Initial State Assumptions

P3. B *believes* $PK(k_A, A)$

P4. A *believes* $A \leftrightarrow^{kAB} B$

P5. A *believes* *fresh*$(A \leftrightarrow^{kAB} B)$

P6. B *believes* *fresh*(n_A)

P7. B *believes* A *controls* $(A \leftrightarrow^{kAB} B)$

Note P6 whereby n_a is more naturally thought of as a timestamp rather than a nonce

Nessett Protocol Derivations for Bob

1. ***B believes A said*** $(n_A, A \leftrightarrow^{kAB} B)$

   By Message Meaning using P3, P1.
2. ***B believes fresh***$(n_A, A \leftrightarrow^{kAB} B)$

   By Freshness Conjuncatenation using P6.
3. ***B believes A believes*** $(n_A, A \leftrightarrow^{kAB} B)$

   By Nonce Verification using 2, 1.
4. ***B believes A believes*** $A \leftrightarrow^{kAB} B$

   By Belief Conjuncatenation using 3.
5. ***B believes*** $A \leftrightarrow^{kAB} B$

   By Jurisdiction using P7, 4.

Nessett Protocol Derivations for Alice

6. ***A believes B said*** $A \leftrightarrow^{kAB} B$

   By Message Meaning using P4, P2.
7. ***A believes B believes*** $A \leftrightarrow^{kAB} B$

   By Nonce Verification using P5, 6.

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

The Nesset Protocol

- Nessett traces the source of the "flaw" to the scope of BAN. It addresses who gets and acknowledges a key (authentication), but it does not address who should not get a key (confidentiality).
- Burrows et al. respond to Nessett in [BAN90b] by noting that their paper explicitly limits discussion to authentication of honest principals. They explicitly do not attempt to detect unauthorized release of secrets.
- Alice's action is inconsistent with meaning of *A believes* $A \leftrightarrow^{kAB} B$. What is needed is a way to reflect this mathematically. Suppose we could derive *A believes C has* k_{AB} (for arbitrary *C*). Increasing expressiveness would let us formally demonstrate this.

Beyond BAN

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