

A Logic of Authentication

M. Burrows, M. Abadi, R. Needham

Robert Harper

15–819 Logics and Languages for Security
12 September 2007

Motivation: Protocol Analysis

- Wish to verify correctness of security protocols.
 - e.g., ensure that parties A and B both believe that they share a secret.
- Standard formulation is operational and often ambiguous.
 - Phrased in terms of message exchanges $A \rightarrow B : M$.
 - Items are keys, nonces, principals, possibly encrypted.
- Security protocols are remarkably subtle.
 - It pays to be precise about what is achieved by a given protocol.

Contributions

- A formalism for specifying authentication protocols.
 - Entities include principals (keys), messages, nonces.
 - Based on abstract model of encryption (Dolev-Yao).
 - Assertions involve belief, “seeing”, communication paths.
- Analysis of some well-known authentication protocols.
 - Kerberos.
 - Andrew RPC.
 - Needham-Schroeder.
 - CCITT X.509.
- The first formalism of its kind. [???

Overview of BAN Logic

- A version of many-sorted predicate logic.
 - Limited forms of quantification.
 - Conjunction as only propositional connective.
- Sorts include principals, keys, and propositions. [???
- **[Is it HOL or FOL?]**
- A collection of basic predicates for security.
 - Assertions about belief, attestation, *etc.*
- Identifies propositions with messages. [???
- **[Seems suspicious from a logical viewpoint.]**

Basic Predicates of BAN Logic

- P **believes** X : Principal P believes proposition X .
 - The workhorse of the formalism.
- P **sees** X : Principal P sees the message X .
- P **said** X : Principal P once sent the message X .
 - Implies that P **believes** X .
- P **controls** X : Principal P has jurisdiction over X . [???]
 - [What does it mean to have jurisdiction over a proposition?]
- X **fresh**: The proposition X is “fresh.” [???]
 - [What does it mean for a proposition to be fresh?]

Basic Predicates of BAN Logic

- $P \xleftrightarrow{K} Q$: Principals P and Q communicate via shared key K .
- $\stackrel{K}{\mapsto} P$: Principal P has K as its public key.
 - Corresponding secret key is K^{-1} .
- $P \stackrel{X}{\rightleftharpoons} Q$: Principals P and Q share X as a “secret”.
 - **[What does it mean for a proposition X to be a secret?]**
- $\{X\}_K$: Proposition X encrypted by key K .
 - $\{X\}_K^P$: Proposition X encrypted by key K by principal P .
 - **[What does it mean to specify who encrypted X ?]**
- $\langle X \rangle_Y$: Proposition X with a “secret” Y attached.
 - **[What does this mean?]**

Message Rules

$$\frac{P \text{ believes } Q \xleftrightarrow{K} P \quad P \text{ sees } \{X\}_K^R \quad R \neq P}{P \text{ believes } Q \text{ said } X}$$

- If P and Q share a symmetric key K , then P can decode anything encrypted with K .
- The encrypted message *cannot* be from P itself, otherwise P would attribute its own beliefs to Q !

Message Rules

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

- If P knows Q 's public key, then P can recognize signed messages from Q .
- It would appear that the same restrictions on principals apply here, but they are not explicitly discussed.
- It is not clear to me why P must be distinct from R (if it must).

Message Rules

$$\frac{P \text{ believes } Q \stackrel{Y}{\rightleftharpoons} P \quad P \text{ sees } \langle X \rangle_Y}{P \text{ believes } Q \text{ said } X}$$

- If P believes that P and Q share a secret Y , and P sees a message with Y attached, then the rest of that message can only be from Q .
- Some invariant ensures that the message with Y attached cannot be from P itself, but I don't understand the harm in that.

Nonce Rule

$$\frac{P \text{ believes } X \text{ fresh} \quad P \text{ believes } Q \text{ said } X}{P \text{ believes } Q \text{ believes } X}$$

- If P believes that X is “current” and that Q said X , then P believes that Q believes X .
- Anything Q said, Q must also believe, stated from the point of view of P .
- Requirement of currency seems to import some temporal element into the logic that is not well-developed.
- For some reason X is restricted to be “cleartext”.

Jurisdiction Rule

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

- If P believes that Q has jurisdiction over X and P believes that Q believes X , then P believes X as well.
- That is, P defers to Q 's authority over X .

Vision Rules

$$\frac{P \text{ believes } Q \xleftrightarrow{K} P \quad P \text{ sees } \{X\}_K^R \quad P \neq R}{P \text{ sees } X}$$

- P can “see through” encryption on a shared symmetric key, provided that the encryption was done by a principal other than P itself.

Vision Rules

$$\frac{P \text{ believes } \overset{K}{\mapsto} P \quad P \text{ sees } \{X\}_K^R \quad R \neq P}{P \text{ sees } X}$$

- P knows its own secret key, so it can decrypt messages encrypted with its public key.
- Regardless of who they are from? [???

Vision Rules

$$\frac{P \text{ believes } \stackrel{K}{\mapsto} Q \quad P \text{ sees } \{X\}_{K^{-1}}^R \quad R \neq P}{P \text{ sees } X}$$

- P can decrypt messages signed by Q if P believes that it knows Q 's public key.
- **[Do principals believe only true propositions?]**

Freshness Rules

$$\frac{X \text{ fresh}}{X \wedge Y \text{ fresh}}$$

- Conjunction preserves freshness.
- Stated only for left conjunct; appears to demand closure conditions on assertions about propositions. [???

Restricted Quantification

$$\frac{P \text{ believes } \forall x_1 \dots \forall x_n. Q \text{ controls } X}{P \text{ believes } [a_1, \dots, a_n / x_1, \dots, x_n](Q \text{ controls } X)}$$

- Restricted form of universal elimination.
- **[But surely general principles of substitution are required for the logic to make sense?]**

Verification Method

- Essentially a version of Hoare logic for imperative programs.
 - **[Not clear why imperative model is relevant or even useful.]**
 - Annotate actions of protocol with assertions from BAN logic.
 - Rule of consequence links together steps.
 - Implied accumulation of facts about what has been seen.
- But the protocol itself is represented in *idealized* form.
 - Steps are phrased in terms of BAN logic primitives.
 - Expresses *intent* of a message, rather than *content*.
 - Idealization is *not* a mechanical process!

Generic Annotation Principles

$$\frac{}{\{X\}P \longrightarrow Q : Y \{X \wedge Q \text{ sees } Y\}}$$

- Q sees messages sent to it
- Frame-like rule: “other facts” persist across messages.

Generic Annotation Principles

$$\frac{X \vdash X' \quad \{X'\} S \{Y'\} \quad Y' \vdash Y}{\{X\} S \{Y\}}$$

- Rule of consequence from Hoare logic.
- S is any step of the protocol.

Goals of Verification

- For mutual authentication, the goal is to derive post-condition

$$A \text{ believes } A \xleftrightarrow{K} B \wedge B \text{ believes } A \xleftrightarrow{K} B$$

That is, both parties believe that they share a symmetric key.

- Pre-conditions reflect presumed relationships, such as jurisdiction assumptions.

Conventional Kerberos Protocol

① $A \longrightarrow S : A, B.$

② $S \longrightarrow A : \{ T_s, L, K_{a,b}, B, \{ T_s, L, K_{a,b}, A \}_{K_{b,s}} \}_{K_{a,s}}.$

③ $A \longrightarrow B : \{ T_s, L, K_{a,b}, A \}_{K_{b,s}}, \{ A, T_a \}_{K_{a,b}}.$

④ $B \longrightarrow A : \{ T_a + 1 \}_{K_{a,b}}.$

- Phrased in terms of messages, timestamps, lifetimes, keys.
- Intent is not clear from specification.

Conventional Kerberos Protocol

① $A \longrightarrow S : A, B.$

② $S \longrightarrow A : \{ T_s, L, K_{a,b}, B, \{ T_s, L, K_{a,b}, A \}_{K_{b,s}} \}_{K_{a,s}}.$

③ $A \longrightarrow B : \{ T_s, L, K_{a,b}, A \}_{K_{b,s}}, \{ A, T_a \}_{K_{a,b}}.$

④ $B \longrightarrow A : \{ T_a + 1 \}_{K_{a,b}}.$

- Phrased in terms of messages, timestamps, lifetimes, keys.
- Intent is not clear from specification.

Conventional Kerberos Protocol

- 1 $A \longrightarrow S : A, B.$
- 2 $S \longrightarrow A : \{ T_s, L, K_{a,b}, B, \{ T_s, L, K_{a,b}, A \}_{K_{b,s}} \}_{K_{a,s}}.$
- 3 $A \longrightarrow B : \{ T_s, L, K_{a,b}, A \}_{K_{b,s}}, \{ A, T_a \}_{K_{a,b}}.$
- 4 $B \longrightarrow A : \{ T_a + 1 \}_{K_{a,b}}.$

- Phrased in terms of messages, timestamps, lifetimes, keys.
- Intent is not clear from specification.

Conventional Kerberos Protocol

- 1 $A \longrightarrow S : A, B.$
 - 2 $S \longrightarrow A : \{ T_s, L, K_{a,b}, B, \{ T_s, L, K_{a,b}, A \}_{K_{b,s}} \}_{K_{a,s}}.$
 - 3 $A \longrightarrow B : \{ T_s, L, K_{a,b}, A \}_{K_{b,s}}, \{ A, T_a \}_{K_{a,b}}.$
 - 4 $B \longrightarrow A : \{ T_a + 1 \}_{K_{a,b}}.$
- Phrased in terms of messages, timestamps, lifetimes, keys.
 - Intent is not clear from specification.

Idealized Kerberos Protocol

$$2. S \longrightarrow A : \{ T_s, A \xleftrightarrow{K_{a,b}} B, \{ T_s, A \xleftrightarrow{K_{a,b}} B \}_{K_{b,s}} \}_{K_{a,s}}.$$

$$3. A \longrightarrow B : \{ T_s, A \xleftrightarrow{K_{a,b}} B \}_{K_{b,s}}, \{ T_a, A \xleftrightarrow{K_{a,b}} B \}_{K_{a,b}}^A.$$

$$4. B \longrightarrow A : \{ T_a, A \xleftrightarrow{K_{a,b}} B \}_{K_{a,b}}^B.$$

- Already clearer, because specification expresses *intent*, not *content*.
- Dispenses with irrelevant details such as lifetimes and principals that are otherwise recoverable.

Idealized Kerberos Protocol

$$2. S \longrightarrow A : \{ T_s, A \xleftrightarrow{K_{a,b}} B, \{ T_s, A \xleftrightarrow{K_{a,b}} B \}_{K_{b,s}} \}_{K_{a,s}}.$$

$$3. A \longrightarrow B : \{ T_s, A \xleftrightarrow{K_{a,b}} B \}_{K_{b,s}}, \{ T_a, A \xleftrightarrow{K_{a,b}} B \}_{K_{a,b}}^A.$$

$$4. B \longrightarrow A : \{ T_a, A \xleftrightarrow{K_{a,b}} B \}_{K_{a,b}}^B.$$

- Already clearer, because specification expresses *intent*, not *content*.
- Dispenses with irrelevant details such as lifetimes and principals that are otherwise recoverable.

Idealized Kerberos Protocol

$$2. S \longrightarrow A : \{ T_s, A \xleftrightarrow{K_{a,b}} B, \{ T_s, A \xleftrightarrow{K_{a,b}} B \}_{K_{b,s}} \}_{K_{a,s}}.$$

$$3. A \longrightarrow B : \{ T_s, A \xleftrightarrow{K_{a,b}} B \}_{K_{b,s}}, \{ T_a, A \xleftrightarrow{K_{a,b}} B \}_{K_{a,b}}^A.$$

$$4. B \longrightarrow A : \{ T_a, A \xleftrightarrow{K_{a,b}} B \}_{K_{a,b}}^B.$$

- Already clearer, because specification expresses *intent*, not *content*.
- Dispenses with irrelevant details such as lifetimes and principals that are otherwise recoverable.

Preconditions

- **A believes** $A \xleftrightarrow{K_{a,s}} S$, **B believes** $B \xleftrightarrow{K_{b,s}} S$,
S believes $A \xleftrightarrow{K_{a,s}} S$, **S believes** $B \xleftrightarrow{K_{b,s}} S$.
- **S believes** $A \xleftrightarrow{K_{a,b}} B$.
- **B believes S controls** $\forall K. A \xleftrightarrow{K} B$,
A believes S controls $\forall K. A \xleftrightarrow{K} B$.
- **B believes** T_s fresh, **A believes** T_s fresh,
B believes T_a fresh.

Consequences of Message 2

- $S \longrightarrow A : \{ X \}_{K_{a,s}}$, where
 $X = Z, \{ Z \}_{K_{b,s}}$ and $Z = T_s, A \xleftrightarrow{K_{a,b}} B$.
- A sees $\{ X \}_{K_{a,s}}$.
- A believes S said X , because A believes $A \xleftrightarrow{K_{a,s}} S$ and previous.
- A believes S said Z and A believes S said $\{ Z \}_{K_{b,s}}$, because $X = Z, \{ Z \}_{K_{b,s}}$ and previous.
- A believes Z fresh, and so A believes S believes $A \xleftrightarrow{K_{a,b}} B$.
- A believes S controls $A \xleftrightarrow{K_{a,b}} B$ by instantiation of assumption.
- A believes $A \xleftrightarrow{K_{a,b}} B$ by delegation of authority.

Consequences of Message 2

- $S \longrightarrow A : \{X\}_{K_{a,s}}$, where
 $X = Z, \{Z\}_{K_{b,s}}$ and $Z = T_s, A \xleftrightarrow{K_{a,b}} B$.
- **A sees $\{X\}_{K_{a,s}}$.**
- **A believes S said X**, because **A believes $A \xleftrightarrow{K_{a,s}} S$** and previous.
- **A believes S said Z** and **A believes S said $\{Z\}_{K_{b,s}}$** , because $X = Z, \{Z\}_{K_{b,s}}$ and previous.
- **A believes Z fresh**, and so **A believes S believes $A \xleftrightarrow{K_{a,b}} B$** .
- **A believes S controls $A \xleftrightarrow{K_{a,b}} B$** by instantiation of assumption.
- **A believes $A \xleftrightarrow{K_{a,b}} B$** by delegation of authority.

Consequences of Message 2

- $S \longrightarrow A : \{X\}_{K_{a,s}}$, where
 $X = Z, \{Z\}_{K_{b,s}}$ and $Z = T_s, A \stackrel{K_{a,b}}{\longleftrightarrow} B$.
- **A sees $\{X\}_{K_{a,s}}$.**
- **A believes S said X**, because **A believes $A \stackrel{K_{a,s}}{\longleftrightarrow} S$** and previous.
- **A believes S said Z** and **A believes S said $\{Z\}_{K_{b,s}}$** , because $X = Z, \{Z\}_{K_{b,s}}$ and previous.
- **A believes Z fresh**, and so **A believes S believes $A \stackrel{K_{a,b}}{\longleftrightarrow} B$** .
- **A believes S controls $A \stackrel{K_{a,b}}{\longleftrightarrow} B$** by instantiation of assumption.
- **A believes $A \stackrel{K_{a,b}}{\longleftrightarrow} B$** by delegation of authority.

Consequences of Message 2

- $S \longrightarrow A : \{ X \}_{K_{a,s}}$, where
 $X = Z, \{ Z \}_{K_{b,s}}$ and $Z = T_s, A \stackrel{K_{a,b}}{\longleftrightarrow} B$.
- **A sees** $\{ X \}_{K_{a,s}}$.
- **A believes S said X**, because **A believes** $A \stackrel{K_{a,s}}{\longleftrightarrow} S$ and previous.
- **A believes S said Z** and **A believes S said** $\{ Z \}_{K_{b,s}}$, because $X = Z, \{ Z \}_{K_{b,s}}$ and previous.
- **A believes Z fresh**, and so **A believes S believes** $A \stackrel{K_{a,b}}{\longleftrightarrow} B$.
- **A believes S controls** $A \stackrel{K_{a,b}}{\longleftrightarrow} B$ by instantiation of assumption.
- **A believes** $A \stackrel{K_{a,b}}{\longleftrightarrow} B$ by delegation of authority.

Consequences of Message 2

- $S \longrightarrow A : \{ X \}_{K_{a,s}}$, where
 $X = Z, \{ Z \}_{K_{b,s}}$ and $Z = T_s, A \xleftrightarrow{K_{a,b}} B$.
- **A sees** $\{ X \}_{K_{a,s}}$.
- **A believes S said X**, because **A believes** $A \xleftrightarrow{K_{a,s}} S$ and previous.
- **A believes S said Z** and **A believes S said** $\{ Z \}_{K_{b,s}}$, because $X = Z, \{ Z \}_{K_{b,s}}$ and previous.
- **A believes Z fresh**, and so **A believes S believes** $A \xleftrightarrow{K_{a,b}} B$.
- **A believes S controls** $A \xleftrightarrow{K_{a,b}} B$ by instantiation of assumption.
- **A believes** $A \xleftrightarrow{K_{a,b}} B$ by delegation of authority.

Consequences of Message 2

- $S \longrightarrow A : \{ X \}_{K_{a,s}}$, where
 $X = Z, \{ Z \}_{K_{b,s}}$ and $Z = T_s, A \stackrel{K_{a,b}}{\longleftrightarrow} B$.
- **A sees** $\{ X \}_{K_{a,s}}$.
- **A believes S said X**, because **A believes** $A \stackrel{K_{a,s}}{\longleftrightarrow} S$ and previous.
- **A believes S said Z** and **A believes S said** $\{ Z \}_{K_{b,s}}$, because $X = Z, \{ Z \}_{K_{b,s}}$ and previous.
- **A believes Z fresh**, and so **A believes S believes** $A \stackrel{K_{a,b}}{\longleftrightarrow} B$.
- **A believes S controls** $A \stackrel{K_{a,b}}{\longleftrightarrow} B$ by instantiation of assumption.
- **A believes** $A \stackrel{K_{a,b}}{\longleftrightarrow} B$ by delegation of authority.

Consequences of Message 2

- $S \longrightarrow A : \{ X \}_{K_{a,s}}$, where
 $X = Z, \{ Z \}_{K_{b,s}}$ and $Z = T_s, A \xleftrightarrow{K_{a,b}} B$.
- **A sees** $\{ X \}_{K_{a,s}}$.
- **A believes S said X**, because **A believes** $A \xleftrightarrow{K_{a,s}} S$ and previous.
- **A believes S said Z** and **A believes S said** $\{ Z \}_{K_{b,s}}$, because $X = Z, \{ Z \}_{K_{b,s}}$ and previous.
- **A believes Z fresh**, and so **A believes S believes** $A \xleftrightarrow{K_{a,b}} B$.
- **A believes S controls** $A \xleftrightarrow{K_{a,b}} B$ by instantiation of assumption.
- **A believes** $A \xleftrightarrow{K_{a,b}} B$ by delegation of authority.

Consequences of Messages 3 and 4

- $A \longrightarrow B : \{Z\}_{K_{b,s}}, \{Z'\}_{K_{a,b}}^A$, where $Z' = T_a, A \xleftrightarrow{K_{a,b}} B$.
 - B believes $A \xleftrightarrow{K_{a,b}} B$ by similar reasoning as above.
 - B believes Z' fresh, because B believes T_a fresh, and so B believes A believes $A \xleftrightarrow{K_{a,b}} B$.
- $B \longrightarrow A : \{Z'\}_{K_{a,b}}^B$.
 - B believes A believes $A \xleftrightarrow{K_{a,b}} B$.

Consequences of Messages 3 and 4

- $A \longrightarrow B : \{Z\}_{K_{b,s}}, \{Z'\}_{K_{a,b}}^A$, where $Z' = T_a, A \xleftrightarrow{K_{a,b}} B$.
 - **B believes $A \xleftrightarrow{K_{a,b}} B$** by similar reasoning as above.
 - B believes Z' fresh, because B believes T_a fresh, and so B believes A believes $A \xleftrightarrow{K_{a,b}} B$.
- $B \longrightarrow A : \{Z'\}_{K_{a,b}}^B$.
 - B believes A believes $A \xleftrightarrow{K_{a,b}} B$.

Consequences of Messages 3 and 4

- $A \longrightarrow B : \{ Z \}_{K_{b,s}}, \{ Z' \}_{K_{a,b}}^A$, where $Z' = T_a, A \xleftrightarrow{K_{a,b}} B$.
 - B **believes** $A \xleftrightarrow{K_{a,b}} B$ by similar reasoning as above.
 - B **believes** Z' **fresh**, because B **believes** T_a **fresh**, and so B **believes** A **believes** $A \xleftrightarrow{K_{a,b}} B$.
- $B \longrightarrow A : \{ Z' \}_{K_{a,b}}^B$.
 - B **believes** A **believes** $A \xleftrightarrow{K_{a,b}} B$.

Consequences of Messages 3 and 4

- $A \longrightarrow B : \{Z\}_{K_{b,s}}, \{Z'\}_{K_{a,b}}^A$, where $Z' = T_a, A \xleftrightarrow{K_{a,b}} B$.
 - B **believes** $A \xleftrightarrow{K_{a,b}} B$ by similar reasoning as above.
 - B **believes** Z' **fresh**, because B **believes** T_a **fresh**, and so B **believes** A **believes** $A \xleftrightarrow{K_{a,b}} B$.
- $B \longrightarrow A : \{Z'\}_{K_{a,b}}^B$.
 - B **believes** A **believes** $A \xleftrightarrow{K_{a,b}} B$.

Consequences of Messages 3 and 4

- $A \longrightarrow B : \{ Z \}_{K_{b,s}}, \{ Z' \}_{K_{a,b}}^A$, where $Z' = T_a, A \xleftrightarrow{K_{a,b}} B$.
 - B **believes** $A \xleftrightarrow{K_{a,b}} B$ by similar reasoning as above.
 - B **believes** Z' **fresh**, because B **believes** T_a **fresh**, and so B **believes** A **believes** $A \xleftrightarrow{K_{a,b}} B$.
- $B \longrightarrow A : \{ Z' \}_{K_{a,b}}^B$.
 - B **believes** A **believes** $A \xleftrightarrow{K_{a,b}} B$.

Other Examples

- AFS Handshake. Found error that admits replay attack.
- Needham-Schroeder key exchange. Found error that admits replay attack.
- CCITT X.509 protocol. Found errors during idealization and verification stages.

AFS Handshake

- 1 $A \longrightarrow B : \{ N_a \}_{K_{a,b}}$.
- 2 $B \longrightarrow A : \{ N_a, N_b \}_{K_{a,b}}$.
- 3 $A \longrightarrow B : \{ N_b \}_{K_{a,b}}$.
- 4 $B \longrightarrow A : \{ A \xleftrightarrow{K'_{a,b}} B, N'_b \}_{K_{a,b}}$.

- N_a, N_b, N'_b are nonces.
- Goal is to generate a new session key $K'_{a,b}$ for A and B , given a starting session key $K_{a,b}$.
- The verification fails because the protocol is in error.

AFS Handshake

- 1 $A \longrightarrow B : \{ N_a \}_{K_{a,b}}$.
- 2 $B \longrightarrow A : \{ N_a, N_b \}_{K_{a,b}}$.
- 3 $A \longrightarrow B : \{ N_b \}_{K_{a,b}}$.
- 4 $B \longrightarrow A : \{ A \xleftrightarrow{K'_{a,b}} B, N'_b \}_{K_{a,b}}$.

- N_a, N_b, N'_b are nonces.
- Goal is to generate a new session key $K'_{a,b}$ for A and B , given a starting session key $K_{a,b}$.
- The verification fails because the protocol is in error.

AFS Handshake

① $A \longrightarrow B : \{ N_a \}_{K_{a,b}}$.

② $B \longrightarrow A : \{ N_a, N_b \}_{K_{a,b}}$.

③ $A \longrightarrow B : \{ N_b \}_{K_{a,b}}$.

④ $B \longrightarrow A : \{ A \overset{K'_{a,b}}{\longleftrightarrow} B, N'_b \}_{K_{a,b}}$.

- N_a, N_b, N'_b are nonces.
- Goal is to generate a new session key $K'_{a,b}$ for A and B , given a starting session key $K_{a,b}$.
- The verification fails because the protocol is in error.

AFS Handshake

- 1 $A \longrightarrow B : \{ N_a \}_{K_{a,b}}$.
- 2 $B \longrightarrow A : \{ N_a, N_b \}_{K_{a,b}}$.
- 3 $A \longrightarrow B : \{ N_b \}_{K_{a,b}}$.
- 4 $B \longrightarrow A : \{ A \xleftrightarrow{K'_{a,b}} B, N'_b \}_{K_{a,b}}$.

- N_a, N_b, N'_b are nonces.
- Goal is to generate a new session key $K'_{a,b}$ for A and B , given a starting session key $K_{a,b}$.
- The verification fails because the protocol is in error.

Initial Conditions

- Both principals agree on starting key: **A believes $A \xleftrightarrow{K_{a,b}} B$, B believes $A \xleftrightarrow{K_{a,b}} B$.**
- A defers to B 's authority on session keys:
 A believes B controls $\forall K. A \xleftrightarrow{K} B$.
- B generates the new session key: **B believes $A \xleftrightarrow{K'_{a,b}} B$.**
- Nonces are fresh: **A believes N_a fresh, B believes N_b fresh, B believes N'_b fresh.**

Initial Conditions

- Both principals agree on starting key: **A believes $A \xleftrightarrow{K_{a,b}} B$, B believes $A \xleftrightarrow{K_{a,b}} B$.**
- A defers to B 's authority on session keys:
 A believes B controls $\forall K. A \xleftrightarrow{K} B$.
- B generates the new session key: B believes $A \xleftrightarrow{K'_{a,b}} B$.
- Nonces are fresh: A believes N_a fresh, B believes N_b fresh, B believes N'_b fresh.

Initial Conditions

- Both principals agree on starting key: **A believes $A \xleftrightarrow{K_{a,b}} B$, B believes $A \xleftrightarrow{K_{a,b}} B$.**
- A defers to B 's authority on session keys:
 A believes B controls $\forall K. A \xleftrightarrow{K} B$.
- B generates the new session key: **B believes $A \xleftrightarrow{K'_{a,b}} B$.**
- Nonces are fresh: A believes N_a fresh, B believes N_b fresh, B believes N'_b fresh.

Initial Conditions

- Both principals agree on starting key: A **believes** $A \xleftrightarrow{K_{a,b}} B$,
 B **believes** $A \xleftrightarrow{K_{a,b}} B$.
- A defers to B 's authority on session keys:
 A **believes** B **controls** $\forall K. A \xleftrightarrow{K} B$.
- B generates the new session key: B **believes** $A \xleftrightarrow{K'_{a,b}} B$.
- Nonces are fresh: A **believes** N_a **fresh**, B **believes** N_b **fresh**,
 B **believes** N'_b **fresh**.

Derived Properties

- **A believes B said $A \xleftrightarrow{K'_{a,b}} B, N'_b$.**
- Cannot deduce **A believes B believes $A \xleftrightarrow{K_{a,b}} B$** because we do not have **A believes N'_b fresh**.
- Reveals a replay attack: step 4 can be replayed by an intruder, leading to unwarranted beliefs if freshness conditions are ignored.
- Solution is to add N_a to message in step 4.

Derived Properties

- **A believes B said** $A \xleftrightarrow{K'_{a,b}} B, N'_b$.
- Cannot deduce **A believes B believes** $A \xleftrightarrow{K_{a,b}} B$ because we do not have **A believes** N'_b **fresh**.
- Reveals a replay attack: step 4 can be replayed by an intruder, leading to unwarranted beliefs if freshness conditions are ignored.
- Solution is to add N_a to message in step 4.

Derived Properties

- **A believes B said** $A \xleftrightarrow{K'_{a,b}} B, N'_b$.
- Cannot deduce **A believes B believes** $A \xleftrightarrow{K_{a,b}} B$ because we do not have **A believes** N'_b **fresh**.
- Reveals a replay attack: step 4 can be replayed by an intruder, leading to unwarranted beliefs if freshness conditions are ignored.
- Solution is to add N_a to message in step 4.

Derived Properties

- A **believes** B **said** $A \xleftrightarrow{K'_{a,b}} B, N'_b$.
- Cannot deduce A **believes** B **believes** $A \xleftrightarrow{K_{a,b}} B$ because we do not have A **believes** N'_b **fresh**.
- Reveals a replay attack: step 4 can be replayed by an intruder, leading to unwarranted beliefs if freshness conditions are ignored.
- Solution is to add N_a to message in step 4.

Revised AFS Handshake

① $A \longrightarrow B : A, N_a.$

② $B \longrightarrow A : \{ N_a, K'_{a,b} \}_{K_{a,b}}.$

③ $A \longrightarrow B : \{ N_a \}_{K'_{a,b}}.$

④ $B \longrightarrow A : N'_b.$

• A believes $A \xleftrightarrow{K'_{a,b}} B$, B believes $A \xleftrightarrow{K'_{a,b}} B$.

• A believes B believes $A \xleftrightarrow{K'_{a,b}} B$,
 B believes A believes $A \xleftrightarrow{K'_{a,b}} B$.

Revised AFS Handshake

- 1 $A \longrightarrow B : A, N_a.$
- 2 $B \longrightarrow A : \{ N_a, K'_{a,b} \}_{K_{a,b}}.$
- 3 $A \longrightarrow B : \{ N_a \}_{K'_{a,b}}.$
- 4 $B \longrightarrow A : N'_b.$

- A believes $A \xleftrightarrow{K'_{a,b}} B$, B believes $A \xleftrightarrow{K'_{a,b}} B$.
- A believes B believes $A \xleftrightarrow{K'_{a,b}} B$,
 B believes A believes $A \xleftrightarrow{K'_{a,b}} B$.

Revised AFS Handshake

- 1 $A \longrightarrow B : A, N_a.$
- 2 $B \longrightarrow A : \{ N_a, K'_{a,b} \}_{K_{a,b}}.$
- 3 $A \longrightarrow B : \{ N_a \}_{K'_{a,b}}.$
- 4 $B \longrightarrow A : N'_b.$

- A believes $A \xleftrightarrow{K'_{a,b}} B$, B believes $A \xleftrightarrow{K'_{a,b}} B.$
- A believes B believes $A \xleftrightarrow{K'_{a,b}} B,$
 B believes A believes $A \xleftrightarrow{K'_{a,b}} B.$

Revised AFS Handshake

- 1 $A \longrightarrow B : A, N_a.$
- 2 $B \longrightarrow A : \{ N_a, K'_{a,b} \}_{K_{a,b}}.$
- 3 $A \longrightarrow B : \{ N_a \}_{K'_{a,b}}.$
- 4 $B \longrightarrow A : N'_b.$

- A believes $A \xleftrightarrow{K'_{a,b}} B$, B believes $A \xleftrightarrow{K'_{a,b}} B.$
- A believes B believes $A \xleftrightarrow{K'_{a,b}} B,$
 B believes A believes $A \xleftrightarrow{K'_{a,b}} B.$

Revised AFS Handshake

- 1 $A \longrightarrow B : A, N_a.$
 - 2 $B \longrightarrow A : \{ N_a, K'_{a,b} \}_{K_{a,b}}.$
 - 3 $A \longrightarrow B : \{ N_a \}_{K'_{a,b}}.$
 - 4 $B \longrightarrow A : N'_b.$
- **A believes $A \xleftrightarrow{K'_{a,b}} B$, B believes $A \xleftrightarrow{K'_{a,b}} B.$**
 - A believes B believes $A \xleftrightarrow{K'_{a,b}} B,$
 B believes A believes $A \xleftrightarrow{K'_{a,b}} B.$

Revised AFS Handshake

- 1 $A \longrightarrow B : A, N_a.$
 - 2 $B \longrightarrow A : \{ N_a, K'_{a,b} \}_{K_{a,b}}.$
 - 3 $A \longrightarrow B : \{ N_a \}_{K'_{a,b}}.$
 - 4 $B \longrightarrow A : N'_b.$
- **A believes** $A \xleftrightarrow{K'_{a,b}} B$, **B believes** $A \xleftrightarrow{K'_{a,b}} B.$
 - **A believes** **B believes** $A \xleftrightarrow{K'_{a,b}} B,$
B believes **A believes** $A \xleftrightarrow{K'_{a,b}} B.$

Summary

- It is possible, and profitable, to think clearly about protocols by applying rudimentary logical methods.
- The status of the proposed logic is far from clear! Uses dubious concepts such as confusing messages with propositions, freshness of propositions, underspecified logic of belief.
- Historically, the first step in rigorous protocol analysis. Presumably modern logics are much more sophisticated and better-grounded!