A Logic of Authentication

Borrows, Abadi and Needham

TOCS 1990, DEC-SRC 1989

Logic Constructs

- **P believes X** : P may act as though X is true.

- **P sees X** : a message containing X was sent to P; P can read and repeat X.

- **P said X** : principal P at some time sent a message containing X.

- **P controls X** : P has jurisdiction over X; P has authority over X and should be trusted on this matter.

- **fresh(X)** : X is fresh; X has not been sent in a message at any time before the current run of the protocol (i.e., nonces).

Logic Constructs (continued)

- $\mathbf{P} \overset{K}{\longleftrightarrow} \mathbf{Q}$: P and Q may used the shared key K to communicate.

- $\overset{K}{\longmapsto} \mathbf{P}$: P has K as a public key.

- $\mathbf{P} \overset{X}{\Longleftrightarrow} \mathbf{Q}$: X is a secret known only to P and Q (and maybe to principals trusted by them).

- $\mathbf{\{X\}_K}$: formula X encrypted under the key K.

- $\mathbf{\langle X \rangle_Y}$: X combined with the formula Y; Y is secret and its presence proves the identity of whoever utters $\langle X \rangle_{Y}$.

Logical postulates

(1) The message meaning rules :

- for shared keys :

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

If P believes key K is shared with Q and sees X encrypted with K then it believes Q once said X.

- for public keys :

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

If P believes key K is Q’s public key and sees X encrypted with K^{-1} then it believes Q once said X.

- for shared secrets :

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

If P believes secret Y is shared with Q and it sees $\langle X \rangle_Y$ then P believes Q once said X.

Logical Postulates

(2) The nonce-verification rule :

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

- expresses the check that a message is recent and that its sender still believes in it.

(3) The jurisdiction rule :

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

- if P believes that Q has jurisdiction over X then P trusts Q on the truth of X.

Logical Postulates

(4) If a principal sees a formula then he also sees its components provided and knows the necessary keys :

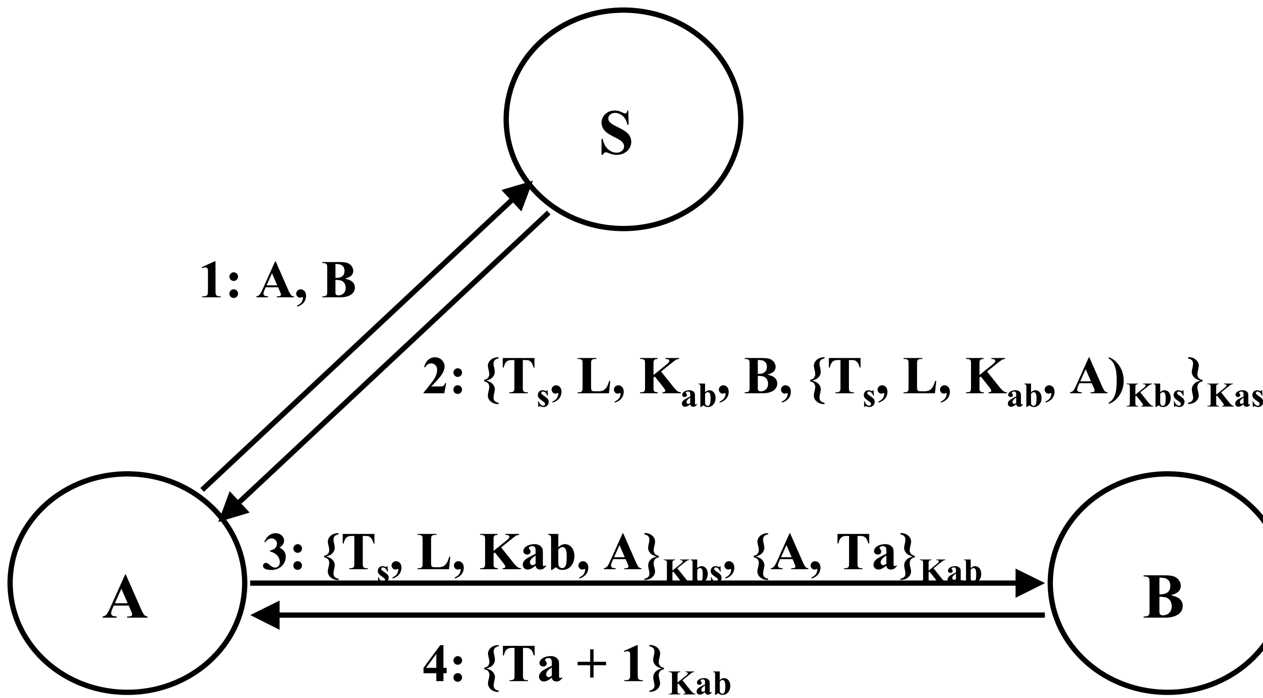
$$\frac{P \text{ sees } (X,Y)}{P \text{ sees } X} \qquad \frac{P \text{ sees } \langle X \rangle_Y}{P \text{ sees } X}$$

$$\frac{P \text{ believes } Q \overset{K}{\longleftrightarrow} P,\ P \text{ sees } \{X\}_K}{P \text{ sees } X}$$

$$\frac{P \text{ believes } \overset{K}{\longmapsto} P,\ P \text{ sees } \{X\}_K}{P \text{ sees } X}$$

$$\frac{P \text{ believes } \overset{K}{\longmapsto} Q,\ P \text{ sees } \{X\}_{K^{-1}}}{P \text{ sees } X}$$

The Kerberos protocol



A, **B** : principals
S : the authentication server
$\mathbf{T_s}$, $\mathbf{T_a}$: time stamps
L : lifetime of the key K_{ab}
$\mathbf{K_{as}}$, $\mathbf{K_{bs}}$: keys A respectively B share with S

The idealization of the Kerberos protocol

Message 2 :

$$S \dashrightarrow A : \{T_s, A \overset{K_{ab}}{\longleftrightarrow} B, \{T_s, A \overset{K_{ab}}{\longleftarrow} B\}_{Kbs}\}_{Kas}$$

Message 3 :

$$A \dashrightarrow B : \{T_s, A \overset{K_{ab}}{\longleftrightarrow} B\}_{Kbs}, \{Ta, A \overset{K_{ab}}{\longleftrightarrow} B\}_{Kab} \text{ from } A$$

Message 4 :

$$B \dashrightarrow A : \{T_a, A \overset{K_{ab}}{\longleftrightarrow} B\}_{Kab} \text{ from } B$$

NOTES :

- the lifetime L was combined with the time stamp Ts
- the first message is omitted, since it doesn't contribute to the logical properties of the protocol

The analysis of the Kerberos protocol

- Assumptions :

A believes A $\overset{K_{as}}{\longleftrightarrow}$ S

S believes A $\overset{K_{as}}{\longleftrightarrow}$ S

S believes A $\overset{K_{ab}}{\longleftrightarrow}$ B

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

A believes fresh(Ts)

B believes B $\overset{K_{bs}}{\longleftrightarrow}$ S

S believes B $\overset{K_{bs}}{\longleftrightarrow}$ S

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

B believes fresh(Ts)

B believes fresh(Ta)

- Message 2 :

A receives message 2 : **A sees $\{T_s, A \overset{K_{ab}}{\longleftrightarrow} B, \{T_s, A \overset{K_{ab}}{\longleftrightarrow} B\}_{Kbs}\}_{Kas}$**

Using the hypothesis we get : **A believes A $\overset{K_{as}}{\longleftrightarrow}$ S**

Applying the message meaning rule for shared keys :

A believes S said $\{T_s, A \overset{K_{ab}}{\longleftrightarrow} B, \{T_s, A \overset{K_{ab}}{\longleftrightarrow} B\}_{Kbs}\}_{Kas}$

By breaking the conjunction (the "**,**") we get : **A believes S said (T_s, (A $\overset{K_{ab}}{\text{<--->}}$ B))**

We have the hypothesis : **A believes fresh(Ts)**

Using the nonce-verification rule yields : **A believes S believes (T_s, (A $\overset{K_{ab}}{\text{<--->}}$ B))**

By breaking the conjunction : **A believes S believes (A $\overset{K_{ab}}{\text{<--->}}$ B)**

By instantiating K to Kab in the hypothesis : **A believes S controls A $\overset{K}{\text{<--->}}$ B**

Then we derive the more concrete : **A believes S controls A $\overset{K_{ab}}{\text{<--->}}$ B**

Applying the jurisdiction rule : **A believes A $\overset{K_{ab}}{\text{<--->}}$ B**

•**Message 3 :** A passes the ticket to B

Applying the same procedure we get :

B believes A believes A $\overset{K_{ab}}{\longleftrightarrow}$ B

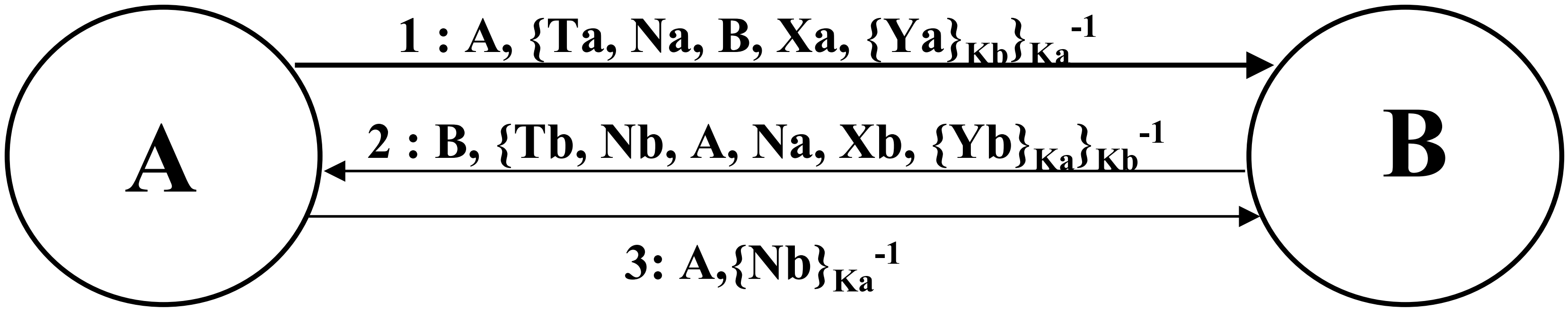
• **Message 4 :** assures A that B believes in the key and received A's last message

The final result is :

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

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

The CCITT X.509 protocol



- The protocol idealization :

Message 1 : **A --> B :** $\{Ta, Na, Xa, \{Ya\}_{Kb}\}_{Ka}^{-1}$

Message 2 : **B --> A :** $\{Tb, Nb, Na, Xb, \{Yb\}_{Ka}\}_{Kb}^{-1}$

Message 3 : **A --> B :** $\{Nb\}_{Ka}^{-1}$

The analysis of the CCITT X.509 protocol

- Assumptions :

A believes $\overset{K_a}{\mid\!\!\longrightarrow}$ **A**	**A believes** $\overset{K_b}{\mid\!\!\longrightarrow}$ **A**
A believes $\overset{K_b}{\mid\!\!\longrightarrow}$ **B**	**A believes** $\overset{K_a}{\mid\!\!\longrightarrow}$ **A**
A believes fresh(Na)	**A believes fresh(Nb)**
A believes fresh(Tb)	**A believes fresh(Ta)**

- We can derive : **A believes B believes Xb** and **B believes A believes Xa**

- The outcome is weaker than desired. We don’t obtain :
  A believes B believes Yb or **B believes A believes Ya**

- A third party could copy encrypted data and replace the signature with its own.
  - a fix could be signing the secret data (Ya, Yb) before encrypting it for privacy.

- There is some redundancy in massage 2 : either Tb or Na is sufficient to ensure timeliness.

CCITT X.509 flaw

- CCITT X.509 document suggests Ta need not be checked => serious problem :
  - An intruder C replays one of A's old messages, then impersonates A :

    C --> B : A, $\{Ta, Na, B, Xa, \{Ya\}_{Kb}\}_{Ka^{-1}}$

  - B doesn't check Ta and replies with new nonce Nb :

    B --> C : B, $\{Tb, Nb, A, Na, Xb, \{Yb\}_{Ka}\}_{Kb^{-1}}$

  - C causes A to initiate authentication with C :

    A --> C : A, $\{Ta', Na', C, Xa', \{Ya'\}_{Kc}\}_{Ka^{-1}}$

  - C replies to A providing the nonce Nb (which is not secret) :

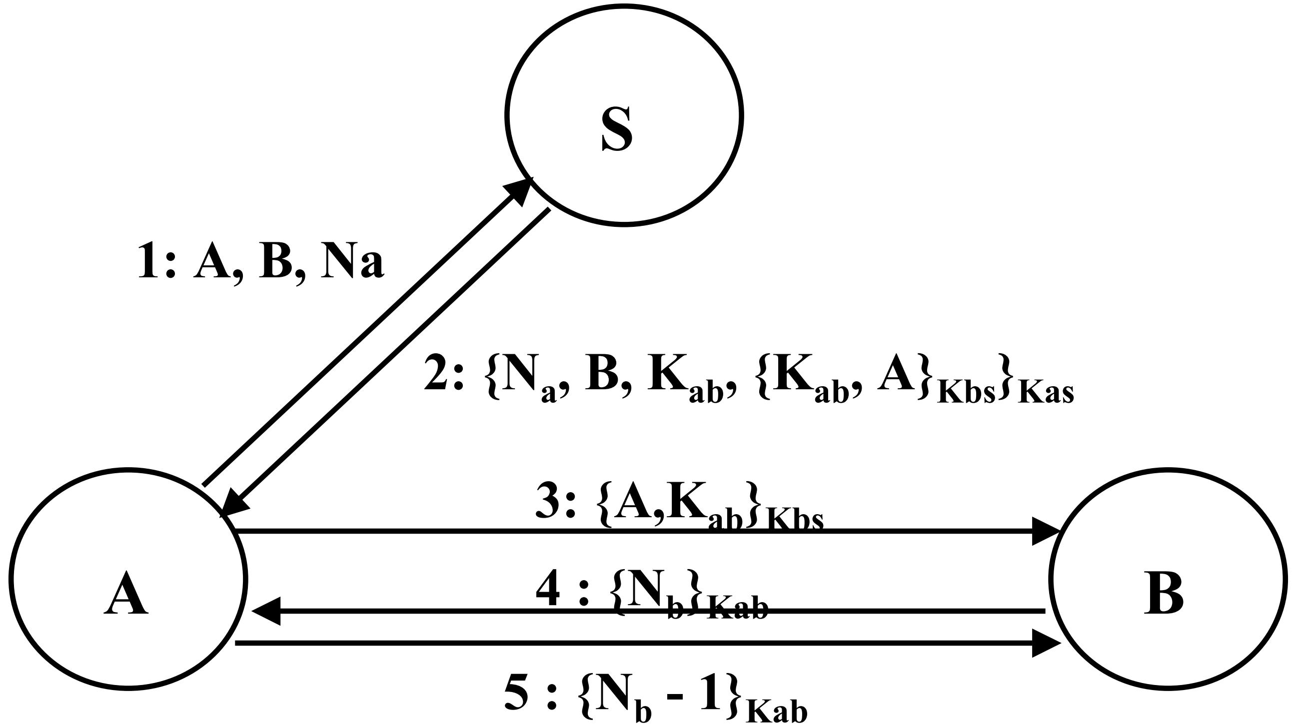
    C --> A : C, $\{Tc, Nb, A, Na', Xc, \{Yc\}_{Ka}\}_{Kc^{-1}}$

  - A replies to C, signing Nb => C can convince first message was recently sent by A :

    A --> C A, $\{Nb\}_{Ka^{-1}}$

•**Solution :** provide name of B in the last message

The Needham-Schroeder protocol (with shared keys)



- The idealized protocol :

  Message 2 : **S --> A : $\{Na, (A \overset{K_{ab}}{\longleftrightarrow} B), \#(A \overset{K_{ab}}{\longleftrightarrow} B), \{A \overset{K_{ab}}{\longleftrightarrow} B\}_{Kbs}\}_{Kas}$**

  Message 3 : **A --> B : $\{A \overset{K_{ab}}{\longleftrightarrow} B\}_{Kbs}$**

  Message 4 : **B --> A : $\{Nb, (A \overset{K_{ab}}{\longleftrightarrow} B)\}_{Kab}$ from B**

  Message 5 : **A --> B : $\{Nb, (A \overset{K_{ab}}{\longleftrightarrow} B)\}_{Kab}$ from A**

NOTE :
#(X) means **fresh(X)**

The analysis of the Needham-Schroeder protocol

- Assumptions :

A1. A believes A $\overset{K_{as}}{\longleftrightarrow}$ S

A2. B believes B $\overset{K_{bs}}{\longleftrightarrow}$ S

A3. S believes A $\overset{K_{as}}{\longleftrightarrow}$ S

A4. S believes B $\overset{K_{bs}}{\longleftrightarrow}$ S

A5. S believes A $\overset{K_{ab}}{\longleftrightarrow}$ B

A6. A believes (S controls A $\overset{K}{\longleftrightarrow}$ B)

A7. B believes (S controls A $\overset{K}{\longleftrightarrow}$ B)

A8. A believes (S controls #(A $\overset{K}{\longleftrightarrow}$ B))

A9. A believes #(Na)

A10. B believes #(Nb)

A11. S believes #(A $\overset{K_{ab}}{\longleftrightarrow}$ B)

A12. B believes #(A $\overset{K}{\longleftrightarrow}$ B)

- **NOTE :**
  - this assumption is unusual and its use was criticized
  - the protocol's authors did not realized they made it
  - we will show the assumption is needed to attain authentication

• A sends to S a nonce; S replies including new key to be used by A and B :

Message 2: **A sees {Na, (A $\overset{K_{ab}}{\longleftrightarrow}$ B), fresh(A $\overset{K_{ab}}{\longleftrightarrow}$ B), {A $\overset{K_{ab}}{\longleftrightarrow}$ B}$_{Kbs}$}$_{Kas}$**

I. Using the Message Meaning postulate with Message 2 and A1:

(1) A believes S said Na

(2) A believes S said (A $\overset{K_{ab}}{\longleftrightarrow}$ B)

(3) A believes S said *fresh* (A $\overset{K_{ab}}{\longleftrightarrow}$ B)$_{K_{ab}}$

(4) A believes S said {A $\overset{K_{ab}}{\longleftrightarrow}$ B}$_{Kbs}$

II. Using the Nonce Verification postulate with 1-3 and A9:

(5) A believes S believes (A $\overset{K_{ab}}{\longleftrightarrow}$ B)

(6) A believes S believes *fresh* (A $\overset{K_{ab}}{\longleftrightarrow}$ B)

III. Using the Jurisdiction postulate with (5) and A6; and also with (6) and A8:

(7) A believes (A $\overset{K_{ab}}{\longleftrightarrow}$ B)

(8) A believes *fresh* (A $\overset{K_{ab}}{\longleftrightarrow}$ B)

IV. Also from **Message 2** and the "component" postulate:

(9) A sees $\{A \overset{K_{ab}}{\longleftrightarrow} B\}_{Kbs}$

Message 3 : **B sees** $\{A \overset{K_{ab}}{\longleftrightarrow} B\}_{Kbs}$

V. Using the Message Meaning postulate with **Message 3** and A2:

(10) B believes S said $(A \overset{K_{ab}}{\longleftrightarrow} B)$

VI. Using the Nonce Verification postulate with (10) and (artificially included) ***A12***:

(11) B believes S believes $(A \overset{K_{ab}}{\longleftrightarrow} B)$

VII. Using the Jurisdiction postulate with (11) and A7:

(12) | **B believes** $(A \overset{K_{ab}}{\longleftrightarrow} B)$ |

Message 4 : **A sees** $\{Nb\}_{Kab}$

VIII. Using Message Meaning postulate with **Message 4** and (7):

(13) A believes B said Nb => **(14) A believes B said** $(A \overset{K_{ab}}{\longleftrightarrow} B)$

By idealization of msg 4

IX. Using the Nonce Verification postulate with (8) and (14)

(15) | **A believes B believes (A $\overset{K_{ab}}{\longleftrightarrow}$ B)** |

Message 5 : **B sees $\{Nb\text{-}1\}_{Kab}$**

X. Using Message Meaning postulate with **Message 5** and (12):

(16) B believes A said Nb-1 => (17) B believes A said (A $\overset{K_{ab}}{\longleftrightarrow}$ B)

By idealization of msg 5

XI. Using the Nonce Verification postulate with (A12) and (17) :

(18) | **B believes A believes (A $\overset{K_{ab}}{\longleftrightarrow}$ B)** |

NOTES :

- result reached at the cost of assuming B accepts the key as new
- compromise of a session key has very bad results => can be reused as new