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)

• $P \triangleleft K \triangleright Q$: P and Q may use the shared key K to communicate.

• $K \triangleleft P$: P has K as a public key.

• $P \triangleleft X \triangleright Q$: X is a secret known only to P and Q (and maybe to principals trusted by them).

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

• $<X>_Y$: X combined with the formula Y; Y is secret and its presence proves the identity of whoever utters $<X>_Y$. 
Logical postulates

(1) The message meaning rules:

• for shared keys:

\[ P \text{ believes } Q \overset{K}{\rightarrow} P, \text{ P sees } \{X\}_K \]

\[ P \text{ believes Q said X} \]

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:

\[ P \text{ believes } Q \overset{K}{\rightarrow} P, \text{ P sees } \{X\}_{K^{-1}} \]

\[ P \text{ believes Q said X} \]

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:

\[ P \text{ believes } Q \overset{Y}{\rightarrow} P, \text{ P sees } <X>_Y \]

\[ P \text{ believes Q said X} \]

If P believes secret Y is shared with Q and it sees $<X>_Y$ then P believes Q once said X.
Logical Postulates

(2) The nonce-verification rule:

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

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

(3) The jurisdiction rule:

\[ \text{P believes Q controls } X, \text{P believes Q believes } X \]
\[ \Rightarrow \text{P believes } X \]

- 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:

<table>
<thead>
<tr>
<th>P sees (X,Y)</th>
<th>P sees &lt;X&gt;_y</th>
</tr>
</thead>
<tbody>
<tr>
<td>P sees X</td>
<td>P sees X</td>
</tr>
</tbody>
</table>

P believes $Q \xleftarrow{\sim} P$, P sees $\{X\}_K$

P sees X

P believes $\xrightarrow{\sim} P$, P sees $\{X\}_K$

P sees X

P believes $\xrightarrow{\sim} Q$, P sees $\{X\}_{K^{-1}}$

P sees X
The Kerberos protocol

1: A, B

2: \{T_s, L, K_{ab}, B, \{T_s, L, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}

3: \{T_s, L, K_{ab}, A\}_{K_{bs}}, \{A, T_a\}_{K_{ab}}

4: \{T_a + 1\}_{K_{ab}}

A, B : principals
S : the authentication server
T_s, T_a : time stamps
L : lifetime of the key K_{ab}
K_{as}, K_{bs} : keys A respectively B share with S
The idealization of the Kerberos protocol

Message 2:

\[ S \rightarrow A : \{T_s, A \xleftarrow{K_{ab}} B, \{T_s, A \xleftarrow{K_{ab}} B\}_Kbs\}_Kas \]

Message 3:

\[ A \rightarrow B : \{T_s, A \xleftarrow{K_{ab}} B\}_Kbs, \{T_a, A \xleftarrow{K_{ab}} B\}_Kab \text{ from } A \]

Message 4:

\[ B \rightarrow A : \{T_a, A \xleftarrow{K_{ab}} B\}_Kab \text{ from } B \]

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

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

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

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

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

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

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

B believes fresh(Ts)

A believes fresh(Ts)

B believes fresh(Ta)

• Message 2:

A receives message 2: A sees $\{T_s, A \overset{K_{ab}}{\leftrightarrow} B, \{T_s, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}\}_{K_{as}}$

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

Applying the message meaning rule for shared keys:

A believes S said $\{T_s, A \overset{K_{ab}}{\leftrightarrow} B, \{T_s, A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}\}_{K_{as}}$
By breaking the conjunction (the “,”) we get: \( A \text{ believes } S \text{ said } (T_s, (A \langle \rightarrow \rangle B)) \)

We have the hypothesis: \( A \text{ believes } \text{fresh}(T_s) \)

Using the nonce-verification rule yields: \( A \text{ believes } S \text{ believes } (T_s, (A \langle \rightarrow \rangle B)) \)

By breaking the conjunction: \( A \text{ believes } S \text{ believes } (A \langle \rightarrow \rangle B) \)

By instantiating \( K \) to \( K_{ab} \) in the hypothesis: \( A \text{ believes } S \text{ controls } A \langle K \rangle B \)

Then we derive the more concrete: \( A \text{ believes } S \text{ controls } A \langle K_{ab} \rangle B \)

Applying the jurisdiction rule: \( A \text{ believes } A \langle K_{ab} \rangle B \)
• **Message 3**: A passes the ticket to B

  Applying the same procedure we get:

  \[ B \text{ believes } A \text{ believes } A \quad \mathcal{K}_{ab} \quad B \]

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

  The final result is:

  \[ A \text{ believes } A \quad \mathcal{K}_{ab} \quad B \quad B \text{ believes } A \quad \mathcal{K}_{ab} \quad B \]

  \[ A \text{ believes } B \text{ believes } A \quad \mathcal{K}_{ab} \quad B \quad B \text{ believes } A \text{ believes } A \quad \mathcal{K}_{ab} \quad B \]
The CCITT X.509 protocol

1: A, \{Ta, Na, B, Xa, \{Ya\}_Kb\}_Ka^{-1}

2: B, \{Tb, Nb, A, Na, Xb, \{Yb\}_Ka\}_Kb^{-1}

3: A, \{Nb\}_Kb^{-1}

- 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 $K_a \rightarrow A$
  A believes $K_b \rightarrow B$
  A believes fresh(Na)
  A believes fresh(Tb)

  A believes $K_a \rightarrow A$
  A believes $K_b \rightarrow A$
  A believes fresh(Nb)
  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:
    \[ C \rightarrow B : A, \{Ta, Na, B, Xa, \{Ya\}_{Kb}\}_{Ka}^{-1} \]
  
  • B doesn’t check Ta and replies with new nonce Nb:
    \[ B \rightarrow C : B, \{Tb, Nb, A, Na, Xb, \{Yb\}_{Ka}\}_{Kb}^{-1} \]
  
  • C causes A to initiate authentication with C:
    \[ A \rightarrow C : A, \{Ta’, Na’, C, Xa’, \{Ya’\}_{Ke}\}_{Ka}^{-1} \]
  
  • C replies to A providing the nonce Nb (which is not secret):
    \[ C \rightarrow A : C, \{Tc, Nb, A, Na’, Xc, \{Yc\}_{Ka}\}_{Kc}^{-1} \]
  
  • A replies to C, signing Nb => C can convince first message was recently sent by A:
    \[ A \rightarrow C A, \{Nb\}_{Ka}^{-1} \]

• Solution: provide name of B in the last message
The Needham-Schroeder protocol (with shared keys)

- The idealized protocol:

  Message 2: $S \rightarrow A: \{Na, (A \leftrightarrow B), #(A \leftrightarrow B), \{A \leftrightarrow B\}_{Kbs}\}_{Kas}$

  Message 3: $A \rightarrow B: \{A, K_{ab}\}_{Kbs}$

  Message 4: $B \rightarrow A: \{Nb, (A \leftrightarrow B)\}_{Kab}$ from B

  Message 5: $A \rightarrow B: \{Nb, (A \leftrightarrow B)\}_{Kab}$ from A

  **NOTE:**

  $(X)$ means $\text{fresh}(X)$
The analysis of the Needham-Schroeder protocol

- Assumptions:
  
  A1. $A$ believes $A \leftrightarrow S$  
  A2. $B$ believes $B \leftrightarrow S$  
  A3. $S$ believes $A \leftrightarrow S$  
  A4. $S$ believes $B \leftrightarrow S$  
  A5. $S$ believes $A \leftrightarrow B$  
  A6. $A$ believes $(S \text{ controls } A \leftrightarrow B)$  
  A7. $B$ believes $(S \text{ controls } A \leftrightarrow B)$  
  A8. $A$ believes $(S \text{ controls } #(A \leftrightarrow B))$  
  A9. $A$ believes #(Na)  
  A10. $B$ believes #(Nb)  
  A11. $S$ believes #(A $\leftrightarrow_{ab} B$)  
  A12. $B$ believes #(A $\leftrightarrow_{K} B$)

- 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 \leftrightarrow B), \text{fresh}(A \leftrightarrow B), \{A \leftrightarrow 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 \( (A \leftrightarrow B) \)
3. A believes S said fresh \( (A \leftrightarrow B) \)
4. A believes S said \( \{A \leftrightarrow B\}_Kbs \)

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

5. A believes S believes \( (A \leftrightarrow B) \)
6. A believes S believes fresh \( (A \leftrightarrow B) \)

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

7. A believes \( (A \leftrightarrow B) \)
8. A believes fresh \( (A \leftrightarrow B) \)
IV. Also from \textbf{Message 2} and the “component” postulate:

(9) A sees $\{A \leftrightarrow B\}_{Kbs}$

\hspace{1cm}

\underline{Message 3 : B sees $\{A \leftrightarrow B\}_{Kbs}$}

V. Using the Message Meaning postulate with \textbf{Message 3} and $A_2$:

(10) B believes S said $(A \leftrightarrow B)$

VI. Using the Nonce Verification postulate with (10) and (artificially included) $A_{12}$:

(11) B believes S believes $(A \leftrightarrow B)$

VII. Using the Jurisdiction postulate with (11) and $A_7$:

(12) B believes $(A \leftrightarrow B)$

\hspace{1cm}

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

VIII. Using Message Meaning postulate with \textbf{Message 4} and (7):

(13) A believes B said $Nb$  \hspace{1cm} \Rightarrow \hspace{1cm} (14) A believes B said $(A \leftrightarrow B)$

\hspace{1cm}

By idealization of msg 4
IX. Using the Nonce Verification postulate with (8) and (14)

(15) \( A \) believes \( B \) believes \( (A \leftrightarrow B) \)

Message 5: \( B \) sees \( \{Nb-1\}_{K_{ab}} \)

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

(16) \( B \) believes \( A \) said \( Nb-1 \) \( \Rightarrow \) (17) \( B \) believes \( A \) said \( (A \leftrightarrow B) \)

\( K_{ab} \)

By idealization of msg 5

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

(18) \( B \) believes \( A \) believes \( (A \leftrightarrow B) \)

\( K_{ab} \)

NOTES:

- result reached at the cost of assuming \( B \) accepts the key as new
- compromise of a session key has very bad results \( \Rightarrow \) can be reused as new