Special topics in Logic and Security I

Master Year II, Sem. I, 2025-2026

Ioana Leuștean
FMI, UB

We thank Alexandru Dragomir (Faculty of Philosophy) for the initial version of this presentation.

BAN Logic: A Logic of Authentication

- "In barest outline, an *authentication protocol* guarantees that if the principals really are who they say they are then they will end up in possession of one or more shared secrets, or at least they will become able to recognize the use of other principals' secrets" (BAN1989a)
- "After authentication, two principuls (people, computers, services) should be entitled to believe that they are communicating with each other and not with intruders." (BAN1990)
- "A simple logic has allowed us to describe the beliefs of trustworthy parties involved in authentication protocols and the evolution of these beliefs as a consequence of communication." (BAN1990)

BAN Logic: The Language

Principals

- $A, B, \ldots$ denote (are names of) principals.
- $P, Q, R, \ldots$ are variable, ranging over principals.

Keys

- K_{AB} is read: K_{AB} is a key shared by A and B.
- K_A is read: K is A's public key.
- K_A^{-1} is A's secret key iff K is A's public key.
- K is a variable, ranging over encryption keys.

Statements

- N_A, N_B are nonces (e.g. statements representing large random numbers).
- $X, Y, \ldots$ are variables, ranging over statements.

BAN Language (1)

Keep in mind that P is a variable ranging over principals, K over keys, X over messages!

- $P \mid\equiv X$: Agent P **believes** that X (is *true*).
- $P \triangleleft X$: Agent P (**receives**) **sees** message X.
- $P \mid\sim X$: Agent P once (**sent**) **said** that X.
  Agent P sent a message including the statement X. It is not known whether P sent X during the current run of the protocol, but at that moment, P also believed X.
- $P \mid\Rightarrow X$: Agent P (**controls**) **has jurisdiction over** X.
  Agent P should be trusted regarding X.
- $\sharp(X)$: X is a fresh message (has not been sent before the run of the current protocol). This is defined to be *true* for *nonces*.

BAN Language (2)

Keep in mind that P is a variable ranging over principals, K over keys, X over messages!

- $P \leftrightarrow^{K} Q$: Agents P and Q share key K and can communicate safely using it. Assumption: key K is *good*:
  "...it will never be discovered by any principal except P or Q, or a principal trusted by either P or Q" (BAN1989a).
- $\mapsto^{K} P$: K is a public key of P. Recall that K^{-1} is P's secret key.
- $P \rightleftharpoons^{X} Q$: Agents P and Q share message X as a secret. Note that X is a statement (e.g. a password), not a key!
- $\{X\}_K$: formula X is encrypted by key K.

BAN Logic: Inference Rules

The following rules state the conditions under which a principal can infer the originator of a message.

(1) Message meaning rules for shared keys:

$$MM - SK \quad \frac{P \mid\equiv (Q \leftrightarrow^{K} P), P \triangleleft \{X\}_K}{P \mid\equiv (Q \mid\sim X)}$$

$$MM - SK \quad \frac{P \textbf{ believes } (Q \leftrightarrow^{K} P), P \textbf{ sees } \{X\}_K}{P \textbf{ believes } (Q \textbf{ said } X)}$$

If agent P believes that he shares the secret key K with agent Q and P receives a message encrypted with K, then P believes that Q sent X.

BAN Logic: Inference Rules

The following rules state the conditions under which a principal can infer the originator of a message.

(1) Message meaning rules for shared keys:

$$MM - SK \quad \frac{P \mid\equiv (Q \overset{K}{\leftrightarrow} P), P \triangleleft \{X\}_K}{P \mid\equiv (Q \mid\sim X)}$$

(2) Message meaning rules for public keys:

$$MM - PK \quad \frac{P \mid\equiv \overset{K}{\mapsto} Q, P \triangleleft \{X\}_{K^{-1}}}{P \mid\equiv (Q \mid\sim X)}$$

BAN Logic: Inference Rules

The following rule express the fact that recent messages are believed by their sender.

The nonce-verification rule:

$$NV \quad \frac{P \mid\equiv \sharp(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv (Q \mid\equiv X)}$$

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

The above rule states the conditions under which something said (in the past) can be *promoted* to present belief (Syverson & Cervesato 2001).

BAN Logic: Inference Rules

The following rule express the fact that recent messages are believed by their sender.

The nonce-verification rule:

$$NV \quad \frac{P \mid\equiv \sharp(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv (Q \mid\equiv X)}$$

"Note that our logic has not, and does not need, any notion of time to be associated with individual statements. The requirement to deal with time is entirely satisfied by the division of time into past and present, and by the semantics of the constructs themselves. This is possible because we found it sufficient to reason with stable formulas, that is, formulas that stay true for the whole run of the protocol once they become true. In addition, we represent protocols as sequential algorithms and ignore concurrency issues." [BAN1989a revised]

BAN Logic: Inference Rules

The following rule *promotes* beliefs about some other principal's beliefs to one's beliefs:

The jurisdiction rule:

$$JR \; \frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$$

$$JR \; \frac{P \textbf{ believes } (Q \textbf{ controls } X), P \textbf{ believes } (Q \textbf{ believes } X}{P \textbf{ believes } X}$$

In order to gather that P it is not enough to know that someone believes that P. In addition, I have to consider that person an authority on the matter.

BAN Logic: Structural Inference Rules

Belief and components:

$$BC1 \quad \frac{P \mid\equiv X, P \mid\equiv Y}{P \mid\equiv (X, Y)} \qquad BC2 \quad \frac{P \mid\equiv (X, Y)}{P \mid\equiv X}$$

$$BC3 \quad \frac{P \mid\equiv Q \mid\equiv (X, Y)}{P \mid\equiv Q \mid\equiv X} \qquad BC4 \quad \frac{P \mid\equiv Q \mid\sim (X, Y)}{P \mid\equiv Q \mid\sim X}$$

Seeing and components:

$$SC1 \quad \frac{P \triangleleft (X, Y)}{P \triangleleft X} \qquad SC2 \quad \frac{P \mid\equiv \mapsto^{K} Q, P \triangleleft \{X\}_{K^{-1}}}{P \triangleleft X}$$

$$SC3 \quad \frac{P \mid\equiv Q \leftrightarrow^{K} P, P \triangleleft \{X\}_{K}}{P \triangleleft X} \qquad SC4 \quad \frac{P \mid\equiv \mapsto^{K} P, P \triangleleft \{X\}_{K}}{P \triangleleft X}$$

BAN Logic: Inference Rules

Seeing and components:

Note that the following:

$$\frac{P \triangleleft X, P \triangleleft Y}{P \triangleleft (X, Y)}$$

is **not** an inference rule, since it would mean that seeing X and seeing Y implies seeing both of them at the same time.

Nonces concatenation

$$NC \quad \frac{P \mid\equiv \sharp(X)}{P \mid\equiv \sharp(X, Y)}$$

If one part of a formula is fresh, then the entire formula must also be fresh.

BAN Logic: Commutativity Inference Rules

Commutativity of secrets:

$$\frac{P \mid\equiv R \overset{X}{\rightleftharpoons} R'}{P \mid\equiv R' \overset{X}{\rightleftharpoons} R} \qquad \frac{P \mid\equiv Q \mid\equiv R \overset{X}{\rightleftharpoons} R'}{P \mid\equiv Q \mid\equiv R' \overset{X}{\rightleftharpoons} R}$$

Commutativity of keys:

$$\frac{P \mid\equiv R \overset{X}{\leftrightarrow} R'}{P \mid\equiv R' \overset{X}{\leftrightarrow} R} \qquad \frac{P \mid\equiv Q \mid\equiv R \overset{X}{\leftrightarrow} R'}{P \mid\equiv Q \mid\equiv R' \overset{X}{\leftrightarrow} R}$$

Verifying protocols using BAN

van Oorschot (1994) argues that analyzing a protocol using BAN involves four stages:

(1) Idealizing the protocol. The output of idealizing the protocol is a sequence Γ of steps

$$A \longrightarrow B : X$$

where A and B are principals, and X is a formula in the language of BAN.

(2) Identifying and formalizing the assumptions of the protocol. Call this set of assumptions Γ_0.
Examples: key K_{AS} is used by A to communicate with S, or: A trusts S to deliver a key for starting a secure message exchange with B.

(3) Identifying the goal G of the protocol.
Example: $A \mid\equiv A \leftrightarrow^{K} B$
A believes that K is a good key for talking to B

(4) Deriving G from Γ_0 and Γ using the inference rules.

Idealization: an example (BAN1989a)

Think of the protocol step:

$$A \longrightarrow B : \{A, K_{ab}\}_{K_{bs}}$$

If the intention is to tell B that K_{ab} is a good communication key with A, then the idealized version of this step should be

$$A \longrightarrow B : \{A \leftrightarrow^{K_{ab}} B\}_{K_{bs}}$$

and the following formula should be an assumption:

$$B \triangleleft \{A \leftrightarrow^{K_{ab}} B\}_{K_{bs}}$$

The Needham-Schroeder Protocol - with shared keys

The original BAN paper (1989a, pp. 17 – 22) worked out an analysis of The Needham-Schroeder Protocol, one of the most discussed protocols in the literature – but mostly for pedagogical reasons.

The Needham-Schroeder Protocol

$$\begin{array}{lll}
\text{Step 1.} & A \longrightarrow S: & A, B, N_A \\
\text{Step 2.} & S \longrightarrow A: & \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}} \\
\text{Step 3.} & A \longrightarrow B: & \{K_{AB}, A\}_{K_{BS}} \\
\text{Step 4.} & B \longrightarrow A: & \{N_B\}_{K_{AB}} \\
\text{Step 5.} & A \longrightarrow B: & \{N_B - 1\}_{K_{AB}}
\end{array}$$

- We have to intuitively understand the entire working of the protocol before idealizing it. Working in a methodical step-by-step translation of the protocol won't work.

”Only knowledge of the entire protocol can determine the essential logical contents of the message. ” (BAN1989a, p. 10)

The Needham-Schroeder Protocol - Step by Step

Step 1. $A \longrightarrow S: \quad A, B, N_A$

Step 2. $S \longrightarrow A: \quad \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$

- Principal A contacts the server and sends A and B in order to make it clear that it wants a key for communicating with B. Note the nonce N_A and the fact that the message is not encrypted.
- S sends A a message encrypted by K_{AS}. The message contains a ticket for B, encrypted by K_{BS} (which A cannot read). Beside the ticket, the message contains nonce N_A, such that A will know that S replied to its asking for K_{AB}, and B that could notice A that K_{AB} is supposed to be A's desired key. Note that the ticket intended for B also contains the identity of A.

$$
\begin{array}{lll}
\text{Step 1.} & A \longrightarrow S: & A, B, N_A \\
\text{Step 2.} & S \longrightarrow A: & \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}} \\
\text{Step 3.} & A \longrightarrow B: & \{K_{AB}, A\}_{K_{BS}}
\end{array}
$$

- A sends B the ticket it has just received from S.
- Note that the ticket includes A, so B understands what K_{AB} is for.

The Needham-Schroeder Protocol - Step by Step

Step 4. $B \longrightarrow A: \ \{N_B\}_{K_{AB}}$
Step 5. $A \longrightarrow B: \ \{N_B - 1\}_{K_{AB}}$

- B generates a new nonce N_B.
- Last two steps represent a *handshake* between A and B: B tells A something new, that only B would know and encrypts it by K_{AB}. A replies using the same key and slightly changes the nonce that B just sent.
- "Almost any function N_B would do, as long as B can distinguish his message from A's - thus, subtraction is used to indicate that the message is from A, rather than from B" (BAN1989a, p. 18).

The Needham-Schroeder Protocol - Idealization

BAN (1989a, pp. 18–19, 1989b, p. 336) proposed the following idealization of the Needham-Schroeder protocol.

Needham-Schroeder Idealized

Step 1. $A \longrightarrow S: \quad N_A$
Step 2. $S \longrightarrow A: \quad \{N_A, (A \leftrightarrow^{K_{AB}} B), \sharp(A \leftrightarrow^{K_{AB}} B), \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}\}_{K_{AS}}$
Step 3. $A \longrightarrow B: \quad \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}$
Step 4. $B \longrightarrow A: \quad \{N_B, (A \leftrightarrow^{K_{AB}} B)\}_{K_{AB}}$ from B
Step 5. $A \longrightarrow B: \quad \{N_B, (A \leftrightarrow^{K_{AB}} B)\}_{K_{AB}}$ from A

- Note that in Step 2, the message contains $\sharp(A \leftrightarrow^{K_{AB}} B)$. A way to represent the fact that S lets A know that $A \leftrightarrow^{K_{AB}} B$ can be used as a nonce!

Assumptions of the Needham-Schroeder protocol

If a message is sent o B, i.e.

$A \longrightarrow B : \quad \mathit{message}$

then we may assert that B received the message, so

$B \triangleleft \mathit{message}$

is also an assumption of the protocol.

Assumptions of the Needham-Schroeder protocol

If a message is sent o B, i.e.

$A \longrightarrow B: \quad message$

then we may assert that B received the message, so

$B \triangleleft message$

is also an assumption of the protocol.

Assumptions on the messages in the idealized protocol

Step 1. $S \triangleleft N_A$
Step 2. $A \triangleleft \{N_A, (A \leftrightarrow^{K_{AB}} B), \sharp(A \leftrightarrow^{K_{AB}} B), \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}\}_{K_{AS}}$
Step 3. $B \triangleleft \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}$
Step 4. $A \triangleleft \{N_B, (A \leftrightarrow^{K_{AB}} B)\}_{K_{AB}}$ from B
Step 5. $B \triangleleft \{N_B, (A \leftrightarrow^{K_{AB}} B)\}_{K_{AB}}$ from A

Assumptions of the Needham-Schroeder

Assumptions of the Needham-Schroeder Protocol. See BAN (1989, p. 19)

(1) $A \mid\equiv A \leftrightarrow^{K_{AS}} S$ (2) $B \mid\equiv B \leftrightarrow^{K_{BS}} S$
(3) $S \mid\equiv A \leftrightarrow^{K_{AS}} S$ (4) $S \mid\equiv B \leftrightarrow^{K_{BS}} S$
(5) $S \mid\equiv A \leftrightarrow^{K_{AB}} B$

(6) $A \mid\equiv (S \mid\Rightarrow A \leftrightarrow^{K} B)$ (7) $B \mid\Rightarrow (S \mid\equiv A \leftrightarrow^{K} B)$
(8) $A \mid\equiv (S \mid\Rightarrow \sharp(A \leftrightarrow^{K} B))$

(9) $A \mid\equiv \sharp(N_A)$ (10) $B \mid\equiv \sharp(N_B)$
(11) $S \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$

The assumptions are easy to understand, they inform us:

- on what the principals believe regarding the keys that they should use,
- on the fact that the principals believe that the server has jurisdiction over keys,
- on the fact that the agents believe that what they generate is fresh.

The Goal of Authentication

What is the goal of authentication? No single answer. Possible answers:

- (1) An authentication is complete when there is a key K such that all principals know that using it they may safely exchange messages. Using the BAN formalism (see BAN1990, p. 25, BAN1989a, p. 13):

$A \mid\equiv A \leftrightarrow^{K} B$ and $B \mid\equiv A \leftrightarrow^{K} B$ for some K

- (2) The condition in (1) holds, but, in addition, all principals know that all principals know that they may safely exchange message using the key K.

$$(A \mid\equiv A \leftrightarrow^{K} B) \wedge (A \mid\equiv A \leftrightarrow^{K} B) \wedge$$
$$(A \mid\equiv B \mid\equiv A \leftrightarrow^{K} B) \wedge (B \mid\equiv A \mid\equiv A \leftrightarrow^{K} B) \text{ for some } K$$

The Needham-Schroeder Protocol: BAN derivations

Step 1. $A \longrightarrow S: \quad A, B, N_A$

Step 2. $S \longrightarrow A: \quad \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$

After Step 2:

(1) $A \triangleleft \{N_A, (A \leftrightarrow^{K_{AB}} B), \sharp(A \leftrightarrow^{K_{AB}} B), \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}\}_{K_{AS}}$ Step 2

The Needham-Schroeder Protocol: BAN derivations

Step 1. $A \longrightarrow S : \quad A, B, N_A$

Step 2. $S \longrightarrow A : \quad \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$

After Step 2:

(1) $A \triangleleft \{N_A, (A \leftrightarrow^{K_{AB}} B), \sharp(A \leftrightarrow^{K_{AB}} B), \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}\}_{K_{AS}}$ Step 2

The principal A sees (receives) a message encrypted with the shared key K_{AS} so, by

(2) $A \mid\equiv A \leftrightarrow^{K_{AS}} S$ As. 1

The Needham-Schroeder Protocol: BAN derivations

Step 1. $A \longrightarrow S: \quad A, B, N_A$
Step 2. $S \longrightarrow A: \quad \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$

After Step 2:

(1) $A \triangleleft \{N_A, (A \leftrightarrow^{K_{AB}} B), \sharp(A \leftrightarrow^{K_{AB}} B), \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}\}_{K_{AS}}$ Step 2

The principal A sees (receives) a message encrypted with the shared key K_{AS} so, by

(2) $A \mid\equiv A \leftrightarrow^{K_{AS}} S$ As. 1

and the message-meaning rule he infers that S said (sent) the message:

(3) $A \mid\equiv S \mid\sim (N_A, (A \leftrightarrow^{K_{AB}} B), \sharp(A \leftrightarrow^{K_{AB}} B), \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}})$ MM-SK: 1 ,2

The Needham-Schroeder Protocol: BAN derivations

Step 1. $A \longrightarrow S: \quad A, B, N_A$

Step 2. $S \longrightarrow A: \quad \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$

After Step 2:

(1) $A \triangleleft \{N_A, (A \leftrightarrow^{K_{AB}} B), \sharp(A \leftrightarrow^{K_{AB}} B), \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}\}_{K_{AS}}$ Step 2

The principal A sees (receives) a message encrypted with the shared key K_{AS} so, by

(2) $A \mid\equiv A \leftrightarrow^{K_{AS}} S$ As. 1

and the message-meaning rule he infers that S said (sent) the message:

(3) $A \mid\equiv S \mid\sim (N_A, (A \leftrightarrow^{K_{AB}} B), \sharp(A \leftrightarrow^{K_{AB}} B), \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}})$ MM-SK: 1 ,2

In this moment, agent A believes that S said something, however, it might not be clear if the action happened in the past or in the present. In order to conclude that the message "belongs" to the present we have to use the nonce verification rule.

The Needham-Schroeder Protocol: BAN derivations

(3) $A \mid\equiv S \mid\sim (N_A, (A \leftrightarrow^{K_{AB}} B), \sharp(A \leftrightarrow^{K_{AB}} B), \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}})$ MM-SK: 1 ,2
(4) $A \mid\equiv \sharp(N_A)$ As. 9
(5) $A \mid\equiv \sharp(N_A, (A \leftrightarrow^{K_{AB}} B), \sharp(A \leftrightarrow^{K_{AB}} B), \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}})$ NC: 4
(6) $A \mid\equiv S \mid\equiv (N_A, (A \leftrightarrow^{K_{AB}} B), \sharp(A \leftrightarrow^{K_{AB}} B), \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}})$ NV: 3, 5

If a message is believed (to be true) then each of its components are also belived (to be true), so:

(7) $A \mid\equiv S \mid\equiv N_A$ BC3: 6
(8) $A \mid\equiv S \mid\equiv A \leftrightarrow^{K_{AB}} B$ BC3: 6
(9) $A \mid\equiv S \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$ BC3: 6
(10) $A \mid\equiv S \mid\equiv \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}$ BC3: 6

The Needham-Schroeder Protocol: BAN derivations

So far, principal A beliefs are related to those of S, which has jurisdiction over keys. In order to derive A's beliefs from those of S we have to use the jurisdiction rule as follows:

(8)	$A \mid\equiv S \mid\equiv A \leftrightarrow^{K_{AB}} B$	BC3: 6
(9)	$A \mid\equiv S \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$	BC3: 6
(11)	$A \mid\equiv S \mid\Rightarrow A \leftrightarrow^{K_{AB}} B$	As. 6
(12)	$A \mid\equiv S \mid\Rightarrow \sharp(A \leftrightarrow^{K_{AB}} B)$	As. 8
(13)	$A \mid\equiv A \leftrightarrow^{K_{AB}} B$	JR: 8,11
(14)	$A \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$	JR: 9, 12
(15)	$A \triangleleft \{A \leftrightarrow_{K_{AB}} B\}_{K_{BS}}$	SC2: 1

Note that (13) is one of the authentication goals, stating that A believes that K_{AB} is a good communication key with B.

The Needham-Schroeder Protocol: BAN derivations

After performing Step 3, we analyze B's beliefs in a similar manner:

(16)	$B \triangleleft \{A \leftrightarrow_{K_{AB}} B\}_{K_{BS}}$	Step 3
(17)	$B \mid\equiv B \leftrightarrow^{K_{BS}} S$	As. 2
(18)	$B \mid\equiv S \mid\sim A \leftrightarrow^{K_{AB}} B$	MM-SK: 16, 17

We need to prove that $B \mid\equiv A \leftrightarrow^{K_{AB}} B$, so the information B has on $A \leftrightarrow^{K_{AB}} B$ should be promoted to present. Note that, in order to use the nonce-verification rule, an additional assumption on freshness is needed.

Assumptions of the Needham-Schroeder

Assumptions of the Needham-Schroeder Protocol. See BAN (1989, p. 19)

(1) $A \mid\equiv A \overset{K_{AS}}{\leftrightarrow} S$ (2) $B \mid\equiv B \overset{K_{BS}}{\leftrightarrow} S$
(3) $S \mid\equiv A \overset{K_{AS}}{\leftrightarrow} S$ (4) $S \mid\equiv B \overset{K_{BS}}{\leftrightarrow} S$
(5) $S \mid\equiv A \overset{K_{AB}}{\leftrightarrow} B$

(6) $A \mid\equiv (S \mid\Rightarrow A \overset{K}{\leftrightarrow} B)$ (7) $B \mid\Rightarrow (S \mid\equiv A \overset{K}{\leftrightarrow} B)$
(8) $A \mid\equiv (S \mid\Rightarrow \sharp(A \overset{K}{\leftrightarrow} B))$

(9) $A \mid\equiv \sharp(N_A)$ (10) $B \mid\equiv \sharp(N_B)$
(11) $S \mid\equiv \sharp(A \overset{K_{AB}}{\leftrightarrow} B)$ (12) $B \mid\equiv \sharp(A \overset{K_{AB}}{\leftrightarrow} B)$

- Assumption 12 is needed in order to derive that

  B believes the key K_{AB}

The Needham-Schroeder Protocol: BAN derivations

We analyze B's beliefs in a similar manner:

(16)	$B \triangleleft \{A \leftrightarrow_{K_{AB}} B\}_{K_{BS}}$	Step 3
(17)	$B \mid\equiv B \leftrightarrow^{K_{BS}} S$	As. 2
(18)	$B \mid\equiv S \mid\sim A \leftrightarrow^{K_{AB}} B$	MM-SK: 16, 17
(19)	$B \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$	As. 12
(20)	$B \mid\equiv S \mid\equiv A \leftrightarrow^{K_{AB}} B$	NV: 18, 19
(21)	$B \mid\equiv S \mid\Rightarrow A \leftrightarrow^{K} B$	As. 7
(22)	$B \mid\equiv A \leftrightarrow^{K_{AB}} B$	JR: 20, 21

By (22), the principal B also believes that K_{AB} is a good communication key. However, we had to use Assumption 12 and the nonce verification rule in order to bring S's message to present.

The Needham-Schroeder Protocol: BAN derivations

After performing the last steps stronger authentication goals - (29) and (33) - are proved:

(23)	$A \triangleleft \{N_B, (A \leftrightarrow^{K_{AB}} B)\}_{K_{AB}}$ from B	Step 4
(24)	$B \triangleleft \{N_B, (A \leftrightarrow^{K_{AB}} B)\}_{K_{AB}}$ from A	Step 5
(25)	$A \mid\equiv B \mid\sim N_B, (A \leftrightarrow^{K_{AB}} B)$	MM-SK: 23, 13
(26)	$A \mid\equiv \sharp(N_B, A \leftrightarrow^{K_{AB}} B)$	NC: 14
(27)	$A \mid\equiv B \mid\equiv (N_B, A \leftrightarrow^{K_{AB}} B)$	NV: 25, 26
(28)	$A \mid\equiv B \mid\equiv N_B$	BC3: 27
(29)	$A \mid\equiv B \mid\equiv A \leftrightarrow^{K_{AB}} B$	BC3: 27
(30)	$B \mid\equiv A \mid\sim (N_B, A \leftrightarrow^{K_{AB}} B)$	MM-SK: 22, 24
(31)	$B \mid\equiv \sharp(N_B, A \leftrightarrow^{K_{AB}} B)$	NC: As(10)
(32)	$B \mid\equiv A \mid\equiv N_B$	NV: 30, 31, BC3.
(33)	$B \mid\equiv A \mid\equiv A \leftrightarrow^{K_{AB}} B$	NV: 30, 31, BC3.

Goals and Interesting Derivations

(14) $A \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$

(As 12) $B \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$

(13) $A \mid\equiv A \leftrightarrow^{K_{AB}} B$
(29) $A \mid\equiv B \mid\equiv A \leftrightarrow^{K_{AB}} B$

(22) $B \mid\equiv A \leftrightarrow^{K_{AB}} B$
(33) $B \mid\equiv A \mid\equiv A \leftrightarrow^{K_{AB}} B$

(28) $A \mid\equiv B \mid\equiv N_B$

(32) $B \mid\equiv A \mid\equiv N_B$

- Note that A derived the freshness of $A \leftrightarrow^{K_{AB}} B$ (at line 14), whereas B assumed it (Assumption 12, used at line 19).
- The derivation of $B \mid\equiv A \leftrightarrow^{K_{AB}} B$ at line 22, is made possible by using Assumption 12 ($B \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$) at line 19.
- However, the derivation of $B \mid\equiv A \mid\equiv A \leftrightarrow_{K_{AB}} B$ at line 33, does not need Assumption 12 (but only Assumption 10, i.e. $B \mid\equiv \sharp(N_B)$ at line 31).

A known vulnerability

Denning and Sacco, 1981

Step 1. $A \longrightarrow S: \quad A, B, N_A$

Step 2. $S \longrightarrow A: \quad \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$

Step 3. $E(A) \longrightarrow B$: $\{K'_{AB}, A\}_{K_{BS}}$

Step 4. $B \longrightarrow E(A)$: $\{N'_B\}_{K'_{AB}}$

Step 5. $E(A) \longrightarrow B$: $\{N'_B - 1\}_{K_{AB}}$

- an intruder has unlimited time to find an old session key (an old session ticket) and reuse it as though it were fresh (BAN1989a, p. 21; the observation is due to Denning and Sacco, 1981)
- the intruder should also know the handshake function $(n - 1)$, but the problem of securing the handshake function is as difficult as securing the session keys (Dennig and Sacco, 1981)

Some conclusions

- The derivation of $B \mid\equiv A \leftrightarrow^{K_{AB}} B$ at line 22, is made possible by using Assumption 12 ($B \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$) at line 19. Deriving that principal B knows the key is conditioned by assuming that B takes the key to be fresh, an intruder might use an old session key.
- If proving a certain goal using BAN entails assuming that φ, then the non-formal specification of the protocol *also* uses assumption φ. So an analysis using BAN might be useful in making explicit *some tacit assumptions* of the protocol.

This is not an argument against using BAN!

A known vulnerability: solutions

An attacker might find a session key from past runs of the protocol.

- To overcome this problem, Denning and Sacco (1981) proposed using timestamps:

  Step 1. $A \longrightarrow S: \quad A, B$

  Step 2. $S \longrightarrow A: \quad \{B, K_{AB}, T_S, \{A, K_{AB}, T_S\}_{K_{BS}}\}_{K_{AS}}$

  Step 3. $A \longrightarrow B: \quad \{A, K_{AB}, T_S\}_{K_{BS}}$

- In a revised version of their protocol, Needham and Scroeder (1987) proposed an additional interaction between A and B:

  Step 01. $A \longrightarrow B: \quad A$

  Step 02. $B \longrightarrow A: \quad \{A, J\}_{K_{BS}}$

  Step 1. $A \longrightarrow S: \quad A, B, N_A, \{A, J\}_{K_{BS}}$

  Step 2. $S \longrightarrow A: \quad \{N_A, B, K_{AB}, \{K_{AB}, A, J\}_{K_{BS}}\}_{K_{AS}}$

  Step 3. $A \longrightarrow B: \quad \{K_{AB}, A, J\}_{K_{BS}}$

  ...

BAN Logic: finding a semantics?

- Note that we are not able to prove that $B \mid\equiv A \leftrightarrow^{K_{AB}} B$ without assuming that $B \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$.
- If we would be in hold of a suitable semantics for BAN logic, we would be able to check that:

For Γ the set of assumptions:

$$\Gamma \setminus \{B \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)\} \not\models B \mid\equiv A \leftrightarrow^{K_{AB}} B$$

- Note the importance of a suitable semantic apparatus! This observation is important since it is widely argued that BAN lacks a suitable semantics.

Thank you!

References I

- Burrows, M., Abadi. M., & Needham, R. (1990)
  A Logic of Authentication.
  ACM Transactions on Computer Systems, Vol. 8, No. 1: 18–36. 1990.

- Burrows, M., Abadi. M., & Needham, R. (1989a)
  A Logic of Authentication.
  SRC Research Report 39, 1 – 50, 1989; revised version 1990.

- Burrows, M., Abadi, M., & Needham, R. (1989b)
  Authentication: A Practical Study in Belief and Action
  TARK '88 Proceedings of the 2nd conference on Theoretical aspects of reasoning about knowledge, 325 – 342. 1989.

- van Oorschot, P.C. (1994)
  An Alternate Explanation of two BAN-logic "failures".
  Proceeding EUROCRYPT '93 Workshop on the theory and application of cryptographic techniques on Advances in cryptology, 443 – 447, 1994.

References II

Teepe, W. (2009).
On BAN Logic and hash functions or: How an unjustified inference rule causes problems.
Autonomous Agents and Multi-Agent Systems, 19(1): 76–88. 2009.

Teepe, W. (2006).
BAN logic is not 'sound', constructing epistemic logics for security is difficult.
Workshop on Formal Approaches to Multi-Agent Systems, 6: 79—91, 2006.

Syverson, P. & Cervesato, I. (2001).
The Logic of Authentication Protocols.
Foundations of Security Analysis and Design, eds. Focardi, R. & Gorrieri, R., Springer, 63–136 , 2001.

Nessett, D.M. (1990).
A Critique of the Burrows, Abadi, Needham Logic.
ACM SIGOPS Operating Systems Review, 24(2), 35–38.

References III

- Boyd, C. & Mao, W. (1994).
  On a Limitation of BAN Logic.
  Advances in Cryptology - EUROCRYPT 93, LNCS 765, T. Helleseth (ed.), Springer-Verlag, pp. 240–247. 1994.

- Boyd, C. & Mathuria, A. (2002).
  Protocols for Authentication and Key Establishment.
  Springer-Verlag.

- Sierra, J.M., Hernández, J.C., Alcaide, A., Torres, J. (2004).
  Validating the Use of BAN LOGIC.
  In: Laganá, A., Gavrilova, M.L., Kumar, V., Mun, Y., Tan, C.J.K., Gervasi, O. (eds) Computational Science and Its Applications – ICCSA 2004. ICCSA 2004. Lecture Notes in Computer Science, vol 3043. Springer, Berlin, Heidelberg

- Cohen, M., & Dam, M. (2005).
  A completeness result for BAN logic.
  In Prococeedings of Methods for Modalities 4, Berlin.