Topici speciale în logică și securitate I

Verificarea protocoalelor de securitate folosind logica BAN

Alexandru Dragomir
FMI, UB

Master anul II, Sem. I, 2019-2020

Contents

- The Needham-Schroeder Protocol.
- The Otway-Rees Protocol.
- BAN Logic: The Language of BAN logic.
- BAN Logic: The Inference Rules of BAN logic.
- Verifying the Needham-Schroeder Protocol using BAN
- Verifying the Otway-Rees Protocol using BAN
- Objections: Teepes (2009) and Boyd & Mao (1994).
- Conclusions

BAN Logic: A Logic of Authentication

Authentication protocols

"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)

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

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

The Needham-Schroeder Protocol - Step by Step

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

- 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.
- Question: Sending C and D would mean that it wants a good key under which C and D would securely communicate?
- Note the nonce N_A!
- Also note that the message is not encrypted!

The Needham-Schroeder Protocol - Step by Step

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

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

- S sends A a message encrypted by K_{AS}.
- The message contains a ticket for B, encrypted by K_{BS} – so that A cannot read it.
- Beside the ticket, the message contains nonce N_A such that A will know that S replied to its asking for K_{AB}. Moreover, the nonce N_A might be useful against a replay attack?
- Also, there's B – this could notice A that K_{AB} is supposed to be A's desired key. Is it redundant, since N_A is also present? Note that the ticket intended for B also contains the identity of A.

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

- A sends B the ticket it has just received from S.
- Note that the ticket includes A – in order for B to understand what K_{AB} is for.

The Needham-Schroeder Protocol - Step by Step

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

- 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 (but only B would know 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.
- Question: wouldn't it be just as well for A to reply with the same N_B? Why the need for changing it? Preventing ping-pong!
- "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 Otway-Rees Protocol

Let A and B be two principals, M, N_A and N_B be nonces generated by the principals, and K_{AB} a key generated by the server S.

The Otway-Rees Protocol

A non-formal description of the protocol (BAN1989, p. 14) is the following:

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

The Otway-Rees Protocol: In Slow(er) Motion

Let A and B be two principals, M, N_A and N_B be nonces generated by the principals, and K_{AB} a key generated by the server S.

Step 1. $A \longrightarrow B: \quad M, A, B, \{N_A, M, A, B\}_{K_{AS}}$

What happens here:

- Principal A sends both encrypted and non-encrypted information to B. Note that the first occurences of M, A, B are *cleartext*!
- Wonder why A sends M, A, B in both encrypted and non-encrypted way? Me too. Note that B will not be able to understand anything encrypted with K_{AS}. Cf. BAN(1989, p. 14): the non-encrypted info is "enough information for B to make up a similar encrypted message".
- The reason will be clear in the following steps! Perhaps not only idealization is holistic, but also protocol specification in the non-formal (non-BAN) way.

The Otway-Rees Protocol: In Slow(er) Motion

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

- B sends a similar message to the server.
- Without the non-encrypted info received from A, it would not have been able to concoct the message.
- Oorschot (1994): S used the cleartext A and B parts in order to identify the keys necessary for decrypting the messages (i.e. K_{AS} and K_{BS}).
- Before offering a reply, S checks whether "the components M, A, and B match in the encrypted messages" (BAN1989a, p. 14). So S checks whether the last three components of the two messages are identical (nonces N_A and N_B cannot be identical). If they are, jump to step 3:

The Otway-Rees Protocol: In Slow(er) Motion

Step 3. $S \longrightarrow B: \ \{N_A, K_{AB}\}_{K_{AS}}, \{N_B, K_{AB}\}_{K_{BS}}$

- S generates a key for A and B and sends two tickets two B. Each ticket contains the key and the nonce that the intended recipient has generated earlier (Steps 1 and 2).
- Note that S has sent B a message that it can understand (encrypted with K_{BS}) and that contains the nonce N_B (same for A's message!). Why is that? Without N_B, B would not know what K_{AB} is for.
- Without the nonce: "I've received a key, but with whom am I to use it?!"
- Even worse: "I've received something from S, but I don't know what it is". Note that only us, as descriptors of the protocol, know the intended meaning of the message!
- With the nonce: "I've received something, a key, and I know that I'm supposed to use it with A, since N_B is what I sent the server in order to send me a key to talk to A".

The Otway-Rees Protocol: In Slow(er) Motion

Step 4. $B \longrightarrow A: \ \{N_A, K_{AB}\}_{K_{AS}}$

- After both principals received their tickets, they decrypt their message and check the nonces.
- Why check the nonces? (1) Make sure that they are the intended recipients of the message sent by the server. (2) Make sure that what they have received is what they have requested. (3) In order to prevent replay attacks (Oorschot 1994).

The Otway-Rees Protocol

Note the following:

- Cleartext information is used by the server in order to ”retrieve the keys K_{AS} and K_{BS}" (van Oorschot 1994). Without the cleartext, S would not know with what to decrypt B's message; unless trying all K_{xS} (for x a principal) keys.
- Cleartext information is used by B in order to produce a similar message with A. The consequences of not sending a similar message are dire: S will not issue a key if the components of the messages are not identical (except for the nonces N_A and N_B).
- Nonces are used to prevent replays.
- In steps 3 and 4, without the right nonces, the agents would not know what K_{AB} is for. Analogy: ordering a pizza and finding a strange package on your doormat 30 minutes later. Is the package the reply to your request or something else?

Note the following

Note

It seems that the following holds:

- (1) Premise: A knows *that* (A sent at t1 message N_A)
- (2) Premise: A knows *that* (A received at t2 from S a message $(K_{AB} \wedge N_A)$)
- (3) Conclusion: A knows *what* K_{AB} is.

BAN (1989, p. 15): "when A receives N_A and K_{AB} he can deduce that the key K_{AB} is intended for use in talking to B, because the nonce N_A appears both in this message and in A's request for such a key."

Question. Understanding the role of nonces

The following two protocols have the following aim: A wants to receive from S a key for talking to B. S sends K_{AB}, but it most let A know that whatever it sent is indeed a key for talking to B. This can be done by either sending back A and B, or N_A.

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

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

The Otway-Rees Protocol supports Variant 2. But why?
Possible answer: Imagine A receives a key. But is it the key that A requested at time t_n or a key that was released on a previous run of the protocol, at $t_{k<n}$? Of course, A wants the new key, unless coping with the danger of receiving an already compromised key.

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 - Constructs (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.
- $P \triangleleft X$: Agent P sees message X.
- $P \mid\sim X$: Agent P has said that X (not necessarily during the current run of the protocol!). It is not known whether P said X during the current run of the protocol, but at the moment P said X, P also believed that X.
- $P \mid\Rightarrow X$: Agent P has jurisdiction over X (should be trusted regarding X).
- $\sharp(X)$: X is a fresh message (has not been sent before the run of the current protocol). Note: if P knows that Q said X and X is *fresh*, then P is entitled to believe that Q still believes that X.

BAN Language - Constructs (2)

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

- $P \overset{K}{\longleftrightarrow} Q$: 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, p. 4).

- $\overset{K}{\mapsto} P$: K is a public key of P. Recall that K^{-1} is P's secret key.
- $P \overset{X}{\rightleftharpoons} Q$: 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.
- $\langle X \rangle_Y$: formula X is combined (concatenated) with formula Y. If P sees $\langle X \rangle_Y$ and knows that Y is a secret between P and Q, then P would know who is the sender.

BAN Logic: Inference Rules

The following rules state the conditions under which a principal can infer the originator of a message she has received (Syverson & Cervesato 2001).

(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:

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

(3) Message meaning rules for shared secrets:

$$MM - SS \quad \frac{P \mid\equiv Q \overset{Y}{\rightleftharpoons} P, P \triangleleft \langle X \rangle_Y}{P \mid\equiv (Q \mid\sim X)}$$

BAN Logic: Inference Rules

Question

What is the difference between the following:

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

$$MM - SS \quad \frac{P \mid\equiv Q \rightleftharpoons^{Y} P, P \triangleleft \langle X \rangle_Y}{P \mid\equiv (Q \mid\sim X)}$$

Answer

Note that:

- Note that K is a shared key, whereas Y is a shared secret. K and Y are of different sorts: keys vs. messages.
- Note that in $MM - SK$ message X is *encrypted* by key K, whereas in $MM - SS$, Y is *concatenated* with message X

BAN Logic: Inference Rules

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

The nonce-verification rule:

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

- **Intuition**. Note that if the message is not fresh, we may be in the situation of someone who has found an SOS message in a bottle. Would it be wise to start a rescuing mission? Only if the sender is still in distress.

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

The jurisdiction rule:

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

BAN Logic: Inference Rules

The jurisdiction rule:

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

- **Intuition**. 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.

Belief and components:

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

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

BAN Logic: Inference Rules

Seeing and components:

$$SC1\ \frac{P \triangleleft (X, Y)}{P \triangleleft X} \qquad SC2\ \frac{P \triangleleft \langle X \rangle_Y}{P \triangleleft X}$$

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

$$SC5\ \frac{P \mid\equiv \mapsto^K Q, P \triangleleft \{X\}_{K^{-1}}}{P \triangleleft X}$$

Note that the following is **not** an inference rule, since it would mean that seeing X and seeing Y implies seeing both of them at the same time (BAN1990, p. 22):

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

BAN Logic: Inference Rules

Nonces concatenation

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

Intuition: "If one part of a formula is fresh, then the entire formula must also be fresh" (BAN1989, p. 8)

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:

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

Delegations

Principal A *delegates* S to offer a shared key for safely exchanging messages with B:

- $A \mid\equiv S \mid\Rightarrow A \leftrightarrow^{K} B$
- $A \mid\equiv \forall K.(S \mid\Rightarrow A \leftrightarrow^{K} B)$

Remark

Note that the *scope* of the universal quantifier matters (BAN1989, p.9):

- $A \mid\equiv \forall K.(S \mid\Rightarrow B \mid\Rightarrow A \leftrightarrow^{K} B)$
- $A \mid\equiv S \mid\Rightarrow \forall K.(B \mid\Rightarrow A \leftrightarrow^{K} B)$
  Compare with:
- $\exists x K_A(culprit(x))$
- $K_A \exists x(culprit(x))$

van Oorschott (1994) on verifying protocols using BAN

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

- Idealizing the protocol. The output of idealizing the protocol is a sequence S^* of steps $A \longrightarrow B : X$, for principals A and B and X a formula in the language of BAN.
- Identifying and formalizing the assumptions of the protocol. 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. Call this set of assumptions Q.
- Identifying the goals of the protocol. Example: A's knowing that key K is safe for talking to B: $A \mid\equiv A \leftrightarrow^{K} B$.
- Deriving G from Q and S^*. The output should be a proof of form $Q.S^*.G$.

Some Notes on Idealization

- 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. Why?

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

- Take a real message m. How do we interpret it in a BAN formula X. A BAN formula X in the idealized protocol = what the recipient believes (as a result of deduction) the sender believed when sending m.

> "Roughly, a real message m can be interpreted as a formula X if whenever the recipient gets m he may deduce that the sender must have believed X when he sent m." (BAN1989a, p. 10)

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):

$$\exists K : A \mid\equiv A \leftrightarrow^{K} B \text{ and } B \mid\equiv A \leftrightarrow^{K} B$$

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

$$\exists K : (A \mid\equiv A \leftrightarrow^{K} B) \wedge (A \mid\equiv A \leftrightarrow^{K} B) \wedge (A \mid\equiv B \mid\equiv A \leftrightarrow^{K} B) \wedge (B \mid\equiv A \mid\equiv A \leftrightarrow^{K} B)$$

- (3) Common belief in the goodness of the key is established. However:

...common belief in the goodness of K is never required - that is, A and B need not believe that they both believe that they both believe that... they both believe that k is good” (BAN1989a, p. 13)

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

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

- First 5 assumptions are easy to understand: they simply inform us on what the principals know regarding the keys that they should use.
- Assumption 12 is needed in order to derive that B knows the key K_{AB}: see step 19 in the proof below.

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
(2)	$A \mid\equiv A \leftrightarrow^{K_{AS}} S$	Assumptio
(3)	$S \mid\equiv S \mid\sim (N_A, (A \leftrightarrow^{K_{AB}} B), \sharp(A \leftrightarrow^{K_{AB}} B), \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}})$	MM-SK: 1
(4)	$A \mid\equiv \sharp(N_A)$	Assumptio
(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
(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 $\surd$
(9)	$A \mid\equiv S \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$	BC3: 6 $\surd$
(10)	$A \mid\equiv S \mid\equiv \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}$	BC3: 6
(11)	$A \mid\equiv S \mid\Rightarrow A \leftrightarrow^{K} B$	As. 6
(12)	$A \mid\equiv S \mid\Rightarrow \sharp(A \leftrightarrow^{K} B)$	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
(16)	$B \triangleleft \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}$	Step 3

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

Some conclusions

Goals and Interesting Derivations

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

(As 19) $B \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$

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

- Better than Otway-Rees: both A and B will be sure that the other still exists! Recall that in Otway-Rees we were only able to derive that $B \mid\equiv A \mid\sim N_C$
- Better than Otway-Rees: not only that both principals will know the key, both will know that they both know the key!

Some conclusions

Goals and Interesting Derivations

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

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

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

(As 19) $B \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B$

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

(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.

Some conclusions

- 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.
- BAN(1989a, p. 21): This is not an argument against using BAN, but an argument against using Needham-Schroeder! Why? Their reasoning seems to be the following:

> If proving a certain goal using BAN entails assuming that A, then the non-formal specification of the protocol *also* uses assumption A.

- So an analysis using BAN might be useful in making explicit some tacit assumptions of the protocol.

Some conclusions: Vulnerabilities

Vulnerability: Replay Attacks

Deriving that principal B knows the key is conditioned by assuming that B takes the key to be fresh. If B takes the key to be fresh, then, "an intruder has unlimited time to find an old session key and reuse it as though it were fresh" (BAN1989a, p. 21; the observation is due to Denning and Sacco (1981), as the authors of BAN note).

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

Denning-Sacco Protocol

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

Why finding a semantics for BAN logic is important

- Note that we are told that there is no proof of $B \mid\equiv A \leftrightarrow^{K_{AB}} B$ if we are not to assume 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.

The idealized Otway-Rees Protocol

Idealized Protocol, cf. BAN (1989a), p. 15

$$
\begin{array}{lll}
\text{Step 1.} & A \longrightarrow B: & \{N_A, N_C\}_{K_{AS}} \\
\text{Step 2.} & B \longrightarrow S: & \{N_A, N_C\}_{K_{AS}}, \{N_B, N_C\}_{K_{BS}} \\
\text{Step 3.} & S \longrightarrow B: & \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C)\}_{K_{AS}} \\
 & & \{N_B, (A \leftrightarrow^{K_{AB}} B), (A \mid\sim N_C)\}_{K_{BS}} \\
\text{Step 4.} & B \longrightarrow A: & \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C)\}_{K_{AS}}
\end{array}
$$

The idealized protocol. In slow(er) motion

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

- The cleartext components M, A and B are dropped: "we omit cleartext communication throughout, since it provides no guarantees of any kind" (BAN 1989a, p. 15).
- Components M, A and B are replaced with a nonce N_C.
- Recall that A and B need to send similar messages to S. This condition is met, since they send the same N_C!
- **Objection**: but A does not send B whatever it takes to make up a similar message! **Reply**: the idealized protocol states what the agents come to believe as a result of the message exchange in the non-idealized protocol, not the message exchange *per se*.

"a real message m can be interpreted as formula X if whenever the recipient gets m he may deduce that the sender must have believed X when he sent m" (BAN 1989a, p. 10)

The idealized protocol. In slow(er) motion

$$\begin{array}{lll}
\text{Step 3.} & S \longrightarrow B: & \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C)\}_{K_{AS}} \\
 & & \{N_B, (A \leftrightarrow^{K_{AB}} B), (A \mid\sim N_C)\}_{K_{BS}} \\
\text{Step 4.} & B \longrightarrow A: & \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C)\}_{K_{AS}}
\end{array}$$

- The reason behind the first two components is easy to understand. Sending N_B to B makes it know what K_{AB} is for & that it is a reply to its initial request. Redundant, since $A \leftrightarrow^{K_{AB}} B$? No! Only we know what $A \leftrightarrow^{K_{AB}} B$ is.
- Recall that $A \leftrightarrow^{K_{AB}} B$ is read *P and Q may use key K_{AB} to communicate*.
- Why $B \mid\sim N_C$ and $A \mid\sim N_C$ in steps 3 and 4?

"These do not appear to correspond to anything in the concrete protocol; they represent the fact that the messages are sent at all, because if the common nonces had not matched nothing would ever have happend." (BAN 1989a, p. 16).

The idealized protocol. In slow(er) motion

$$
\begin{array}{lll}
\text{Step 3.} & S \longrightarrow B: & \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C)\}_{K_{AS}} \\
 & & \{N_B, (A \leftrightarrow^{K_{AB}} B), (A \mid\sim N_C)\}_{K_{BS}} \\
\text{Step 4.} & B \longrightarrow A: & \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C)\}_{K_{AS}}
\end{array}
$$

- Why $B \mid\sim N_C$ and $A \mid\sim N_C$?

"These do not appear to correspond to anything in the concrete protocol; they represent the fact that the messages are sent at all, because if the common nonces had not matched nothing would ever have happend." (BAN 1989a, p. 16).

- Note that in step 3: (1) S mentions to A that B has said the same nonce as it did, and (2) S mentions to B that A has the same nonce.
- Note step 4: after A comes to believe that B has said N_C, A comes to know what K_{AB} is for! This is not already explicitly contained in $A \leftrightarrow^{K_{AB}} B$.

The Ottway-Rees Protocol: Assumptions

Assumptions of the Otway-Rees Protocol. See BAN (1989, p. 14)

(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) $B \mid\equiv (S \mid\Rightarrow A \leftrightarrow^{K} B)$

(8) $A \mid\equiv (S \mid\Rightarrow (B \mid\sim X))$ (9) $B \mid\equiv (S \mid\Rightarrow (A \mid\sim X))$

(10) $A \mid\equiv \sharp(N_A)$ (11) $B \mid\equiv \sharp(N_B)$

(12) $A \mid\equiv \sharp(N_C)$

- First 5 formulas state the shared keys between the principals.
- 6–9 state that A and B trust S to issue a good key and to correctly report what the other said.
- 10-12 state what A and B consider to be fresh.

The Ottway-Rees Protocol: Proving Goals

After step 3:

(1) $B \triangleleft \{N_B, (A \leftrightarrow^{K_{AB}} B), (A \mid\!\sim N_C))\}_{K_{BS}}$ (Step 3)

(2) $B \mid\equiv B \leftrightarrow^{K_{BS}} S$ (Assumption 2)

(3) $B \mid\equiv S \mid\!\sim (N_B, (A \leftrightarrow^{K_{AB}} B), (A \mid\!\sim N_C))$ (MM-SK: 1 and 2)

(4) $B \mid\equiv \sharp N_B$ (Assumption 11)

(5) $B \mid\equiv \sharp(N_B, (A \leftrightarrow^{K_{AB}B}), (A \mid\!\sim N_C))$ (NC: 4)

(6) $B \mid\equiv S \mid\equiv (N_B, (A \leftrightarrow^{K_{AB}} B), (A \mid\!\sim N_C))$ (NV: 3, 5)

(7) $B \mid\equiv S \mid\equiv N_B$ (BC3: 6)

(8) $B \mid\equiv S \mid\equiv A \leftrightarrow^{K_{AB}} B$ (BC3: 6)

(9) $B \mid\equiv S \mid\equiv A \mid\!\sim N_C$ (BC3: 6)

(10) $B \mid\equiv S \mid\Rightarrow A \mid\!\sim N_C$ (Assumption 9)

(11) $B \mid\equiv S \mid\Rightarrow A \leftrightarrow^{K_{AB}} B$ (Assumption 7)

(12) $B \mid\equiv A \leftrightarrow^{K_{AB}} B$ (JR: 8, 11) $\surd$

(13) $B \mid\equiv A \mid\!\sim N_C$ (JR: 9, 10) $\surd$

The Ottway-Rees Protocol: Proving Goals

After step 4:

(1)	$A \triangleleft \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C)\}_{K_{AS}}$	(Step 4)
(2)	$A \mid\equiv A \leftrightarrow^{K_{AS}} S$	(Assumption 1)
(3)	$A \mid\equiv S \mid\sim (N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C))$	(MM-SK: 1 and 2)
(4)	$A \mid\equiv \sharp N_A$	(Assumption 10)
(5)	$A \mid\equiv \sharp(N_A, (A \leftrightarrow^{K_{AB}B}), (B \mid\sim N_C))$	(NC: 4)
(6)	$A \mid\equiv S \mid\equiv (N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C))$	(NV: 3, 5)
(7)	$A \mid\equiv S \mid\equiv N_A$	(BC: 6)
(8)	$A \mid\equiv S \mid\equiv A \leftrightarrow^{K_{AB}} B$	(BC: 6)
(9)	$A \mid\equiv S \mid\equiv B \mid\sim N_C$	(BC: 6)
(10)	$A \mid\equiv S \mid\Rightarrow B \mid\sim N_C$	(Assumption 8)
(11)	$A \mid\equiv S \mid\Rightarrow A \leftrightarrow^{K_{AB}} B$	(Assumption 6)
(12)	$A \mid\equiv A \leftrightarrow^{K_{AB}} B$	(JR: 8, 11) $\surd$
(13)	$A \mid\equiv B \mid\sim N_C$	(JR: 9, 10)
(14)	$A \mid\equiv \sharp(N_C)$	(Assumption 12)
(15)	$A \mid\equiv B \mid\equiv N_C$	(JR: 13, 14) $\surd$

The Ottway-Rees Protocol: Proving Goals

In the proofs above we have arrived at:

(1) $A \mid\equiv A \leftrightarrow^{K_{AB}} B$	(2) $B \mid\equiv A \leftrightarrow^{K_{AB}} B$
(3) $A \mid\equiv B \mid\equiv N_C$	(4) $B \mid\equiv A \mid\sim N_C$

- **Question**: Are (1) and (2) sufficient?
- **Answer**: No, since although both principals have knowledge of the key, neither knows whether the other knows it (BAN1989, p. 17). What we would need in addition:
- A proof that $A \mid\equiv B \mid\equiv A \leftrightarrow^{K_{AB}} B$ and $B \mid\equiv A \mid\equiv A \leftrightarrow^{K_{AB}} B$. What about common belief? The authors of BAN think that:

"However, common belief in the goodness of K is never required - that is, A and B need not believe that they both believe that they both believe that... they both believe that K is good. Some protocols may attain only weaker goals, as for example $A \mid\equiv B \mid\equiv X$, for some X, which reflects only that A believes that B has recently sent messages and exists at present." (BAN1989a, p. 13)

The Ottway-Rees Protocol: Proving Goals

In the proofs above we have arrived at:

(1) $A \mid\equiv A \overset{K_{AB}}{\leftrightarrow} B$	(2) $B \mid\equiv A \overset{K_{AB}}{\leftrightarrow} B$
(3) $A \mid\equiv B \mid\equiv N_C$	(4) $B \mid\equiv A \mid\sim N_C$

- **Question**: Are (1) and (2) sufficient?
- **Answer**: No, since although both principals have knowledge of the key, neither knows whether the other knows it (BAN1989, p. 17). What we would need in addition:
- A *handshake* between A and B. However, it is not clear whether it is possible, since it would imply using K_{AB}, and neither knows whether the other knows it (cf. BAN1989b, p. 335).

The Ottway-Rees Protocol: Proving Goals

In the proofs above we have arrived at:

(1) $A \mid\equiv A \leftrightarrow^{K_{AB}} B$ (2) $B \mid\equiv A \leftrightarrow^{K_{AB}} B$
(3) $A \mid\equiv B \mid\equiv N_C$ (4) $B \mid\equiv A \mid\sim N_C$

- Principal B is at a loss: it does not know whether N_C is fresh or not, i.e. whether the message containing N_C is a *replay*.
- Moreover, it is conceivable, for B, that A does not exist anymore, since any trace of A's existence is not guaranteed to be *fresh*. Much like finding an SOS message in a bottle and finding yourself in the position of not knowing whether it nowadays makes sense to start a rescuing mission.

"A is in a slightly better position that B, in that A has been told that B emitted a message containing a nonce that A believes to be fresh. This allows A to infer that B has sent a message recently - B exists. B has been told by the server that A has used a nonce, but B has no idea whether this is a replay of an old message or not."
(BAN1989a, p. 17)

The Ottway-Rees Protocol: Proving Goals

- The authors of BAN (1989a, p. 17) claim that A's generating nonce N_A is redundant and that the goals could have been proven only using N_C. However, let's see the result of not using nonce N_A:

(1)	$A \triangleleft \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C))\}_{K_{AS}}$	(Step 4)
(2)	$A \mid\equiv A \leftrightarrow^{K_{AS}} S$	Assumption 1
(3)	$A \mid\equiv S \mid\sim (N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C))$	MM-SK: 1,2
(4)	$A \mid\equiv S \mid\sim N_A$	BC4: 3
(5)	$A \mid\equiv S \mid\sim A \leftrightarrow^{K_{AB}} B$	BC4: 3
(6)	$A \mid\equiv S \mid\sim (B \mid\sim N_C)$	BC4: 3
(7)	$A \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$	EXTRA ASSUMPTION!
(8)	$A \mid\equiv S \mid\equiv A \leftrightarrow^{K_{AB}} B$	NV: 5, 7
(9)	$A \mid\equiv S \mid\Rightarrow A \leftrightarrow^{K_{AB}} B$	Assumption 6
(10)	$A \mid\equiv A \leftrightarrow^{K_{AB}} B$	JR: 7,8.

(1)	$A \triangleleft \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C))\}_{K_{AS}}$	(Step 4)
(2)	$A \mid\equiv A \leftrightarrow^{K_{AS}} S$	Assumption 1
(3)	$A \mid\equiv S \mid\sim (N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C))$	MM-SK: 1,2
(4)	$A \mid\equiv S \mid\sim N_A$	BC4: 3
(5)	$A \mid\equiv S \mid\sim A \leftrightarrow^{K_{AB}} B$	BC4: 3
(6)	$A \mid\equiv S \mid\sim (B \mid\sim N_C)$	BC4: 3
(7)	$A \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$	EXTRA ASSUMPTION!
(8)	$A \mid\equiv S \mid\equiv A \leftrightarrow^{K_{AB}} B$	NV: 5, 7
(9)	$A \mid\equiv S \mid\Rightarrow A \leftrightarrow^{K_{AB}} B$	Assumption 6
(10)	$A \mid\equiv A \leftrightarrow^{K_{AB}} B$	JR: 7,8.

- Without using the EXTRA ASSUMPTION at line (7), A would not be in the position to know that key K_{AB} is good for exchanging messages with B.
- Why is that? It is not sufficient to be told that P in order to believe that P. No, in advance, you need to know that P is fresh. Recall the message in a bottle analogy.

Some conclusions regarding BAN logic

Knowledge of a principal's existence

Apparently, $A \mid\equiv B \mid\equiv X$ (for any X) implies that A knows that B exists, but $A \mid\equiv B \mid\sim X$ is consistent with A not believing that B exists (any longer). Why is that?

(A) It seems that it is assumed that whatever is believed is fresh, whereas what is said may not be.

(B) it seems that it is assumed that whatever is believed to be believed is fresh, whereas what is believed to be said may not be.

It seems somewhat justified, since only freshness guarantees an inference from what is believed to have been said to what is believed to be believed.

From fresh belief to true belief

Note that $A \mid\equiv \sharp(T_S)$ (assumption 8), but we cannot derive that $A \mid\equiv T_S$. At line 7, although we have that $A \mid\equiv S \mid\equiv T_S$, we cannot derive knowledge of the nonce since A does not fully trust S, i.e. $A \mid\equiv S \mid\Rightarrow X$ is not assumed. Likewise for $B \mid\equiv \sharp T_S$ and $B \mid\equiv T_S$.

Some conclusions regarding BAN logic

Belief, not true belief

Recall the analysis on the Needham-Schroeder Protocol. As the BAN authors suggest, it is a vulnerability to **assume** that the key is a nonce. This, since an attacker might have caught an old session key. A consequence is that we should not understand the $|\equiv$ operator as meaning *true belief*, but mere belief (that can be false).

Some conclusions regarding BAN logic

On the use of BAN logic

One use of BAN logic can be highlighted by exposing the following argument (underlying the analysis of the Needham-Schroeder Protocol).

- (1) Idealize the protocol in BAN language.
- (2) Try to derive a certain intuitive goal of a protocol.
- (3) Supppose the derivation is not possible unless an assumption A is made.
- (4) The non-idealized protocol uses that assumption.
- (5) If the idealized protocol is vulnerable because of A, then the non-idealized protocol is vulnerable because of A.

This use of BAN logic invites for a discussion on the very idea of idealizing protocols.

- Are there rules for correct idealization?
- What is correct idealization?

Some conclusions regarding BAN logic

Let *Prot* be a set of assumptions and the messages in the idealized protocol. Suppose you want to prove that you cannot derive a certain goal from *Prot*. How can this be accomplished?

- $\mathit{Prot} \nvdash \mathit{Goal} \Leftrightarrow \mathit{Prot} \vdash \neg \mathit{Goal}$. But BAN does not have negation. Can it be recovered from the rules? (does it make sense?)
- $\mathit{Prot} \nvdash \mathit{Goal} \Leftrightarrow \mathit{Prot} \not\models \mathit{Goal}$. But it is not clear whether BAN has a suitable semantics.

So: (1) try to define negation or recover it from the apparatus as it is (?) or (2) find a suitable semantics.

Question. Understanding the role of nonces

The following two protocols have the following aim: A wants to receive from S a key for talking to B. S sends K_{AB}, but it most let A know that whatever it sent is indeed a key for talking to B. This can be done by either sending back A and B, or N_A.

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

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

The Otway-Rees Protocol supports Variant 2. But why?
Possible answer: Imagine A receives a key. But is it the key that A requested at time t_n or a key that was released on a previous run of the protocol, at $t_{k<n}$? Of course, A wants the new key, unless coping with the danger of receiving an already compromised key.

Teepe's (2009) objection to BAN logic

Teepe's Objection

BAN logic is not sound, i.e. one can prove false statements using the inference rules of BAN Logic.

Question

How can I persuade X that I'm in possession of file F, but I do not want to send it.

Answer

Then, I can simply send the *hash value* of that file (Schneier (1990, p.31) *apud* Teepe (2009, p. 77)).
A hash function is a one-way function, i.e. one whose inverse is not computable.

Teepe (2009, p. 78): WRONG ANSWER! Why: if someone else comes into possession of the hash value of F, then s/he can also persuade anyone of their possessing the file itself!

BAN Logic: Reasoning about Hash Functions

In the following slides we will need the following BAN inference rules, so it's better to get reacknowledged with them.

BAN rule for reasoning about Hash function (BAN1989a, p. 42)

$$H \quad \frac{P \mid\equiv (Q \mid\sim H(X)), P \triangleleft X}{P \mid\equiv (Q \mid\sim X)}$$

Message meaning rules for public keys:

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

The nonce-verification rule:

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

The Two Parrots Protocol

The Two Parrots Protocol

Step 1	$A \rightarrow C$:	N
Step 2	$C \rightarrow A$:	N
Step 3	$A \rightarrow B$:	H(N)
Step 4	$B \rightarrow A$:	$\{H(N)\}_{K^{-1}}$

- As we can see in the Two Parrots Protocol, B is not supposed to know N. This, since B only gathers, from A, the hash value of N, but not N itself. As such, it is unreasonable for A to know that B knows N. As such, the following BAN formula should not be derivable: $A \mid\equiv B \mid\equiv N$.
- What Teepe (2009, p. 82) proves is that using BAN logic we can derive that: $A \mid\equiv B \mid\equiv N$, i.e. that A will think of B as knowing the value of N itself.

Teepe's (2009), p. 82 proof

1.	$A \mid\equiv \mapsto^{K} B$	Assumption 1
2.	$A \mid\equiv N$	Assumption 2
3.	$A \mid\equiv \sharp(N)$	Assumption 3
4.	$A \triangleleft N$	Step 2
5.	$A \triangleleft \{H(N)\}_{K^{-1}}$	Step 4
6.	$A \mid\equiv B \mid\sim H(N)$	MM-PK: 1,5
7.	$A \mid\equiv B \mid\sim N$	H: 4,6
8.	$A \mid\equiv B \mid\equiv N$	NV: 3, 7

- As such, a false statement is derived using BAN inference rules from true assumptions.

Boyd & Mao (1994): Objection 1

- Another objection to BAN logic stems from not being able to predict a certain attack on the Otway-Rees protocol. Recall the protocol:

Step 1.	$A \longrightarrow B$:	$M, A, B, \{N_A, M, A, B\}_{K_{AS}}$
Step 2.	$B \longrightarrow S$:	$M, A, B, \{N_A, M, A, B\}_{K_{AS}}, \{N_B, M, A, B\}_{K_{BS}}$
Step 3.	$S \longrightarrow B$:	$\{N_A, K_{AB}\}_{K_{AS}}, \{N_B, K_{AB}\}_{K_{BS}}$
Step 4.	$B \longrightarrow A$:	$\{N_A, K_{AB}\}_{K_{AS}}$

- But an attacker C may impersonate B after intercepting the first message (step 1), creating the similar message and generating a personal nonce N_C:

Step 1.	$A \longrightarrow B$:	$M, A, B, \{N_A, M, A, B\}_{K_{AS}}$
Step 2.	$C \longrightarrow S$:	$M, A, C, \{N_A, M, A, B\}_{K_{AS}}, \{N_C, M, A, B\}_{K_{CS}}$
Step 3.	$S \longrightarrow C$:	$\{N_A, K_{AB}\}_{K_{AS}}, \{N_C, K_{AB}\}_{K_{CS}}$
Step 4.	$C \longrightarrow A$:	$\{N_A, K_{AB}\}_{K_{AS}}$

Boyd & Mao (1994): Objection 1

$$\begin{array}{lll}
\text{Step 1.} & A \longrightarrow B: & M, A, B, \{N_A, M, A, B\}_{K_{AS}} \\
\text{Step 2.} & C \longrightarrow S: & M, A, C, \{N_A, M, A, B\}_{K_{AS}}, \{N_C, M, A, B\}_{K_{CS}} \\
\text{Step 3.} & S \longrightarrow C: & \{N_A, K_{AB}\}_{K_{AS}}, \{N_C, K_{AB}\}_{K_{CS}} \\
\text{Step 4.} & C \longrightarrow A: & \{N_A, K_{AB}\}_{K_{AS}}
\end{array}$$

Wherein lies the vulnerability?

- S issues the key after checking only whether M, A and B appear in both encrypted messages!
- S could figure out the impersonation if, after step 2, would check whether M, A and B are the same with cleartext M, A and C.
- Note that a vulnerable protocol may be idealized into a protocol that can be proved as sound using BAN inference rules.
- Recall that BAN (1989a) deemed the cleartext messages as useless. They are not: if the server would have checked the identity of encrypted M, A, B with cleartext M, A and C, it would've realized the impersonation.

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.

- 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.

References II

- 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.

- 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.

References III

- 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.

- 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.