Special topics in Logic and Security I

Master Year II, Sem. I, 2025-2026

Ioana Leuștean
FMI, UB

October 22, 2025

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 (selection)

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*.
- $P \leftrightarrow^K Q$: Agents P and Q share key K and can communicate safely using it.
  Assumption: key K is *good*
- $\{X\}_K$: 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 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 *promotes* beliefs about some other principal's beliefs to one's beliefs:

The jurisdiction rule:

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

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

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.

Structural rules

...

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:
- assumptions about the initial state,
- assumptions for the steps of the protocol.

Call this set of assumptions Γ_0.

(3) Identifying the goal G of the protocol.

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

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:

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

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.
- M, A, B are *cleartext*.M is a session identifier and a common challenge. [Otway-Ress,1987]
  "In mutual authentication, both parties are suspicious of each other and of the freshness of the authentication messages; therefore each must generate independent challenges in order to assure themselves of the timeliness of the interaction."
- Note that B will not be able to understand anything encrypted with K_{AS}. The non-encrypted part contains "enough information for B to make up a similar encrypted message" [BAN,1989].

Understanding the Otway-Rees Protocol

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

- Using the non-encrypted info received from A, the principal B sends a similar message to the server.
- 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}) [van Oorschot, 1994].
- N_A and N_B are the challenges generated by each party and M is a common challenge.
- Before offering a reply, S checks whether "the components M, A, and B match in the encrypted messages" [BAN1989a] (i.e. both contain M, A, B).

Understanding the Otway-Rees Protocol

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

- 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). In this way B knows that K_{AB} is a good key for him and A.

Understanding the Otway-Rees Protocol

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

- After both principals received their tickets, they decrypt their message and check the nonces. In this way, they

  (1) are sure that they are the intended recipients of the message sent by the server,

  (2) are sure that what they have received is what they have requested.

The idealized protocol - notes on cleartext

- "M must be in clear to allow the second party to encipher it. It may also be used to associate all the messages in the same authentication sequence and may be an identifier used in the underlying protocol layer. A, B must be in clear to identify the principals to the other parties , in particular, the authentication service needs them to look up the corresponding private keys." [Otway-Rees, 1987]
- "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, 1989]

The idealized protocol - notes on cleartext

- "M must be in clear to allow the second party to encipher it. It may also be used to associate all the messages in the same authentication sequence and may be an identifier used in the underlying protocol layer. A, B must be in clear to identify the principals to the other parties , in particular, the authentication service needs them to look up the corresponding private keys." [Otway-Rees, 1987]
- "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, 1989]
- The solution found in [BAN, 1989]:
  - The cleartext components M, A and B are dropped: "we omit cleartext communication throughout, since it provides no guarantees of any kind" [BAN, 1989].
  - Components M, A and B are replaced with a nonce N_C.
  - The principals A and B send N_C to S.
  - In Step 3, S sends the messages $B \mid\sim N_C$ 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 happened." [BAN,1989]

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

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 replaced by the nonce N_C, which is sent by both A and B.
- Note that in the idealized Step 1, the principal A does **not** send B the nonce N_C in clear. Actually, it does not send anything that might allow B to make up a similar message.

  The reason is the following:

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*.

The idealized protocol

Step 3. $S \longrightarrow B : \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C)\}_{K_{AS}}$
$\{N_B, (A \leftrightarrow^{K_{AB}} B), (A \mid\sim N_C)\}_{K_{BS}}$

Step 4. $B \longrightarrow A : \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C)\}_{K_{AS}}$

- Note that $A \leftrightarrow^{K_{AB}} B$ is sent as in NSSK protocol.
- In Step 3, sending $B \mid\sim N_C$ and $A \mid\sim N_C$, the server "informs" A that B has said the same nonce as it did, and "informs" B that A has said the same nonce.
- In Step 4, after A comes to believe that B has said N_C, A comes to know what K_{AB} is for.
- Note that the principals do not use K_{AB}, there is no handshake.

The Otway-Rees Protocol: Assumptions

Assumptions on the messages in the idealized protocol

Step 1. $B \triangleleft \{N_A, N_C\}_{K_{AS}}$

Step 2. $S \triangleleft \{N_A, N_C\}_{K_{AS}}, \{N_B, N_C\}_{K_{BS}}$

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

Step 4. $A \triangleleft \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C)\}_{K_{AS}}$

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

"It is interesting to note that this protocol does not make use of K_{AB} as an encryption key, so neither principal can know whether the key is known to the other. A is in a slightly better position than 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." [BAN1989]

- Note that, in this way, we proved another form of authentication: aliveness (for B).

The Ottway-Rees Protocol: Proving Goals

- The authors of [BAN, 1989] claim that A's generating nonce N_A is redundant and that the goals could have been proven only using N_C:

Idealized Protocol without N_A

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

The Ottway-Rees Protocol: Proving Goals

- Derivations without N_A

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

The Ottway-Rees Protocol: Proving Goals

In order to use the EXTRA ASSUMPTION from the previous slide, we can modify the idealized protocol as follows:

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

- Is this reasonable? In Step 3 it is since the message is received form the server. Is Step 4 susceptible to the same issues as in the analysis of the NSSK protocol (i.e. might some impersonator use an old session key, using a reply attack)?

  I would say that in this this case the EXTRA ASSUMPTION is reasonable since N_C is used as a replacement for M, A, B and M was intended to be an identifier for the current session.

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

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

Step 1. $A \longrightarrow B: \quad M, A, B, \{N_A, M, A, B\}_{K_{AS}}$
Step 2. $E \longrightarrow S: \quad M, A, E, \{N_A, M, A, B\}_{K_{AS}}, \{N_E, M, A, B\}_{K_{ES}}$
Step 3. $S \longrightarrow E: \quad \{N_A, K_{AB}\}_{K_{AS}}, \{N_C, K_{AB}\}_{K_{ES}}$
Step 4. $E \longrightarrow A: \quad \{N_A, K_{AB}\}_{K_{AS}}$

Boyd & Mao (1994): Objection

Step 1. $A \longrightarrow B : \quad M, A, B, \{N_A, M, A, B\}_{K_{AS}}$
Step 2. $E \longrightarrow S : \quad M, A, E, \{N_A, M, A, B\}_{K_{AS}}, \{N_E, M, A, B\}_{K_{ES}}$
Step 3. $S \longrightarrow E : \quad \{N_A, K_{AB}\}_{K_{AS}}, \{N_C, K_{AB}\}_{K_{ES}}$
Step 4. $E \longrightarrow A : \quad \{N_A, K_{AB}\}_{K_{AS}}$

Wherein lies the vulnerability?

- Recall that [BAN, 1989] deemed the cleartext messages as useless, so the vulnerable protocol may be idealized into a protocol that can be proved as sound using BAN inference rules.

Assumptions on the messages in the idealized protocol

Step 1. $B \triangleleft \{N_A, N_C\}_{K_{AS}}$
Step 2. $S \triangleleft \{N_A, N_C\}_{K_{AS}}, \{N_E, N_C\}_{K_{ES}}$
Step 3. $E \triangleleft \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C)\}_{K_{AS}}, \{N_E, (A \leftrightarrow^{K_{AB}} B), (A \mid\sim N_C)\}_{K_{ES}}$
Step 4. $A \triangleleft \{N_A, (A \leftrightarrow^{K_{AB}} B), (B \mid\sim N_C)\}_{K_{AS}}$

Understanding the Otway-Rees Protocol

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

[van Oorschot, 1994]
"Whether this attack is successful or not depends on the actions taken by the server S in Step 2:

- Case 1.1 S simply checks that the values obtained by decrypting the identifier fields (A, B) under the two different keys (K_{AS}, K_{BS}) in message 2 are equal. **In this case the attack will succeed.**
- Case 2. S checks that the values in the cleartext identifier fields (A, B) are equal to the values obtained by decrypting the corresponding identifier fields under each of the keys (K_{AS}, K_{BS}). **In this case the attack will not succeed. Clearly this is the desirable version of the protocol.**"

Understanding the Otway-Rees Protocol

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

[van Oorschot, 1994]
"Whether this attack is successful or not depends on the actions taken by the server S in Step 2:

- Case 1. S simply checks that the values obtained by decrypting the identifier fields (A, B) under the two different keys (K_{AS}, K_{BS}) in message 2 are equal. **In this case the attack will succeed.**
- Case 2. S checks that the values in the cleartext identifier fields (A, B) are equal to the values obtained by decrypting the corresponding identifier fields under each of the keys (K_{AS}, K_{BS}). **In this case the attack will not succeed. Clearly this is the desirable version of the protocol.**"

"It should be clear now that in Case 1 (i.e. the flawed version) of the protocol, this trust is ill-founded, and in fact S should not be trusted on statements regarding a shared key with B; however in Case 2 (i.e. the secure version), S is trustworthy on this matter."
Consequently, the assumptions $A \mid\equiv (S \mid\Rightarrow A \leftrightarrow^K B)$ and $B \mid\equiv (S \mid\Rightarrow A \leftrightarrow^K B)$ mean that **Case 2 is the valid one**.

Understanding the Otway-Rees Protocol

In [Sierra, Hernández, Alcaide, Torres, 2004] the authors note that, in the correct version of the protocol, after Step 2, we have the following derivations:

(1)	$S \triangleleft \{N_A, N_C\}_{K_{AS}}, \{N_B, N_C\}_{K_{BS}}$	(Step 2)
(2)	$S \mid\equiv B \leftrightarrow^{K_{BS}} S$	(Assumption 4)
(3)	$S \mid\equiv B \mid\sim N_C$	(MM-SK: 1 and 2)

However, in the flawed version one can only prove that $S \mid\equiv E \mid\sim N_C$!

We note that, even if this derivation is not actually used for proving the protocol goals, the logic reflects the situation correctly.

"We believe BAN logic foundations are valid. BAN logic represents a simple but sound and powerful tool to describe and validate authentication protocols. However we are also aware of the limitations of BAN's initial versions."
[Sierra, Hernández, Alcaide, Torres, 2004]

The Nesset Objection

The following protocol was defined in [Nesset, 1990], to demonstrate "that a significant flaw exists in the Burrows, Abadi and Needham logic".

The Nesset protocol

Step 1. $A \longrightarrow B : \{N_A, K_{AB}\}_{K_A^{-1}}$

Step 2. $B \longrightarrow A : \{N_B\}_{K_{AB}}$

Note that, in this case the $A \mid\equiv A \leftrightarrow^{K_{AB}} B$ and $A \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$ are reasonable assumptions. Under further natural assumptions and using a straightforward idealization, one can prove that $B \mid\equiv A \leftrightarrow^{K_{AB}} B$. Obviously, this is not true, since **the key is compromised** in the first step.

The Nesset Objection

The following protocol was defined in [Nesset, 1990], to demonstrate "that a significant flaw exists in the Burrows, Abadi and Needham logic".

The Nesset protocol

Step 1. $A \longrightarrow B : \{N_A, K_{AB}\}_{K_A^{-1}}$

Step 2. $B \longrightarrow A : \{N_B\}_{K_{AB}}$

Note that, in this case the $A \mid\equiv A \leftrightarrow^{K_{AB}} B$ and $A \mid\equiv \sharp(A \leftrightarrow^{K_{AB}} B)$ are reasonable assumptions. Under further natural assumptions and using a straightforward idealization, one can prove that $B \mid\equiv A \leftrightarrow^{K_{AB}} B$. Obviously, this is not true, since **the key is compromised** in the first step.

Burrows et al. respond to Nessett by noting that "there is no attempt to deal with the authentication of an untrustworthy principal". Consequently, the initial assumption $A \mid\equiv A \leftrightarrow^{K_{AB}} B$ is inconsistent with this point of view.

from absurd assumptions come absurd conclusions. The logic does not preclude ridiculous assumptions.

Thank you!

References I

Otway, D., Rees, O. (1987)

Effcient and Timely Mutual Authentication.

Operating Systems Review Vol. 21, No. 1, 8 – 10. 1987.

Burrows, M., Abadi. M., & Needham, R. (1989)

A Logic of Authentication.

SRC Research Report 39, 1 – 50, 1989; revised version 1990.

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

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.

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