Analysis and design of cryptographic protocols

Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
Email: gianluca.dini@unipi.it
Version: 2021-05-16

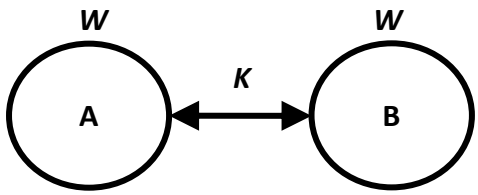
1

Preliminaries

ESTABLISHING A SESSION KEY

2

Establishing a session key



- A and B a priori share a long term key W
- A and B wants to establish a **session key** K

- Session key is used for bulk encryption
- A session key is used for one communication session
- Long term key is used for many runs of the key establishment protocols; in each run, the key encrypts a small amount of data

3

Establishing a session key

one-pass

$$M1 \quad A \to B: \quad E\left(W, t_A \,||\, "B,A" \,||\, K\right)$$

- t_A is a timestamp (a "fresh" quantity) that requires synchronized clocks

with challenge-response

$$M1 \quad A \neg B: \quad n_B$$
$$M2 \quad A \to B: \quad E_W\left(W, n_B \,||\, "A,B" \,||\, K\right)$$

- n_B is a nonce (a "fresh" quantity) e.g., a counter or a random number

both parties contribute to the session key

$$M1 \quad A \neg B: \quad n_B$$
$$M2 \quad A \to B: \quad E\left(W, K_A \,||\, n_B \,||\, n_A \,||\, "A,B"\right)$$
$$M3 \quad A \neg B \quad E\left(W, K_B \,||\, n_A \,||\, n_B \,||\, "B,A"\right)$$

- n_A and n_B are nonces
- K_A and K_B are keying materiale
- $K = K_A \oplus K_B$

4

Remember

Security protocols are three-line programs that people still manage to get wrong.

Roger M. Needham

5

Design and verification of security protocols

THE BAN LOGIC – FORMALISM AND POSTULATES

6

Main topics

- The BAN logic
- Design principles
- Case studies
  - Needham-Schroeder ➔ Kerberos, Active Directory
  - Otway-Rees
  - SSL (an old version)
  - …

The BAN logic

- After its inventors: Burrows, Abadi, Needham
- Logic based on *belief* and *action*
- How to use the logic
  - The logic cannot prove that a protocol is wrong
  - However, if you cannot prove a protocol correct, then consider that protocol with great suspicion

Google Scholar – all versions

- M. Burrows, M. Abadi, R.M, Needham, A Logic of Authentication, Symposium on Operating Systems Principles, 1989
- M. Burrows, M. Abadi, R.M, Needham, A Logic of Authentication, ACM Transactions on Computer Systems, 1990

9

Formalism

$P \mid\equiv X$	**P believes X**. P behaves as if X were true
$P \triangleleft X$	**P sees X**. P has received/read a message/file containing X, either in the past or in the present execution of the protocol. P can read X and repeat it
$P \mid\sim X$	**P once said X**. P sent/wrote X in a message/file. P believed X when P sent/wrote it.
$P \Rightarrow X$	**P controls X**. P is an authority on X and we should trust P on this regard
$\#(X)$	**X is fresh**
$P \overset{K}{\leftrightarrow} Q$	**K is a shared key between P e Q**

10

Formalism

$P \overset{K}{\leftrightarrow} Q$ X is a shared secret between P e Q

$\overset{K}{\mapsto} P$ K is P's public key

$\langle X \rangle_Y$ X is a combined with Y

$\{X\}_K$ X has been encrypted with K

11

Examples

$A \mid\equiv \#(N_a)$ A believes that N_a is fresh

$A \mid\equiv A \overset{K}{\leftrightarrow} B$ A believes K to be a shared key with B

$T \mid\equiv A \overset{K}{\leftrightarrow} B$ T believes that K is a shared key between A and B

$A \mid\equiv T \Rightarrow A \overset{K}{\leftrightarrow} B$ A believes T an authority on generating session keys

$A \mid\equiv T \Rightarrow \#\left(A \overset{K}{\leftrightarrow} B \right)$ A believes that T is competent in generating fresh session keys

12

Preliminaries

- BAN logic considers two epochs: the present and the past
- The present begins with the start of the protocol
- Beliefs achieved in the present are stable for all the protocol duration
- Assumption: If P says X then P believes X
- Beliefs of the past may not hold in the present

Postulates: message meaning rule

$$\frac{P \mid\equiv Q \overset{K}{\leftrightarrow} P, P \triangleleft \{X\}_K}{P \mid\equiv Q \mid\sim X}$$

If *K* is a shared key between *P* and *Q*, and *P* sees a message encrypted by *K* containing *X* (and P did not send that message), then *P* believes that *X* was sent by *Q*

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

If *K* is *Q*'s public key, and *P* sees a message signed by con K^{-1} containing *X*, then *P* believes that *X* was sent by *Q*

$$\frac{P \mid\equiv Q \overset{Y}{\rightleftharpoons} P, P \triangleleft \langle X \rangle_Y}{P \mid\equiv Q \mid\sim X}$$

If Y is a shared secrete between P and *Q*, and *P* sees a message where Y is combined with X (and P did not send the message), then*P* believes that *X* was sent by *Q*

Postulates: nonce verification rule

$$\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$$

- If *P* believes *Q* said *X* and P believes *X* is *fresh*, then *P* believes Q believes X (now, in this protocol execution)
- If *P* believes *X* was sent by *Q*, and *P* believes *X* is *fresh*, then *P* believes *Q* has sent *X* in this protocol execution instance

Postulates: jurisdiction rule

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

- If *P* believes *Q* believes *X* and *P* believes *Q* is an authority on *X*, then *P* believes *X too*
- If *P* believes *Q* says *X* and *P* trusts *Q* on *X*, then *P* believes *X* too

More postulates

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

$$\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$$

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

$$\frac{P|\equiv Q\overset{K}{\leftrightarrow}P,\quad P\lhd \{X\}_K}{P\lhd X} \qquad \frac{P|\equiv \overset{K}{\mapsto}P,\quad P\lhd \{X\}_K}{P\lhd X} \qquad \frac{P|\equiv \overset{K}{\mapsto}Q,\quad P\lhd \{X\}_{K^{-1}}}{P\lhd X}$$

$$\frac{P|\equiv R\overset{K}{\leftrightarrow}R'}{P|\equiv R'\overset{K}{\leftrightarrow}R} \qquad \frac{P|\equiv Q|\equiv R\overset{K}{\leftrightarrow}R'}{P|\equiv Q|\equiv R'\overset{K}{\leftrightarrow}R} \qquad \frac{P|\equiv R\overset{K}{\rightleftharpoons}R'}{P|\equiv R'\overset{K}{\rightleftharpoons}R} \qquad \frac{P|\equiv Q|\equiv R\overset{K}{\rightleftharpoons}R'}{P|\equiv Q|\equiv R'\overset{K}{\rightleftharpoons}R}$$

May 22 BAN Logic 17

17

Idealized protocol

In the *real protocol*, each protocol step is represented as

$$A\to B: message$$

For example:

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

This notations is ambiguous. Thus the protocol has to be *idealized*

$$A\to B:\left\{\overset{K_{ab}}{A\leftrightarrow B}\right\}_{K_{bs}}$$

The resulting specification is more clear and you can desume the formula

$$\overset{K_{ab}}{B\lhd A\leftrightarrow B}$$

May 22 BAN Logic 18

18

Protocol analysis

- Protocol analysis consists in the following steps
  1. Derive the idealized protocol from the real one
  2. Determine assumptions
  3. Apply postulates to each protocol step and determine beliefs achieved by principals at the step
  4. Draw conclusions

19

Protocol analysis

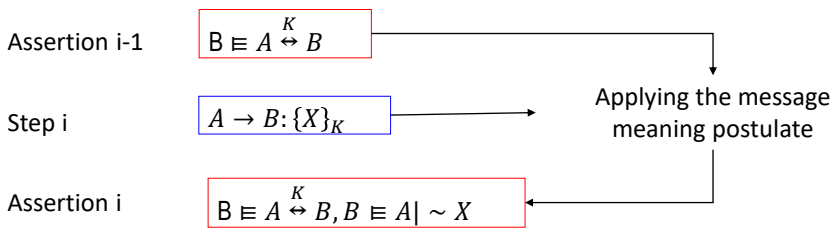
[assumption] **S_1** [assertion 1]

....

[assertion i-1] **S_i** [assertion i]

...

[assertion n-1] **S_n** [conclusions]



20

Objectives of a protocol

Objectives depend on the context

- **Typical objectives**

$A \mid\equiv A \overset{K}{\leftrightarrow} B$ $B \mid\equiv A \overset{K}{\leftrightarrow} B$ (***key authentication***)

often $A \mid\equiv B \mid\equiv A \overset{K}{\leftrightarrow} B$ $B \mid\equiv A \mid\equiv A \overset{K}{\leftrightarrow} B$ (***key confirmation***)

also $A \mid\equiv \#\left(A \overset{K}{\leftrightarrow} B\right)$ $B \mid\equiv \#\left(A \overset{K}{\leftrightarrow} B\right)$ (***key freshness***)

- **Interaction with a certification authority**

$A \mid\equiv \overset{e_b}{\mapsto} B$

BAN Logics

THE NEEDHAM-SCHROEDER PROTOCOL

Needham-Schroeder (1978)

Real protocol

$$
\begin{array}{lll}
M1 & A \to T & A, B, N_a \\
M2 & T \to A & E_{K_a}\left(N_a, B, K_{ab}, E_{K_b}\left(K_{ab}, A\right)\right) \\
M3 & A \to B & E_{K_b}\left(K_{ab}, A\right) \\
M4 & B \to A & E_{K_{ab}}\left(N_b\right) \\
M5 & A \to B & E_{K_{ab}}\left(N_b - 1\right)
\end{array}
$$

Needham-Schroeder (1978)

***Implicit statement**, not explicitly derived from the real protocol*

- *The idealized protocol may contain implicit statements*

Idealized protocol

$$
\begin{array}{lll}
M2 & T \to A & \left\{ N_a, \left(A \overset{K_{ab}}{\leftrightarrow} B \right), \#\left(A \overset{K_{ab}}{\leftrightarrow} B \right), \left\{ A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_b} \right\}_{K_a} \\
M3 & A \to B & \left\{ A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_b} \\
M4 & B \to A & \left\{ N_b, A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_{ab}} \text{ from } B \\
M5 & A \to B & \left\{ N_b, A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_{ab}} \text{ from } A
\end{array}
$$

Needham-Schroeder (%)

$M2 \quad T \to A \quad \left\{ N_a, \left(A \overset{K_{ab}}{\leftrightarrow} B \right), \#\left(A \overset{K_{ab}}{\leftrightarrow} B \right), \left\{ A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_b} \right\}_{K_a}$

After receiving N_a, T said K_{ab} is "good" to talk to *Bob*

$M3 \quad A \to B \quad \left\{ A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_b}$

T said K_{ab} is good to talk to *Alice*

$M4 \quad B \to A \quad \left\{ N_b, A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_{ab}}$ from B

After receiving K_{ab}, B has said K_{ab} is good to talk to A

$M5 \quad A \to B \quad \left\{ N_b, A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_{ab}}$ from A

After receiving N_b, A has said K_{ab} is good to talk to *Bob*

Principle 1. We have to specify the meaning of each message; specification must depend on the message contents; it must be possible to write a sentence describing such a meaning

May 22 BAN Logic 25

25

Needham-Schroeder

Assumptions

$A \mid\equiv A \overset{K_a}{\leftrightarrow} T$ $\quad$ $B \mid\equiv B \overset{K_b}{\leftrightarrow} T$

$T \mid\equiv A \overset{K_a}{\leftrightarrow} T$ $\quad$ $T \mid\equiv B \overset{K_b}{\leftrightarrow} T$

$T \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$

$A \mid\equiv \left(T \Rightarrow A \overset{K_{ab}}{\leftrightarrow} B \right)$ $\quad$ $B \mid\equiv \left(T \Rightarrow A \overset{K_{ab}}{\leftrightarrow} B \right)$

$A \mid\equiv \left(T \Rightarrow \#\left(A \overset{K_{ab}}{\leftrightarrow} B \right) \right)$

$A \mid\equiv \#(N_a)$ $\quad$ $B \mid\equiv \#(N_b)$

$T \mid\equiv \#\left(A \overset{K_{ab}}{\leftrightarrow} B \right)$ $\quad$ $B \mid\equiv \#\left(A \overset{K_{ab}}{\leftrightarrow} B \right)$

Objectives

$A \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$

$B \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$

$A \mid\equiv B \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$

$B \mid\equiv A \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$

Principle 2. Designer must know the trust relationships upon which the protocol is based. He/she must know why they are necessary. Such reasons must be made explicit.

May 22 BAN Logic **26**

26

Needham-Schroeder

After M2

message meaning e
nonce verification

$$A \mid\equiv T \mid\equiv \left(A \overset{K_{ab}}{\leftrightarrow} B \right)$$

$$A \mid\equiv T \mid\equiv \#\left(A \overset{K_{ab}}{\leftrightarrow} B \right)$$

jurisdiction rule

$$A \mid\equiv \left(A \overset{K_{ab}}{\leftrightarrow} B \right)$$

$$A \mid\equiv \#\left(A \overset{K_{ab}}{\leftrightarrow} B \right)$$

After M3

message meaning

$$B \mid\equiv T \mid\sim A \overset{K_{ab}}{\leftrightarrow} B$$

nonce verification

$$B \mid\equiv T \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$$

jurisdiction rule

$$B \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$$

Principle 3. A key may have been used recently to encrypt a nonce but it may be old or compromised. The recent use of a key does not make it more secure

After M4

message meaning

$$A \mid\equiv B \mid\sim A \overset{K_{ab}}{\leftrightarrow} B$$

nonce verification

$$A \mid\equiv B \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$$

After M5

message meaning

$$B \mid\equiv A \mid\sim \left(N_b, A \overset{K_{ab}}{\leftrightarrow} B \right)$$

nonce verification

$$B \mid\equiv A \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$$

May 22 BAN Logic 27

27

Needham-Schroeder: replay attack

- As Bob blindly believes that any key he receives in M3 is fresh then
- If the adversary is able to obtain a session key Kab
- If the adversary records the messages that lead to establish Kab, in particular M3
- Then, the adversary is able to impersonate A w.r.t. B and establish K_{ab} at his/her will

May 22 BAN Logic 28

28

A good design practice

- It is always a *good design practice* to analyse the consequences from a situation in which
  a session key gets compromised and
  the adversary recorded the protocol run that led to that key establishment

29

BAN Logics

THE OTWAY-REES PROTOCOL

30

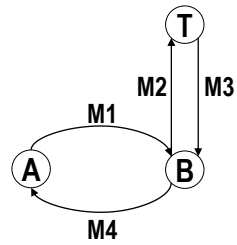
Otway-Rees – real protocol

M1. $A \rightarrow B$: $M, A, B, E_{K_A}(N_A, M, A, B)$

M2. $B \rightarrow T$: $M, A, B, E_{K_A}(N_A, M, A, B), E_{K_B}(N_B, M, A, B)$

M3. $T \rightarrow B$: $M, E_{K_A}(N_A, K_{ab}), E_{K_B}(N_B, K_{ab})$

M4. $B \rightarrow A$: $M, E_{K_A}(N_A, K_{ab})$



May 22 BAN Logic 31

31

Otway-Rees

- The protocol presents odd aspects
  - Na ed Nb are nonces, they are supposed to prove freshness. Then, why are they encrypted in messages M1 and M2?
  - Why do we need M in addition to Na and Nb?
  - Why does M disappear after M2?
  - Actually, Na and Nb are alternative names for M
    - Na is Alice's name for M
    - Nb is Bob's name for M
    - Na and Nb are a sort of "local" names

May 22 **BAN Logic** 32

32

Otway-Rees – idealized protocol

M1. $A \to B$: $\{N_A, M, A, B\}_{K_a}$

M2. $B \to T$: $\{N_A, M, A, B\}_{K_a}, \{N_B, M, A, B\}_{K_b}$

M3. $T \to B$: $\{N_a, A \overset{K_{ab}}{\leftrightarrow} B, B| \sim M\}_{K_a}, \{N_b, A \overset{K_{ab}}{\leftrightarrow} B, A| \sim M\}_{K_b}$

M4. $B \to A$: $\{N_b, A \overset{K_{ab}}{\leftrightarrow} B, A| \sim M\}_{K_a}$

Otway-Rees

M1. $A \to B$: $\{N_A, M, A, B\}_{K_a}$

M2. $B \to T$: $\{N_A, M, A, B\}_{K_a}, \{N_B, M, A, B\}_{K_b}$

M3. $T \to B$: $\{N_a, A \overset{K_{ab}}{\leftrightarrow} B, B| \sim M\}_{K_a}, \{N_b, A \overset{K_{ab}}{\leftrightarrow} B, A| \sim M\}_{K_b}$

M4. $B \to A$: $\{N_a, A \overset{K_{ab}}{\leftrightarrow} B, B| \sim M\}_{K_a}$

M1: Alice says that *M* is a transaction with Bob and N_a is another name of Alice in *M*

M2: Bob says that *M* is a transaction with Bob and N_b is another name of Bob in *M*

M3: After receiving N_b, *T* says that K_{ab} is good and that Alice believed to be in *M*

M4: After receiving N_a, *T* says that K_{ab} is good and that Bob believed to be in *M*

Otway-Rees protocol

Assumptions

$A| \equiv A \overset{K_a}{\leftrightarrow} T$ $\quad$ $B| \equiv A \overset{K_b}{\leftrightarrow} T$

$T| \equiv A \overset{K_a}{\leftrightarrow} T$ $\quad$ $T| \equiv A \overset{K_b}{\leftrightarrow} T$

$T| \equiv A \overset{K_{ab}}{\leftrightarrow} B$

$A| \equiv (T \Rightarrow A \overset{K}{\leftrightarrow} B)$ $\quad$ $B| \equiv (T \Rightarrow A \overset{K}{\leftrightarrow} B)$

$A| \equiv (T \Rightarrow B| \sim M)$ $\quad$ $B| \equiv (T \Rightarrow A| \sim M)$

$A| \equiv \#(N_a)$ $\quad$ $B| \equiv \#(N_b)$

$A| \equiv \#(M)$

Goals

$A| \equiv A \overset{K_{ab}}{\leftrightarrow} B$

$B| \equiv A \overset{K_{ab}}{\leftrightarrow} B$

$A| \equiv B| \equiv M$

$B| \equiv A| \sim M$

Protocollo di Otway-Rees

After M2

$T \mid\equiv A \mid\sim (N_a, M, A, B)$ $\quad$ $T \mid\equiv B \mid\sim (N_b, M, A, B)$

After M3

$B \mid\equiv T \mid\sim \left(N_b, A \overset{K_{ab}}{\leftrightarrow} B, A \mid\sim M \right)$ Given Bob's belief in N_b freshness

$B \mid\equiv T \mid\equiv \left(N_b, A \overset{K_{ab}}{\leftrightarrow} B, A \mid\sim M \right)$ Given Bob's trust in T about keys and its capability to relay

$B \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B, \quad B \mid\equiv A \mid\sim M$

After M4

$A \mid\equiv T \mid\sim \left(N_a, A \overset{K_{ab}}{\leftrightarrow} B, B \mid\sim M \right)$ Given Alice's belief in N_a

$A \mid\equiv T \mid\equiv \left(N_a, A \overset{K_{ab}}{\leftrightarrow} B, B \mid\sim M \right)$ Given Alice's trust in T about keys and its capability to relay and given Alice's belief in *M* freshness

$A \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B, \quad A \mid\equiv B \mid\equiv M$

Otway-Rees Protocol

- Nonces N_a and N_b are for freshness but also to link messages M1 and M2 to messages M3 and M4, respectively
  - Nonce N_a (N_b) is a reference to Alice (Bob) within M or, equivalently,
  - nonce N_a (N_b) is another name for Alice (Bob) in M
- In M1 (M2), encryption is not for secrecy but to indissolubly link Alice (Bob), N_a (N_b) and M together

Principle 4. Properties required to nonces must be clear. What it is fine to guarantee freshness might not be to guarantee an association between parts

Principles 5. The reason why encryption is used must be clear

Otway-Rees modified

- If nonces have to guarantee freshness only, then messages M1 and M2 could be modified as follows

$$\text{M1.} \quad A \rightarrow B: \quad M, A, B, N_A, E_{K_A}(M, A, B)$$
$$\text{M2.} \quad B \rightarrow T: \quad M, A, B, N_A, E_{K_A}(M, A, B), N_B, E_{K_B}(M, A, B)$$

- M1 and M3 (M2 and M4) are not linked anymore =>

  The resulting protocol is subject to a man-in-the-middle attack
  - An adversary may impersonate Bob (Alice) with respect to Alice (Bob)

Otway-Rees modified – the MITM attack

- The Attack assumptions
  - Carol (the adversary) has already carried out a protocol instance with Alice (M')
  - Carol holds an "old" ciphertext $E_{Ka}(M', A, C)$

Otway-Rees modified – The MITM attack

The Attack

M1. $A \rightarrow B[C]$: $M, A, B, N_a, E_{K_A}(M, A, B)$

M2. $C \rightarrow T$: $M', A, C, N_a, E_{K_A}(M', A, C), N_c, E_{K_c}(M', A, C)$

M3. $T \rightarrow C$: $M', E_{K_a}(N_a, K_{ac}), E_{K_c}(N_c, K_{ac})$

M4. $[C]B \rightarrow A$: $E_{K_a}(N_a, K_{ac})$

Otway-Rees protocol: an improvement

- If we need to insert references to Alice and Bob in M3 and M4, then the protocol can ben modified as follows

M1. $A \to B: \quad A, B, N_a$
M2. $B \to T: \quad A, B, N_a, N_b$
M3. $T \to B: \quad E_{K_A}(N_a, A, B, K_{ab}), E_{K_B}(N_b, A, B, K_{ab})$
M4. $B \to A: \quad E_{K_A}(N_a, A, B, K_{ab})$

Principle 6. If an identifier is necessary to complete the meaning of a message, it is prudent to explicitly mention such an identifier in the message

BAN Logics

SSL PROTOCOL (OLD VERSION)

The protocol

Protocol objectives:

- establish a shared key K_{ab}
- mutual authentication

$$\text{M1.} \quad A \to B: \quad \{K_{ab}\}_{K_b}$$
$$\text{M2.} \quad B \to A: \quad \{N_b\}_{K_{ab}}$$
$$\text{M3.} \quad A \to B: \quad \left\{C_A, \{N_b\}_{K_a^{-1}}\right\}_{K_{ab}}$$

M1: Bob sees key K_{ab}

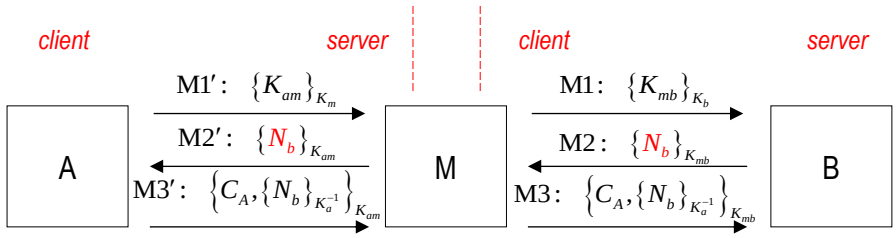
M2: After receiving it, Bob says N_b

M3: After receiving it, Alice says she saw N_b

In the protocol there is no link between A and key K_{ab}

The MiM attack

The adversary plays a MIM attack and impersonates *A* with respect to *B*



A possible countermeasure

- The attack may be avoided by modifying M3 as follows

$$\text{M3 } A \rightarrow B: \quad \left\{C_A, \{A, B, K_{ab}, N_b\}_{K_a^{-1}}\right\}_{K_{ab}}$$

after receiving N_b, Alice says that K_{ab} is a good key to communicate with Bob

- Important
  - In message M3, it's necessary to introduce identifiers A and B in addition to K_{ab} because, otherwise, the attack would be still possible by setting $\boldsymbol{K_{am} = K_{bm}}$

May 22 BAN Logic 45

45

BAN Logics

OTHER ISSUES

May 22 BAN Logic 48

48

Sign encrypted data

Principle 7.
- If an entity signs an encrypted message, it is not possible to infer that such an entity knows the message contents
- In contrast, if an entity signs a message and then encrypts it, then it is possible to infer that the entity knows the message contents

Esempio: X.509

$$A \rightarrow B: \quad A, \left\{ T_a, N_a, B, X_a, \{Y_a\}_{K_b} \right\}_{K_a^{-1}}$$

The message contains no proof that the sender (Alice) knows Y_a

Predictable nonces

Principle 8. A predictable quantity can be used as a nonce in a challenge-response protocol. In such a case, the nonce must be protected by a replay attack

Example: Alice receives a time stamp from a Time Server
(ex. Alice uses the time stamp to synchronize her clock)

$$M1 \quad A \rightarrow S \quad A, N_a$$
$$M2 \quad S \rightarrow A \quad \{T_s, N_a\}_{K_{as}}$$

- N_a: predictable nonce
- (M2): After receiving N_a, S said T_s

Ipotesi

$$A \mid\equiv S \overset{K_{as}}{\leftrightarrow} A$$
$$A \mid\equiv S \Rightarrow T_s$$
$$A \mid\equiv \#(N_a)$$

Risultati

$$A \mid\equiv S \mid\sim T_s$$
$$A \mid\equiv S \mid\equiv T_s$$
$$A \mid\equiv T_s$$

Predictable nonces

An attack

At time T_s, M predicts the next value of N_a

$M1 \quad M \rightarrow S \quad A, N_a$

$M2 \quad S \rightarrow M \quad \{T_s, N_a\}_{K_{as}}$ (S receives M2 at time T_s)

At time $T_S' > T_S$, Alice initiates a protocol instance using N_a

$M1 \quad A \rightarrow S[M] \quad A, N_a$

$M2 \quad S[M] \rightarrow A \quad \{T_s, N_a\}_{K_{as}}$

Alice is led to believe that the current time is T_s and not T_s'

Since N_a is predictable then it must be protected

$M1 \quad A \rightarrow S \quad A, \{N_a\}_{K_{as}}$

$M2 \quad S \rightarrow A \quad \{T_s, \{N_a\}_{K_{as}}\}_{K_{as}}$

Nonce: timestamp

Principle 9. If freshness is guaranteed by time stamp, then the difference between the local clock and that of other machines must be largely smaller than the message validity. Furthermore, the clock synchronization mechanisms is part of the Trusted Computing Base (TCB)

Example

- Kerberos. If the server clock can be turned back, then authenticators can be reused
- Kerberos. If the server clock can be set ahead, then it is possible to generate post-dated authenticators

On coding messages

Principle 10. The contents of a message must allow us to determine: (i) the protocol the message belongs to, (ii) the execution instance of the protocol, (iii) the number of the message within the protocol

Example Needham-Schroeder

$$M4 \quad B \to A \quad E_{K_{ab}}(N_b)$$
$$M5 \quad A \to B \quad E_{K_{ab}}(N_b - 1)$$

$N_b - 1$ distinguishes challenge from response

It would be more clear

$$M4 \quad B \to A \quad E_{K_{ab}}(\text{N-S Message 4}, N_b)$$
$$M5 \quad A \to B \quad E_{K_{ab}}(\text{N-S Message 5}, N_b)$$

On hash functions

For efficiency, we sign the hash of a message rather than the message itself

$$A \to B: \quad \{X\}_{K_b}, \{h(X)\}_{K_a^{-1}}$$

- The message does not contain any proof that the signer Alice actually knows X
- However, the signer Alice expects that the receiver Bob behaves as if the sender Alice knew the message
- Therefore, unless the signer Alice is *unwary**, signing the hash is equivalent to sign the message

* Metaphore: a manager who signs without reading

BAN postulates for hash functions

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

The postulate can be generalized to composite messages

$$\frac{P \mid\equiv Q \mid\sim h(X_1,\cdots,X_n), \quad P \triangleleft X_1,\cdots,P \triangleleft X_n}{P \mid\equiv Q \mid\sim (X_1,\cdots,X_n)}$$

Notice that *P* may receive X_i from different channels in different moments

May 22 BAN Logic 55

55

BAN Logic

ON SECURE CHANNELS

May 22 BAN Logic 56

56

Secure and timely channels

- Let *L* be a secure and timely channel
  - Keyword **on**
- $$\frac{Q\ \mathbf{sees}_L\ X, Q\ \mathbf{believes} \prec_L P}{Q\ \mathbf{believe}\ P\ \mathbf{said}\ X}$$
- $$\frac{Q\ \mathbf{believes}\ P\ \mathbf{said}_L\ X, Q\ \mathbf{believes\ timely}\ (L)}{Q\ \mathbf{believe}\ P\ \mathbf{believes}\ X}$$
- Input channel, output channel

May 22 BAN Logic 57

57