Analysis and design of cryptographic protocols

Main topics

- The BAN logic
- Design principles
- Case studies
  - Needham-Schroeder ⇒ Kerberos
  - Otway-Rees
  - SSL (an old version)
  - GSM

The problem

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

Roger M. Needham

The BAN logic

- After its inventors: **Burrows, Abadi, Needham**
- **Belief and action**
- The logic cannot prove that a protocol is wrong
- However, if you cannot prove a protocol correct, then consider that protocol with great suspicion

Formalism

$P \mid\equiv X$ **P believes X.** P behaves as if X were true

$P \triangleleft X$ **P sees X**:

$P \mid\sim X$ **P once said X**:

$P \Rightarrow X$ **P controls X.**

$\#(X)$ **X is fresh**

$P \overset{K}{\leftrightarrow} Q$ **K is a shared key between P e Q**

Formalism

$P \overset{K}{\rightleftharpoons} Q$ **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**

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

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
- If *P says X* then *P believes X*
- Beliefs of the past may not hold in the present

Postulates: message meaning rule

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

If *K* is a shared key between *P* and *Q*, a *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

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

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*

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

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

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

- 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

Altri postulati

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

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

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

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

$$\frac{P \mid\equiv R \stackrel{K}{\leftrightarrow} R'}{P \mid\equiv R' \stackrel{K}{\leftrightarrow} R} \qquad \frac{P \mid\equiv Q \mid\equiv R \stackrel{K}{\leftrightarrow} R'}{P \mid\equiv Q \mid\equiv R' \stackrel{K}{\leftrightarrow} R} \qquad \frac{P \mid\equiv R \stackrel{K}{\rightleftharpoons} R'}{P \mid\equiv R' \stackrel{K}{\rightleftharpoons} R} \qquad \frac{P \mid\equiv Q \mid\equiv R \stackrel{K}{\rightleftharpoons} R'}{P \mid\equiv Q \mid\equiv R' \stackrel{K}{\rightleftharpoons} R}$$

Protocollo idealizzato

Each protocol step is represented as

$\boxed{A \to B : messaggio}$

For example:

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

This notations is ambiguous. Thus the protocol is **idealized**

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

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

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

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

Protocol analysis

[*assumption*] $\mathbf{S_1}$ [*assertion* 1]

....

[*assertion i*-1] $\mathbf{S_i}$ [*assertion i*]

...

[*assertion n*-1] $\mathbf{S_n}$ [*conclusions*]

Assertion i-1 $\boxed{A \mid\equiv A \overset{K}{\leftrightarrow} B}$

Step i $\boxed{A \rightarrow B : \{X\}_K}$

By applying the message meaning postulate

Assertion i $\boxed{A \mid\equiv A \overset{K}{\leftrightarrow} B, B \mid\equiv A \mid\sim X}$

Objectives of a protocol

Objectives depend on the context

- Typical objectives

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

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

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

- Interaction with a certification authority

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

Needham-Schroeder (1978)

Real protocol

$M1$	$A \rightarrow T$	A, B, N_a
$M2$	$T \rightarrow A$	$E_{K_a}\left(N_a, B, K_{ab}, E_{K_b}\left(K_{ab}, A\right)\right)$
$M3$	$A \rightarrow B$	$E_{K_b}\left(K_{ab}, A\right)$
$M4$	$B \rightarrow A$	$E_{K_{ab}}\left(N_b\right)$
$M5$	$A \rightarrow B$	$E_{K_{ab}}\left(N_b - 1\right)$

Needham-Schroeder (1978)

Idealized protocol

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

- *The idealized protocol may contain implicit statements*

$M2$	$T \rightarrow A$	$\left\{N_a, \left(A \overset{K_{ab}}{\leftrightarrow} B\right), \#\left(A \overset{K_{ab}}{\leftrightarrow} B\right), \left\{A \overset{K_{ab}}{\leftrightarrow} B\right\}_{K_b}\right\}_{K_a}$
$M3$	$A \rightarrow B$	$\left\{A \overset{K_{ab}}{\leftrightarrow} B\right\}_{K_b}$
$M4$	$B \rightarrow A$	$\left\{N_b, A \overset{K_{ab}}{\leftrightarrow} B\right\}_{K_{ab}}$ from B
$M5$	$A \rightarrow B$	$\left\{N_b, A \overset{K_{ab}}{\leftrightarrow} B\right\}_{K_{ab}}$ from A

Needham-Schroeder

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

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

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

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

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

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

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

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

Needham-Schroeder

Assumptions

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

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

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

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

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

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

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

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.

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

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

Dopo M5

message meaning

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

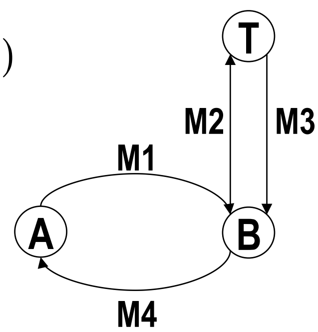
nonce verification

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

Otway-Rees protocol

Real protocol

$$\begin{array}{lll} \text{M1.} & A \to B: & M, A, B, E_{K_A}(N_A, M, A, B) \\ \text{M2.} & B \to T: & M, A, B, E_{K_A}(N_A, M, A, B), E_{K_B}(N_B, M, A, B) \\ \text{M3.} & T \to B: & M, E_{K_A}(N_A, K_{ab}), E_{K_B}(N_B, K_{ab}) \\ \text{M4.} & B \to A: & M, E_{K_A}(N_A, K_{ab}) \end{array}$$



Idealized protocol

$$\begin{array}{lll} \text{M1.} & A \to B: & \{N_A, M, A, B\}_{K_a} \\ \text{M2.} & B \to T: & \{N_A, M, A, B\}_{K_a}, \{N_B, M, A, B\}_{K_b} \\ \text{M3.} & T \to B: & \left\{ N_a, A \overset{K_{ab}}{\leftrightarrow} B, B \mid\sim M \right\}_{K_a}, \left\{ N_b, A \overset{K_{ab}}{\leftrightarrow} B, A \mid\sim M \right\}_{K_b} \\ \text{M4.} & B \to A: & \left\{ N_b, A \overset{K_{ab}}{\leftrightarrow} B, A \mid\sim M \right\}_{K_a} \end{array}$$

Otway-Rees

The protocol presents two strange features

- ***N**$_a$* ed ***N**$_b$* 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 ***N**$_a$* and ***N**$_b$*?
  - Actually it disappears after M2

Otway-Rees

$$\text{M1.} \quad A \rightarrow B: \quad \{N_A, M, A, B\}_{K_a}$$

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

$$\text{M3.} \quad T \rightarrow B: \quad \left\{N_a, A \overset{K_{ab}}{\leftrightarrow} B, B \mid\sim M\right\}_{K_a}, \left\{N_b, A \overset{K_{ab}}{\leftrightarrow} B, A \mid\sim M\right\}_{K_b}$$

$$\text{M4.} \quad B \rightarrow A: \quad \left\{N_a, A \overset{K_{ab}}{\leftrightarrow} B, B \mid\sim M\right\}_{K_a}$$

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

Protocollo di Otway-Rees

Ipotesi

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

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

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

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

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

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

$A \mid\equiv \#(M)$

Risultati

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

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

$A \mid\equiv B \mid\equiv M$

$B \mid\equiv A \mid\sim M$

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, then

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

Given Bob's trust in T about keys and its capability to relay, then

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

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, then

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

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

- 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

$$\begin{array}{lll} \text{M1.} & A \rightarrow B: & M, A, B, N_A, E_{K_A}(M, A, B) \\ \text{M2.} & B \rightarrow T: & M, A, B, N_A, E_{K_A}(M, A, B), N_B, E_{K_B}(M, A, B) \end{array}$$

- 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 resulting protocol is subject to a man-in-the-middle attack
  - An adversary may impersonate Bob (Alice) with respect to Alice (Bob)
- Let us suppose that Carol (the adversary)
  - has already carried out a protocol instance with Alice
  - holds an ”old” ciphertext $\mathbf{E_{\mathit{Ka}}(\mathit{M'}, \mathit{A}, \mathit{C})}$

Otway-Rees modified

The Attack

$$
\begin{array}{lll}
\text{M1.} & A \rightarrow B[C]: & M, A, B, N_a, E_{K_A}(M, A, B) \\
\text{M2.} & C \rightarrow T: & M', A, C, N_a, E_{K_A}(M', A, C), N_c, E_{K_c}(M', A, C) \\
\text{M3.} & T \rightarrow C: & M', E_{K_a}(N_a, K_{ab}), E_{K_c}(N_c, K_{ab}) \\
\text{M4.} & [C]B \rightarrow A: & E_{K_a}(N_a, K_{ab})
\end{array}
$$

Protocollo di Otway-Rees "migliorato"

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

$$
\begin{array}{lll}
\text{M1.} & A \rightarrow B: & A, B, N_a \\
\text{M2.} & B \rightarrow T: & A, B, N_a, N_b \\
\text{M3.} & T \rightarrow B: & E_{K_A}(N_a, A, B, K_{ab}), E_{K_B}(N_b, A, B, K_{ab}) \\
\text{M4.} & B \rightarrow A: & E_{K_A}(N_a, A, B, K_{ab})
\end{array}
$$

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

SSL (old version)

Protocol objectives:

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

$$
\begin{array}{lll}
\text{M1.} & A \rightarrow B: & \{K_{ab}\}_{K_b} \\
\text{M2.} & B \rightarrow A: & \{N_b\}_{K_{ab}} \\
\text{M3.} & A \rightarrow B: & \left\{C_A, \{N_b\}_{K_a^{-1}}\right\}_{K_{ab}}
\end{array}
$$

M1: Bob sees key K_{ab}

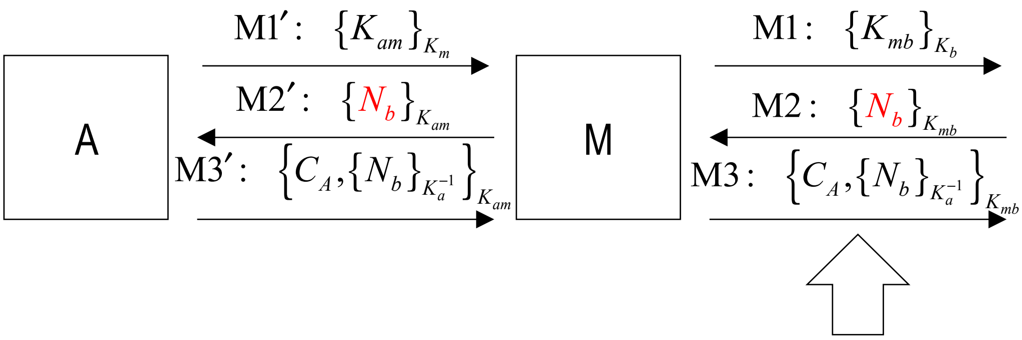
M2: After receiving it, Bob says he saw K_{ab}

M3: After receiving it, Alice says she saw N_b

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

SSL (old version)

Adversary Mallet plays an MIM attack and impersonates *A* with respect to *B*



After M3, Bob believes he is talking to Alice

SSL (old versione)

- The attack may be avoided by modifying M3 as follows

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

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

•Important

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

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 the 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

On hash functions

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

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

- 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 Bob 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

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

The GSM case

Real protocol

$$\begin{array}{llr} \text{M1.} & C \rightarrow S: & C \\ \text{M2.} & C \leftarrow S: & \rho \\ \text{M3.} & C \rightarrow S: & \sigma \end{array}$$

- ρ random challenge generated by *S*
- **<σ, K> = *h*(*K*$_C$, ρ)**

Assumptions

$$S \mid\equiv C \overset{K_c}{\leftrightarrow} S \quad C \mid\equiv S \overset{K_c}{\leftrightarrow} C$$
$$S \mid\equiv \#(\rho)$$

Idealized protocol

$$\text{M3.} \quad C \rightarrow S: \left\langle C \overset{K}{\leftrightarrow} S, \rho \right\rangle_{K_c}$$

Results

$$S \mid\equiv C \mid\equiv S \overset{K}{\leftrightarrow} C$$

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 stam 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

M predicts the next value of N_a

$$M1 \quad M \rightarrow S \quad A, N_a$$
$$M2 \quad S \rightarrow M \quad \{T_s, N_a\}_{K_{as}} \quad (S \text{ receives M2 at time } T_s)$$

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

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

Alice is led to believe that the current time is $\mathbf{T_s}$ and not $\mathbf{T_s'}$

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 set 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 messafe 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

$$\boxed{\begin{array}{lll} M4 & B \rightarrow A & E_{K_{ab}}(N_b) \\ M5 & A \rightarrow B & E_{K_{ab}}(N_b - 1) \end{array}}$$

***N_b* – 1** distinguishes challenge from response

It would be more clear

$$\boxed{\begin{array}{lll} M4 & B \rightarrow A & E_{K_{ab}}(\text{N-S Message 4}, N_b) \\ M5 & A \rightarrow B & E_{K_{ab}}(\text{N-S Message 5}, N_b) \end{array}}$$