Cryptographic Protocols and their Goals

Giampaolo Bella

Universita` di Catania
Dipartimento di Matematica e Informatica

Background

- Protocols concern communication
- Look easy but are extremely hard to get right
- There are alternatives to cryptography
- Protocols aim at specific goals (i.e. Security)

Example.

$$
\begin{array}{llllll}
1. & A & \rightarrow & B & : e_{Kb}(A, Na) \\
2. & B & \rightarrow & A & : e_{Ka}(Na, Nb) \\
3. & A & \rightarrow & B & : e_{Kb}(Nb)
\end{array}
$$

Different designs to achieve different sets of goals.

Cryptographic Protocol

Definition. A sequence of exchanges of *cryptographic messages* between agents over *insecure means*.

- Sequence? Implemented as distributed concurrent program.
- Agents? Humans, machines, processes, …

Cryptographic Messages

Atomic

- Agent names: *A*, *B*, *C*, …
- Keys:
  - Long-term: *Ka*, *Kb*, …
  - Short-term: *Kab*,… (also said *session keys*)
- Nonces: *Na*, *Nb*, …
- Timestamps: *Ta*, *Tb*, …
- Hashes

How to recognise them?

Cryptographic Messages

Compound

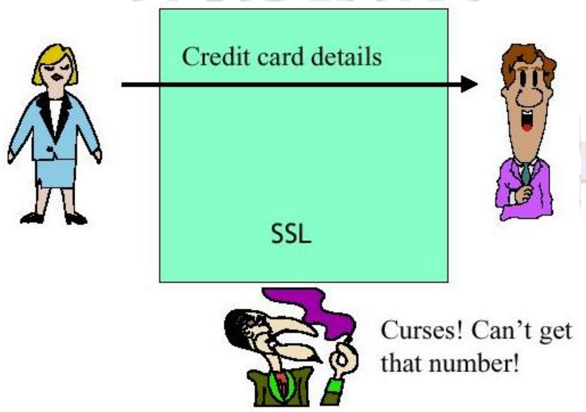
- Concatenated: m, m' …
- Encrypted: $e_K(m)$ …

Problem: can we prove the originator of a concat'd message?

By the way: could define set of messages inductively!

Insecure Means

Internet Shopping with SSL



Insecure Means

A computer network monitored by an attacker who can:

- Intercept messages and prevent delivery
- Forward intercepted messages at will
- Learn cleartexts and ciphertexts
- Try out known keys to decrypt ciphertexts
- Use her own – legal – credentials
- Pay to get some credentials illegally
- Issue fake messages from learnt components
- …

Computational Assumption

The attacker doesn't have unlimited computational resources.

Our Example Protocol

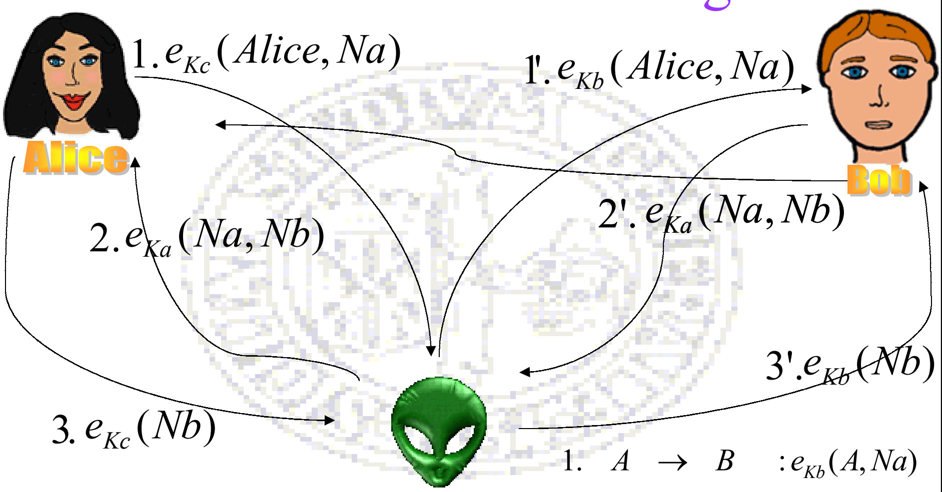
Asymmetric Needham-Schroeder, 1978

$$
\begin{array}{llll}
1. & A & \rightarrow & B & : e_{Kb}(A, Na) \\
2. & B & \rightarrow & A & : e_{Ka}(Na, Nb) \\
3. & A & \rightarrow & B & : e_{Kb}(Nb)
\end{array}
$$

Growth in specification complexity:

- This protocol: 1978, 6 pages
- SSL: mid 90's, 80 pages
- SET: late 90's, 1000 pages

An Attack on 3 Messages



$$
\begin{array}{llll}
1. & A & \rightarrow & B & : e_{Kb}(A, Na) \\
2. & B & \rightarrow & A & : e_{Ka}(Na, Nb) \\
3. & A & \rightarrow & B & : e_{Kb}(Nb)
\end{array}
$$

The Unicity Goal

Def. 1. **(Unicity of a session key) :**
the session key is associated to a single pair of agents.

Violated if, e.g., both steps

$$\mathrm{S} \rightarrow A : e_{Ka}(T, B, Kab, e_{Kb}(T, A, Kab))$$

$$\mathrm{S} \rightarrow C : e_{Kc}(T', D, Kab, e_{Kd}(T', C, Kab))$$

occur and $A \neq C \vee B \neq D$

Def. 2. **(Unicity of a session key) :**
the session key is issued once.

There's more to the goals than insecure means!
Timestamps make the difference.

The Integrity Goal

Def. **(Integrity of a message):**
the message is received in the same form as it was generated.

Violated if, e.g.

$$\mathrm{S} \rightarrow A : e_{Ka}(T, B, Kab, e_{Kb}(T, A, Kxy))$$

There's more to the goals than cautious implementations!

The Authenticity Goal

Def. (Authenticity of a message) :
the message "claim" of its originator is true.

Example.

If Ka^{-1} is only known to *A*, then

$$e_{Ka^{-1}}(m)$$

claims to have originated with *A*.

The Authenticity Goal

Def. (Authenticity of a message) :
the message "claim" of its originator is true.

Claim depends on context protocol.

In general, e.g.

$$e_{Kb}(Nb)$$

claims nothing. But…

The Authenticity Goal

Def. (Authenticity of a message) :
the message "claim" of its originator is true.

…with our protocol…

1. $A \rightarrow B \quad : e_{Kb}(A, Na)$
2. $B \rightarrow A \quad : e_{Ka}(Na, Nb)$
3. $A \rightarrow B \quad : e_{Kb}(Nb)$

$e_{Kb}(Nb)$ claims to come from *A*. Why?

Non trivial because of insecure means.

The Authenticity Goal

Def. (Authenticity of a message) :
the message "claim" of its originator is true.

Violated if, e.g., message

$$e_{Kb^{-1}}(T, A, Kab)$$

did NOT originate with *B* or with a trusted agent.

Non trivial because of insecure means.

The Confidentiality Goal

Def. (**Confidentiality of a message) :**
the message is unknown to the attacker.

Risks arising from:

- incautious design
- session interleaving
- use of the message (cryptanalysis)
- unexpected accidents
- cascade attacks

The Authentication Goal

Def. (Authentication of *A* with *B*) :

•**Aliveness of *A*:**
A has been running the protocol.

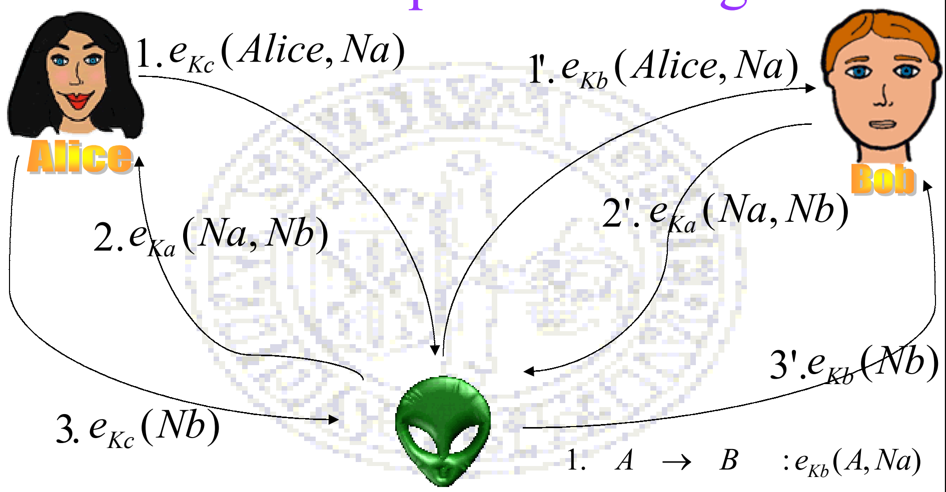
•**Weak agreement of *A* with *B*:**
A has been running the protocol with B.

•**Non-injective agreement of *A* with *B*:**
A has been running the protocol with B, and the two agree on a set of messages.

•...

Applying these def's raises the issue of the *viewpoint.*

B's viewpoint is wrong!



1. $A \rightarrow B \quad : e_{Kb}(A, Na)$
2. $B \rightarrow A \quad : e_{Ka}(Na, Nb)$
3. $A \rightarrow B \quad : e_{Kb}(Nb)$

Goal-Availability Principle

Def. (Availability of goal *g*) **:** *a protocol conforms to the principle "availability of goal g" iff there exists a formal proof stating that g is met,* ***based on assumptions that the protocol peers can verify.***

When the definition is verified, we say that "the protocol makes the goal *g* available to its peers".

This principle was extremely useful when analysing
- Kerberos
- Shoup-Rubin
- Otway-Rees

The Non-Repudiation Goal

Def. (Non-repudiation of origin on a message):
agent B holds valid, irrefutable evidence that A ***sent*** *the message*

Def. (Non-repudiation of receipt on a message):
agent A holds valid, irrefutable evidence that B ***received*** *the message*

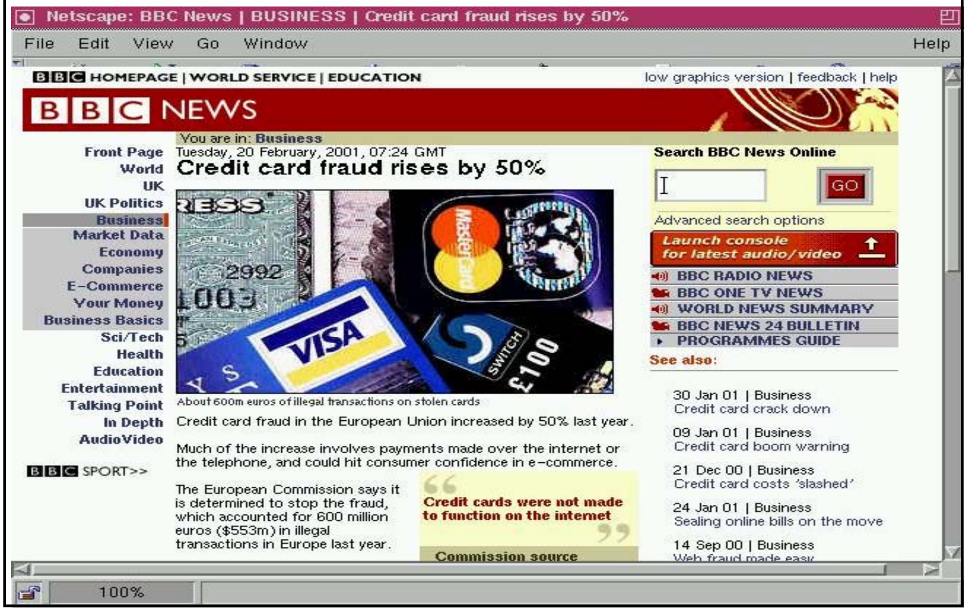
Recent, dedicated protocols to achieve NRO, NRR, NR-SUB,…

Emerging Goals

- Group key-distribution
- Delegation (of trust or of responsibility)
- Non-denial of service
- Anonymity
- …

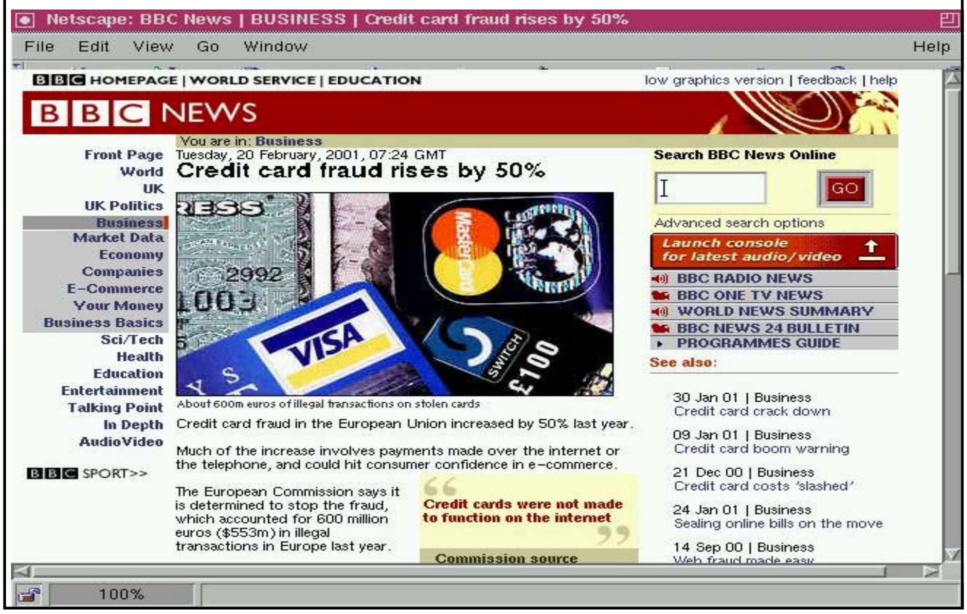
Conclusions

- These were hot issues!



Conclusions

- Careful protocol design and implementation required



Conclusions

•Stringent demand for protocol verification techniques and tools