

Cryptographic Protocols and their Goals

Giampaolo Bella



Universita` di Catania
Dipartimento di Matematica e Informatica

Giampaolo Bella - Cryptographic Protocols and their Goals

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. 1. $A \rightarrow B : e_{K_b}(A, Na)$
2. $B \rightarrow A : e_{K_a}(Na, Nb)$
3. $A \rightarrow B : e_{K_b}(Nb)$

Different designs to achieve different sets of goals.

Giampaolo Bella - Cryptographic Protocols and their 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, ...

Giampaolo Bella - Cryptographic Protocols and their Goals

Cryptographic Messages

Atomic

- Agent names: A, B, C, \dots
- Keys:
 - Long-term: K_a, K_b, \dots
 - Short-term: K_{ab}, \dots (also said *session keys*)
- Nonces: N_a, N_b, \dots
- Timestamps: T_a, T_b, \dots
- Hashes

How to recognise them?

Giampaolo Bella - Cryptographic Protocols and their Goals

Cryptographic Messages

Compound

- Concatenated: $m, m' \dots$
- Encrypted: $e_K(m) \dots$

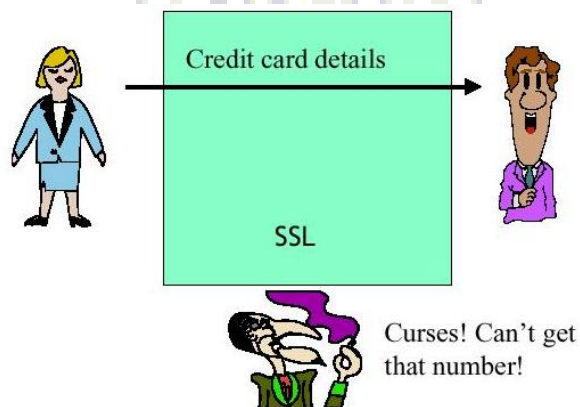
Problem: can we prove the originator of a concat'd message?

By the way: could define set of messages inductively!

Giampaolo Bella - Cryptographic Protocols and their Goals

Insecure Means

Internet Shopping with SSL



Giampaolo Bella - Cryptographic Protocols and their Goals

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
- ...

Giampaolo Bella - Cryptographic Protocols and their Goals

Computational Assumption

The attacker doesn't have unlimited computational resources.

Giampaolo Bella - Cryptographic Protocols and their Goals

Our Example Protocol

Asymmetric Needham-Schroeder, 1978

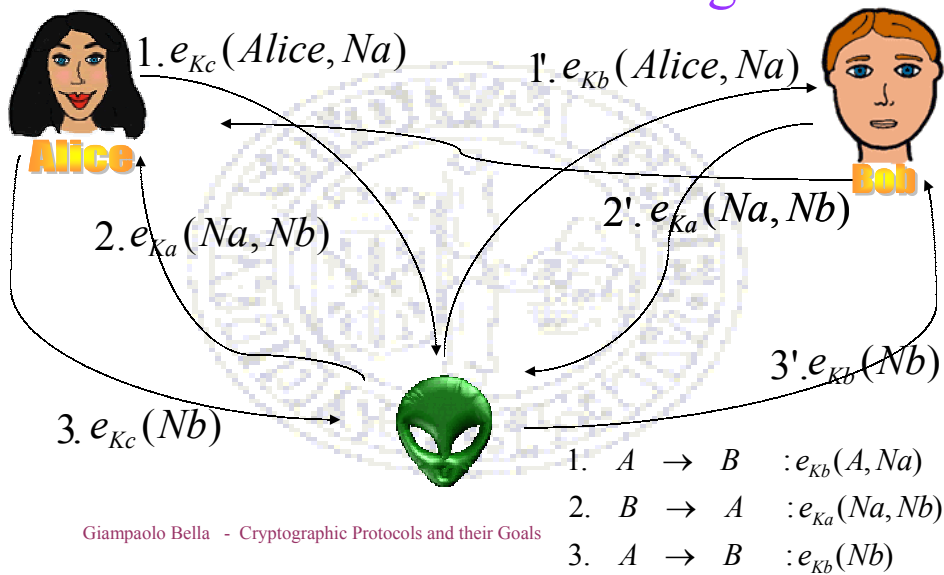
1. $A \rightarrow B : e_{K_b}(A, Na)$
2. $B \rightarrow A : e_{K_a}(Na, Nb)$
3. $A \rightarrow B : e_{K_b}(Nb)$

Growth in specification complexity:

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

Giampaolo Bella - Cryptographic Protocols and their Goals

An Attack on 3 Messages



Giampaolo Bella - Cryptographic Protocols and their Goals

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

$$S \rightarrow A : e_{K_a}(T, B, Kab, e_{K_b}(T, A, Kab))$$

$$S \rightarrow C : e_{K_c}(T', D, Kab, e_{K_d}(T', C, Kab))$$

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

Def. 2. (Unicity of a session key) :

the session key is issued once.

~~There's something called a secure means!~~

Giampaolo Bella - Cryptographic Protocols and their Goals

The Integrity Goal

Def. (Integrity of a message):

the message is received in the same form as it was generated.

Violated if, e.g.

$$S \rightarrow A : e_{K_a}(T, B, Kab, e_{K_b}(T, A, Kxy))$$

There's more to the goals than cautious implementations!

Giampaolo Bella - Cryptographic Protocols and their Goals

The Authenticity Goal

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

Example.

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

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

claims to have originated with A .

Giampaolo Bella - Cryptographic Protocols and their Goals

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.

$$e_{K_b}(Nb)$$

claims nothing. But...

Giampaolo Bella - Cryptographic Protocols and their Goals

The Authenticity Goal

Def. (Authenticity of a message) :

the message “claim” of its originator is true.

...with our protocol...

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

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

Non trivial because of insecure means.

Giampaolo Bella - Cryptographic Protocols and their Goals

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.

Giampaolo Bella - Cryptographic Protocols and their Goals

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

Giampaolo Bella - Cryptographic Protocols and their Goals

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 .

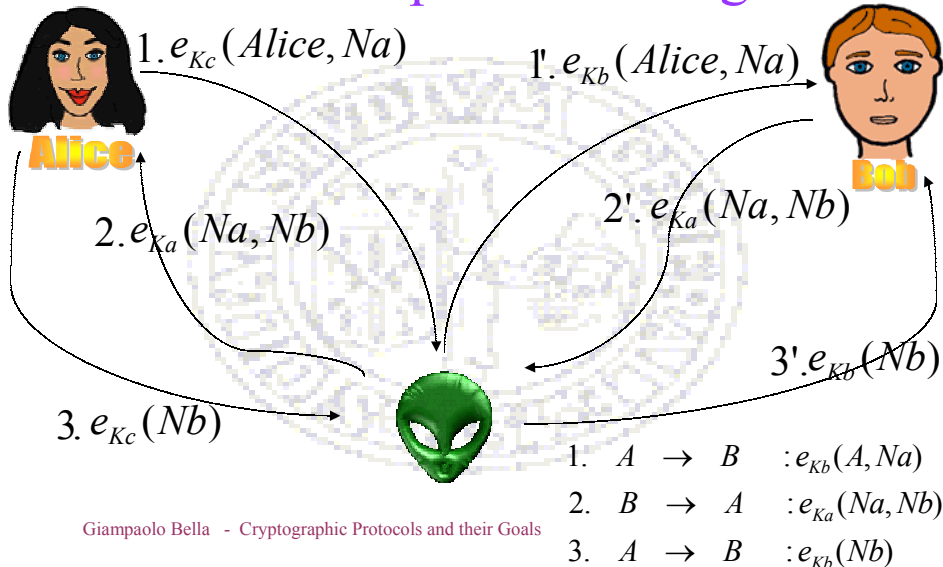
• **Non-injective agreement of A with B :**

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.

Giampaolo Bella - Cryptographic Protocols and their Goals

B's viewpoint is wrong!



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,...

Giampaolo Bella - Cryptographic Protocols and their Goals

Emerging Goals

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

Giampaolo Bella - Cryptographic Protocols and their Goals

Conclusions •These were hot issues!



Conclusions

- Stringent demand for protocol verification techniques and tools

The screenshot shows a Netscape browser window with the address bar displaying "Netscape: BBC News | BUSINESS | Credit card fraud rises by 50%". The browser interface includes a menu bar (File, Edit, View, Go, Window, Help) and a status bar at the bottom showing "100%".

The main content area displays the BBC News homepage with the following elements:

- Navigation:** Links for Front Page, World, UK, UK Politics, Business (highlighted), Market Data, Economy, Companies, E-Commerce, Your Money, Business Basics, Sci/Tech, Health, Education, Entertainment, Talking Point, In Depth, and AudioVideo.
- Header:** "BBC HOME PAGE | WORLD SERVICE | EDUCATION" and "low graphics version | feedback | help".
- Section:** "You are in: Business" and "Tuesday, 20 February, 2001, 07:24 GMT".
- Headline:** "Credit card fraud rises by 50%".
- Image:** A collage of credit cards including Visa, American Express, and Switch, along with a £100 banknote.
- Text:**
 - "About 600m euros of illegal transactions on stolen cards"
 - "Credit card fraud in the European Union increased by 50% last year."
 - "Much of the increase involves payments made over the internet or the telephone, and could hit consumer confidence in e-commerce."
 - "The European Commission says it is determined to stop the fraud, which accounted for 600 million euros (\$553m.) in illegal transactions in Europe last year."
- Quote:** "Credit cards were not made to function on the internet" attributed to "Commission source".
- Search:** "Search BBC News Online" with a search box and a "GO" button.
- Advanced search options:** "Launch console for latest audio/video" button.
- Programmes Guide:** Links for BBC Radio News, BBC One TV News, World News Summary, and BBC News 24 Bulletin.
- See also:** A list of related news items:
 - 30 Jan 01 | Business: Credit card crack down
 - 09 Jan 01 | Business: Credit card boom warning
 - 21 Dec 00 | Business: Credit card costs 'slashed'
 - 24 Jan 01 | Business: Sealing online bills on the move
 - 14 Sep 00 | Business: Web fraud made easy