An Optimal Non-Interactive Message Authentication Protocol

Sylvain Pasini and **Serge Vaudenay**

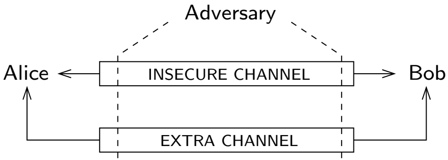
EPFL / LASEC

February the 16^{th} 2006

RSACONFERENCE2006

Setting up a Secure Communication

- Suppose Alice and Bob want to communicate securely:



- No prior exchanged key
- Insecure channel:
  - Adversaries have full control.
- Extra channel:
  - confidentiality, **integrity, authenticity**?

Possible Extra Channels

	Interactive		Non-interactive	
	Encounter	Telephone	Voice mail	Email
Authenticity	✓	✓	✓	
Confidentiality	✓			
Low cost		✓	✓	✓
Availability			✓	✓

Using symmetric cryptography, we need confidentiality:

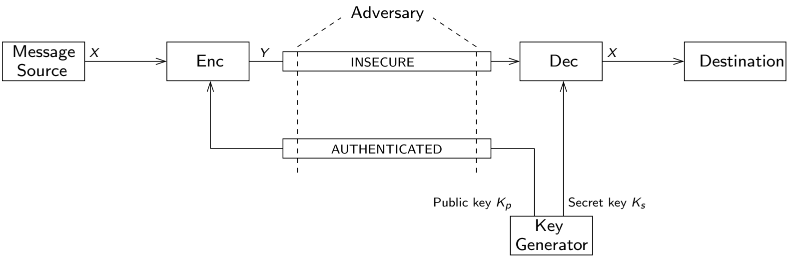
$\longrightarrow$ encounter.

Using public-key cryptography, we need authentication:

$\longrightarrow$ e.g. voice mail.

Public-Key Cryptography

The semi-authenticated key transfer:



- We no longer need confidentiality.
- An authenticated (extra) channel is enough.

Authentication Problem

In a nutshell:

- Setup a secure communication
  $\longrightarrow$ Exchange and authenticate a public key.
- Exchange by phone is tedious (1024 bits).

Objective

Reduce the amount of authenticated data
by using a message authentication protocol.

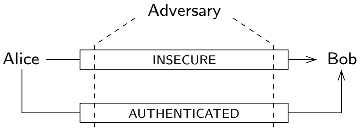
For practical reasons, we prefer a non-interactive protocol.

Authenticated Channels

How does a message authentication protocol work?

- It sends the message through the insecure channel.
- The authentication is done by authenticating a shorter string.

Channels model:



Existing Protocol

Today...

SSH and GPG use the following:

Alice		Bob
input: m		
	$\xrightarrow{\quad m \quad}$	$\hat{h} \leftarrow \mathrm{H}(\hat{m})$
$h \leftarrow H(m)$	$\xrightarrow{\mathrm{authenticate}_{Alice}(h)}$	check $h = \hat{h}$
		output: $Alice, \hat{m}$

The symbol ˆ on a received message indicates that it may be different from the one originally sent.
(e.g. when an attack is performed)

What about Security?

Known message attack:

Alice		Adversary		Bob
input: m				
	$\xrightarrow{m}$		$\xrightarrow{\hat{m}}$	$\hat{h} \leftarrow \mathrm{H}(\hat{m})$
$h \leftarrow H(m)$	$\xrightarrow{\text{authenticate}_{Alice}(h)}$			check $h = \hat{h}$

H **only** has to be weakly collision resistant (80 bits).

Chosen message attack:

	$\xleftarrow{m}$			
	$\xrightarrow{m}$		$\xrightarrow{\hat{m}}$	$\hat{h} \leftarrow \mathrm{H}(\hat{m})$
$h \leftarrow H(m)$	$\xrightarrow{\text{authenticate}_{Alice}(h)}$			check $h = \hat{h}$

H must be collision resistant (160 bits).

What about Security?

Known message attack:

Alice	Adversary	Bob
input: m		
	$\xrightarrow{m}$ $\xrightarrow{\hat{m}}$	$\hat{h} \leftarrow \mathsf{H}(\hat{m})$
$h \leftarrow H(m)$	$\xrightarrow{\text{authenticate}_{Alice}(h)}$	check $h = \hat{h}$

H **only** has to be weakly collision resistant (80 bits).

Chosen message attack:

Alice	Adversary	Bob
	$\xleftarrow{m}$	
	$\xrightarrow{m}$ $\xrightarrow{\hat{m}}$	$\hat{h} \leftarrow \mathsf{H}(\hat{m})$
$h \leftarrow H(m)$	$\xrightarrow{\text{authenticate}_{Alice}(h)}$	check $h = \hat{h}$

H must be collision resistant (160 bits).

A Generic Attack

Generic Attack

The protocol uses k authenticated bits.
The adversary is limited to Q_A runs with Alice.
The adversary is bounded by a time complexity T.

Theorem

For a non-interactive message authentication protocol which uses a weak authenticated channel, there exists a generic attack s.t.

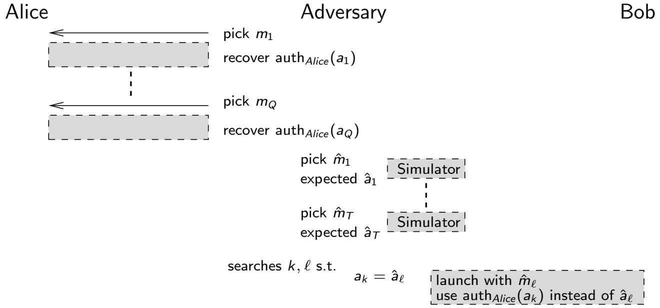
$$\Pr[\text{success}] \approx 1 - e^{-\frac{T \cdot Q_A}{2^k}}$$

No protocol can remain secure when
$T \cdot Q_A$ is non negligible against 2^k

If a protocol reaches this security level, it is **optimal**.

Sketch

Instances of Bob can be simulated.



Success probability:

$$\Pr[\text{success}] \approx 1 - e^{-\frac{T \cdot Q_A}{2^k}}$$

The Proposed Protocol

Overview

Main idea

Avoid the authenticated message to be predictable by adding randomness.

Given an input message m:

1. commit on m

   yield c and d (not deterministic).
2. reveal c and d.

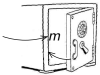
   given (c, d), anyone can recover m (deterministic)
3. authenticate $H(c)$

   c is not foreseeable, thus $H(c)$ neither.

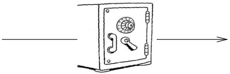
Commitment Schemes

A commitment is like a locked combination safe:

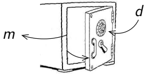
- When Alice wants to commit on m,
  she places m inside the safe and closes it.



- The safe is the commit object c,
  it can be given to Bob.



- When Alice wants to reveal m,
  she gives the combination d.

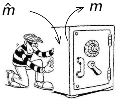


Hiding property:

m cannot be known before c is opened

Binding property:

m cannot be modified after c is closed



Commitment Schemes, More Formally

There are two algorithms:

- $(c, d) \leftarrow \textbf{commit}(m)$
- $m \leftarrow \textbf{open}(c, d)$

Completeness property:

$$\forall m, (c, d) \leftarrow \text{commit}(m),$$
$$m = \text{open}(c, d)$$

Binding property:

For any m, $(c, d) \leftarrow \text{commit}(m)$,
it is impossible to find d' s.t. :
$m' \neq m$ and $m' \neq \perp$
where $m' \leftarrow \text{open}(c, d')$

The Proposed Protocol

Alice		Bob
input: m		
$(c, d) \leftarrow \text{commit}(m)$	$\xrightarrow{c\|\|d}$	$\hat{m} \leftarrow \text{open}(\hat{c}, \hat{d})$
$h \leftarrow H(c)$	$\xrightarrow{\text{authenticate}_{Alice}(h)}$	check $h = H(\hat{c})$
		output: $Alice, \hat{m}$

Example using a random oracle:

pick r		
$c \leftarrow H'(m\|\|r)$	$\xrightarrow{c\|\|m\|\|r}$	check $\hat{c} = H'(\hat{m}\|\|\hat{r})$
$h \leftarrow H(c)$	$\xrightarrow{\text{authenticate}_{Alice}(h)}$	check $h = H(\hat{c})$

Intuitive Security Proof

input: m		
$(c, d) \leftarrow \text{commit}(m)$	$\xrightarrow{c\|\|d}$	$\hat{m} \leftarrow \text{open}(\hat{c}, \hat{d})$
$h \leftarrow H(c)$	$\xrightarrow{\text{authenticate}_{Alice}(h)}$	check $h = H(\hat{c})$
		output: $Alice, \hat{m}$

An adversary can only replace (c, d) by $(\hat{c}, \hat{d})$

Two cases:

- By choosing $\hat{c} = c$, he fullfils the condition $H(\hat{c}) = h$

  He must find a $\hat{d}$ which defeats the binding property $(p \leq \epsilon_c)$.
- By choosing $\hat{c} \neq c$, he avoids the binding problem.

  He must find a $\hat{c}$ s.t. $H(\hat{c}) = h$ $(p \leq \epsilon_h)$.

Security

Overall Security

Consider an adversary bounded by complexity T and Q_A protocol runs with Alice.

He succeeds with probability at most $p \leq Q_A(\epsilon_c + \epsilon_h)$.

We assume that the commitment scheme is (T, ϵ_c)-binding and the hash function is (T, ϵ_h)-weakly collision resistant.

Note that

- ϵ_c can be as small as desired

  c is sent over the broadband channel

- h must be as short as possible

  h is sent over the (expensive) authenticated channel

Applications

- Distant host authentication, e.g. SSH
- E-mail authentication, e.g. GPG signature
- Secure e-mail, e.g. GPG encryption
- Secure voice over IP, e.g. PGPfone
- Digital signature, e.g. RSA signature with MD5:

$$\mathrm{Sig}'(m) = c||d||\mathrm{Sig}\,(c)$$

Summary of our results

A new non-interactive protocol which

- only requires a **weakly** collision resistant hash function.
- is secure against **chosen** message attacks.
- is **optimal**.