# Security models

1st Semester 2014/2015

F.Autreau<br>
P.Lafourcade<br>
M. Gagné<br>
JL. Roch

A. Kumar<br>
P. Lafourcade<br>
M. Gagné

## SET 2*

Date: 26.11.2014

This exercise sheet is devoted to the design and security analysis of "*mutual authentication protocols*". The setting consists of two agents $A$ and $B$ who wish to agree on some value, *e.g.*, a secret key $K$, that they may later use for fast confidential communication. The agents only have access to a public communication channel(for instance a postal service, the Internet or a mobile phone). The transport of the messages on such channels is insecure. Indeed, a malicious agent might intercept the message, look at its content and possibly replace it with another message or even simply destroy it.

In the following exercises, we incrementally build and analyze mutual authentication protocols using asymmetric primitives. We suppose that the agent $A$ has the public-private key pair $(\mathtt{pk}(A), \mathtt{sk}(A))$ and so does the agent $B$, $(\mathtt{pk}(B), \mathtt{sk}(B))$. We suppose that the each agent has in possession the public key of the other. Pairing of two message $m_1$ and $m_2$ is denoted by $\langle m_1, m_2 \rangle$.

### Exercise 1

Consider the first naive protocol:

$$\begin{array}{l} 1.\ A \to B : \langle A, \{K\}_{\mathtt{pk}(B)} \rangle \\ 2.\ B \to A : \langle B, \{K\}_{\mathtt{pk}(A)} \rangle \end{array}$$

First, $A$ generates a fresh key $K$ and sends it encrypted with the public key of $B$ along with his identity. Only $B$ will be able to decrypt this message. In this way, $B$ learns $K$ and also knows that this message comes from $A$ as indicated in the first part of the message he received. Hence, $B$ answers to $A$ by sending again the key this time encrypted with the public key of $A$.

Show that an attacker can learn the key $K$ generated by an honest agent $A$ for another honest agent $B$.

### Exercise 2

The previous protocol is corrected in the following manner, we add the identity of the agent inside each encryption.

$$\begin{array}{l} 1.\ A \to B : \{\langle A, K \rangle\}_{\mathtt{pk}(B)} \\ 2.\ B \to A : \{\langle B, K \rangle\}_{\mathtt{pk}(A)} \end{array}$$

1. Check that the previous attack does not exist anymore.
2. Two agents use this protocol to establish a session key. Show that there is an attack.

### Exercise 3

For double security, all the messages in the previous protocol are encrypted twice. The modified protocol is:

[*] A part of these exerices have been taken from the MPRI lecture notes on Cryptographic Protocols Formal and Computational Proofs by Blanchet et al.

$$\begin{array}{l} 1.\ A \to B:\ \{\langle A, \{K\}_{\mathtt{pk}(B)}\rangle\}_{\mathtt{pk}(B)} \\ 2.\ B \to A:\ \{\langle B, \{K\}_{\mathtt{pk}(A)}\rangle\}_{\mathtt{pk}(A)} \end{array}$$

Show that the protocol then becomes insecure in the sense that an attacker can learn the key $K$ generated by an honest agent $A$ for another honest agent $B$.

**Exercise 4**
Consider the following modification:

$$\begin{array}{l} 1.\ A \to B : \{\langle A, N_A\rangle\}_{\mathtt{pk}(B)} \\ 2.\ B \to A : \{\langle N_B, N_A\rangle\}_{\mathtt{pk}(A)}, \{B\}_{\mathtt{pk}(A)} \\ 3.\ A \to B : \{N_B\}_{\mathtt{pk}(B)} \end{array}$$

Is this protocol secure ?

**Exercise 5**
We consider a variant of the Needham-Schroeder-Lowe protocol. This protocol is as follows:

$$\begin{array}{l} 1.\ A \to B:\ \{\langle A, N_A\rangle\}_{\mathtt{pk}(B)} \\ 2.\ B \to A:\ \{\langle N_A, \langle N_B, B\rangle\rangle\}_{\mathtt{pk}(A)} \\ 3.\ A \to B:\ \{N_B\}_{\mathtt{pk}(B)} \end{array}$$

1. Check that the afore-found "*man-in-the-middle*" attacks do not exist.

2. Show that there is an attack on the secrecy of the nonce $N_B$.

3. Do you think that this attack is realistic ?

**Exercise 6**
Up to now, the encryption is black-box: nothing can be learnt on a plaintext from a ciphertext and two ciphertexts are unrelated. In the sequel, we however use a simple El-Gamal encryption scheme. Roughly, the encryption scheme is given by a cyclic group $G$ of order $q$ and generator $g$; these parameters are public. Each agent $X$ ($A$ or $B$) may randomly chose a secret key $\mathtt{sk}(X)$ and publish the corresponding public key $\mathtt{pk}(X) = g^{\mathtt{sk}(X)}$. Given a message $m = g^{m'}$, encrypting $m$ with the public key $\mathtt{pk}(X)$ consists in drawing a random number $r$ and letting $\{m\}_{\mathtt{pk}(X)} = \langle \mathtt{pk}(X)^r \times g^{m'}, g^r\rangle$. Decrypting the message consists in raising $g^r$ to the power $\mathtt{sk}(X)$ and dividing by the first component of the pair by $g^{r\times \mathtt{sk}(X)}$.

Assume now that we are using such an encryption scheme in the Needham-Schroeder-Lowe protocol and that pairing two group elements $m_1 = g^{m'_1}$ and $m_2 = g^{m'_2}$ is performed in the following way : $\langle m_1, m_2\rangle$ is mapped to $g^{m'_1 + 2^{|m'_1|} \times m'_2}$.

1. What does the mapping signify in layman terms ?

2. Find an attack against the El-Gamal instantiated protocol.

3. What if the pairing is implemented in a different way ? Conclude.