ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Implementation of SPA

Yoan Martin

School of Computer and Communication Sciences

Semester Project

December 2017

Responsible
Prof. Serge Vaudenay
EPFL / LASEC

Supervisor
Ms. Handan Kilinç
EPFL / LASEC

LASEC

The blind signature is an extension of the digital signature. It permits to sign a message without revealing the message to the signer. The concept can be hard to understand because it is difficult to guess why a signer would sign a message without knowing it. Let's consider this simple example. Imagine a political party which wants to hold an election. The party wants to authenticate each vote but each elector does not want his vote to be known. The blind signature is a solution to this problem.
For this project, we use a blind signature based on RSA. The idea is to use a blind factor to blind the message. So, the signer is unable to know the message.
The original message is represented as m and the signature as s. First, we add the blind factor r to the message.

$$m' = r^e m \mod N$$

Then, the signer signs the message using its private key.

$$s' = (m')^d \mod N = r^{ed} m^d \mod N = rm^d \mod N$$

Finally, we remove the blind factor using the inverse.

$$s = r^{-1} s' \mod N = r^{-1} r m^d \mod N = m^d \mod N$$

Nevertheless, the RSA blind signature is not perfect because it is vulnerable to blinding attack. This comes from the fact that RSA uses the same key to sign or to decrypt a message. Let's consider an example where Alice is a server. She has a single private key to sign and to exchange messages. Imagine that Bob sends a message m to Alice using Alice's public key.

$$m' = m^d \mod N$$

Now, imagine that Oscar wants to read this message. If Oscar can intercept the message from Bob, he can send it to Alice by asking to sign it. Since Alice is using her private key to sign a message, Oscar gets the original message of Bob.

$$m = m'^d \mod N = m^{ed} \mod N$$

In other words, Alice decrypt the message when she signs it. The solution to this problem is to use a different key pair for signing and exchanging messages. In this project, we do not have any message exchange. Therefore, the blinding attack does not concern us.

The oblivious transfer is a protocol which permits to exchange data between a client and a server. Let's imagine that the server has n tuples of the form (w_i, c_i), w_i is an index and c_i the corresponding data. The particularity of this protocol is that the client can retrieve the data c_j from the index w_j without revealing the value w_j and without learning the value c_i with $i \neq j$ To achieve this, let's first consider a hash function H and a random generator G. Let's also assume that the server has an RSA key pair. The server starts by creating n keys using the indexes w_i.

$$K_i = (H(w_i))^d \mod N$$

Then it uses these keys to encrypt the data in the following way :

$$E_i = G(w_i \| K_i \| i) \oplus (0^l \| c_i)$$

Then, the server sends every E_i to the client. Now, let's consider that the client wants to retrieve data for index w_j. Using blind signature, the client is able to reconstruct the key K_j corresponding to w_j. So, using a blind factor r, the client generates :

$$Y = r^e H(w_j) \mod N$$

Then, the client asks the server for a blind signature. This way, the server cannot learn the value w_j choosen. At the end, the client received the value :

$$K_j = H(w_j)^d \mod N$$

Finally, he can find the corresponding data using :

$$(a_i \| b_i) = E_i \oplus G(w_j \| K_j \| i)$$

If $a_i = 0^l$, b_i corresponds to the data wanted by the client. Since, the client has only one K_j, he can only decrypt the data c_j corresponding to w_j. So, he cannot learn any other value of c_i with $i \neq j$.