Identity Management

II – Sharing the Secret

A didactic game proposal for Security Awareness

The goal of this activity is to sensitize children between 11 and 12 years old, about a few security aspects, namely the need for confidentiality when exchanging information in hostile environments, such as social networks, emails, forae, chats, etc...

This is a group activity, to be held in classes or workshops.

This time, Alice and Bob will learn a way to share the secret in front of their classmates, with no need of doing it in an isolated place.

To do so, they will use a "trick" allowing each one of them to reach a secret number, never saying it directly to each other, by sending two messages that everybody in the room can read.

Isto

This seems impossible, or one of those magic tricks with an unexpected explanation ...

This trick has a name: it's known as Diffie-Hellman's key exchange, and it's widely used to ensure safety in the internet. Let's see how it works!

In front of all the class, Alice and Bruno agree to use two "magic numbers" that have a special relation between them (which will be explained to the most curious in the end of the session). For now, we will call them the **base** and the **modulus**.

For example, let's suppose Alice and Bruno agree, in front of all the class, that the base will be 5 and the modulus will be 23.

Base: g = 5

Modulus: m = 23

Then, both choose a secret number, which they keep to themselves. In this example, these numbers should be greater than zero and less than 10.

So, for example, let's suppose Alice chooses 5 as secret value (her private key) and Bruno chooses 8 as secret value (his private key).

Alice's secret number: a = 9

Bruno's secret number: b = 8

Here, we have to use a calculator or a small mobile app, capable of doing some simple math operations, which would be too long to perform by hand.

Thus, using the calculator, Alice calculates the following value A (her public key):

A = g^a mod m i.e: g raised to the power of a, modulus m

On his side, Bob calculates his public key B, using a similar calculator:

B = g^b mod m i.e: g raised to the power of b, modulus m

In this example, we will have:

A = 7^9 mod 23 **= 15**

B = 7^8 mod 23 **= 12**

Next, Alice and Bruno send to each other their public keys A and B, without requiring secrecy, saying them loud or writing them in a piece of paper, and passing them through the classmates. But they never should reveal the secret numbers a and b, which were used to calculate A and B.

Thus, Alice receives Bob´s public key (12) and Bob receives Alice's public key A (15).

From these values, Alice and Bruno will finally be able to calculate the secret.

Alice calculates:

S = B^a mod m = 12^9 mod 23 **= 4**

Bob calculates:

S = A^b mod m **=** 15^8 mod 23 **= 4**

Amazing!

Alice and Bruno **reached the exact same secret value**, the number **4** in this case, without communicating with each other. They only shared publicly the values from which nobody is able to deduce the secret, since they don't know the secret numbers they chose.

During the activity, the students can form groups with 2 elements, choosing a classmate with whom they will share the secret (Alice and Bob).

The activity may follow the following steps:

1. Alice and Bob agree on the magic numbers **g** and **m**, in front of the class, or passing a clear text message through the classmates (in fact, there are countless pairs of numbers of this kind which can be used by several groups).
2. Alice chooses one secret number **a** and calculates her public key **A**, which she sends to Bruno, in a clear text message.
3. Bruno chooses one secret number **b** and calculates the public key **B**, which he sends to Alice, also in a clear text message.
4. Alice receives Bob's public key **B** and calculates the secret **S**.
5. Bruno receives Alice's public key **A** and calculates the secret **S**.

6. Now, Alice and Bruno can communicate by using the previous session magic alphabet and this session secret **S**.
7. Etc...

The rest of the session can be filled with some professors' explanations about Diffie-Hellman's exchange, and about the way it's used on the Internet to ensure users' privacy.