Introduction:

Nowadays everyone uses the internet to communicate with their friends, their family, or to buy things on websites like amazon, but a security question arises, how to secure personal information like bank identities during communications on the internet?

We will focus on how this security is implemented by using the asymmetrical encryption, which is used in the HTTPS protocol, today ubiquitous/omnipresent on the websites we use to guarantee security and integrity of the data we exchange.

First, we will see the differences between the HTTP protocol and its successor, the HTTPS protocol, then we will focus on the assumption of asymmetric encryption based on the notions of public and private keys. Finally, we will see how "trusted third parties" are necessary to guarantee the integrity and security of communications.

I. What's the difference between http and https?

HTTP of is full name Hypertext Transfer Protocol is a language who is used for structuring website.

This protocol was created at the end of 1980 in the CERN. HTTP allowed a client and server to communicate. HTTP only works on the request and answer and the data is not crypted. The HTTP protocol is governed by many rules who define how the protocol works and, in the time, old versions were updated.

But HTTP protocol is problematic because data could be intercepted and could be edit by a hacker.

HTTPS was created in 1994, this protocol is a secured extension of the HTTP with the "S" who significate "Secured". This protocol is supply by the TLS technology who establish an encrypted connexion between the server web and the browser. To obtain the "S" you need to acquire and install an SSL / TLS certificate. Which will bring the green lock, and the word Secure in the browser's address bar.

The difference between this both protocols are of HTTPS is just a sub branch of HTTP and not its opposite. However, https has a slight difference but important: it is more advanced and much more secure than http.

So, if the URL of your website don't use the HTTPS protocol, all the data you enter on the site therefore be sent in clear and may be intercepted by hackers. It's for that you need to use an asymmetric cryptography with public and private keys.

II. What are the public and private keys?

Main idea:

The main idea of such a system is that each speaker has two keys. One is public and the other one is private and shouldn't be shared under any circumstances. These two keys are the reverse of each other in the sense that if one is used for encryption, the other must be used for decryption. The difference with symmetric encryption methods is therefore that the keys used to encrypt, and decrypt must be different.

If A wants to send a message to B, this one will retrieve B's public key which will be used for the encryption of the message, when B receives the encrypted message from A he will use his private key that only he knows to decrypted this message.
We quickly understand that there is a problem if a people who want to intercept data called hacker comes to act between A and B.

A want to send a message to B without knowing that the hacker wants to intercept the communication.

For example:
A want to send a message to B without knowing that the hacker wants to intercept the communication. A will send a message encrypted with the hacker's public key, thinking of sending it to B. B will retrieve the information that he will decrypt with his private key and will encrypt the message again to send it to B. The man in the middle will therefore manage the sending of messages between A and B and will retrieve everything that happens there and vice versa during the response from B to A. We can therefore see the interest of trusted third parties who make it possible to prove that the person to whom we wish to speak is indeed the right one, to avoid the intervention of a hacker who would like to recover confidential information by usurping the identity of the two people who exchange.

III. How are trusted third-parties useful and necessary to secure communications?

To remedy this problem, trusted third parties have been set up to secure communications on the Internet by adding more security by the principle of public and private keys explained previously.
Trusted third parties is a legal or natural person who is authorized to set up electronic signatures from public keys.
In the world of digital security, we can define three categories of trusted third parties:
- Certification authorities: This is a trusted body that provides certificates (Digicert) to companies to prove that a particular site belongs to them. The Certification authorities are also responsible for setting up a certification policy and make sure of is practical application.
- Registration authorities: This kind of authority checks if the person or company who request an electronic signature is the person or company they claim to be.
- Certification operators: Take care of the management of electronic certificates. They must set up place services to prove the identity of two communicating people to ensure that there are no identity theft companies that deliver technical infrastructure.
In France, ANSSI has a recommendation role about the rules for awarding certificates.
The body then issues an electronic certificate containing the following information:
• A public key.
• The identity of the owner of the public key.
• A validity date for this key.
• A signature.
So, we can compare a certificate to a passport and the trusted third party to the administration that provides the passport

Conclusion:

We were able to see the evolution of communications on the Internet, moving from the HTTP protocol, which was not secure enough, to the HTTPS protocol, which today makes it possible to guarantee the integrity and the security of communications on the Internet.

We were also able to see how the HTTPS protocol that we see every day without even realizing it works and deals with communications, using the idea of asymmetrical encryption and trusted third parties.

Unfortunately, with the development of quantum computers, this system may no longer be sufficient in the coming years, it will quickly be necessary to find an alternative allowing it to continue to be able to communicate on the internet without fear of seeing our data recovered by hackers.

Thomas RAYNAUD

Thomas Mirbey