# Implementation of a secure web architecture

David Alejandro Vasquez Carreño
*Ingeniería de sistemas*
*Escuela Colombiana de Ingeniería Julio Garavito*
Bogotá, Colombia
david.vasquez@mail.escuelaing.edu.co

***Abstract*—Thought java and http protocols, we have made simple web architecture, consisting in the communication of systems with SSL over http. Https offer to modern companies the capacity of guarantee privacy and protection of the information in a http communication, where information could fly in plain text. The protection of all this information is something wanted by attackers and malicious users that already this king of vulnerabilities, and by only putting a sniffer between a communication they could discover our username and password.**

***Index Terms*—Http, Https, SSL, TLS, Privacy, Authentication, Authorization**

## I. Introduction

Laws and regulations make that companies have to implement different kind of services and architectures oriented to security, in order to be able to offer trust to the their customers, and protect general information of people and other partners, like vendors, that have very sensible information of other companies, like passwords, access to their servers or privileges access to information,

All companies have to implement this services in order to maintain competitive and to keep the trust that customers have into them. The privacy of information guarantees that all information will be seen only by those who are allowed to see it and change it. Authentication give us track of the person that is looking the information, so all companies can keep history of changes or transactions, and detect possibles users that represent a security risk. Authorization guarantee that the users only have access to a fixed set of data and information, and other information or services are behind a security wall that keep users in proper roles and actions.

We are going to see a simple protection for secure web pages. SSL and TLS allow developers to interchange information between the client and the server in a secure way, by encrypting all information with certifications given by trusted partners that provides the confirmation that a specific company has good security practices,

## II. The need of security

As we said previously, security has become an important part of a company architecture, all because security must be guaranteed for the customers, because if not, a big hit could be taken by lawsuits or lose of clients that represent a major part of the income that keeps the company on the road. A company that want to keeps competitive has to maintain a very strong level of security, so the customers can have the trust on their technologies.

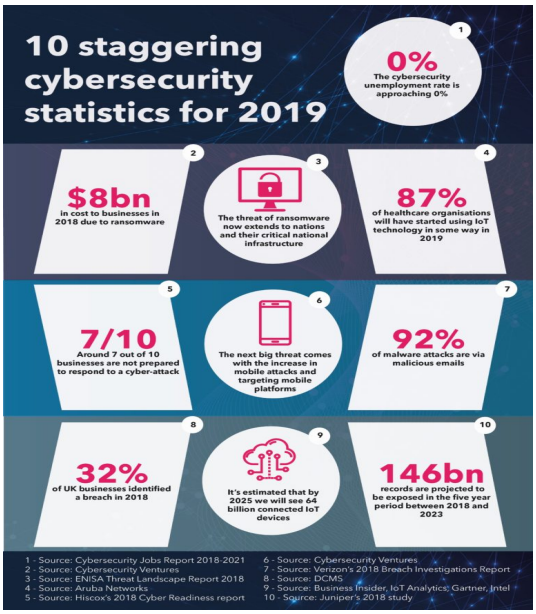


Fig. 1. Cyber attacks

The image[1] shows all the possible looses that a cibersecurity attack could represent in a company,hitting billions of dollars that the company has to recover for their customers somehow.

Sadly, most companies does not have the ability to respond efficiently to this king of ciber attacks, so most information is filtered and used by malicious users, by selling or requesting money for the recover of it [1].

## III. What is TLS?

Transport layer security of TLS, is a set of cryptography protocols for secure communication in the internet, so all

information travelling between a communication is correctly encrypted, and protected at the time of the communication. TLS is commonly used in application protocols like HTTPS, IMAPS o POP3S for the communication of simple messages in a mail architecture inside a company [2].

Simple web pages use HTTP protocol for communication, but some information can be seen in the network with some kind of sniffer like burp, and some passwords can be compromised in logins or register processes.

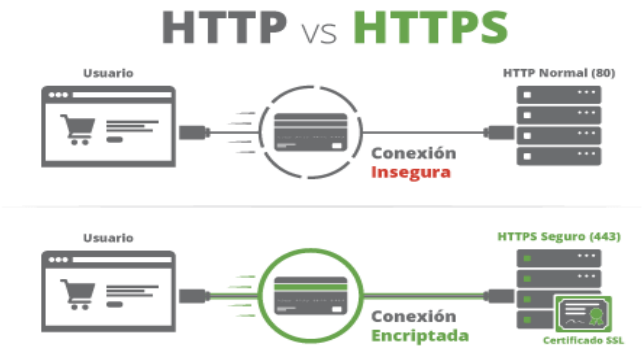


Fig. 2. Http vs Https

The figure 2 shows the main difference between a connection with HTTP and HTTPS, so we see the importance of the implementation of a security protocol in a simple web page. A web page that implements a login system can have vulnerabilities by all sides, but we will see how to protect web pages with HTTP secure.

## IV. Solution

Our implementation is a simple communication with authentication through https between browser client and java,m and two java server that communicate between secure certificates.

A java server received the request from the client and send it immediately to a second server that will process the information and return the result.

## V. Evaluation

With out simple implementation, we have seen how to make a login service with all the features that spark has, and with some limitations of the web server, the server protects the information that is behind a wall of authentication.

A limitation of the case study is the implementation of certifications not provided by a third party that is specialized in giving certifications, but as I said it is only a limitation of this time. In a serious implementation, all certifications should be provided by a third party that provide security to the users.

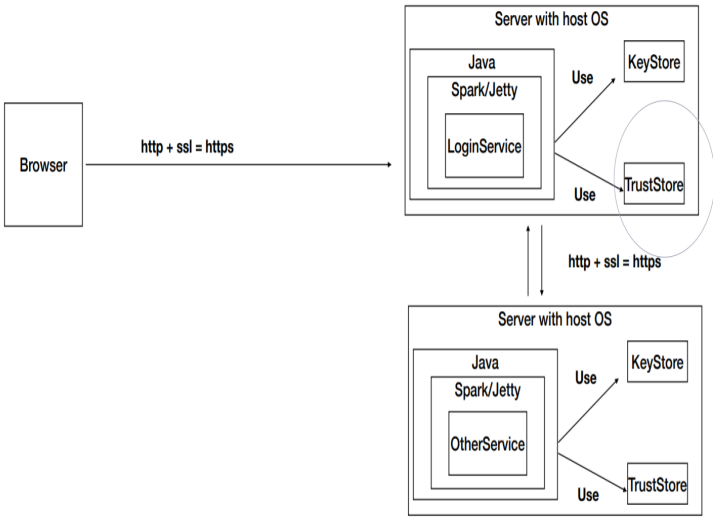


Fig. 3. Design

## VI. Conclusions

Security must be guaranteed in all fronts of a web application, in HTTP, in authorization, authentication and privacy of information, so clients can make secure transactions with our company, and all information in communication channels is properly protected.

At the moment of implementing secure apps, we must look closely at all the kind of vulnerabilities that all the technologies we are using have, like xss, sql injection or man in the middle, that are a different kind of attack that can get into out systems and steal information like passwords, or even shut down all the infrastructure.

## References

[1] I. security, "10 staggering cybersecurity statistics for 2019." https://www.irmsecurity.com/resources/10-staggering-cybersecurity-statistics-for-2019/, October 2019. Accessed on 2020-10-01.

[2] Wikipedia, "Transport layer security." https://en.wikipedia.org/wiki/Transport_Layer_Security, October 2020. Accessed on 2020-10-01.