Network Security Laboratory – Lecture 2

SSL AND TLS

Dott. Andrea Baffa
email: abaffa94@servizimicrosoft.unical.it

Secure Socket Layer (SSL) and Transport Layer Security (TLS)

- Are cryptographic protocols designed to provide secutiry over network
- TLS protocol born to provide privacy and data integrity between hosts
- The connection is **SECURE** because data is encrypted with symmetric cryptography
- The **IDENTITY** of hosts communicating is authenticated with public key cryptography
- The connection is **RELIABLE** because messages includes a message integrity check using a Message Authentication Code to prevent manipulation during transmission

Certificates

- Is an electronic document used for verification of owner identity
- It includes information about owner identity, public key and signature of an entity that has verified certificate's content
- In a common Public Key Infrastructure (PKI) the certificates are released by a Certification Authority (CA)
- A Certification Authority usually is a company that charges customers to issue certificates for them
- Based on X509 protocol

Certificate Validation

- When a connection is made up the server send at the client his certificate and client must ensure that is valid.

- In order to do that the client will perform the **certification path validation algorithm**:

1. The subject of the certificate matches the hostname (i.e. domain name) to which the client is trying to connect;
2. The certificate is signed by a trusted certificate authority.

- A TLS server may be configured with a self-signed certificate. In this case clients will generally be unable to verify the certificate, and will terminate the connection unless certificate checking is disabled.

Self Signed Certificates

- We could generate self-signed certificates
- In order to create a self-signed certificate we must create a custom Certificate Authority
- This type of certificate could be used only for testing purposes
- They are seen as not valid because other hosts consider our CA as not “TRUSTED”

Simple SSL/TLS Stream

- In order to create a simple stream, using SSL/TLS protocol, we could use openssl tool
- Server Side: openssl s_server –key [key] –cert [cert]
- Client side: openssl s_client
- On wireshark we could see handshake and how message are encrypted

SSL/TLS in practice

- Download from course website **PySSL**, our python script for testing SSL/TLS
- Configure Server.py with your self-signed certificate
- Run Server.py && Client.py
- Why there is an error?

SSL/TLS in practice

- Configure Client.py in order to handle our custom CA
- Test connection, now it will work!
- We can see handshake on wireshark

Letsencrypt certificates

- Letsencrypt it’s a free Certificate Authority
- Basically provides certificates at everyone has a domain
- We will use it in order to obtain a valid certificate
- On course website there is a guide for obtaining a new valid certificate

Build a Web Server with a valid certificare

- Now that we have a valid cerficate, obtained from letsencrypt we could use in a web server
- On Course website there is a guide for installing apache web server and install our certificate
- At the end of configuration we can go on our custom domain and see, through the brower, the information of certificate

Questions?

The lesson is over.

Thank you!