Résumé CyberEdu semestre 1 module 3 –
Les protocoles de sécurité et la cryptographie

Protocoles de sécurité :

Communication sécurisée : garantir la confidentialité, l'authenticité et l'intégrité des données

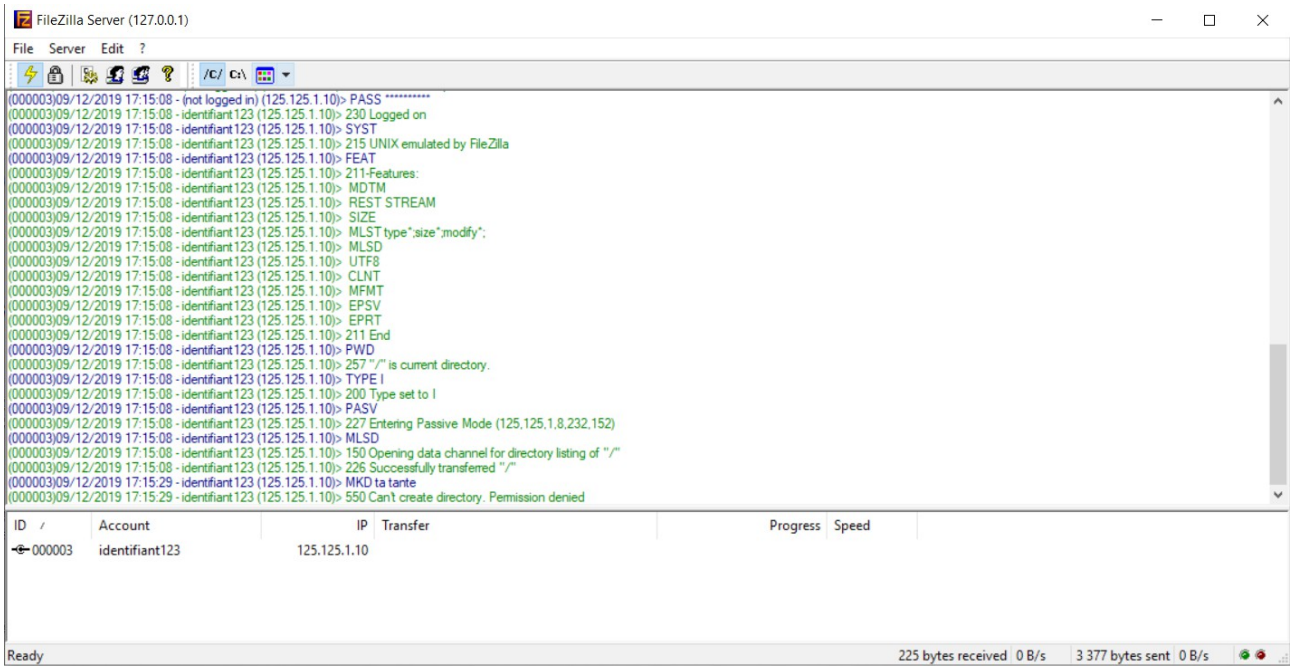
Chiffrement : information qui par une succession de calculs mathématiques va devenir illisible.
Chiffrement symétrique : utilisation de la même clé pour le chiffrement et le déchiffrement.
Chiffrement asymétrique : cryptage et décryptage par 2 clés différentes.

Principe du chiffrement asymétrique :
Envoi d'une requête au récepteur > obtention de sa clé publique > chiffrement avec sa clé publique > envoi des données chiffrés > décryptage via la clé privé qui est associé à la clé publique envoyé.

HTTPS : ajout du protocole TLS au HTTP qui va sécuriser le transfert de données
Bloquer le protocole SSL est recommandé car il y a eu des failles dans celui-ci qui permettait d'accéder aux données chiffrés plutôt facilement.

Test en réel de l'interception de données par un *man in the middle* :

Communication des deux postes réussie du côté serveur et du côté client :

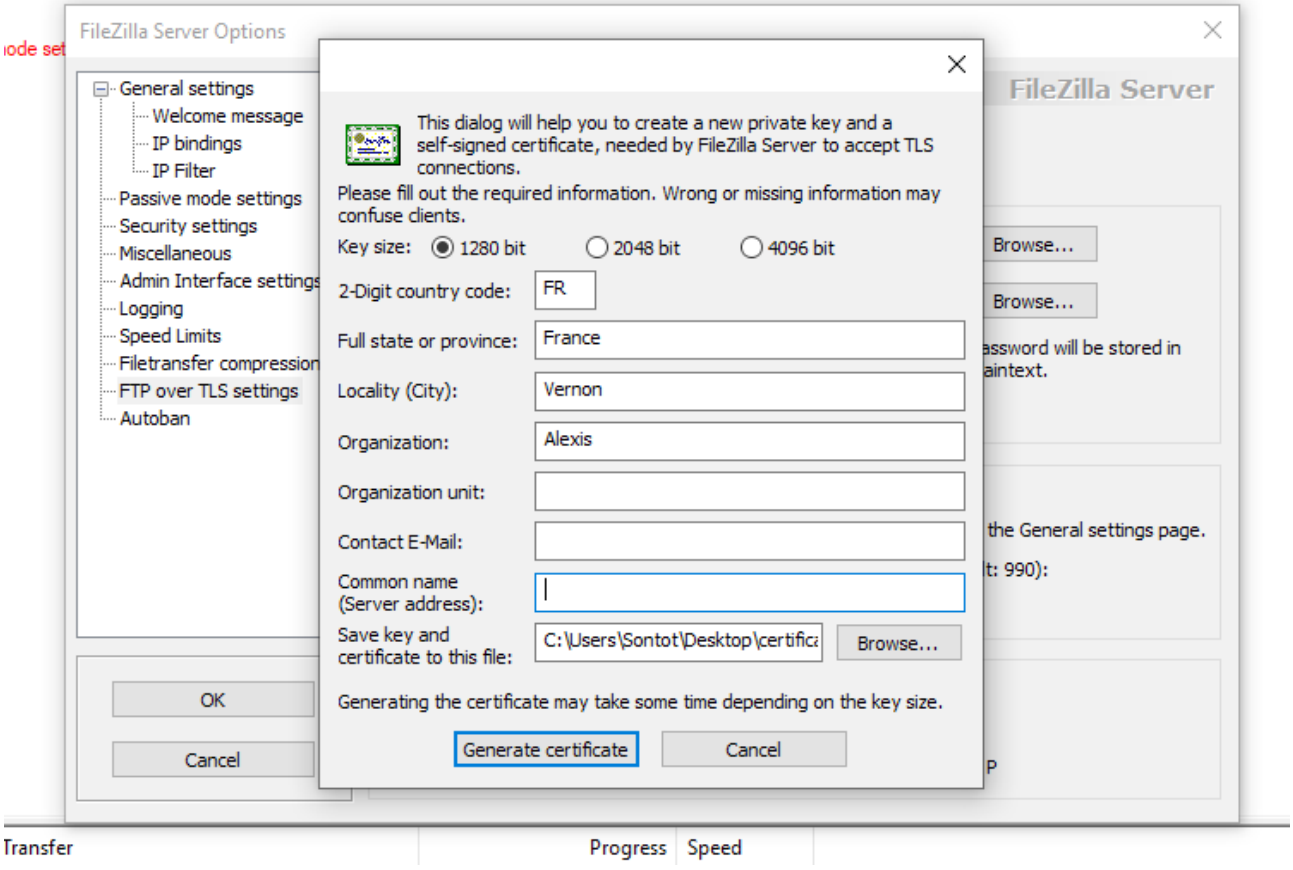


Interception du login et mot de passe en clair par le *man in the middle* :

378	28…	169.254.137.245	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
379	28…	CiscoInc_9a:0e:83	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/dc:a5:f4:9a:0e:80 Cost = 0 Port = 0x8003
380	28…	fe80::6044:2d17:b3f…	ff02::1:2	DHCPv6	160 Solicit XID: 0xefde7b CID: 0001000124cf8405f8b46aa0c661
381	28…	169.254.137.245	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
382	28…	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x144f708e
383	28…	CiscoInc_9a:0e:83	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/dc:a5:f4:9a:0e:80 Cost = 0 Port = 0x8003
384	28…	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x2bebb8f3
385	28…	CiscoInc_9a:0e:83	CDP/VTP/DTP/PAgP/UD…	DTP	60 Dynamic Trunk Protocol
386	28…	CiscoInc_9a:0e:83	CDP/VTP/DTP/PAgP/UD…	DTP	90 Dynamic Trunk Protocol
387	29…	CiscoInc_9a:0e:83	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/dc:a5:f4:9a:0e:80 Cost = 0 Port = 0x8003
388	29…	169.254.137.245	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
389	29…	CiscoInc_9a:0e:83	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/dc:a5:f4:9a:0e:80 Cost = 0 Port = 0x8003
390	29…	CiscoInc_9a:0e:83	CiscoInc_9a:0e:83	LOOP	60 Reply
391	29…	169.254.137.245	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
392	29…	CiscoInc_9a:0e:83	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/dc:a5:f4:9a:0e:80 Cost = 0 Port = 0x8003
393	29…	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x144f708e
394	29…	CiscoInc_9a:0e:83	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/dc:a5:f4:9a:0e:80 Cost = 0 Port = 0x8003
395	29…	169.254.137.245	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
396	29…	fe80::f8ec:9c35:a16…	ff02::1:2	DHCPv6	160 Solicit XID: 0x2acac6 CID: 0001000124cf84ebf8b46aa03217
397	29…	CiscoInc_9a:0e:83	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/dc:a5:f4:9a:0e:80 Cost = 0 Port = 0x8003
398	30…	169.254.137.245	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
399	30…	CiscoInc_9a:0e:83	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/dc:a5:f4:9a:0e:80 Cost = 0 Port = 0x8003
400	30…	CiscoInc_9a:0e:83	CDP/VTP/DTP/PAgP/UD…	CDP	429 Device ID: Switch Port ID: FastEthernet0/3
401	30…	CiscoInc_9a:0e:83	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/dc:a5:f4:9a:0e:80 Cost = 0 Port = 0x8003
402	30…	CiscoInc_9a:0e:83	CiscoInc_9a:0e:83	LOOP	60 Reply
403	30…	fe80::6044:2d17:b3f…	ff02::1:2	DHCPv6	160 Solicit XID: 0xefde7b CID: 0001000124cf8405f8b46aa0c661

```
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
AUTH TLS
502 Explicit TLS authentication not allowed
AUTH SSL
502 Explicit TLS authentication not allowed
USER leesingod
331 Password required for leesingod
PASS 15853
230 Logged on
PWD
257 "/" is current directory.
```

mise en place d'une connexion TSL via le certificat pour empêcher les *man in the middle* :


FileZilla Server Options
General settings
Welcome message
IP bindings
IP Filter
Passive mode settings
Security settings
Miscellaneous
Admin Interface settings
Logging
Speed Limits
Filetransfer compression
FTP over TLS settings
Autoban
OK
Cancel
FileZilla Server
Browse...
Browse...
assword will be stored in
aintext.
the General settings page.
t: 990):
This dialog will help you to create a new private key and a self-signed certificate, needed by FileZilla Server to accept TLS connections.
Please fill out the required information. Wrong or missing information may confuse clients.
Key size:
1280 bit
2048 bit
4096 bit
2-Digit country code:
FR
Full state or province:
France
Locality (City):
Vernon
Organization:
Alexis
Organization unit:
Contact E-Mail:
Common name (Server address):
Save key and certificate to this file:
C:\Users\Sontot\Desktop\certific
Browse...
Generating the certificate may take some time depending on the key size.
Generate certificate
Cancel
Transfer
Progress
Speed