

## CyberEdu A9 : La sécurité des protocoles IP, ICMP, TCP, UDP

De nos jours les données circulent tous les jours et doivent rester privées. Les échanges ont donc été sécurisés au fil du temps et répondent à 3 critères :

- Confidentialité : Les trames ne doivent pas être accessibles par un tiers.
- Authenticité : L'expéditeur doit savoir qui est le destinataire et inversement.
- Intégrité : L'information ne doit pas être modifiée entre l'envoi et la réception.

Pour répondre à ce besoin de sûreté, les chiffrements ont été inventés. Un chiffrement est un procédé par lequel un message est changé à l'aide d'un algorithme qui se nomme la clé. Il existe 2 types de chiffrement : le chiffrement symétrique et celui asymétrique. Le premier impose un échange de clé (impossible en clair sur internet) pour décrypter le message, les personnes qui échangent doivent donc avoir la même clé. Quant au chiffrement asymétrique, pour être efficace on doit être sûr de l'authenticité des paires c'est-à-dire que leurs clés doivent être différentes et que l'expéditeur doit posséder une image de la clé privée du destinataire pour pouvoir grâce à sa clé publique créer un codage uniquement décryptable par le destinataire. Chaque message est donc crypté différemment selon le destinataire.

Les clés publiques et privées ont donc une utilité différente dans le procédé de cryptage/décryptage :

- La clé publique sert uniquement à chiffrer le message.
- La clé privée est une clé personnelle, propre à chacun, et sert à décrypter un message avec l'aide de la clé publique de notre clé publique.

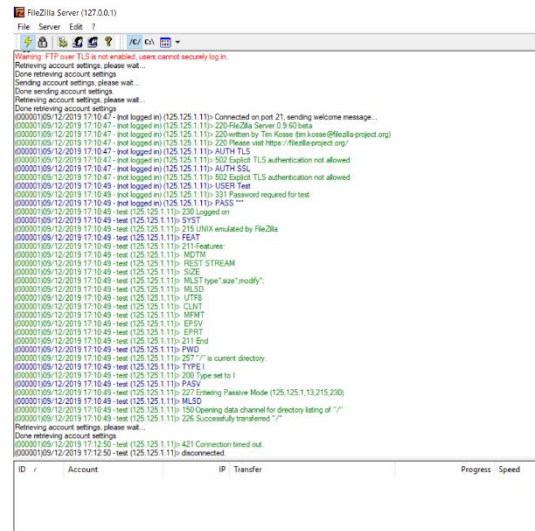
Des protocoles ont été élaborés pour différents types d'activité d'échange comme le protocole HTTPS. Celui-ci est un protocole d'échange web sur un réseau (internet ou intranet). Il existe aussi le protocole TLS (Transparent Layer Security) qui repose sur un "Handshake", c'est-à-dire qu'il y a un accord pour transmettre les clés. Ce protocole définit donc les règles de sécurité à suivre lors de l'envoi d'un message par le biais d'un réseau. Ce protocole possédait de nombreuses failles permettant aux pirates d'être un "man in the middle", c'est-à-dire de se mettre au milieu de la communication soit en se faisant passer pour l'expéditeur soit pour le destinataire. Ce protocole a donc été remplacé par son successeur le protocole SSL (Secure Sockets Layer) lequel crée un canal sécurisé entre les 2 machines réalisant l'échange, c'est aujourd'hui le protocole de sécurité le plus répandu. Pour se prémunir des risques que constitue le TLS (non-patché) et encore présent sur de nombreuses machines, il faut le désactiver des serveurs afin que les pirates ne puissent repasser les serveurs en protocole TLS et exploiter les failles et porter atteinte aux données.

Enfin, pour se prémunir des risques de piratages, il existe les certificats de domaines SSL correspondant à une carte d'identité numérique. Il en existe 3 : Organisation, Validation et étendu. Ces trois certificats sont gérés par l'organisme OCSP (Online Certificat Status Protocol), celui-ci s'assure de la validité des certificats et gère l'attribution et le contrôle de ceux-ci.

## Démonstration :

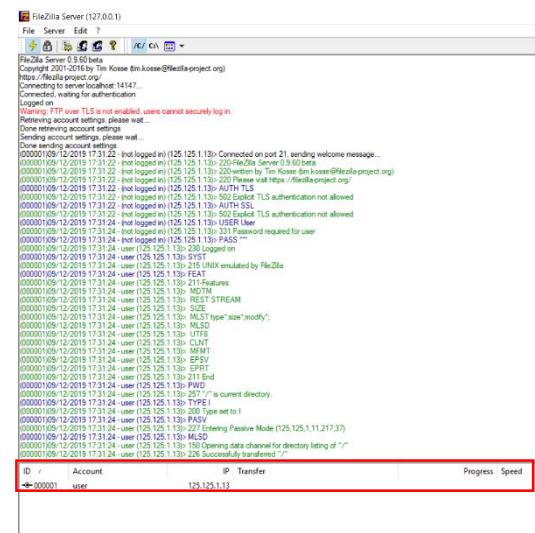
Ici trois personnes sont présentes : un serveur, un client et un pirate. Le serveur crée l'espace d'échange et un compte pour que le client puisse accéder à cet espace, le pirate lui va jouer le rôle du "man in the middle" et donc va vouloir intercepter les données. (Ici aucun protocole de sécurité n'est appliqué sur le serveur mis à notre disposition, le FTP utilisé est FileZilla Serveur et FilleZilla Client.)

- Tout d'abord on a ici la création du serveur par la personne qui gère celui-ci. On peut ici voir que le TLS n'est pas activé et que l'espace d'échange a bien été créé.



```
FileZilla Server (127.0.0.1)
File Server Edit ?
Warning: FTP over TLS is not enabled, users cannot securely log in.
Retrieving account settings, please wait...
Done retrieving account settings
Sending account settings, please wait...
Done sending account settings
Retrieving account settings, please wait...
Done retrieving account settings
(000001/09-12-2019 17:10:47 - not logged in) (125.125.1.13): Connected on port 21, sending welcome message...
(000001/09-12-2019 17:10:47 - not logged in) (125.125.1.13): 220-FileZilla Server 0.9.60 beta
(000001/09-12-2019 17:10:47 - not logged in) (125.125.1.13): 220-Welcome by Tim Koster (tm.koster@filezilla-project.org)
(000001/09-12-2019 17:10:47 - not logged in) (125.125.1.13): 200 Please visit https://filezilla-project.org/
(000001/09-12-2019 17:10:47 - not logged in) (125.125.1.13): AUTH TLS
(000001/09-12-2019 17:10:47 - not logged in) (125.125.1.13): 502 Explicit TLS authentication not allowed
(000001/09-12-2019 17:10:47 - not logged in) (125.125.1.13): AUTH SSL
(000001/09-12-2019 17:10:47 - not logged in) (125.125.1.13): 502 Explicit TLS authentication not allowed
(000001/09-12-2019 17:10:49 - not logged in) (125.125.1.13): USER Test
(000001/09-12-2019 17:10:49 - not logged in) (125.125.1.13): 331 Password required for test
(000001/09-12-2019 17:10:49 - not logged in) (125.125.1.13): PASS ---
(000001/09-12-2019 17:10:49 - user (125.125.1.13): 230 Logged on
(000001/09-12-2019 17:10:49 - user (125.125.1.13): 215 UNIX emulated by FileZilla
(000001/09-12-2019 17:10:49 - user (125.125.1.13): FEAT
(000001/09-12-2019 17:10:49 - user (125.125.1.13): 211-Features:
(000001/09-12-2019 17:10:49 - user (125.125.1.13): MOTM
(000001/09-12-2019 17:10:49 - user (125.125.1.13): REST STREAM
(000001/09-12-2019 17:10:49 - user (125.125.1.13): SIZE
(000001/09-12-2019 17:10:49 - user (125.125.1.13): MLST type*size*modify*
(000001/09-12-2019 17:10:49 - user (125.125.1.13): MLSD
(000001/09-12-2019 17:10:49 - user (125.125.1.13): UTF8
(000001/09-12-2019 17:10:49 - user (125.125.1.13): CWD
(000001/09-12-2019 17:10:49 - user (125.125.1.13): MFMT
(000001/09-12-2019 17:10:49 - user (125.125.1.13): EPRT
(000001/09-12-2019 17:10:49 - user (125.125.1.13): EPRF
(000001/09-12-2019 17:10:49 - user (125.125.1.13): 211 End
(000001/09-12-2019 17:10:49 - user (125.125.1.13): PWD
(000001/09-12-2019 17:10:49 - user (125.125.1.13): 257 "/" is current directory.
(000001/09-12-2019 17:10:49 - user (125.125.1.13): TYPE I
(000001/09-12-2019 17:10:49 - user (125.125.1.13): 200 Type set to I
(000001/09-12-2019 17:10:49 - user (125.125.1.13): PASV
(000001/09-12-2019 17:10:49 - user (125.125.1.13): 227 Entering Passive Mode (125,125,1,13,215,230)
(000001/09-12-2019 17:10:49 - user (125.125.1.13): 226 Successfully transferred "/"
Retrieving account settings, please wait...
Done retrieving account settings
(000001/09-12-2019 17:12:50 - user (125.125.1.13): 421 Connection timed out.
(000001/09-12-2019 17:12:50 - user (125.125.1.13): disconnected
```

- Ici, on peut voir que le client est connecté en bas et donc que celui-ci a accès à l'espace d'échange.



```
FileZilla Server (127.0.0.1)
File Server Edit ?
FileZilla Server 0.9.60 beta
Copyright 2001-2016 by Tim Koster (tm.koster@filezilla-project.org)
https://filezilla-project.org/
Connecting to server localhost:14141...
Connected, waiting for authentication
Logged in
Warning: FTP over TLS is not enabled, users cannot securely log in.
Retrieving account settings, please wait...
Done retrieving account settings
Sending account settings, please wait...
Done sending account settings
Retrieving account settings, please wait...
Done retrieving account settings
(000001/09-12-2019 17:31:22 - not logged in) (125.125.1.13): Connected on port 21, sending welcome message...
(000001/09-12-2019 17:31:22 - not logged in) (125.125.1.13): 220-FileZilla Server 0.9.60 beta
(000001/09-12-2019 17:31:22 - not logged in) (125.125.1.13): 220-Welcome by Tim Koster (tm.koster@filezilla-project.org)
(000001/09-12-2019 17:31:22 - not logged in) (125.125.1.13): 200 Please visit https://filezilla-project.org/
(000001/09-12-2019 17:31:22 - not logged in) (125.125.1.13): AUTH TLS
(000001/09-12-2019 17:31:22 - not logged in) (125.125.1.13): 502 Explicit TLS authentication not allowed
(000001/09-12-2019 17:31:22 - not logged in) (125.125.1.13): AUTH SSL
(000001/09-12-2019 17:31:22 - not logged in) (125.125.1.13): 502 Explicit TLS authentication not allowed
(000001/09-12-2019 17:31:24 - not logged in) (125.125.1.13): USER User
(000001/09-12-2019 17:31:24 - not logged in) (125.125.1.13): 331 Password required for user
(000001/09-12-2019 17:31:24 - not logged in) (125.125.1.13): PASS ---
(000001/09-12-2019 17:31:24 - user (125.125.1.13): 230 Logged on
(000001/09-12-2019 17:31:24 - user (125.125.1.13): SYST
(000001/09-12-2019 17:31:24 - user (125.125.1.13): 215 UNIX emulated by FileZilla
(000001/09-12-2019 17:31:24 - user (125.125.1.13): FEAT
(000001/09-12-2019 17:31:24 - user (125.125.1.13): 211-Features:
(000001/09-12-2019 17:31:24 - user (125.125.1.13): MOTM
(000001/09-12-2019 17:31:24 - user (125.125.1.13): REST STREAM
(000001/09-12-2019 17:31:24 - user (125.125.1.13): SIZE
(000001/09-12-2019 17:31:24 - user (125.125.1.13): MLST type*size*modify*
(000001/09-12-2019 17:31:24 - user (125.125.1.13): MLSD
(000001/09-12-2019 17:31:24 - user (125.125.1.13): UTF8
(000001/09-12-2019 17:31:24 - user (125.125.1.13): CWD
(000001/09-12-2019 17:31:24 - user (125.125.1.13): MFMT
(000001/09-12-2019 17:31:24 - user (125.125.1.13): EPRT
(000001/09-12-2019 17:31:24 - user (125.125.1.13): 211 End
(000001/09-12-2019 17:31:24 - user (125.125.1.13): PWD
(000001/09-12-2019 17:31:24 - user (125.125.1.13): 257 "/" is current directory.
(000001/09-12-2019 17:31:24 - user (125.125.1.13): TYPE I
(000001/09-12-2019 17:31:24 - user (125.125.1.13): 200 Type set to I
(000001/09-12-2019 17:31:24 - user (125.125.1.13): PASV
(000001/09-12-2019 17:31:24 - user (125.125.1.13): 227 Entering Passive Mode (125,125,1,13,217,37)
(000001/09-12-2019 17:31:24 - user (125.125.1.13): 226 Successfully transferred "/"
(000001/09-12-2019 17:31:24 - user (125.125.1.13): 150 Opening data channel for directory listing of "/"
(000001/09-12-2019 17:31:24 - user (125.125.1.13): 226 Successfully transferred "/"
```

- Le pirate en tant que "man in the middle" a obtenu l'identifiant et le mot de passe du client et donc a pu se connecter au serveur pour obtenir les données de l'hôte.

Io.	Time	Source	Destination	Protocol	Length	Info
1637	47..	125.125.1.11	125.125.1.13	FTP	197	Response: 220-FileZilla Server 0.9.60 beta
1639	47..	125.125.1.13	125.125.1.11	FTP	64	Request: AUTH TLS
1641	47..	125.125.1.11	125.125.1.13	FTP	99	Response: 502 Explicit TLS authentication not allowed
1643	47..	125.125.1.13	125.125.1.11	FTP	64	Request: AUTH SSL
1645	47..	125.125.1.11	125.125.1.13	FTP	99	Response: 502 Explicit TLS authentication not allowed
1669	47..	125.125.1.13	125.125.1.11	FTP	65	Request: USER User
1671	47..	125.125.1.11	125.125.1.13	FTP	86	Response: 331 Password required for user
1673	47..	125.125.1.11	125.125.1.13	FTP	69	[TCP ACKed unseen segment] Response: 230 Logged on
1675	47..	125.125.1.11	125.125.1.13	FTP	86	[TCP ACKed unseen segment] Response: 215 UNIX emulated by FileZilla
1677	47..	125.125.1.13	125.125.1.11	FTP	64	Request: PASS 123
1678	47..	125.125.1.13	125.125.1.11	FTP	64	[TCP Spurious Retransmission] Request: PASS 123
1679	47..	125.125.1.13	125.125.1.11	FTP	60	Request: SYST
1681	47..	125.125.1.13	125.125.1.11	FTP	60	Request: FEAT
1683	47..	125.125.1.11	125.125.1.13	FTP	176	Response: 211-Features:
1685	47..	125.125.1.11	125.125.1.13	FTP	85	[TCP ACKed unseen segment] Response: 257 "/" is current directory.
1687	47..	125.125.1.13	125.125.1.11	FTP	60	Request: PWD
1689	47..	125.125.1.13	125.125.1.11	FTP	62	Request: TYPE I
1691	47..	125.125.1.11	125.125.1.13	FTP	73	Response: 200 Type set to I
1693	47..	125.125.1.13	125.125.1.11	FTP	60	Request: PASV
1695	47..	125.125.1.11	125.125.1.13	FTP	103	Response: 227 Entering Passive Mode (125,125,1,13,217,37)
1697	47..	125.125.1.13	125.125.1.11	FTP	60	Request: MLSD
1705	47..	125.125.1.11	125.125.1.13	FTP	109	Response: 150 Opening data channel for directory listing of "/"
1709	47..	125.125.1.11	125.125.1.13	FTP	88	Response: 226 Successfully transferred "/"