HTTPS, SFTP, FTPS

Group 5
Mok Chun Yiu 1155030166
Yuen Ka King 1155018969
Lui Siu Kwan 1155028809

Agenda

- HTTPS
- FTPS
- SFTP
- Demo of attack

HTTPS

What is HTTP?

- HTTP is called **H**yper**t**ext **T**ransfer **P**rotocol.
- The foundation of WWW (World Wide Web) is HTTP.
- HTTP allows us to **transfer hypermedia** (graphics, videos, texts, etc..).
- It uses port **80**.

Flaw of HTTP

- It transfers data in **PLAIN TEXT!!!**

Flaw of HTTP(Video Demo)

What is HTTPS?

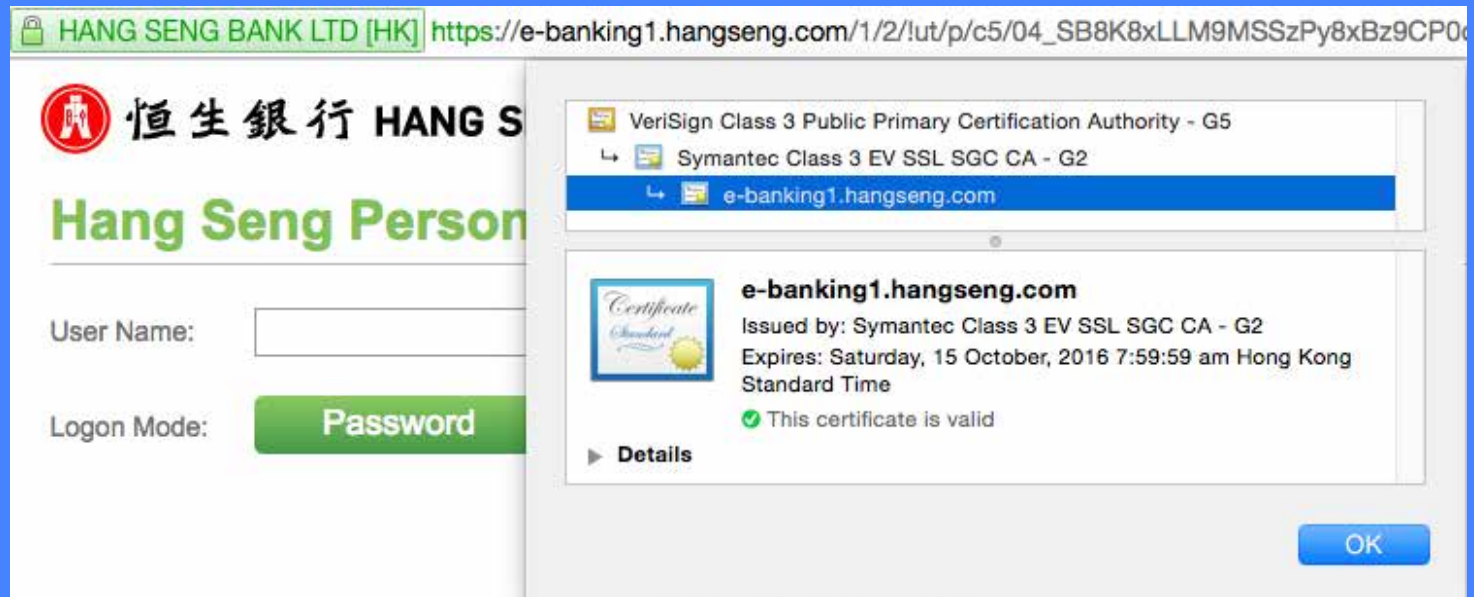
- HTTPS is called Hypertext Transfer Protocol **S**ecure
- It uses port **443**.
- A **communication protocol** for secure communication since the data is **encrypted**.
- It works by **layering** the **HTTP** on top of the **SSL/TLS** protocol.

What is SSL/TLS?

- Both are **cryptographic protocol**
- SSL is the **predecessor** of TLS
- use **X.509 certificates** to authenticate the counter-party

X.509 certificate

- Issuer name (Certification authority)
- Validity period (When it will be expired)
- Subject's Name (for identification)
- Subject's public key(used in encryption)



Encryption in HTTPS

- **Asymmetric encryption** is used in HTTPS.
- Recap:
  - data **encrypted** with **public** key can only be **decrypted** by **private** key

Work flow of HTTPS (Simplified)

- 1) Browser uses the **public** key from the certificate to encrypt the data.
- 2) Browser sends the **encrypted** data to server.
- 3) Server **decrypts** the encrypted data with its own private key.
- Now you know why **symmetric encryption** is not used here.

Types of SSL certificate

1. Extended Validation SSL - Green Bar

2. Standard Validation SSL - No Bar

3. SSL with Errors

Difference between the certificates

- Extend Validation SSL:
  - Long application period(>1 day)
    - the registration authority(RA) need to **valid** your organisation information.
  - Organisation name is shown on the address.
    - ensure the website is from a particular organisation.
  - The price is expensive and it takes at least **USD$100** per year.

Difference between the certificates

- Standard Validation SSL
  - The applications take a few minutes.
  - ensure the website is genuine(correct) **but** not guarantee the website from a particular organisation.
  - The price is cheaper, which is about **USD$7** per year.

When should you use HTTPS

- Handling personal information
- Handling user credentials (username, password)
- Sending secret data (contract)

Benefits of HTTPS

- A proof of a **genuine** website especially if you are using extended certificate.
- Increase user's trust on your website (especially for e-commerce/banking websites)
- Increase the ranking in Google (SEO)

Cons of HTTPS

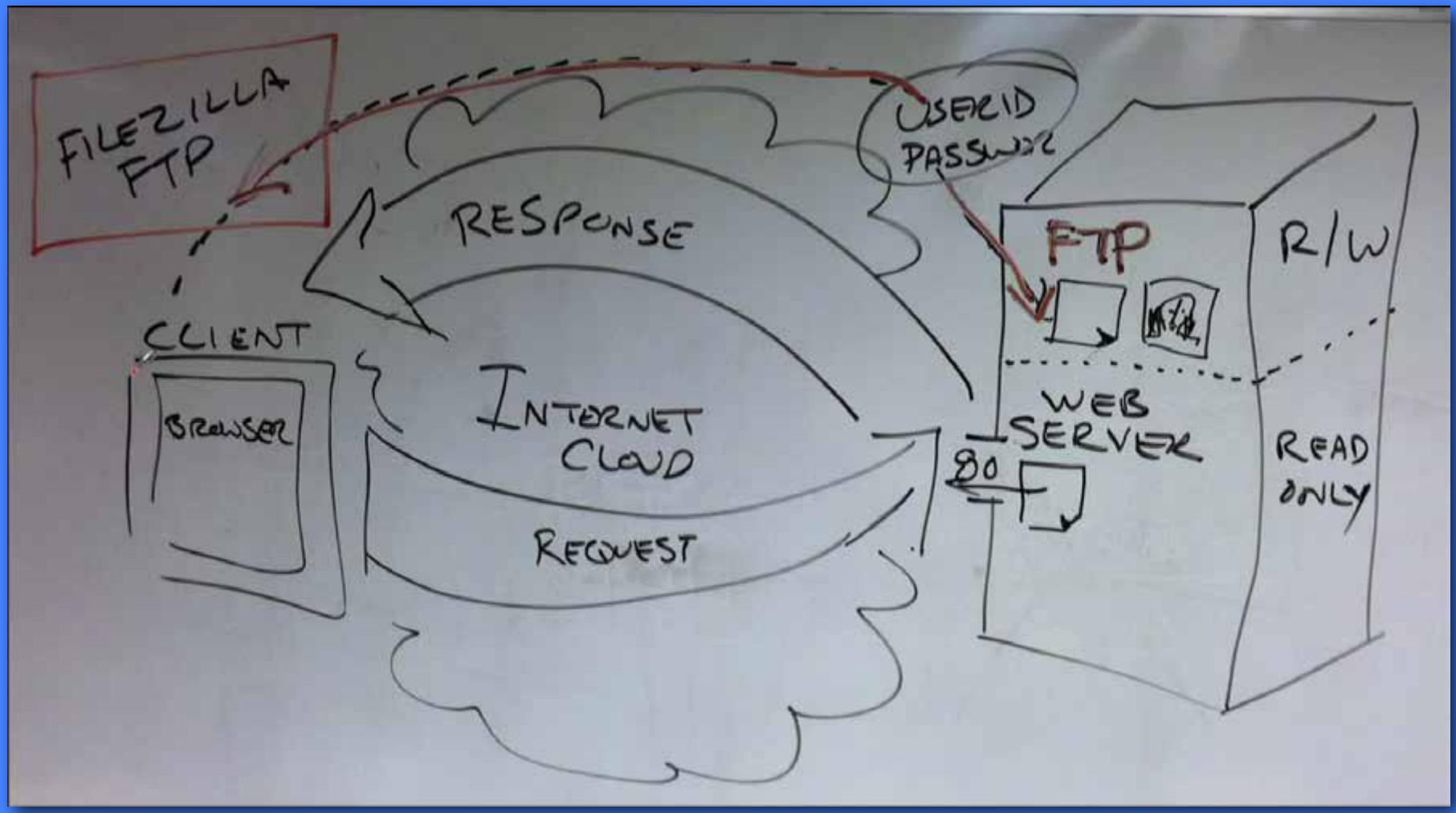
- The fee is not one-off. You need to keep renewing the certificate.
- Needs more configurations like setting firewall rules and web server.
- HTTPS consumes more resources than HTTP since there are encryptions and decryptions.

FTPS

What is FTP?

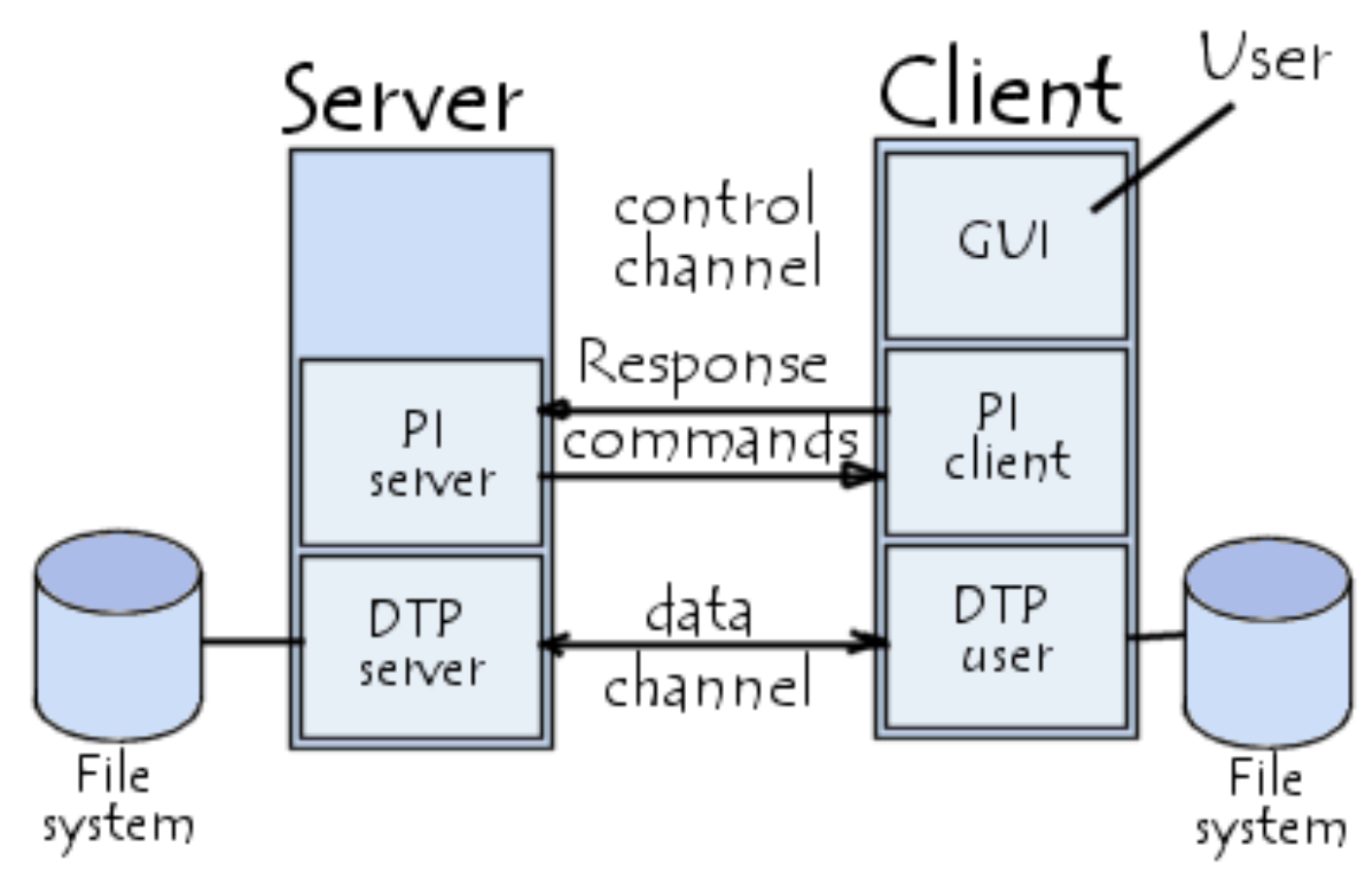
- The protocol for exchanging files over the Internet
- Build on a client-server architecture
- Allow large files for downloading by other computers

What is FTP?



- https://www.youtube.com/watch?v=TyBRbgz-FFs

How FTP works?



Benefits of FTP

- Provide online file storage that enable easier collaboration and higher accessibility
- Provide account management for AAA (authorisation, authentication and accounting)
- Provide all parties to share, manage and update files

Anonymous FTP

- FTP servers normally require authentication, but anonymous FTP allows users with the ability to access the FTP server without password
- Provide fast access to public archives with multiple extended connections
- Have little control over who accesses FTP server or how often they do it

Security of FTP

- FTP transfer data in plaintext
- FTP does not encrypt its traffic
- Username, password, commands and data can be read by anyone (man in-the-middle attack)

What is FTPS?

- **FTPS** is called **F**ile **T**ransfer **P**rotocol **S**ecure
- It is an extension to the commonly used File Transfer Protocol
- Add support for **TLS** and **SSL** cryptographic protocols
- Making FTP safer and easy to use

FTPS Pros

- **Widely known** and **used**
- SSL/TLS has good **authentication mechanisms**
- **FTP** and **SSL/TLS** support is built into many internet communication frameworks

FTPS Cons

- Require **extra CPU power** and **time** to encrypt and decrypt
- Not all FTP servers support **SSL/TLS**
- Not a standard way to **get and change file** and **directory attributes**

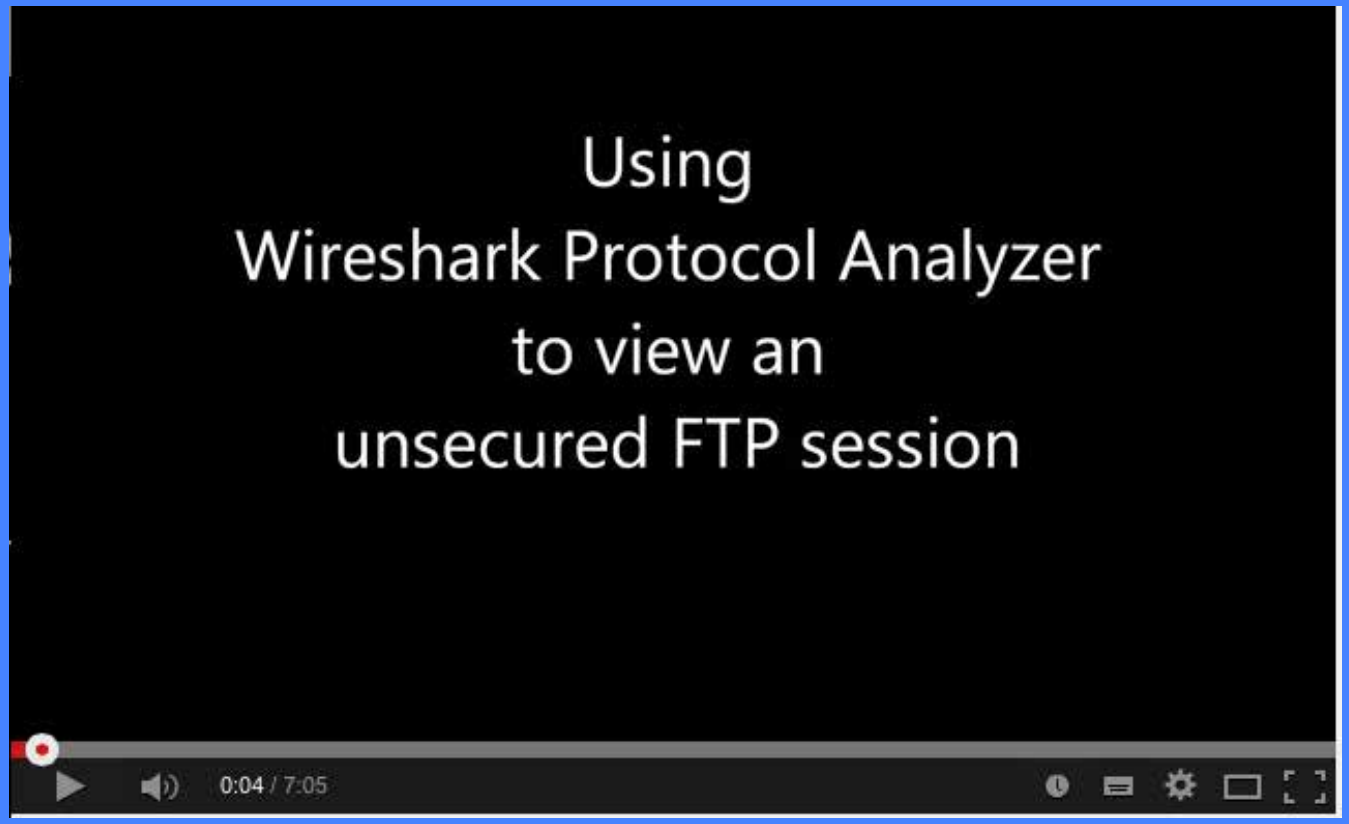
FTP Application

- FileZilla
- CyberDuck
- SmartFTP
- Transmit
- FireFTP
- WinSCP

SFTP

Why use SFTP instead of FTP

Lets watch the youtube !!



https://www.youtube.com/watch?v=DK1MGi5jEtE

FTP and RFC 959

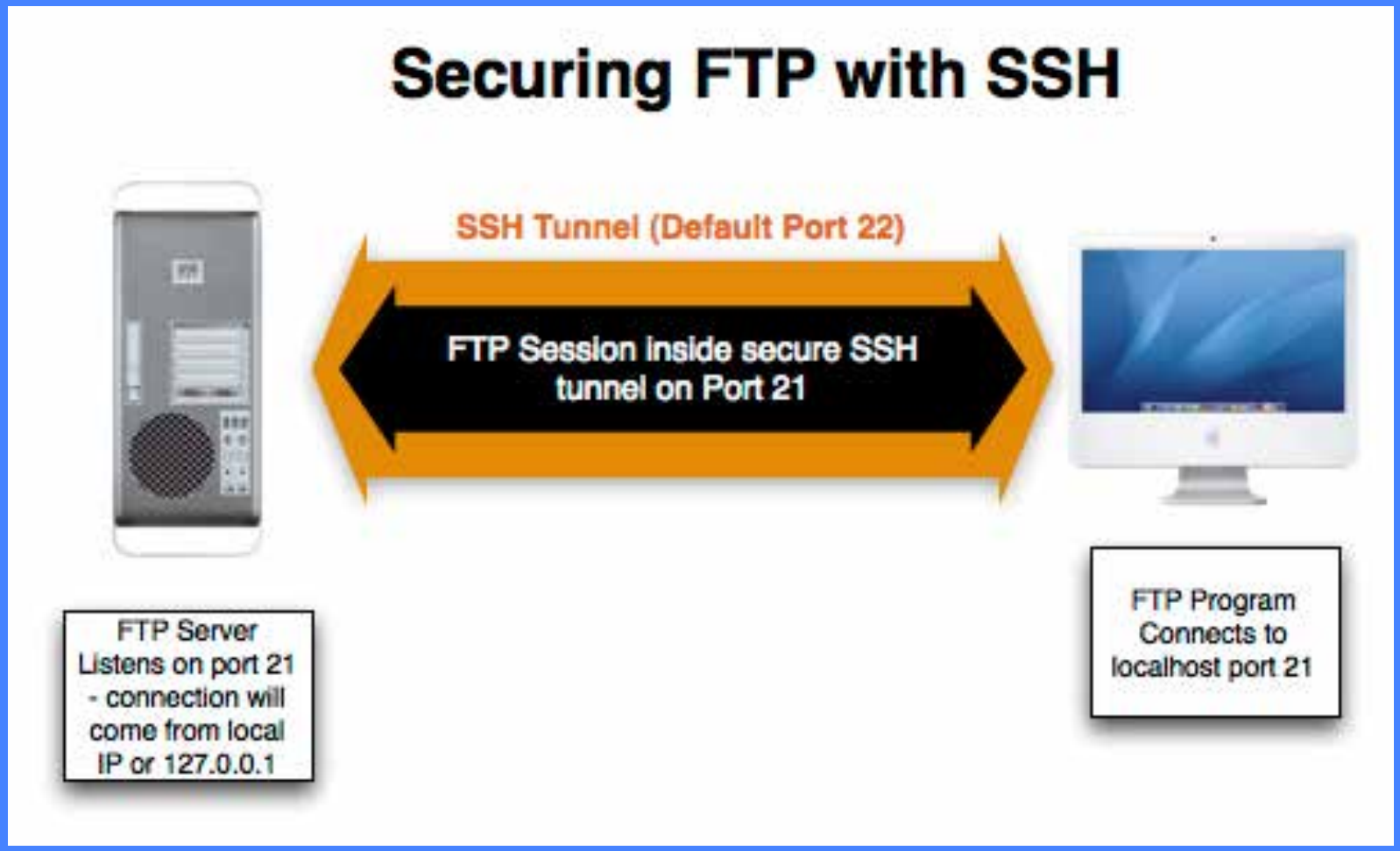
- RFC959 clearly states what the purposes of FTP are:
  - Promote sharing of files...
  - Encourage indirect or implicit (via programs) use of remote computers,
  - Shield a user from variations in file storage systems among hosts,
  - Transfer data reliably and efficiently." (RFC959, J.Postel, J. Reynolds, Oct 1985)

But not force on security!!!!

Why SSH File Transfer Protocol (SFTP)

- Base on SSH
- Operation in port 22
- Encrypted password and file transfer

Why SSH File Transfer Protocol (SFTP)



Why SSH File Transfer Protocol (SFTP)

SSH Encryption

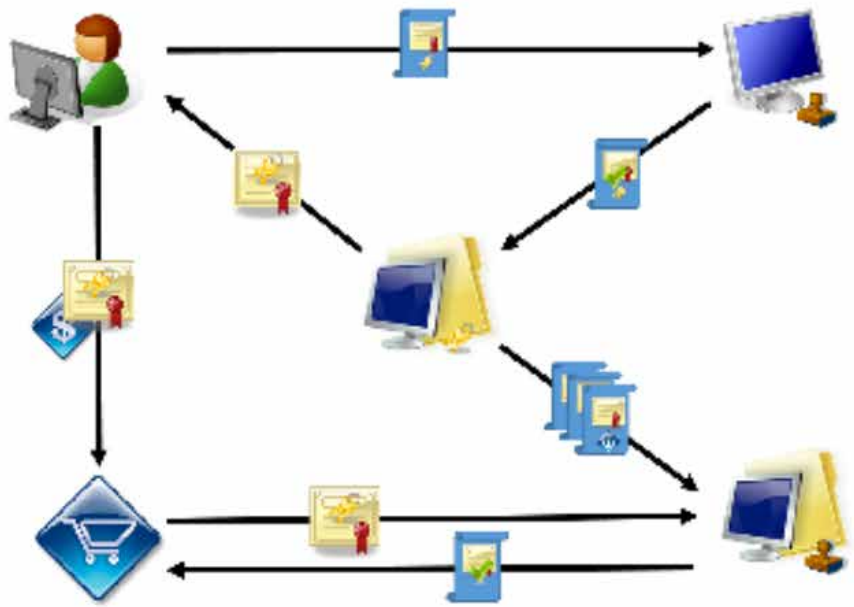
- Application and Transport layer
- Provide Confidentiality and Integrity
- Using public key cryptography to authenticate

PKI infrastructure

Quick Test!!!

A security practitioner is designing a Public key Infrastructure (PKI) to secure transactions over the internet. The design will include a Certificate Authority (CA), a Registration Authority (RA), and a Validation Authority (VA). Choose the correct location for the CA based on the architecture shown below.

Click on the area of the diagram below where the CA should be placed.



Different between SFTP and FTP

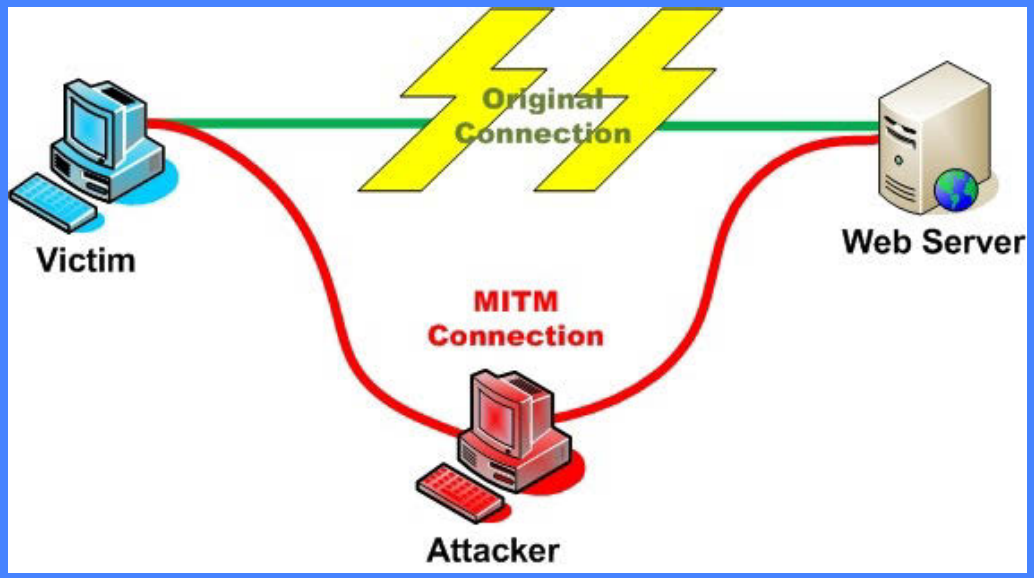
	SFTP	FTPS	FTP
Port	22	21	21
Encryption Method	PKI infrastructure	certification	N/A
Transfer Method	Tunnelling	direct transfer	direct transfer

What happen if we do not use encrypted channel?

Demo Time!!!!!!

Problem!!!!!

- Man-in-the-middle-attack
- Sending Message in Plain Text
- lead to sensitive information disclosure

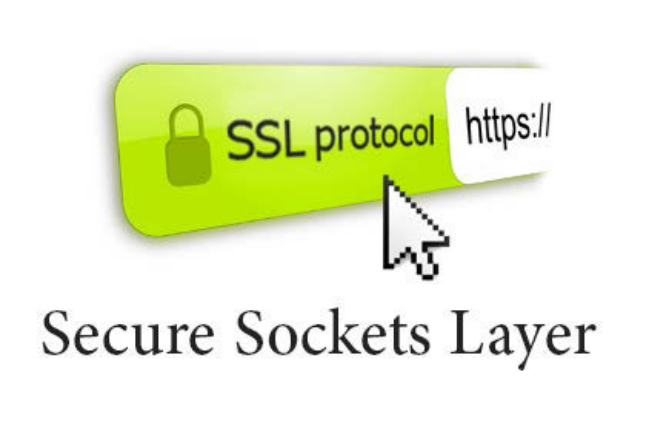


How to protect yourself

- **Secure protocol**

- Do not provide **sensitive information** (such as credit card information) to other

- Be careful when you access the website **without** SSL or HTTPS



Q&A