Université Paris-Est Créteil

Projet Sécurité

Réalisé par :

Mohammed Akram MECHERI

Christopher ARNOULT

Proffesseur :

C. DIMA

2015/2016

Avant Propos:

Ce projet consiste en l'implémentation d'un protocole de transfert de fichiers sécurisé.

Le protocole utulise les algorithmes RSA et DES pour crypter les données transferées entre le serveur et les clients .

Le protocole utilise un systeme d'authentification avec des certificats signés pour valider l'identité du serveur et des clients.

Réalisation du projet :

Pour réaliser ce projet nous avons créé un dossié partagé entre moi et mon binome pour toujours avoir la derniere version du code.

Nous avons communiqué via internet et nous avons travaillé à la bibliotheque universitaire quelques fois.

Etapes de réalisation:

On a commencé par implémenter un serveur qui est créé en SingleTon est lancé sur un port TCP choisis par l'utilisateur .

Le client se connecte sur le serveur en précisant son IP et son port, puis recoit un certificat signé par une authorité unique que lui envoi le serveur, le client vérifi l'authenticité du certificat puis il envoit sont certificat au serveur qui fait la même chose pour vérifié le client.

un certificat contient la clé publique de son possesseur qui est utilisée pour crypter une donée de taille relativement petite (Cryptage Asymétrique RSA), on s'en sert pour crypter la clé de session (qui est une clé DES) et l'envoyer au client.

le client ayant sa clé privée il peut décrypter la clé DES et avoir la la clé de session.

Comme nous avons créé une interface graphique, on a pas besoin d'utiliser des commande pour envoyer et recevoir des fichier, tout est géré par des thread liés à l'interface graphique.

Pour un client donné on a un dossié portant le nom qui apparait sur son certificat oû il peut envoyer ou recevoir des fichiers, en dehors de ce dossier le client n'a pas droit de voir le contenu du serveur.

Difficultées rencontrées :

La principale difficultée qu'on a rencotré est liée à la modélisation du protocole, ça nous a pris pas mal de temps avant qu'on a commencé à coder, nous avons aussi trouvé difficile parfois de débugger les erreurs liées aux buffeurs et au padding des clés.

Mais à la fin de ce projet nous avons bien compris les principe de sécurité des réseaux et la sécurité en Java.