Algorithmes et architectures logicielles de cybersécurité

Projet 1 : Maitriser les bases

Version 1 du 20/09/2024

2024-2025

Samuel Hiard

1. Introduction

Ce document a pour vocation de décrire le projet de programmation que vous devrez réaliser pendant le premier quart de ce quadrimestre. Il est peut être vu comme un « cahier des charges » décrivant le contexte, l'objectif, les fonctionnalités, les modalités, ce qui est attendu, et éventuellement ce qui est autorisé ou interdit. Il peut être soumis à changement.

2. Contexte

Ce premier projet est presque comme une séance d'entrainement. Il a pour objectif de vous familiariser avec l'implémentation des différents concepts du cours théoriques, concepts qui seront les briques de base à réutiliser dans un projet futur.

3. Fonctionnalités souhaitées

Vous écrirez un ou plusieurs programmes dans le(s)quel(s) interviennent un client et un serveur communiquant sur le réseau via le protocole de transport TCP. Dans cet exercice d'entrainement, la communication sera unidirectionnelle (client → serveur), c'est-à-dire que le client enverra un message (chiffré ou non, haché ou non), et le serveur, après traitement éventuel, affichera ce message.

Vous devez implémenter les fonctionnalités suivantes (chaque cas peut faire l'objet d'un test unitaire séparé, voire d'un programme séparé) :

- Le message est chiffré à l'aide de 3DES en mode EBC. Les clés sont hard-codées dans les deux parties. ✓
- Le message est chiffré à l'aide de AES en mode CBC. La clé est générée à l'aide de Diffie-Hellman.
- Le message est haché à l'aide de SHA-1.
- Le message est authentifié à l'aide de HMAC-MD5. La clé peut être hard-codée.
- Le message est signé à l'aide de SHA-1 et RSA. Les clés peuvent être hard-codées ou simplement transmises par le réseau (en tout cas, la clé publique)
- Le message est chiffré à l'aide de RSA. La clé publique provient d'un certificat sauvegardé dans un keystore.

Ensuite, en guise de récapitulatif, vous utiliserez ces morceaux de code pour concevoir une dernière application client/serveur, permettant d'envoyer le message secret : « Coucou », de telle manière que les 4 propriétés cryptographiques soient respectées, à savoir :

- Confidentialité
- Intégrité
- Authentification
- Non-répudiation

Bonus : Idem, mais en laissant le déni plausible.

4. Consignes supplémentaires

- Ce projet est à réaliser par groupe de 3 étudiants.
- Il sera présenté pendant la séance du 4 novembre. Le code source sera envoyé au plus tard ce même jour, par mail à samuel.hiard@hepl.be dans une archive (.rar, .zip ou .7z) au format *XXX-YYY-ZZZ*-MasiSecuProj1.*EXT* où *XXX* et *YYY* sont les noms de famille des trois étudiants ayant participé au projet, et *EXT* l'extension (rar, zip ou 7z) de l'archive.
- Le langage de prédilection est le langage Java, mais vous pouvez utiliser un autre langage si vous le souhaitez. Dans ce cas, l'aide apportée par le professeur pendant les laboratoires sera faible, voire nulle.
- Ce projet compte pour 30% de la note de l'AA (= UE si MASI)
- Considérant le nombre d'étudiants *N* participant au projet,
    - Si $N > 3$, votre cote sera ramenée à 0/20
    - Si $1 \leq N \leq 3$, votre cote sera multipliée par $N/3$, sauf justificatif plausible (ex : le nombre d'étudiants dans la classe n'est pas divisible par 3). Si 3 groupes de 2 étudiants se forment, j'en ferai 2 groupes de 3 étudiants en séparant arbitrairement un groupe en 2 et en assignant ses 2 membres aux 2 autres groupes.
- Amusez-vous bien !