Autorité de certification pour signature d'email

Projet de cryptographie

2022-2023

1 Introduction

Ce projet consiste à créer une autorité de certification (AC) permettant de générer des certificats pour des utilisateurs désirant signer leurs emails. Les certificats seront demandés et délivrés via le portail web d'une autorité d'enregistrement (AE).

Les opérations de l'AC et le l'AE seront majoritairement réalisées à l'aide du logiciel `openssl`.

1.1 Prérequis

Coté utilisateur, vous devez disposer d'au moins deux adresses email de test et installer un client de messagerie pouvant signer et vérifier un message au format S/MIME (comme par exemple Thunderbird). Attention de nombreuses interface web de messagerie (comme par exemple celle de Google) ne permettent pas d'effectuer ces opérations.

Coté serveur, installer un environnement vous permettant de traiter des formulaires simples et de lancer des commandes `openssl` ou autres.

1.2 Réalisation du projet

1. Créer une AC racine (ACR) et son certificat auto-signé avec `openssl ca`. Cette autorité de certification restera hors ligne. Pour la simuler laisser tout ses fichiers sur une clef USB.
2. Créer une autorité de certification intermédiaire (ACI) avec `openssl ca` dont le certificat est émis par l'ACR et qui émettra les certificats des utilisateurs.
3. Créer la page web de l'AE sur laquelle un utilisateur peut soumettre une demande de signature de certificat (*Certificate Signing Request* ou CSR) ainsi que son adresse email.
4. Coté utilisateur générer une paire de clés (avec `openssl genpkey`) et la CSR correspondante (avec `openssl req`).
5. Coté AE traitez la demande de l'utilisateur en commençant par vérifier son email (par exemple en lui envoyant un code à usage unique) et le sujet de la CSR (avec `openssl req`). Si ces vérifications sont positives, demander la génération du certificat à l'ACI et le mettre à disposition de l'utilisateur (avec ceux de l'ACR et de l'ACI).

6. Tester la signature des emails avec votre client de messagerie et leur vérification chez le destinataire.
7. Générer des certificats non valides et tester si le client de messagerie détecte ces cas d'erreur (certificat expiré ou non encore valide, extension *Key Usage* incorrecte, signature par une clé n'appartenant pas à l'ACI, émetteur ne correspondant pas au sujet de l'ACI etc.).
8. Monter une attaque en créant une fausse AC utilisant la paire de clés de l'utilisateur et son certificat. Émettre avec la fausse AC un faux certificat utilisateur (correspondant à une troisième adresse de mail de test). Essayer d'utiliser le faux certificat et vérifier que l'attaque est bien détectée.
9. Créer une page de révocation de certificat sur votre site web permettant à un utilisateur de demander la révocation de son certificat. Pour éviter les dénis de service l'utilisateur devra fournir un code à usage unique qui lui aura été délivré avec son certificat. Il devra également préciser la raison de la révocation. Si le code à usage unique est correct révoquer le certificat.
10. Mettre en place un serveur OCSP avec `openssl ocsp` et renouveler les certificats pour indiquer l'adresse du serveur. Tester une révocation et vérifier qu'elle est bien détectée par le client de messagerie.

1.3 Compte-rendu du projet

Votre compte-rendu du projet comprendra les éléments suivants :
— Une explication de votre choix de logiciels, langages et de librairies.
— Vos choix de sécurité pour les AC et les certificats (algorithmes cryptographiques, tailles de clé, extensions, règles de nommage, périodes de validité ...).
— Description des résultats de chaque étape du projet avec si besoin des scripts et captures d'écrans commentés.
— Retour sur les difficultés rencontrées.
— Les améliorations possibles.
— Une liste des ressources utilisées pour ce projet (site web, code source,...).

1.4 Rendu du projet

Le projet doit être rendu sous forme d'une archive disponible sur un site de partage de fichiers de votre choix que vous me communiquerez par e-mail. L'archive comprendra les fichiers commentés de votre projet ainsi qu'un compte-rendu au format PDF.