Sécurité informatique INF36207

Travail pratique #1

SESSION HIVER 2023

Date limite de remise du TP	14 février 2020 à 22h00
Équipe	Équipe de 2 ou 3 étudiants.
Pondération	15%

Mise en contexte

Vous êtes promu responsable d'un nouveau système de gestion des comptes de banque dans une grande banque mondiale et vous devez assurer l'authentification des utilisateurs qui y accèdent de partout dans le monde. Pour se faire, votre patron vous demande de créer un système d'authentification des utilisateurs à l'aide d'un jeton Ont-Time-Passwrod (OTP) généré électroniquement par une application.

Avant de mettre le tout en application, il vous demande de développer l'algorithme et de faire la preuve de concept en produisant deux applications fonctionnant sous Windows. Soit une application client qui génèrera le jeton OTP et une application serveur qui fera la validation du jeton. Votre patron vous exige d'avoir un jeton ayant une durée de vie maximale de 60 secondes afin de limiter les risques en matière de sécurité.

Développement à faire

Application client :

Il s'agit d'une application fonctionnant sous Windows et qui génère automatiquement un jeton OTP de huit (8) chiffres à toutes les 60 secondes. Vous devez concevoir l'algorithme qui génèrera le jeton pseudo-aléatoire. Vous pouvez utiliser les variables de votre choix sur le poste utilisateur pour la génération du jeton. Notez que l'application doit être autonome et elle ne doit pas recourir à Internet pour générer son jeton. Assurez-vous que l'application serveur puisse être en mesure de générer le même jeton afin de réaliser la fonction d'authentification (comparaison des jetons client/serveur). L'application doit également indiquer dans l'interface utilisateur le temps de validité restant du jeton (compte à rebours de 60s à chaque jeton généré).

Application serveur :

Il s'agit d'une application fonctionnant sous Windows qui attend qu'on y saisisse dans un champ de validation le jeton de huit (8) chiffres générés par l'application client. Si le jeton est valide dans la période de 60 secondes donnée, l'accès est confirmé et l'utilisateur reçoit un message « **Accès confirmé !** ». Si le jeton ne correspond pas, ou encore si la période de 60 secondes est échue, alors l'utilisateur reçoit un message « **Accès refusé !** ». Après 5 tentatives refusées, l'application serveur se ferme. L'utilisateur doit alors l'ouvrir à nouveau.

⇨ Pour des fins de formation, de simplification et d'apprentissage, l'application serveur doit afficher à l'écran le jeton valide du dernier bloc de 60 secondes si aucune entrée n'est saisie dans le champ de validation par l'utilisateur. C'est-à-dire que lorsque le compteur atteint 60 secondes et qu'il passe à un nouveau jeton, l'application doit indiquer le jeton qui était valide dans les 60 secondes précédentes.

Condition de réalisation

Voici les conditions de réalisation dans lesquelles vous devez produire votre travail et vos deux applications :

- Langage de programmation : Libre! Vous pouvez prendre celui de votre choix. Cependant, les applications exécutables (client et serveur) doivent fonctionner dans Windows sans « plug-in » ou framework supplémentaire;

- Algorithme : Il doit être conçu par vous et unique à votre équipe. Il devra être suffisamment robuste pour empêcher les utilisateurs de deviner le prochain jeton qui sera généré sans avoir l'application client en main;
- L'algorithme peut se baser sur des variables internes à l'ordinateur pour générer son jeton mais ne doit pas avoir recours au réseau ou à l'internet;
- Les applications client et serveur doivent être autonomes et doivent être en mesure de fonctionner seules sur des ordinateurs distincts et sans aucune communication entre elles;
- Idéalement, les applications clients et serveurs doivent être portables dans Windows sans nécessiter l'installation d'application, plug-in ou encore de framework particulier.
- Vous devez faire preuve d'une grande autonomie dans le développement de vos applications. Il existe une multitude d'informations à votre portée sur Internet pour vous aider et vous devez en faire usage.

Complément d'information sur le fonctionnement des Jetons OTP

Un jeton d'authentification à un facteur temps (OTP pour One-Time Password) est un type de jeton physique ou logiciel qui génère des codes d'authentification à usage unique. Ces codes sont générés à intervalles réguliers ou sur demande et sont utilisés pour vérifier l'identité de l'utilisateur en combinaison avec un nom d'utilisateur et un mot de passe.

Lorsque l'utilisateur souhaite accéder à une ressource protégée, il est invité à fournir son nom d'utilisateur et son mot de passe standard, ainsi qu'un code OTP généré par son jeton. Le système de validation vérifie alors que le code OTP est valide et correspond à celui attendu pour l'utilisateur déterminé.

Il existe plusieurs façons de générer des codes OTP, mais la plupart des jetons OTP utilisent un algorithme de synchronisation temps qui génère un code basé sur l'heure actuelle et un secret partagé entre le jeton et le système de validation. Cela permet de s'assurer que le code généré par le jeton est valide uniquement pour une courte période de temps.

Il existe différentes façons pour un jeton OTP de communiquer avec le système de validation lors de la synchronisation initiale, cela peut se faire en utilisant un câble USB pour connecter le jeton à l'ordinateur ou en utilisant un protocole de communication dédié pour communiquer à distance tel que OATH (Initiative for Open Authentication) ou RADIUS (Remote Authentication Dial-In User Service). Les jetons peuvent également se synchroniser avec des applications sur smartphones pour générer des codes OTP.

En utilisant un jeton OTP pour l'authentification à double facteur, même si un pirate parvient à découvrir votre nom d'utilisateur et votre mot de passe, il ne pourra pas accéder à la ressource protégée sans le code OTP généré par le jeton. Cela rend les attaques par dictionnaire de mot de passe et d'autres techniques de piratage de comptes beaucoup plus difficiles, car elles nécessitent la possession physique du jeton OTP. C'est pourquoi l'utilisation d'un jeton OTP pour l'authentification à deux facteurs est considérée comme une méthode de sécurité efficace pour protéger les systèmes et les données sensibles.

Livrables pour l'évaluation du travail pratique

Pour que votre travail pratique puisse être évalué par l'enseignant, vous devez déposer les 5 éléments suivants :

1. Un rapport écrit d'un **maximum de 10 pages (sans compter les annexes)** avec les sections suivantes :
    - Page de présentation identifiant le nom des étudiants;
    - Présentation de votre algorithme :
        - Expliquez votre algorithme dans le détail et comment vous garantissez que le même jeton se génère sur les deux applications simultanément
        - Expliquez comment se fait la génération du jeton pseudo-aléatoire sur le client
        - Expliquez comment se fait la validation du jeton pseudo-aléatoire sur le serveur

    - Présentation de votre application client
    - Présentation de votre application serveur
    - Analyse de vos résultats :
        - Problèmes rencontrés, erreurs, bons coups, etc.
    - Conclusion
    - Annexes :
        - Capture d'écran des deux applications
        - Références / Bibliographie
2. Le code source de votre application client
3. Le code source de votre application serveur
4. Un fichier ZIP contenant les applications Client et Serveur exécutables sur Windows (idéalement en version portable ne nécessitant pas l'installation de Framework ou de Plug-In)
5. Les instructions d'utilisation de vos deux applications (documentation typique à remettre aux utilisateurs lors de la remise d'un jeton)

Obligations à respecter

- Vos deux applications doivent fonctionner pour être évaluées.
- Tout comme bon programmeur, votre code doit être bien documenté.
- Si des bouts de code sont inspirés de sources externes (internet, etc.), vous devez documenter vos sources dans l'annexe (références) et faire mention de la portion inspirée.
- Il n'est pas autorisé d'avoir recours à une liste/table de jetons prédéterminés. Les jetons doivent être générés dans l'application client et serveur et ils doivent être différents à chaque redémarrage de l'application.

Barème de correction

Le barème suivant sera respecté pour l'attribution des points sur le travail pratique (total 15 points).

- Applications client et serveur fonctionnelles sur mon poste en Windows 11 : **5 points**
- Rapport complet, clair et bien étoffé : **8 points**
- Appréciation globale (créativité, originalité, ingéniosité, efficacité, simplicité) : **2 points**