IUT DE COLMAR : RESEAUX ET TELECOMUNICATION

Document de Sécurité

MySocket

James Schmitt

Document de Sécurité – MySocket

Confidentialités

Les messages qui sont transmis dans le réseau visible à travers de l'application ne sont pas chiffrés. En effet, ils ne bénéficient d'aucune sécurité et sont transmis en clair sur le réseau, ce qui est une vraie menace pour les utilisateurs souhaitant communiquer de manière anonyme et sécurisée. N'importe quel utilisateur connecté sur le réseau peut voir les messages avec un simple Wireshark. De plus, les données stockées sur la base de données sont elles aussi en clair et peuvent être accédées et crackées facilement avec un outil penteste. L'une des possibilités serait de chiffrer les données sur la base de données avec, par exemple, une clé que seul l'administrateur possède au démarrage du serveur, puis de chiffrer les données transmises entre le client et le serveur avec un système de chiffrement asymétrique pour le chiffrement des messages.

Connexion Serveur/Client

Serveur

Le serveur est la principale vulnérabilité de notre système, car il reçoit tous les messages envoyés par les clients. De plus, les clients transmettent les messages en clair, ce qui fait que si quelqu'un parvient à accéder au serveur par un crack, il pourra lire tous les messages échangés par l'ensemble des clients sur le réseau. Le compte administrateur est créé au premier lancement du serveur, puis enregistré et maintenu actif après connexion. Pour résoudre ce problème, il faudrait mettre en place un système de conteneurisation qui isole complètement le serveur de toute attaque potentielle et chiffrer les requêtes qui sont envoyées vers le serveur.

Client

Le client de MySocket demande un identifiant et un mot de passe à l'utilisateur, mais il n'y a pas de vérification supplémentaire, ce qui représente un risque pour la sécurité et la confidentialité des clients. Une des mesures qui pourrait être prise serait de mettre en place un système d'authentification biométrique ou à deux facteurs. Les comptes sont enregistrés dans la base de données, ce qui est une menace en cas de piratage de celle-

ci, car les mots de passe y sont stockés en clair. Il manque également un système de réinitialisation de mot de passe, qui pourrait être utile, et des bugs sont présents sur l'application.

Limites et avenir

Il est nécessaire de mentionner quelques contraintes propres à ce type d'outil :

- Sécurité et Confidentialité : Le manque de chiffrement des données peut entraîner une fuite des informations à des personnes non autorisées. Il est vivement conseillé de mettre en œuvre des mesures de sécurité efficaces, notamment le chiffrement des communications et des données sensibles.
- Maintenance à Long Terme : Les applications utilisant des sockets peuvent avoir besoin d'une maintenance régulière pour rester compatibles avec les mises à jour des bibliothèques, des systèmes d'exploitation, et pour corriger les problèmes de sécurité. Un plan de maintenance à long terme doit être prévu pour assurer la fiabilité et la sécurité de l'application.

En conclusion, MySocket propose une plateforme de messagerie opérationnelle, mais des améliorations importantes sont nécessaires pour renforcer la sécurité, la confidentialité et assurer une maintenance à long terme.