Rapport de Projet – SAE 3.02
Groupe : Les Pingouins

HARTMANN Quentin & KOUAME Akaza

Table des matières

Architecture distribuée et Routage en Oignon

1. Introduction et genèse du projet

Dans le contexte de la SAE 3.02, nous avons été chargés de concevoir et de mettre en œuvre un système de messagerie anonyme s'appuyant sur le principe du routage en oignon. Lors de la présentation du sujet, une analogie avec le fonctionnement de Tor s'est immédiatement imposée. Ce mécanisme bien connu dans le domaine de la cybersécurité garantit l'anonymat des communications en faisant transiter les messages au travers de plusieurs nœuds intermédiaires, aucun d'eux n'ayant une connaissance complète du chemin parcouru.

L'objectif central était de développer un système cohérent et opérationnel tout en répondant à des contraintes techniques rigoureuses, notamment l'impossibilité d'utiliser des bibliothèques avancées de chiffrement ou de sérialisation. Ces restrictions nous ont poussés à approfondir des concepts abordés en cours, comme la programmation réseau, la gestion des bases de données, et les bases fondamentales de la cryptographie.

2. Organisation du travail et dynamique de groupe

La réalisation du projet s'est appuyée sur une organisation méthodique et une répartition claire des responsabilités. Une phase préliminaire a été dédiée à la définition de l'architecture globale du système, pour identifier le rôle de chaque composant et les interactions entre les nœuds.

Quentin a pris en charge la conception de l'architecture réseau ainsi que le développement du serveur annuaire, une tâche impliquant la gestion des connexions réseau, la communication entre les routeurs et les problématiques liées aux sockets. De son côté,

Akaza s'est occupé du développement de l'interface graphique en utilisant PyQt5, visant à fournir une application utilisateur simple, intuitive et réactive pour visualiser les échanges de messages sans blocage.

Ensemble, nous avons travaillé sur l'implémentation des mécanismes de chiffrement RSA et la gestion de la base de données. Cette étape a nécessité une bonne compréhension des algorithmes mathématiques fondamentaux du chiffrement asymétrique.

3. Problématiques de chiffrement et choix techniques

Le principal défi technologique résidait dans la mise en place d'un mécanisme de chiffrement adéquat. Initialement, nous avons opté pour chiffrer l'intégralité des messages en utilisant le RSA. Bien que viable en théorie, cette solution s'est rapidement avérée inefficace en pratique : à chaque couche de chiffrement ajoutée, la taille des messages augmentait considérablement, entraînant une lenteur excessive des communications.

Pour résoudre ce problème, nous avons adopté un chiffrement hybride : le RSA est utilisé uniquement pour sécuriser une clé de session, tandis que le message lui-même est chiffré avec un algorithme symétrique basique basé sur le XOR. Cette approche a permis de réduire significativement la taille des messages et d'améliorer les performances globales du système.

5. Bilan des compétences acquises et perspectives

Ce projet a été particulièrement instructif sur les plans technique et méthodologique. Il nous a permis de renforcer nos compétences en programmation réseau, sécurité informatique et gestion de projets complexes. Faire face à des choix techniques stratégiques et résoudre des problèmes exigeants nous a appris à adopter une approche structurée et réfléchie dans nos travaux. Avec plus de temps, certaines améliorations seraient envisageables, comme l'intégration d'un mécanisme de surveillance automatisé pour détecter les routeurs inactifs. Malgré cela, le système actuel atteint pleinement les objectifs définis au début du projet.

6. Conclusion

En résumé, cette SAE 3.02 a été une expérience enrichissante qui nous a permis d'explorer concrètement les enjeux de la sécurité et de l'anonymat dans les réseaux. Le projet final abouti démontre qu'il est possible de développer une architecture distribuée sécurisée malgré des contraintes strictes. Cette réalisation consolide notre intérêt pour les domaines des réseaux et de la cybersécurité, tout en renforçant les bases nécessaires pour y évoluer davantage à l'avenir.