Ecole Publique d'Ingénieurs en 3 ans

Rapport

PROJET KEYSHARE - SOUTENANCE DE MI-PARCOURS

Le 22 janvier 2021

HERVAULT Jules, Intégrateur
jules.hervault@ecole.ensicaen.fr
LAMHAMDI Mehdi, Développeur
mehdi.lamhamdi@ecole.ensicaen.fr
PEIGNE Steven, Développeur
steven.peigne@ecole.ensicaen.fr

Client : **Sébastien FOUREY**
Sebastien.Fourey@unicaen.fr

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

www.ensicaen.fr

TABLE DES MATIERES

TABLE DES FIGURES

LE PROJET

Cette partie a pour vocation de rappeler le contexte du projet et de faire une présentation générale du produit.

1. Contexte

L'échange de données est très répandu à travers le monde. On trouve ces données sous plusieurs formes : audios, vidéos, images, etc. Il existe ainsi de nombreux outils qui ont été mis en œuvre pour le partage de ces données entre plusieurs personnes comme les drives ou les serveurs distants. Cependant, n'existerait-il pas un outil spécialisé dans le partage local ?

On entend par partage local le partage à une personne qui est physiquement à proximité comme par exemple dans le même bâtiment. Si on utilise un des outils précédemment cités, on envoie nos données à des dizaines, des centaines voire des milliers de kilomètres pour leur faire parcourir le chemin inverse. Sur la figure ci-dessous, une flèche met en lien le serveur Google de Dublin à Caen : la distance parcourue par les données pour un aller est comprise entre 620 km (distance à vol d'oiseau) à 1120 km (distance en véhicule). Cela est à la fois gourmand en énergie, en temps et en efficacité. Cet échange imparfait met en cause notre responsabilité sociétale et environnementale.

Figure 1 Localisation des Datacenter de Google en Europe

Cette responsabilité sociétale et environnementale prend de plus en plus de place dans le monde de l'informatique. En effet, l'informatique s'étend dans de plus en plus de domaine pour permettre des avancées technologiques plus rapides. Cependant, il ne faut pas avancer au détriment de la société ou de l'environnement. Un exemple concret mettant en avant la responsabilité sociétale est la mise en place de l'open source qui d'ailleurs s'étend au-delà de l'informatique.

2. Présentation de notre solution

Le projet a été nommé partage sur réseau local façon KISS par le client. L'équipe projet nomme la solution Key Share. L'acronyme KISS signifie Keep It Simple, Stupid (*reste simple, idiot* en français).

Le produit réalisé est un logiciel informatique qui permet le partage de fichiers entre deux ordinateurs sur un réseau local tel que celui du bâtiment E de l'école d'ingénieur Ensicaen. L'acronyme KISS fait quant à lui référence à la simplicité d'utilisation du logiciel. Des compétences de programmation réseau seront donc mises en jeu mais aussi des compétences d'interfaces graphiques.

Le principe de notre solution est un échange codifié entre deux acteurs sur deux machines distinctes. Nous expliquons avec détail dans le diagramme de séquence ci-dessous son fonctionnement actuel :

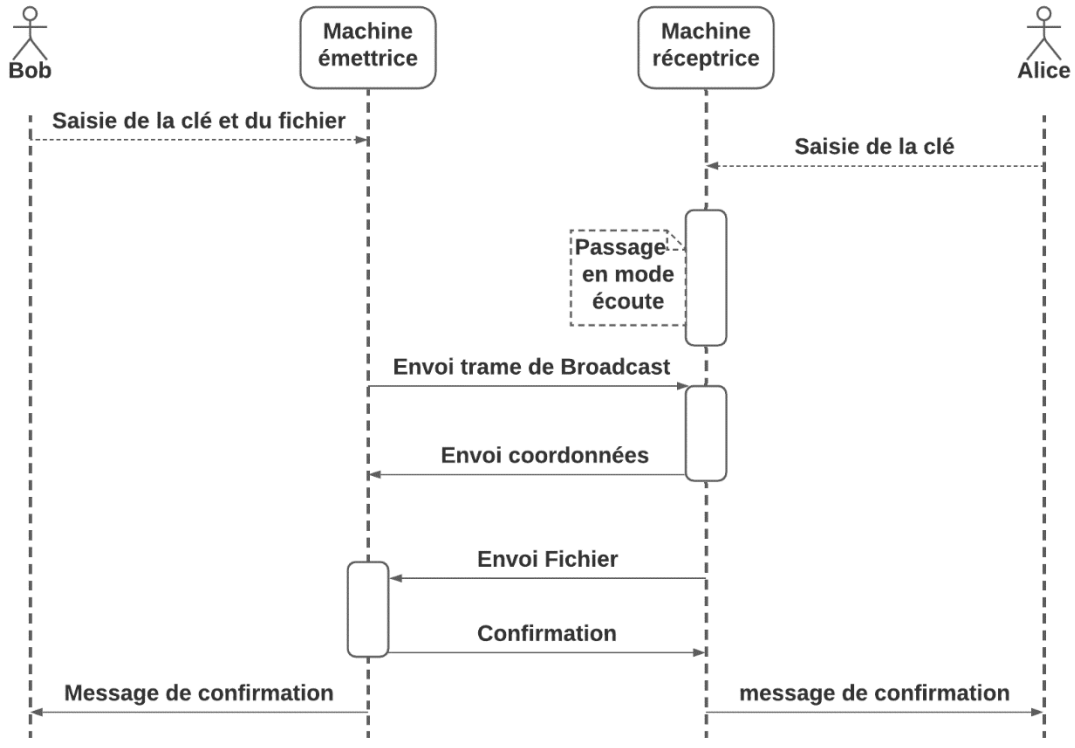

Figure 2 Diagramme de séquence du logiciel KeyShare

Dans ce cas, nous imaginons que Bob initie le transfert de fichier donc que Alice cherche à récupérer le fichier transféré. Les noms Alice et Bob sont purement fictifs. La clé doit être transmise par Bob à Alice dans le monde physique par oral ou par écrit. Cette clé n'est pas nécessairement un code indéchiffrable mais doit être tenu secret par Bob et Alice afin de sécuriser l'échange.

3. Objectifs

Les objectifs ci-dessous reprennent le diagramme de GANTT suivant :

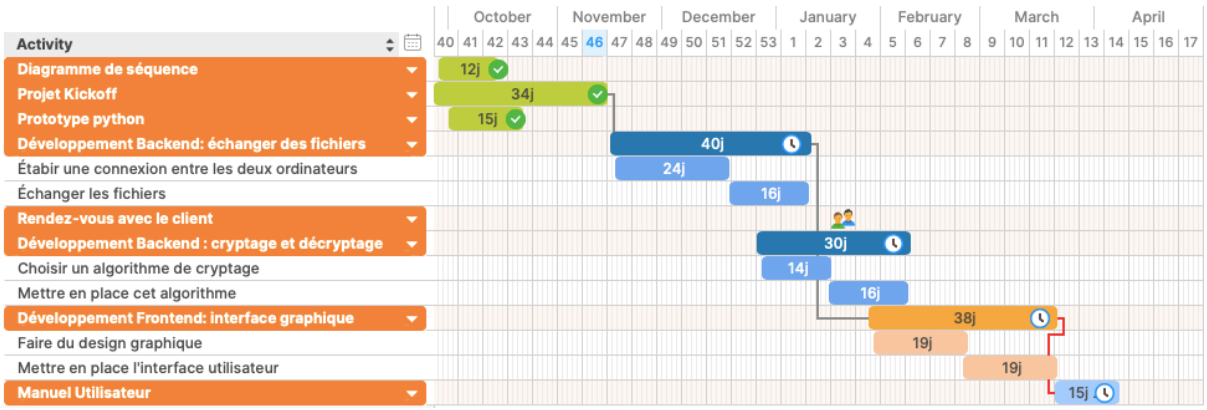

Figure 3 Diagramme de GANTT créé pour le kick-off

3.1. Mi-parcours

1. Echanger les fichiers avec un programme exécutable en ligne de commande
    a. Créer un protocole d'échange
    b. Prouver que ce protocole est cohérent grâce à un prototype
    c. Etablir une connexion entre deux ordinateurs qui souhaitent communiquer
    d. Echanger un fichier entre ces deux ordinateurs
2. Ajouter de la sécurité à l'échange par du cryptage et décryptage de données
    a. S'assurer qu'un cryptage des données est utile pour notre échange
    b. Etudier les algorithmes de cryptage et décryptage existant
    c. Choisir un algorithme de cryptage adapté à notre situation

3.2. Finaux

Les objectifs finaux reprennent les objectifs mi-parcours et les complètent.

2. Ajouter de la sécurité à l'échange par du cryptage et décryptage de données
    d. Implémenter cet algorithme
3. Façonner une interface graphique cohérente et naturelle d'utilisation
    a. Faire un croquis des fenêtres utiles pour notre logiciel
    b. S'assurer de la simplicité et du naturel de l'interface
    c. Implémenter cette interface
4. Préparer un manuel utilisateur

GESTION DE PROJET

Cette partie se concentre sur la gestion de projet les outils utilisés par l'équipe lors de ce début de développement.

1. Méthodologie

Un planning sous la forme d'un diagramme de Gantt a été réalisé (voir Figure 3). Ce planning met en avant des périodes de 2 à 3 semaines pendant lesquelles des tâches précises sont favorisées. Ces tâches ne sont pas dirigées par un membre précis de l'équipe.

Etant donné la taille réduite de l'équipe projet, nous avons opté pour des réunions régulières afin de poursuivre le projet. Cependant, il n'y pas de hiérarchie au sein de l'équipe sauf pour la gestion du code avec un intégrateur et des développeurs.

2. Outils

Afin de partager efficacement le code entre les différents acteurs, nous avons mis en place un dépôt GitLab dont le serveur est hébergé par l'école d'ingénieur Ensicaen. Pour le code, afin de faciliter l'accès à certaines données comme les adresses IP des utilisateurs, nous utilisons la bibliothèque réseau SFML. Elle est légère et efficace quant à la récupération de données réseau. De plus, cette bibliothèque existe aussi sous Windows.

Pour la communication, nous utilisons Facebook Messenger pour les messages d'information dans l'équipe, Microsoft Outlook pour la communication avec le client, Discord pour les réunions de l'équipe et Big Blue Button pour les réunions avec le client. Facebook Messenger est déjà beaucoup utilisé dans la vie étudiante donc nous avons profité d'être tous présents sur l'application pour l'utiliser.

Nous utilisons des environnements de développements différents en ce début de projet. Pour la partie de conception d'interface graphique, nous favoriserons majoritairement le langage Qt et son IDE QtCreator, utilisé pour les travaux pratiques de conception d'interface graphique en C++. Le langage Qt à l'avantage d'être multiplateforme donc nous permet de déjà nous diriger vers l'objectif de développement généralisé pour l'application.

SITUATION ACTUELLE

1. Objectifs et travail réalisé

Nous avons réalisé les tâches suivantes :

- Créer un protocole d'échange
- Prouver que ce protocole est cohérent grâce à un prototype
- Etablir une connexion entre deux ordinateurs qui souhaitent communiquer
- Echanger un fichier entre ces deux ordinateurs
- S'assurer qu'un cryptage des données est utile pour notre logiciel
- Etudier les algorithmes de cryptage et décryptage existant

Cela implique que nous avons un programme fonctionnel en ligne de commande mais des remarques sont à émettre. En effet, nous nous sommes rendu compte que la propagation de la clé par le récepteur pour l'émetteur n'est pas sécurisée. Il faut donc rajouter une étape afin de signifier qu'un récepteur veut se connecter au programme de l'émetteur avant de faire le partage de la clé. Pour l'instant, la clé est partagée en même temps que la demande de connexion qui se fait forcément en broadcast.

Dans le cadre de la sécurité notre projet, on s'est demandé s'il est nécessaire de recourir à un algorithme de cryptage. En effet, le but premier du projet est de permettre un échange de fichier en réseau local. De ce fait, les attaques dans le but de récupérer le fichier envoyé seront limitées à une zone géographique proche. On peut donc voir la simple initiative d'un échange de fichiers en réseau local comme une manière de sécuriser l'envoi et la réception du fichier. Cependant, si l'on prend en compte les connexions de type Wi-Fi, le risque d'une récupération illicite du fichier est accru donc la sécurité plus utile.

2. Objectifs non atteints

Les tests unitaires et fonctionnels de notre programme n'ont pas été réalisés. En effet, la structure du projet ne semble pas adaptée à des tests. Cependant, avec l'interface graphique, nous allons avoir une architecture différente et qui sera peut-être propice au développement de tests.

L'utilisation de la bibliothèque SFML au détriment des sockets du C créé des dépendances qui pourraient ne pas exister. Les sockets du C représentent en effet une alternative intéressante car elle contient très peu de dépendances et est complète. Cependant, son utilisation n'est pas naturelle quand on cherche à contacter un utilisateur spécifique et n'est pas adapté à la programmation objet.

3. Suite du projet

Pour la suite du projet, nous décidons de ne pas implémenter de cryptage pour les raisons émises ci-dessus. Bien qu'il paraisse naturel qu'un échange soit fait de manière sécurisée, ce n'est pas un objectif principal ici. Cependant, il faudra revenir sur le programme exécutable afin de corriger une faille de sécurité inscrite dans le diagramme de séquence.

Ainsi, la suite de projet se consacrera à la création d'une interface graphique dont l'utilisation est naturelle et au développement multiplateforme. En effet, la bibliothèque SFML existe sous Linux et sous Windows donc nous permet de compiler des exécutables adaptés pour Linux et pour Windows. Ce souhait provient de la volonté de rendre le logiciel utilisable par des personnes qui ne connaissent que peu de choses en interface graphique. Or, Windows est le système d'exploitation prépondérant dans le grand public.

BILAN

1. Ce qui a fonctionné

Le diagramme de Gantt et les autres diagrammes permettent d'analyser de manière concise le projet dans ses contraintes et ses objectifs. Cela permet ainsi de bien démarrer le projet et de mieux visualiser les objectifs pour l'équipe projet. Ainsi, nous avons pu découper le travail en tâches bien distinctes et organiser ce travail de manière efficace.

La communication à distance n'a pas posé de problèmes car aux nombreux outils à notre disposition (Discord, BBB, Outlook). Nous avons pu facilement partager le code sur GitLab et donc nous répartir efficacement le développement du code. Malgré un obstacle de perte de matériel sous Linux par Monsieur Peigné, aucun retard n'est à signaler car la perte est récente. Le développement pour la suite ne sera pas impossible car l'IDE cité pour le développement d'interface graphique a été installé sous Windows.

2. Ce qui n'a pas fonctionné

Le diagramme de Gantt n'a pas été suivi à la lettre car nous n'avons pas d'organisation interne afin de s'assurer d'une avancée constante du projet. En effet, il n'y a pas de hiérarchie dans l'équipe projet ce qui fait qu'aucun membre n'est associé au suivi du projet pour s'assurer d'une avancée régulière. Les solutions pour corriger cette erreur sont soit de choisir une méthode de travail comme une méthode agile soit de désigner un chef de projet. Les méthodes agiles assurent un rendu et un travail régulier sur un projet peu importe l'avancement alors qu'un chef de projet permet un suivi régulier du projet et des tâches effectuées.

Dans un premier temps, il a été suggéré par le client de travailler avec le moins de dépendances possibles donc de ne pas utiliser la bibliothèque SFML. Pour un compromis d'efficacité à cause d'un retard pris dans l'avancée du projet, nous avons préféré utiliser cette bibliothèque. De plus, la bibliothèque SFML existe aussi sous Windows et peut permettre de faciliter le développement du logiciel sur plusieurs systèmes d'exploitation.

ENSI CAEN

ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

Ecole Publique d'Ingénieurs en 3 ans

6 boulevard Maréchal Juin, CS 45053
14050 CAEN cedex 04

ministère éducation nationale enseignement supérieur recherche

Normandie Université

Cti Commission des titres d'ingénieur

cdefi Conférence des Directeurs des Écoles Françaises d'Ingénieurs

European Accreditation of Engineering Programmes EUR-ACE®

CONFÉRENCE DES GRANDES ÉCOLES