Louis ALLAIN

CyberKey

Déverrouillage par empreinte biométrique de la salle Cyberlab de l'UBS

Introduction

L'idée principale de ce projet est de faciliter l'accès à la salle D111 (nommée CyberLab) pour le personnel, les enseignants et les étudiants de l'Université de Bretagne Sud. Pour cela, il est proposé de fournir à ces acteurs un outil numérique leur permettant d'accéder au CyberLab.

En effet, l'accès à cette salle doit être surveillé car elle contient du matériel parfois fragile et/ou sensible d'utilisation comme une imprimante 3D, une machine-outil à commande numérique (CNC), divers matériels électroniques tels que des composants, des cartes à micro-contrôleurs. De plus, il est nécessaire que seule des personnes averties se servent des machines informatique puisque celles-ci sont configurées d'une manière bien précise.

C'est pour cela que cette salle est toujours verrouillée par une serrure à clef sauf pendant les heures de cours utilisant cette salle ou sur demande des étudiants. Le système actuel est tel qu'un jeu de clef existe et que les professeurs souhaitant accéder à cette salle peuvent l'ouvrir en récupérant la clef au préalable.
En ce qui concerne les étudiants, cet accès est plus restreint et demande une organisation. Actuellement, les étudiants doivent répondre à un sondage en ligne sur le site web "Framadate" où ils indiquent quels sont les créneaux où ils souhaitent travailler dans la salle puis au moment venu, ils vont chercher la clef du CyberLab auprès d'Axel Jacome, l'ingénieur en charge de la D111.

Pour faciliter l'accès à la salle pour tous les acteurs l'utilisant, je propose de numériser cette clef afin que chacun en dispose selon ses besoins et surtout, selon les disponibilités et les contraintes d'emploi du temps.

Le projet sera constitué de trois éléments principaux. Une serrure électronique communicante. Une clef numérique qui prendra la forme d'une application mobile disponible sur téléphone portable. Et, d'une application d'administration sur le web gérant les accès des personnes selon un calendrier et des horaires.

Présentation du soumissionnaire du projet

Je suis étudiant en Master 2 parcours systèmes et applications pour l'informatique mobile (SAIM) à l'Université de Bretagne Sud. Dans mon parcours universitaire nous avons déjà développé des d'applications mettant en oeuvre des concepts et des technologies susceptible de se rapprocher du projet que je propose.

En effet, le projet sera constitué de programmation web tant côté client que côté serveur, un domaine que nous avons mis en oeuvre à quelques reprises.

Il sera également constitué par de la programmation de cartes à micro-contrôleurs, spécialité que nous traitons à l'heure actuelle dans mon cursus. Et, à titre personnel j'ai déjà développé un projet lié à ces cartes qui était un distributeur automatique de nourriture pour animaux.

Une grande tâche du projet sera aussi de développer une application mobile pour Android destinée aux utilisateurs. Pour cela, j'ai déjà une expérience professionnelle liée à une technologie permettant de programmer une application native disponible sur les deux systèmes d'exploitation en écrivant un seul programme. Cette technologie se nomme "React Native", j'ai pu la mettre en oeuvre lors d'un stage de 3 mois dans l'entreprise "Les Druides du Web" pendant lequel nous avons développé une application citoyenne. J'ai pu également en faire l'expérience à travers un petit projet personnel comme un lecteur de musique sur téléphone.

Enfin, une dernière tâche non négligeable du projet sera de faire communiquer tous les éléments cités ci-dessus. Grâce à la spécialité SAIM, nous avons fait l'expérience de la programmation réseau en faisant communiquer des processus via des sockets TCP/UDP par exemple. Nous avons également des connaissances sur ce qui concerne l'administration d'un système mais aussi et surtout, en ce qui concerne le projet, de la mise en réseau. De plus, nous avons exploré les protocoles et les technologies de réseau sans fil, des notions qui m'ont été importantes lorsque j'ai dû choisir les outils et les procédés de communication.

Plan d'action

Pour le plan d'action, je choisis de le découper en plusieurs éléments constituants le projet avec à chaque fois une description détaillée de ce qui les compose. Je propose par le suite un planning prévisionnel de toutes les tâches.

Gestion des comptes utilisateurs et des données du système

Pour l'ensemble des éléments constituants le projet, j'ai choisi d'utiliser les services Firebase de Google. Ces services fournissent notamment des APIs d'authentification gérant directement les mots de passes et le chiffrement nécessaire relatif à ces données sensibles. De plus Firebase fournit un service de base de données noSQL. Ces services peuvent être utilisés par des applications mobiles, des applications web et des carte à micro-contrôleurs comme les ESP32, les Arduino, ...

Ainsi, le point central où toutes les données transitent sera cette base de données en tant que service.

Application mobile utilisateur

Cette application sera destinée aux utilisateurs du CyberLab, elle leur permettra de déverrouiller la porte de la salle. Pour cela, l'application comprendra trois parties principales.

1. La création/destruction de compte et la connexion

Afin d'identifier de manière unique chaque personne, il est nécessaire d'enregistrer des comptes utilisateurs. Cette création de compte pourra se faire uniquement si la personne est étudiante au sein de l'UBS, c'est-à-dire dans ce cas si la personne possède une adresse mail appartenant au domaine "univ-ubs.fr". Le déroulement de la création de compte se fera comme suit. La personne inscrit son adresse mail et un nouveau mot de passe avec une confirmation de mot de passe dans laquelle l'utilisateur doit inscrire deux fois ce nouveau mot de passe afin d'éviter les erreurs de saisies. De plus, la sécurité du mot de passe sera évalué en vérifiant uniquement si la longueur de celui-ci est supérieur à 8 caractère. Si l'email n'a pas déjà été utilisé par une autre personne (ceci est fait en pratique en consultant la base de données Firebase) et si les conditions sur le mot de passe sont valides alors l'application valide la création de compte en ajoutant ce nouvel utilisateur à la base de données et l'authentifie. Dans le même temps, l'application ajoute à la base de données le couple adresse mail / clef publique RSA. Cette clef publique sera utilisé par la suite afin d'authentifier l'utilisateur lorsqu'il souhaitera déverrouiller la porte (voir le point "3. Le déverrouillage de la porte" de cette partie).
Il est également possible de supprimer son compte utilisateur.

Pour se connecter le procédé est légèrement différent puisqu'il s'agit simplement pour l'utilisateur de saisir son adresse mail et son mot de passe. L'application compare ces données aux données de la base et dans le cas où elles concordent, l'authentifie. Dans le cas contraire, le système prévient l'utilisateur que cet email n'existe pas ou que ce mot de passe n'est pas celui correspondant à l'adresse email saisie.

2. Les demandes d'accès à la salle CyberLab

Pour correspondre au mieux aux contraintes actuelles d'utilisations de la salle, nous distinguerons deux catégories d'utilisateurs. Les professeurs ou personnels de l'université et les étudiants.

La première catégorie doit pouvoir jouir d'un accès plus libre à la salle sans contrainte d'horaire. C'est pour cela qu'il sera possible d'envoyer à l'application d'administration (détaillée dans les parties suivantes) une demande d'accès libre. Si cette demande est acceptée alors l'utilisateur pourra déverrouiller la porte sans contrainte d'horaire. A noter que cet accès "spécial" peut être révoqué à tout moment.

La seconde catégorie, les étudiants, doivent être contraints par des plages horaires. C'est pour cela qu'ils devront procéder à des demandes d'accès régulières en sélectionnant les créneaux disponibles pendant lesquels ils souhaitent accéder à la salle ou bien annuler ceux dont ils n'ont plus besoin. Ces créneaux seront affichés dans l'application sous forme de calendrier en consultant la base de données. Ainsi, l'administrateur ajoute des créneaux de disponibilité et valide les demandes d'accès ou les révoque (le détail de cette procédure est détaillée dans la partie consacrée à l'application d'administration).

Toutes les décisions prises en rapport avec les accès seront notifiés à l'utilisateur par email à l'adresse indiquée lors de la création de son compte.

3. Le déverrouillage de la porte

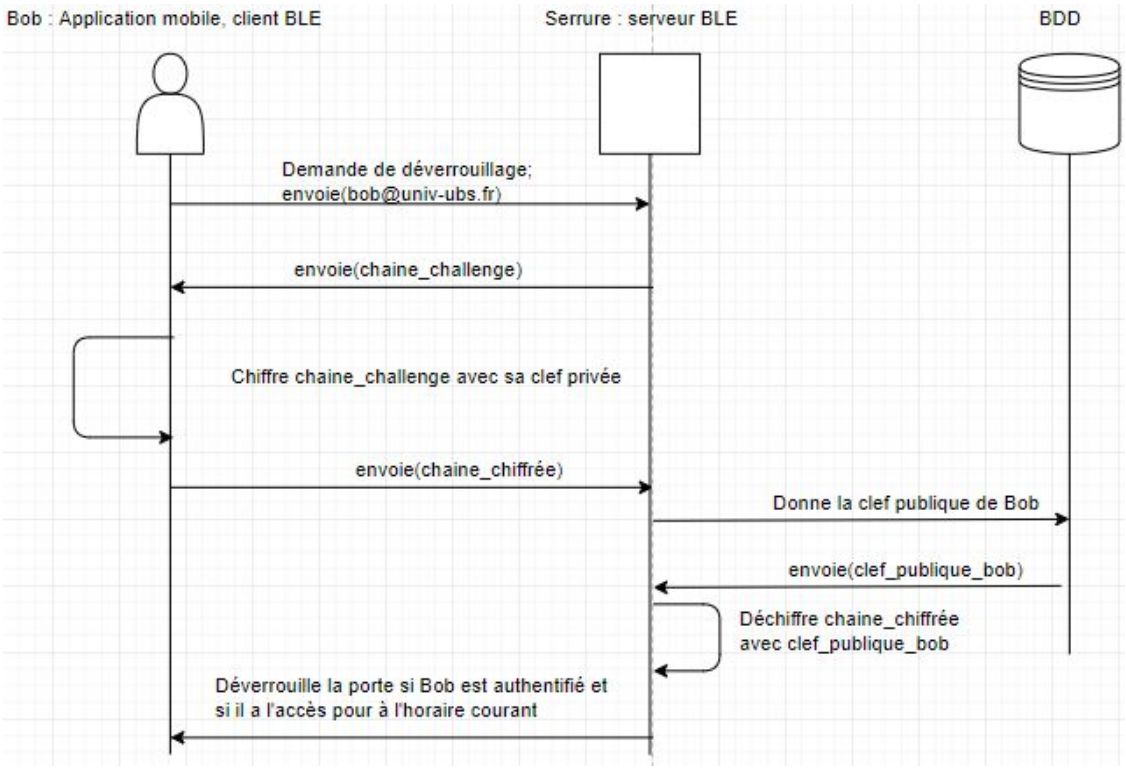
La communication entre l'application mobile et la serrure se fera par Bluetooth Low Energy (BLE). En effet, cette technologie s'y prête tout à fait puisqu'elle permet d'envoyer des petites quantités de données grâce à un Bluetooth beaucoup moins gourmand en énergie. La serrure agira en tant que serveur BLE (voir les détails dans les parties suivantes) et l'application sera le client.

Pour se connecter automatiquement à la serrure (le serveur BLE), le client commence par scanner les équipement BLE alentours, au moment où le client BLE repère la serrure de manière unique grâce à son adresse MAC, le client tente de se connecter à celle-ci. Pour que la connection aboutisse, il faut que le client soit à portée du serveur, que l'application est accès au Bluetooth de l'appareil et que le serveur soit dans un état permettant d'accepter les connections.

Une fois la liaison effectuée, il faut pouvoir authentifier le client. En effet, l'objectif final étant d'envoyer son adresse mail au serveur, il faut éviter que n'importe qui envoie une adresse mail qui n'est pas à lui et qui lui permettrait de déverrouiller la porte sans y avoir été autorisé. Pour cela, une fois la liaison BLE active, le serveur envoie une chaîne de caractère. Lorsque le client récupère cette chaîne, il la chiffre avec la clef privée correspondant à la clef publique transmise à la base de données lors de la création de son compte. Une fois cette chaîne de caractère chiffrée, le client la transmet au serveur. Le serveur va par la suite tenté de déchiffrer cette chaîne de caractère avec la clef publique disponible sur le serveur. Si la chaîne qu'il a envoyé précédemment correspond à la chaîne déchiffrée, alors le client est authentifié.

Une fois l'utilisateur authentifié, la serrure consulte la base de données afin de vérifier si l'administrateur lui a accordé l'accès à l'horaire courant.

Un schéma page suivante résume le procédé après la liaison BLE active. C'est un schéma simplifié dans lequel toutes les préconditions et toutes les initialisations ne sont pas représentées.



Application web d'administration

Cette application sera destinée à l'administrateur du système. Une personne de confiance permettant de coordonner tous les éléments du projet.

Cette interface comportera les éléments suivants :

1. La phase de connexion

Un élément très simple puisque ce sera simplement une authentification par le duo nom d'utilisateur et mot de passe. Ces informations seront insérés en dur via la console Firebase qui permet d'ajouter manuellement un utilisateur dans la base de données.

2. La gestion des accès et des utilisateurs

En ayant accès aux informations depuis la base de données Firebase, l'administrateur pourra ajouter des créneaux de disponibilité de la salle selon le jour et l'horaire sous forme d'un calendrier. En sélectionnant un créneau, il pourra voir quels utilisateurs ont un accès et s'ils ont un accès "spécial" leur permettant d'accéder à la salle sans contrainte de créneaux (avec la possibilité de le révoquer). De plus il pourra voir quels sont les utilisateurs qui sont en attente d'accès pour ce créneau avec une méthode permettant de valider l'accès ou de le refuser.
Sur ce calendrier, l'administrateur pourra également voir le nombre d'utilisateurs acceptés et en attente. De plus, une liste de demandes d'accès de tous les créneaux sera également disponible afin de mettre en évidence ces demandes.

Serrure électronique

Cette serrure sera composée de plusieurs éléments :

1. Une carte à micro-contrôleur ESP32

L'ESP32 sera le contrôleur électronique des opérations de déverrouillage. Il agira en tant que serveur BLE en attente de connexion des utilisateurs souhaitant déverrouiller la porte. Ce contrôleur sera chargé d'authentifier les utilisateurs qui se connectent via la procédure décrite au point 3 de l'application mobile. Pour cela, la carte devra avoir un accès à l'internet en étant connecté à un point d'accès Wifi il aura un accès à la base de données Firebase afin de vérifier les informations transmises.
Le contrôleur sera également chargé de commander le déverrouillage de la porte une fois l'authentification effectuée. Pour cela, la carte pilotera un relai électrique fonctionnant en 5V capable de contrôler des équipements électriques d'une charge maximale en courant continu de 30V/10A (très suffisant pour une serrure électrique dans notre cas).
Ce relais sera déclenché automatiquement par la carte en envoyant un signal de 3.3V à l'authentification d'un utilisateur.

2. Une serrure à commande électrique

La serrure devra être capable d'être contrôlé électriquement lorsqu'elle est alimentée par un courant électrique suffisant. Pour cela je propose pour une première approche que cette alimentation soit fournie par une batterie 12V externe. L'idéal serait d'alimenter la serrure grâce au raccordement électrique de la salle et d'utiliser un transformateur 220V AC/ 12V DC. Néanmoins, je suppose ne pas avoir les autorisations ni les compétences nécessaires à la mise en place de ce système. Cela dit, pour un produit fini, remplacer la batterie 12V par le système décrit ci-dessus ne pose pas réellement de problèmes majeurs.
La serrure devra aussi être ouverte manuellement (en cas de coupure de courant) par une clef classique. Elle devra aussi être déverrouillable de l'intérieur sans aucune clef grâce à l'action d'un bouton mécanique par exemple pour des problèmes de sécurité (incendie, panne de courant).

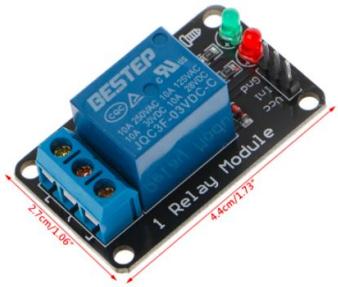
Outils et matériels nécessaires à la réalisation du projet

Pour ce projet, il faudra :

- Un ordinateur pour programmer et développer l'ensemble des éléments (j'utiliserai principalement mon ordinateur personnel),
- un téléphone Android pour tester l'application (j'utiliserai le mien),
- un micro-contrôleur ESP32 (dans le cadre de ma formation, nous en avons en libre accès),
- un relai électrique pilotable en 3.3V ou 5V capable de contrôler des équipements électrique d'au moins 12V/1A en courant continu,
- une serrure électrique actionnable par un courant de 12V/1A en courant continu mais également actionnable par une clef à l'extérieur de la salle et par un bouton mécanique à l'intérieur de la salle.

Après certaines recherches, j'ai pu repérer un relai et une serrure pouvant être utilisée pour ce projet sur le site aliexpress.com dont voici les liens :

Le module relai : https://fr.aliexpress.com/item/4001252221218.html



La serrure électrique : https://fr.aliexpress.com/item/4000051602103.html

Planning prévisionnel, liste des tâches et des résultats produits

Mois d'octobre :

- Création et mise en place de la base de données,
- développement de l'interface web d'administration.

- **Résultat** : fin octobre, livraison de l'application d'administration sous forme d'une URL à laquelle est accessible l'application plus de la documentation sur cette application. L'hébergement sera chez Heroku..

Mois de novembre :

- Développement de l'application mobile utilisateur.
- **Résultat** : fin novembre, livraison de l'application mobile utilisateur sous forme d'un fichier de type "apk" à installer directement sur un mobile Android et la documentation correspondante.

24 Novembre : Revue de mi-projet

A ce moment je présenterai oralement les deux résultats fournis précédemment ainsi que l'avancé globale du projet. Un rapport écrit sera également fourni.

Mois de décembre :

- Développement de la serrure électronique :
    - Programmation de la carte ESP32,
    - montage des composants.
- **Résultat** : le système électronique de déverrouillage sous forme d'assemblage de composants ainsi que des schémas et de la documentation explicative.

8 Janvier : Revue finale du projet

Lors de cette revue finale, je fournirai un rapport qui sera une synthèse de la réalisation du projet. De plus, il y aura une présentation orale du projet avec une démonstration si les conditions s'y prêtent.

Evaluation des risques

Les risques inhérents à ce projet sont essentiellement dû au fait qu'il faudra commander des composants électroniques venant essentiellement de Chine. Le risque étant que ces composants n'arrivent pas à temps entre le moment de la commande et de la livraison. Surtout en cette période de crise sanitaire où beaucoup de livraisons sont retardés.
Si la serrure n'arrive pas dans les temps, je propose de la remplacer par un actionneur quelconque fonctionnant en 12V comme un moteur, une lampe voire même un buzzeur.
Si je ne parviens pas à obtenir le relais, dans ce cas l'utilisation de la serrure ne pourra pas se faire. Je propose donc en cas de problèmes, de remplacer le relais par un voyant lumineux comme une led par exemple.