Louis Allain - M2 SAIM

CyberKey

Présentation de fin de projet

Problématique

- Partager l'accès à la salle Cyberlab
  - Pour tous ses utilisateurs (enseignants, personnels et étudiants)
- Accès contrôlé et surveillé
  - Matériel fragile et/ou coûteux
  - Configuration informatique et réseau particulière
  - Organisation en fonction de la disponibilité de la salle (cours, maintenance, …)

La salle Cyberlab contient du matériel et une configuration qui doivent être surveillés et sauvegardés. Pour cela, il faut que les accès à la salle soit contrôlée. Actuellement, la salle est verrouillée en permanence sauf pour les cours, les TPs et sur demande des étudiants au préalable à l'ingénieur qui s'occupe de cette salle. Pour que les étudiants est accès librement à cette salle, ils doivent d'abord remplir un sondage en ligne où ils indiquent quels sont les créneaux où ils occuperont la salle. Ainsi, l'ingénieur de la salle peut s'organiser pour disposer des créneaux aux étudiants lorsque la salle n'est pas occupée ou en maintenance.

Objectifs

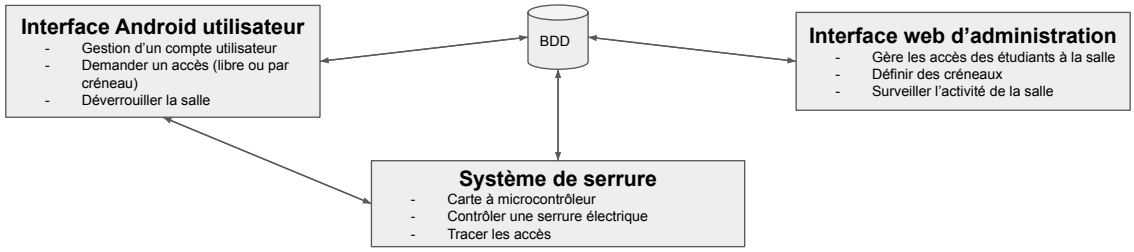
- Développement d’un clef virtuelle disponible pour tous les utilisateurs de la salle
  - Accès à la salle librement
  - Ou accès à la salle selon des contraintes de créneaux
- Création d’une plateforme d'administration
  - Définit des créneaux disponibles aux utilisateurs
  - Gère (accorder / révoquer) des accès pour un utilisateur à un ou plusieurs créneaux
  - Surveille l’activité de la salle

Pour répondre à tous ces problèmes les objectifs étaient de créer une sorte de clef virtuelle pour les utilisateurs dont les accès sont gérés et surveillés par l’ingénieur de salle simplement. Pour cela, la clef virtuelle destinée aux utilisateurs devait permettre d’accéder à la salle soit librement (cas d’utilisation surtout destinée aux enseignants et aux personnels de l’université) soit d’accéder à la salle temporairement pendant des créneaux horaires disponibles

La gestion des utilisateurs et des créneaux se fait grâce à une plateforme d’administration gérée par l’ingénieur de la salle. Elle devait permettre à l’administrateur de la salle de définir des créneaux pour les utilisateurs, d’accorder ou de révoquer les accès libre ou les accès pour des créneaux spécifiques et de surveiller l’activité de la salle.

Solution technique à ces objectifs

- Trois parties
  - Une application web d'administration (destinée à l'ingénieur de la salle uniquement)
  - Une application mobile Android qui sert de clef virtuelle (destinée aux utilisateurs de la salle)
  - Un système de serrure électronique capable d'interagir les autres modules du projet (base de données, application mobile)



Pour répondre à ces objectifs la solution technique proposé était de développer trois modules qui constituait donc le projet dans sa globalité. Une application web d'administration destinée à l'ingénieur de salle uniquement, une application mobile Android destinée aux utilisateurs de la salle et un système de serrure électronique capable de déverrouiller physiquement la porte de la salle D111.

Application web d’administration

- Développé à l’aide du cadre de conception React JS
- Gestion des créneaux sous la forme d’un calendrier
  - Ajout automatique des cours depuis le calendrier ADE de l’UBS
  - Exportation / Importation de créneaux depuis un fichier JSON
- Gestion des accès libre
  - Accorder / révoquer une demande accès libre sans contrainte d’horaire
- Gestion des accès sous contrainte de créneaux
  - Accorder / révoquer une demande d’accès pour un créneau
- Journalisation
  - Visualiser tous les accès à la salle avec l’identité (adresse mail) de l’utilisateur qui a accédé à la salle

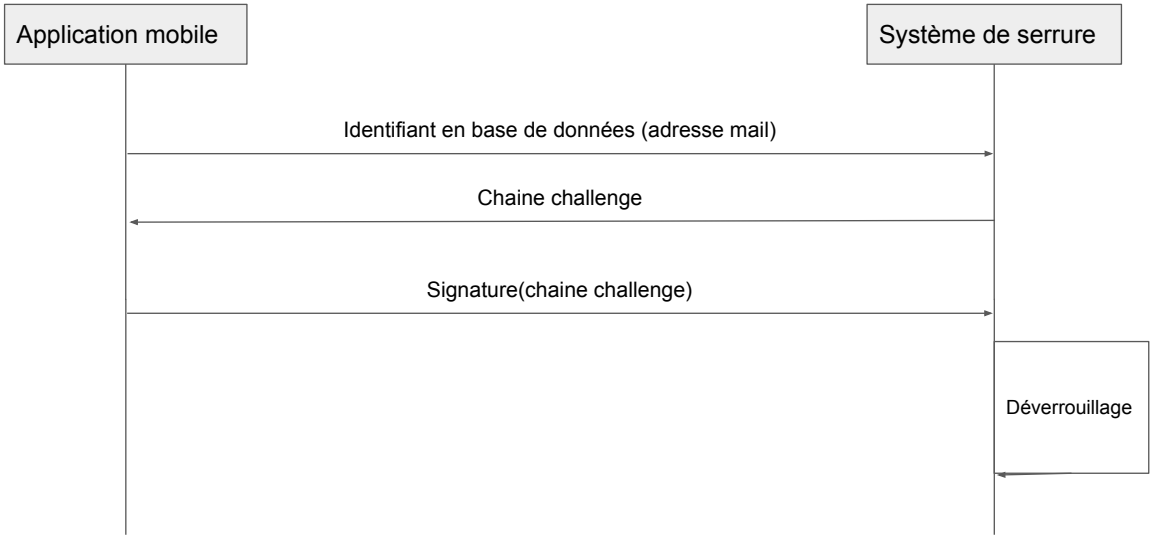
L’application web d’administration à été développé à l’aide du cadre de conception React JS. Elle permet de visualiser les créneaux sous forme d’un calendrier. Sur ce calendrier il est affiché (et ne sont pas supprimables) les créneaux de cours récupérés depuis l’agenda ADE de l’UBS. Sur ce calendrier il est possible de créer des créneaux disponibles aux utilisateurs auxquels ils pourront faire des demandes d’accès. Cette application permet aussi de gérer les accès, que ce soit des accès libre sans contrainte de créneaux ou justement des accès sous contrainte de créneau. L’application permet aussi de visualiser sous forme d’une liste tous les entrées effectuées par des utilisateurs dans la salle.

Application mobile Android utilisateur (1/2)

- Développé à l'aide du cadre de conception React Native
- Gestion d'un compte utilisateur
  - Création / suppression de son compte
- Visualiser les créneaux et gérer ses demandes d'accès
  - Liste de créneaux divisée par semaine
  - Trois états pour un créneau (Accès non demandé, accès demandé, accès accordé)
- Déverrouillage
  - Communication BLE avec la serrure électronique
  - Vérification de l'accès (soit libre soit pour le créneau courant)
  - Scan BLE (cherche le système de serrure), connexion, procédure de déverrouillage

Cette application permet aux utilisateurs de la salle de visualiser tous les créneaux définis par l'administrateur de la salle, de demander des accès et elle permet évidemment de déverrouiller la serrure électronique si l'utilisateur possède effectivement le bon accès.
A la création d'un compte, un couple de clefs asymétriques RSA de taille 1024 octets est créé, la clef publique est sauvegardée en base de donnée et la clef privée est sauvegardé sur le gestionnaire de clef du système mobile. Ce système de clef permet par la suite d'authentifier l'utilisateur au moment du déverrouillage de la serrure électronique.
Lorsque l'utilisateur souhaite déverrouiller, elle tente de communiquer grâce à BLE avec la serrure électronique. Tout d'abord elle scan les équipements BLE à proximité, si la serrure est trouvée l'application s'y connecte et entame la procédure de déverrouillage.

Application mobile Android utilisateur (2/2)



Pour l'application mobile utilisateur la procédure de déverrouillage consiste tout d'abord à envoyer au système de serrure électronique son identifiant en base de données (adresse mail), la serrure répond en envoyant une chaîne de caractère challenge. L'application signe ce challenge avec sa clef privée créé à la création du compte puis envoie cette signature au système de serrure, si la signature est correctement vérifiée par le système de serrure alors la porte est déverrouillée.

Système de serrure électronique (1/3)

- Composants
  - ESP32 Dev Kit
    - Contrôler tous les autres composants
    - Serveur BLE (requêtes de déverrouillage)
  - Ecran OLED SSD1306
    - Retour visuel aux utilisateurs
  - Relais 3.3V
    - Actionne la serrure électrique
  - Serrure électrique
    - Déverrouille la porte

Le système de serrure électronique est composé d'un ESP32 Dev kit qui gère tous les autres composants, d'un écran OLED permettant d'effectuer un retour à l'utilisateur, d'un relais permettant d'actionner la serrure électrique et d'une serrure électrique

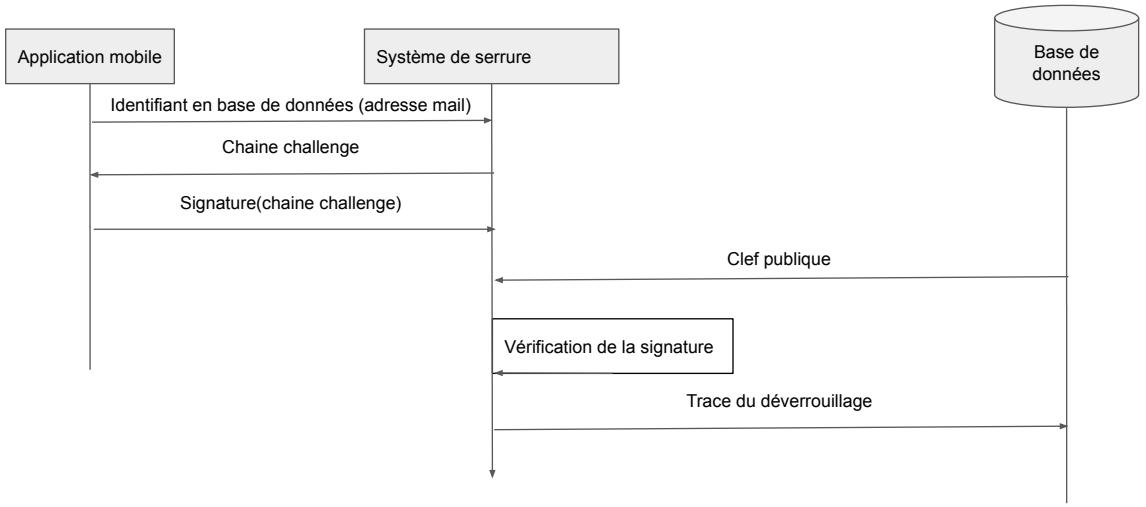
Système de serrure électronique (2/3)

- Serveur
  - Une requête de déverrouillage à la fois
  - Résiste aux erreurs de transmission ou d'abandon de procédure
  - Authentifie l'utilisateur grâce au système de clef RSA
  - Journalise les déverrouillages en base de données

L'ESP32 qui constitue en partie le système de serrure électronique agit en tant que serveur BLE répondant aux requêtes de déverrouillage de la part des applications mobiles utilisateurs. Plusieurs requêtes ne peuvent pas être traitées en parallèle. Ce serveur est résistant aux erreurs de transmission ou d'abandon de procédure en cours. Il authentifie l'utilisateur qui envoie une requête grâce à un système de signature RSA. Il journalise les déverrouillages en base de données.

Système de serrure électronique (3/3)

Procédure de déverrouillage côté système de serrure électronique



La serrure électronique est perpétuellement en attente d'une connexion de la part d'un client. Lorsqu'un client se connecte, la carte attend 3 secondes avant de se réinitialiser si le client n'envoie par son identifiant en base de données. Si un client envoie son identifiant avant ce délais, la carte répond en envoyant une chaîne challenge. Après l'envoie de cette chaine la carte attend de nouveau 3 secondes avant que le client ne réponde en envoyant la signature de la chaîne challenge.
Une fois la signature reçu avant les 3 secondes, alors le client a envoyé toutes les informations nécessaire et la demande de déverrouillage peut être traitée. La carte se connecte donc à un réseau WiFi puis se connecte à un serveur NTP afin de récupérer la date courante.
La carte se connecte ensuite à la base de données du projet afin de récupérer la clef publique de l'utilisateur. Grâce à cette clef publique et avec la signature reçu précédemment, la carte vérifie la signature. Si la signature est authentifiée, alors la carte actionne le relais qui déverrouille la serrure électrique pendant 3 secondes puis ajoute une trace de cette ouverture dans la base de données.
L'utilisateur peut visualiser le traitement de cette procédure grâce aux informations affichées sur l'écran OLED du système de serrure.
Le délais moyen entre l'envoie de la requête de déverrouillage depuis l'application mobile et le déverrouillage effectif est de 7 secondes environ en étant à une porte de moins de 10 mètres.

Démonstration vidéo