Université Internationale de Casablanca
LAUREATE INTERNATIONAL UNIVERSITIES

Ecole privée d'ingénierie
Génie Informatique
Année Académique 2022-2023

Sécurité SI: vote en ligne sécurisé

Objectif : est de mettre en œuvre les techniques de chiffrement vues dans le cours et simulées sous OpenSSL. Ce projet, consiste à mettre en place un système de vote électronique sécurisé avec deux autorités de gestion séparées physiquement ou logiquement. Une autorité pour identifier les votants et l'autre pour compter les votes. Aucune des deux autorités n'a assez de pouvoir pour tricher de son propre chef.

Enoncé du projet :

Dans une entreprise multinationale, son PDG (président-directeur général) désire organiser un vote à distance électronique entre les personnelles des filières de l'entreprise avec moins de coût (sans les déplacer) pour élire un nouveau responsable dans son siège. Pour cela, un ensemble de n correspondant ou personnels désirent participer dans le vote des m candidats en utilisant la messagerie électronique sécurisée via l'outil OpenPGP.

Chaque votant Vi sera identifié par son nom, son prénom et sa date de naissance. On affecte à chaque votant un numéro de vote ID. Vi possède une clé publique KpVi connue de tout le monde et une clé privée KprVi. Un votant envoie deux messages chiffrés contenant son bulletin de vote B et son numéro d'identification ID à deux centres CO et DE. Les clés privée et publique de DE sont KprDE et KpDE. Les clés privée et publique de CO sont KprCO et KpCO.

Un centre de comptage (CO) : Ce centre reçoit un message chiffré d'un votant Vi, contenant les informations (ID, B chiffré et destiné à DE) avec les restrictions suivantes : CO pourra lire ID et ne doit pas accéder au bulletin de vote B. CO possède une liste contenant nom, prénom, date de naissance et ID de tous les votants. Son rôle est de vérifier l'identité de Vi à partir d'ID et la clé publique de Vi. Ensuite, CO marque Vi sur la liste pour éviter un second vote de ID. Enfin, CO chiffre (ID, B chiffré et destiné à DE) et l'envoie au centre DE.

Un centre de dépouillement (DE) : Ce centre reçoit le message de CO et le message chiffré de Vi contenant (ID, B). Sa tâche consiste à déchiffrer les deux messages sans possibilité l'identifier Vi. Si après déchiffrement les deux messages sont égaux à (ID, B) alors le vote de Vi sera validé.

Travail à faire : Proposer et développer un protocole de vote en utilisant les différentes clés publiques et privées, ainsi que les techniques de chiffrement/déchiffrement. Ainsi, d'afficher les statistiques de vote sur le web de l'entreprise.

Durée du projet : Deux semaines.

Chaque groupe doit préparer son rapport final du projet et l'envoie à khalil.ibrahimi@gmail.com.

Outils : html, Java Script, PHP, Mysql, Access, Apache, VB, GnuPGP, …