Université Paul Sabatier
TOULOUSE III

L2 Informatique **Projet S3**

Sécurité et confidentialité du vote électronique.

Vincent Dugat - Octobre 2021

Remarque
- Le protocole et les algorithmes doivent être publiques pour la transparence.

Vote : sécurité et transparence
- le protocole est-il sûr ?
- y a-t-il des bugs d'implémentation (failles involontaires)
- y a-t-il des portes dérobées (failles volontaires)
- le code qui s'exécute est-il le même que celui dont j'ai vérifié le source ?
- qui a accès à la machine ? Connexion internet, ports externes, accès physique ?
- y a-t-il des fichiers de log avec des informations sensibles ?
- La chaîne de traitement des votes est-elle longue ? Quels sont les étapes et fichiers intermédiaires et qui y a accès avec quel droits ?
- Comment puis-je vérifier que mon vote a bien été pris en compte ?
- Comment puis-je vérifier que mon vote est conforme à mon choix ?
- Comment puis-je vérifier que les calculs sont corrects ?
- si le fichier résultat est publique avec les noms des votants anonymisés par hashcoding, avec la liste des votants, peut-on avec une attaque brute force savoir qui a voté quoi ?

Que sait-on ? Les sept premiers points ci-dessus sont des failles potentielles difficiles à maitriser.
Pour les suivantes on peut dire ceci :
- chacun peut, avec sa clef privée, vérifier que son vote est présent dans le fichier et qu'il est conforme.
- le fichier de vote étant publique, chacun peut refaire les calculs pour vérifier les résultats.
- Le HMAC ajoute une clef secrète qui rend les attaques brute-force très compliquées. Malgré tout, il existe des outils puissants pour ce type de calculs. La clef doit être longue et aléatoire pour minimiser ce type de risque. La sécurité est liée à la puissance de calcul d'un attaquant potentiel.