Rapport d'audit sur les élections étudiantes UCL 2018

Édouard Cuvelier

6 avril 2018

1 Préambule

Conformément au règlement électoral en son article 25, la commission électorale a désigné un auditeur pour effectuer l'audit du processus et des résultats du vote électronique. Lors de sa réunion du 6 février 2018, elle a désigné Édouard Cuvelier, auteur de ce rapport, en tant qu'auditeur.

La mission de l'auditeur commence avant le scrutin, se poursuit durant les élections et se termine après celles-ci. Voici en substance ses tâches :

Avant le scrutin

- surveillance de la génération des clés et de leur distribution,
- audit du code informatique.

Pendant le scrutin

- contrôle des valves électorales,
- suivi général des élections et des procédures (revote, annulation de vote).

Après le scrutin

- résolution des votes litigieux,
- contrôle des valves électorales,
- surveillance de l'intégrité de l'urne électorale,
- surveillance de l'anonymisation des bulletins et de leur mélange,
- vérification des preuves de mélanges des votes,
- surveillance du déchiffrement des votes mélangés et anonymisés,
- vérification des preuves de déchiffrement des votes,
- contrôle du dépouillement et de l'attribution des sièges,

— vérification des résultats,
— rapport d'audit.

L'article 25 du règlement électoral prévoit en outre – et c'est une nouveauté en 2018 – que l'auditeur puisse s'entourer de personnes compétentes pour l'entourer dans sa mission. Étant donné que l'élection est un processus qui se veut public et transparent, un appel aux volontaires (pour aider l'auditeur ou pour en apprendre plus sur le processus d'audit) a été fait lors de la réunion de la commission électorale du 22 février 2018. Malheureusement, personne n'a répondu à cet appel.

2 Rapport d'audit

Cette section reprend les missions en détail.

2.1 Avant le scrutin

Le mardi 20 mars 2018, les 3 porteurs de clés (Marie Charue, Véronique Eeckhoudt et Tanguy Massin) ainsi que leur suppléants respectifs (Françoise Nininahazwe, Florence Vanderstichelen et Isabelle Groessens) se sont réunis pour générer leurs paires de clés (une clé publique et une clé privée par porteur). Cette génération se fait en local sur les ordinateurs personnels apportés par les porteurs. La clé privée de chaque porteur est copiée trois fois. Une reste en possession du porteur, une est donnée à son suppléant et une est placée dans une enveloppe scellée. Les clés publiques sont ensuite téléchargées sur le serveur de vote et vérifiées. Elles serviront aux électeurs pour chiffrer leur bulletin de vote.

L'enveloppe numérotée AA094868 contenant les 3 clés privées notées 2c, 3b et 1 (sans note) fut ensuite scellée, signées par les porteurs ainsi que l'auditeur et fut confiée à l'auditeur. Cette enveloppe permet en cas de perte de l'une des clés et de sa copie (porteur et suppléant) de récupérer la clé privée manquante afin de procéder au dépouillement. Cette situation extrême devant être à tout prix évitée.

Les clés publiques générées sont disponibles sur demande à la commission électorale. Les hachés SHA256 des clés publiques sont les suivant :

clé 1 : LcGV8wk1zzP5EJdfoljyM_C0PYrzKJ7iGFvi0BjKwfw
clé 2 : u7b97Yu-E0gx__UOjJnY5UAh0KF5K-NPk4SQBaI7XnM
clé 3 : Nq-MVH4N9XOYvgo7ILuW-BIlA1zxm_CQxPK6pm157uM
clé générale : SGzVZva98C0mHdTXdhNJP_m5iDilWQ2CDaefYfWgjRI

Audit du code informatique. Le code informatique utilisé pour générer les bulletins de vote chiffrés, pour réaliser le mélange des bulletins, pour déchiffrer ceux-ci et pour calculer le dépouillement du scrutin est audité. Ce code sera utilisé par les porteurs de clés pour le mélange et le déchiffrement des bulletins. Il est également utilisé par l'auditeur pour effectuer les vérifications sur les opérations post-électorales.

2.2 Pendant le scrutin

Au début du scrutin, le haché de l'élection est généré :
c8vFdH7zsnCDK8unDdg8OmNDZ0q42bCcH7Nn+I60jjs

Il s'agit du haché SHA256 de la liste des candidats, de la clé publique générale (générée à partir des trois clés publiques) et des paramètres de l'élection (url de l'élection, date de l'ouverture du scrutin et de la fermeture du scrutin).

Durant le scrutin, les valves électorales sont surveillées. Cela consiste à télécharger leur contenu afin de garder une trace de leur remplissage. Plusieurs copies ont été effectuées durant cette période. Les activités suspectes comme un afflux massif de votes (bourrage d'urne) peuvent ainsi être détectés par le système.

Le scrutin a débuté le dimanche 25 mars 2018 à 23h55.

2.3 Après le scrutin

Le mercredi 28 mars 2018 à 23h55, le système de vote est clôturé et les valves électroniques sont gelées. À partir de ce moment, il n'est plus possible de soumettre un vote.

Période blanche. S'en suit une période blanche de 32h qui permet aux électeurs de demander l'annulation de leur vote ainsi qu'à la commission de statuer sur les éventuels litiges. Ce mécanisme garantit en particulier que des votes frauduleux puissent être détectés et écartés. Aucune demande d'annulation n'a été formulée.

L'auditeur a vérifié que les bulletins pris en compte pour le dépouillement reflétait exactement les valves. L'auditeur a vérifié que le haché (numéro de suivi) annoncé sur les valves était bien le haché du vote pris en compte dans le dépouillement. Il s'agit d'un haché SHA256 encodé [1] en base 64.

Au terme de ces vérifications, l'auditeur constate que l'urne électorale a conservé son intégrité et que son contenu est exactement celui qui a été utilisé lors du dépouillement. De plus ce qui a été annoncé sur les valves et vérifié par les électeurs eux-même correspond exactement au contenu de l'urne dépouillée.

Dépouillement. Le vendredi 30 mars 2018 à 8h30 ont commencé les opérations de dépouillement.

Les porteurs de clés ainsi que leurs suppléants étaient présents. Les opérations de dépouillement ont pu commencé.

Les porteurs de clés ont travaillé sur différents ordinateurs amenés par leur soin (laptop de Tanguy Massin dénommé TM, laptop de Isabelle Groessens dénommé IG, laptop de Veronique Eeckhoudt dénommé VE, laptop

1. voir https ://docs.python.org/2/library/base64.html pour l'encodage.

de Édouard Cuvelier dénommé EC et laptop de Florence Vanderstichelen dénomé FV). La multiplicité des stations de travail rend plus difficile les tentatives de corruptions.

Les machines sont lancées avec des clés usb sur lesquelles ont été installé un os Ubuntu 16 live non persistant. Ces clés ont été configurées par les porteurs de clé.

— EC : anonymisation des bulletins et premier mélange des bulletins
— TM : deuxième mélange des bulletins anonymisés
— IG : troisième et dernier mélange des bulletins anonymisés
— VE : déchiffrement partiel avec la clé 2 (Véronique Eeckhoudt)
— FV : déchiffrement partiel avec la clé 1 (Marie Charue)
— IG : déchiffrement final avec la clé 3 (Tanguy Massin)

Durant ce processus, à aucun moment, les trois clés de déchiffrement n'étaient en même temps sur une machine. Les porteurs de clés ont pris soin de ne pas copier leur clés sur les machines en les utilisant.

À la fin du déchiffrement, les porteurs de clés sont chacun repartis avec leur clés. Ils s'engagent à les détruire.

Pour chaque étape de mélange, le responsable du mélange fournit également une preuve cryptographique que le mélange a bien été effectué et en particulier que chaque bulletin est resté intègre durant le mélange. Cette preuve est vérifiée par l'auditeur.

Lors du déchiffrement, chaque porteur de clé fournit une preuve cryptographique que le déchiffrement s'est effectué sans altération des bulletins. Cette preuve sert à vérifier que les bulletins déchiffrés correspondent bien aux votes soumis dans les bulletins chiffrés. Cette preuve est vérifiée par l'auditeur.

Toutes les preuves sont vérifiées avec succès.

Décompte des voix et attribution des sièges. Après le déchiffrement et le décompte des voix, commence l'attribution des sièges qui est une partie délicate car les règles d'attribution ne sont pas simples.

Néanmoins, aucun problème n'est survenu lors de cette attribution.

Recours. Aucun recours concernant le dépouillement et l'attribution des sièges n'a été introduit.

3 Problèmes survenus durant l'élection

Cette section reprend les problèmes survenus durant le scrutin. On peut déplorer une attaque du système de vote électronique survenue le lundi 26 mars 2018.

Faits. Pour rappel, le serveur hébergeant le site web qui sert d'interface de vote est une machine de l'UCL installée au SGSI et prêtée pour les besoins de l'élection. Le code de l'interface est celui de la société BlueKrypt et est lancé sur cette machine durant l'élection. Les installations sont donc propriété de l'UCL et le code propriété de BlueKrypt. Le serveur réceptionne les bulletins de votes chiffrés par les électeurs et les affiche dans les valves électroniques publiques. Il met à disposition des électeurs les outils pour préparer leur bulletin de vote bien que ceci soit optionnel. Finalement, le serveur n'enregistre les bulletins de vote des électeurs qu'au terme d'une phase d'authentification qui impose à chaque électeur de prouver qu'il fait bien partie de l'électorat. Cette phase repose en partie sur les services d'authentification de l'UCL.

Le lundi 26 mars à plusieurs reprises au cours de la matinée, des tentatives d'intrusion du système de vote ont été détectées. Elles émanaient principalement d'une personne, doctorant en ICTEAM/INGI mais aussi de collègues directs de cette personne travaillant dans un bureau proche. Ces tentatives ont eu pour but de contourner le mécanisme d'authentification du système de vote. Ces tentatives d'intrusion se sont prolongées jusque dans l'après-midi du 26 mars.

La société BlueKrypt a informé la permanente AGL responsable du déroulement de l'élection ainsi que l'auditeur. Une discussion a dès lors eu lieu le 26 mars après-midi avec le chercheur auteur des tentatives d'intrusion pour lui demander d'y mettre fin. De nouvelles tentatives d'intrusion n'ont effectivement pas été constatée après le 27 mars.

Notons que les tentatives d'intrusion ont échouées et que le système n'a, à aucun moment, été mis en péril. Le déroulement de l'élection n'a pas du tout été affecté par ces tentatives.

Conséquences. En terme d'impact, l'attaque n'a eu aucune conséquences sur le scrutin.

4 Conclusion et recommandations

On peut conclure que, du point de vue technique, les résultats de l'élection sont corrects et fiables. Toutes les vérifications prévues dans l'audit ayant été réalisées avec succès. Du point de vue de l'attribution des sièges, aucun problème n'a été soulevé et on peut estimer que l'attribution est conforme à ce qui est prévu aux articles 13, 48 et 49 du règlement électoral.

Recommandations.

1. distinguer la fonction de porteur de clé et de mélangeur. Suggestion : les suppléants pourraient être également mélangeurs. En répartissant le plus possible les fonctions entre des personnes différentes, on diminue le risque de collusion.
2. le dépouillement est public, mais peu de public est présent. Une invitation à assister au dépouillement pourrait être envoyée aux listes. *Cette recommandation était déjà formulée après les élections de 2017.*
3. rédiger une feuille de procédure standardisée pour permettre que le mélange et le dépouillement des votes se fasse exclusivement par les personnes désignées (elles interviennent seules sur leur ordinateur sans l'aide d'un tiers).
4. les opérations de dépouillement devraient s'effectuer sur des ordinateurs coupés de leur(s) connexion(s) internet pour mitiger tout risque de transfert de données vers l'extérieur lors de cette étape.
5. bien qu'hébergé sur un serveur de l'UCL, le site de vote n'est pas sur le nom de domaine uclouvain.be. Attacher le site de vote au nom de domaine uclouvain.be pourrait supprimer la crainte que certains électeurs ont formulé quant à la manipulation de leurs login/mot de passe UCL.
6. malgré un appel aux volontaires pour aider (ou simplement s'intéresser) au processus d'audit de l'élection, personne n'a répondu à cet appel. Il y a peut-être lieu de voir comment mieux communiquer autour de cet appel. Les volontaires ne doivent pas avoir un profil technique ou des connaissances en informatique car les tâches d'audit sont variées. Au contraire des profils différents favorisent la démocratie car l'élection ne doit pas être un processus technocratique.