Sujet de stage

Analyse et conception d'un système de vote

Laboratoire, institution et université LORIA, Université de Lorraine

Équipe ou projet dans le labo Équipe Cassis au Loria

Nom et adresse électronique du directeur de stage Véronique Cortier, cortier@loria.fr

Indemnisation Ce stage pourra être indemnisé. En particulier, ce stage a le support de la bourse Européenne **ProSecure** (ERC Starting Grant).

Présentation générale du domaine. Plusieurs types de systèmes de vote permettent de voter à distance. Un système classique de vote par correspondance consiste à glisser son bulletin dans une première enveloppe puis mettre celle-ci dans une 2e, que l'on signe et que l'on expédie. De tels systèmes supposent une confiance totale dans l'entité chargée de la collecte et du comptage des votes. Une variété d'autres systèmes ont été développés, en introduisant par exemple des codes à barres pour faciliter le dépouillement. Cependant, des travaux récents ont montré que ces systèmes pouvaient être sujets à des attaques, comme un bourage d'urne massif [1].

Plus récemment, des protocoles totalement dématérialisés ont été proposés. Les protocoles de vote électronique permettent ainsi de réaliser des élections à distance (depuis son ordinateur), tout en préservant, en théorie, les bonnes propriétés d'un vote standard (confidentialité des votes, fiabilité et vérifiabilité du résultat, résistance à la coercition).

Objectifs du stage. L'objectif de ce stage sera de concevoir un protocole de vote hybride, utilisant le papier et la Poste pour faciliter le vote (nul besoin d'un ordinateur) mais utilsant la cryptographie pour assurer de meilleures garanties de sécurité. On pourra en particulier s'inspirer des techniques développées dans le cadre du vote électronique.

Dans un deuxième temps et si le temps le permet, l'objectif sera de proposer une formalisation de ce protocole, ainsi que la preuve des propriétés de sécurité les plus standards, dans un cadre formel. Nous étudierons en priorité la confidentialité des votes, la vérification de l'éligibilité et la possibilité de vérifier la prise en compte des votes (individuelle et universelle). Il est bien sûr possible que des failles soient détectées à ce stade, auquel cas des modifications seront proposées. Selon les compétences de l'étudiant, nous pourrons nous orienter plutôt vers des preuves de sécurité dans des modèles cryptographiques ou des preuves dans des modèles symboliques, utilisant plutôt des compétences en logique.

Compétences souhaitées. L'étudiant(e) devra avoir de bonnes compétences en logique (déduction automatique, arbres, etc.) et/ou en cryptographie (algorithmes de chiffrement, preuve de sécurité). Dans tous les cas, il/elle devra avoir un goût pour les preuves. Des connaissances en sécurité sont un plus mais ne sont pas requises car elles pourront être assimilées au cours du stage.

Références bibliographiques.

- Attaque d'un système de vote par correspondance :
  Véronique Cortier, Jérémie Detrey, Pierrick Gaudry, Frédéric Sur, Emmanuel Thomé, Mathieu Turuani, and Paul Zimmermann. Ballot stuffing in a postal voting system. International Workshop on Requirements Engineering for Electronic Voting Systems (REVOTE 2011). Trento, Italy, 2011.
- Formalisation et analyse de propriétés de vote :
  Stéphanie Delaune, Steve Kremer and Mark D. Ryan. Verifying Privacy-type Properties of Electronic Voting Protocols. *Journal of Computer Security* 17(4), pages 435-487, 2009.