A Mobile Application for Boardroom Voting

Domaine spécialisé: Information and Communication Technologies
Chargé: Prof. Dr. Reto Koenig
Expert: Prof. Dr. Ulrich Ultes-Nitsche

Durant cette thèse, un système de vote électronique fonctionnant sur des appareils mobiles comme les smartphones et les tablettes a été développé. Il n'a recours à aucune infrastructure centrale, réduisant la complexité de mise en place d'un scrutin et favorisant ainsi la spontanéité. L'implémentation se base sur un protocole assurant la sécurité et la vérifiabilité du scrutin. Un autre élément important de ce travail a été la conception d'interfaces utilisateurs conviviales.

Contexte

Tout comme l'e-banking ou l'e-commerce améliore notre vie journalière, l'e-voting faciliterait grandement la réalisation de scrutins. Toutefois, l'introduction de l'e-voting suscite passablement de scepticisme. Un système insuffisamment sécurisé ouvre la porte à de dangereuses manipulations. A ces risques s'ajoute la peur de l'espionnage informatique qui a été très médiatisé l'année dernière. La recherche, qui étudie depuis plusieurs années la thématique de l'e-voting, a défini des critères précis qu'un système de vote électronique devrait satisfaire. Plusieurs approches cryptographiques décrivant comment de tels systèmes devraient être construits ont été publiées mais peu d'entre elles ont été réellement réalisées en pratique.

Boardroom voting

Pour étudier la faisabilité de systèmes d'e-voting, la recherche considère souvent des scénarios de moins grande ampleur que des votations nationales. Parmi ces scénarios, on trouve le «Boardroom voting» qui peut être utilisé lors de séances de comité de direction. L'électorat (groupe de personnes ayant le droit de vote) est sensiblement plus petit pour ce scénario. Deux approches se rapportant à ce contexte ont été réalisées en pratique dans des travaux de master, l'une dans la thèse de Jürg Ritter et l'autre dans la thèse décrite ici. Une collaboration a pu être réalisée entre ces deux projets en ce qui concerne la conception des interfaces graphiques des applications résultantes.

L'e-voting sur des appareils mobiles

Le but de cette thèse de master était de réaliser une application de boardroom voting fonctionnant sur des appareils mobiles et respectant les consignes de sécurité requises pour l'e-voting, entre autres, la possibilité de vérifier que personne n'a dévié de la marche à suivre dictée par le protocole cryptographique. La plateforme populaire Android a été choisie comme base pour le développement de l'application, permettant ainsi l'utilisation de smartphones et tablettes. La particularité de ce système est l'absence d'infrastructure centrale pour l'échange des données. Ainsi, un vote peut être spontanément mis en place et réalisé sans avoir recours à des composants matériels supplémentaires autres que les smartphones et tablettes utilisés pour voter. Un facteur de sécurité réside dans le fait que toutes les personnes impliquées sont réunies au même endroit, ce qui exclut pratiquement les risques de manipulation de l'extérieur. L'implémentation se base sur un protocole cryptographique publié en 2012 par D. Khader, B. Smyth, P.Y.A. Ryan et F. Hao. Ce protocole est spécifiquement conçu pour un système sans infrastructure centralisée. Il garantit la confidentialité des votes ainsi que l'anonymat par un processus de comptage homomorphe. Cette application fournit donc un système de vote électronique sûr, anonyme, et vérifiable.

Convivialité d'utilisation

Un facteur important pour le succès de l'e-voting est la convivialité d'utilisation du système. La conception d'interfaces graphiques intuitives a donc joué un rôle important dans ce travail. Comme mentionné précédemment, cette conception et la réalisation de ces interfaces ont été effectuées en étroite collaboration avec Jürg Ritter.

Philémon von Bergen