Dezentralisiertes E-Voting mit Homomorpher Verschlüsselung

Fachgebiet: Information and Communication Technologies
Betreuer: Prof. Dr. Rolf Haenni
Experte: Stephan Neumann (Technische Universität Darmstadt)

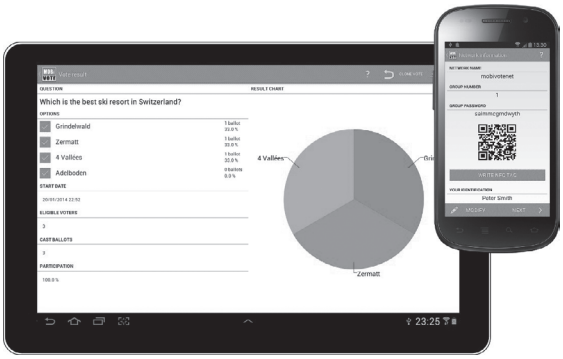
In dieser Masterarbeit wurde ein E-Voting System implementiert, welches auf mobilen Geräten wie Smartphones und Tablets lauffähig ist, ohne dass eine zentrale Infrastruktur nötig ist. Diese Art von E-Voting erlaubt spontanes durchführen von Abstimmungen. Die Implementation basiert auf einem Protokoll, welches Sicherheit und Verifizierbarkeit des Prozesses gewährleistet. Besondere Beachtung während dieser Arbeit galt ausserdem der einfachen Benutzbarkeit des Systems.

Ausgangslage

Genau so wie E-Banking oder E-Commerce unseren Alltag erleichtern, kann auch E-Voting die Durchführung von Wahlen und Referenden massiv vereinfachen. Dennoch nehmen viele beim Einsatz von E-Voting eine skeptische Haltung ein. Unsichere E-Voting Systeme bieten eine Plattform für Wahlmanipulation im grossen Stil. Diese Bedenken wurden zusätzlich durch die zahlreichen Schlagzeilen im Bereich Spionage und IT Sicherheit im letzten Jahr genährt. Die Forschung, welche sich seit längerer Zeit mit der Thematik E-Voting befasst, hat einige Kriterien ausgearbeitet, welches ein ideales E-Voting System erfüllen sollte. Es wurden auch mehrere kryptographische Ansätze publiziert, welche beschreiben, wie solche E-Voting Systeme aufgebaut sein könnten. Im Rahmen dieser Forschung wurden zwei solche Ansätze in die Praxis umgesetzt. Zum einen die Arbeit von Philémon von Bergen, sowie die vorliegende Arbeit. Dabei gab es eine intensive Zusammenarbeit bei der Erarbeitung der Benutzeroberfläche.

Boardroom Voting

Um die Praxistauglichkeit von E-Voting Systemen zu erproben werden in der Forschung oft auch Szenarien angeschaut, welche eine geringere Tragweite haben als Abstimmungen und Wahlen auf kantonaler oder gar nationaler Ebene. Zu diesen Szenarien gehören unter Anderem auch auch «Boardroom Voting», welches beispielsweise an einer Verwaltungsratssitzung stattfindet. Das Elektorat (Gruppe der wahlberechtigten Personen) ist in diesem Szenario deutlich kleiner und von jedem Beteiligten überblickbar.



E-Voting Applikation auf Smartphone und Tablet

E-Voting auf mobilen Geräten

In dieser Masterarbeit wurde ein bekanntes E-Voting Protokoll neu im Kontext Boardroom Voting implementiert. Das ursprüngliche Protokoll wurde im Jahr 1997 von R. Cramer, R. Gennaro und B. Schoenmakers vorgeschlagen und beschreibt einen zentralisierten Ansatz. Das Protokoll nutzt eine Eigenschaft namens «Homomorphismus» des ElGamal Verschlüsselungssystems, welche das anonyme Auszählen einer Abstimmung erlaubt. In der vorliegenden Umsetzung wurde das Protokoll für die dezentrale Nutzung auf mobilen Geräten (Smartphones und Tablets) angepasst. Somit ist für den Einsatz kein zentraler Server für den Datenaustausch mehr erforderlich. Nun können Abstimmungen ohne das Vorhandensein zusätzlicher Hardware spontan aufgesetzt, durchgeführt und ausgezählt werden. Die Umsetzung bezieht explizit eine Besonderheit des Boardroom Voting als Sicherheitselement mit ein: Der gemeinsame Aufenthaltsort von allen beteiligten Personen. So sind Manipulationen von Ausserhalb faktisch ausgeschlossen. Dies erlaubt nun beispielsweise sicheres, verifizierbares und anonymes Abstimmen an einer Verwaltungsratssitzung. Die Umsetzung wurde auf der für mobile Geräte populären Plattform «Android» gemacht, was das Produkt auf Geräten wie Smartphones und Tablets lauffähig macht.

Benutzerfreundlichkeit

Ein wesentlicher Faktor für den Erfolg von sicherem E-Voting ist Einfachheit in der Bedienung. Ein besonderes Augenmerk dieser Arbeit lag auf dem Design und der Implementation einer intuitiv zu bedienenden Benutzeroberfläche. Dieser Teil der Arbeit wurde wie schon erwähnt in enger Zusammenarbeit mit Philémon von Bergen gemacht.

Jürg Ritter
juerg_ritter@bluewin.ch