

Sicheres und effizientes E-Voting

IT-Security / Betreuer: Prof. Dr. Rolf Haenni, Prof. Dr. Eric Dubuis
Experte: Prof. Dr. Andreas Spichiger

Die sichere Durchführung von elektronischen Abstimmungen ist eine der herausforderndsten Anwendungen kryptografischer Protokolle. Ein im Jahr 2005 entworfenes E-Voting-Protokoll hat unter anderem die Eigenschaft, dass der Wähler nicht erpresst werden kann. Das Protokoll besitzt allerdings auch eine markante Einschränkung bei der Stimmenauszählung. Aus diesem Grund wurden an der BFH mehrere optimierte Versionen entwickelt, welche sich diesem Problem annehmen. Der Auftrag lautete, ein Prototyp der neusten Variante zu entwickeln, um die Praktikabilität des Protokolls aufzuzeigen.

Die weltweite Verbreitung des Internets eröffnet unter anderem auch neue Möglichkeiten bei der Interaktion zwischen Bürger und Staat. Mittlerweile beteiligen sich in der Schweiz 13 Kantone an Pilotprojekten zum Thema E-Voting.

Im Bereich von elektronischen Abstimmungen bestehen Anforderungen, welche weit über die von anderen, sicherheitskritischen Internetanwendungen wie z. B. E-Banking oder E-Shopping hinaus gehen. So muss bei E-Voting nicht nur sichergestellt werden, dass es sich bei Wähler und Wahlbehörde um die korrekten Parteien handelt. Die Auszählung der Stimmen muss transparent und für jedermann nachvollziehbar sein, darf jedoch keinen Aufschluss darüber geben, wer wie abgestimmt hat. Zusätzlich darf der Wähler nicht erpressbar sein: Einem Betrüger soll es nicht möglich sein, einen Wähler dazu zu zwingen, auf eine bestimmte Art und Weise zu stim-

men, nicht an der Wahl teilzunehmen oder gar seinen Stimmausweis zu veröffentlichen. Diese Eigenschaft wird als «Coercion Resistance» bezeichnet.

Das E-Voting-Protokoll von Juels et al. (2005) entspricht dem neusten Stand der Technik und liefert eine Lösung für die geforderte «Coercion Resistance». Das Protokoll besitzt allerdings eine gravierende Einschränkung: Die für die Stimmenauszählung benötigte Zeit wächst quadratisch mit der Anzahl Stimmen. Bereits ab einer vergleichsweise kleinen Anzahl von Stimmen dauert die Auszählung so mehrere Stunden, was in der Praxis nicht praktikabel ist. Die E-Voting-Gruppe der Berner Fachhochschule hat mehrere Varianten entwickelt, welche sich diesem Problem annehmen.

Der Auftrag dieser Bachelor Thesis lautete, einen Prototyp der neusten Protokollvariante zu entwickeln. Die Spezifikation war dabei so effizient wie möglich zu implementieren. An gewissen Stellen wurden Vereinfachungen erlaubt. Das Hauptziel der Implementation bestand in einer Proof-of-Concept-Studie, welche die Praktikabilität des Protokolls unter realen Umständen aufzeigen sollte.

Entwickelt wurde eine auf Java RMI basierende Client-/Server-Applikation mit verschiedenen Rollen. Der Fokus bestand dabei

in der Stimmenauszählung. Die Applikation beinhaltet Implementierungen der Konzepte «ElGamal-Verschlüsselung», «Zero-Knowledge-Beweise», «Reencryption Mix-Network» und «verteilte Berechnung und Entschlüsselung». Neben einer interaktiven Stimmentgabe wurde eine Simulation einer Abstimmung entwickelt, um Aussagen über die Leistungsfähigkeit des Protokolls machen zu können. Dabei konnte der lineare Zeitverlauf der Stimmenauszählung erfolgreich unter Beweis gestellt werden.



David Berger

dave.berger@hispeed.ch



Rolf Linder

mail@liro.ch

