Diplomarbeitspräsentationen der Fakultät für Informatik

Mehr Transparenz für den Wähler: Entwicklung eines end-to-end-verifizierbaren Wahlsystems

Peter Kalchgruber

FAKULTÄT FÜR INFORMATIK
Masterstudium Wirtschaftsinformatik

Technische Universität Wien
Institut für Softwaretechnik und Interaktive Systeme
Arbeitsgruppe: Information & Software Engineering Group
1040 Theresianumgasse 27
Betreuer: o.Univ.Prof. Dr. A Min Tjoa
Mitwirkender Assistent: Dr. Edgar Weippl

Das heutige Wahlsystem aus dem 18. Jahrhundert

Das heutige Wahlsystem wird schon sehr lange seiner jetzigen Form angewandt. Neue technische Methoden ermöglichen es, den Wahlprozess für alle Beteiltigten unter den bestehenden Wahlgrundsätzen transparenter zu machen.

In Artikel 1 des österreichischen Bundes-Verfassungsgesetzes ist festgelegt, dass das Recht vom Volk ausgeht.

Um dieses Recht umsetzen zu können, müssen bestimmte Wahlgrundsätze (siehe Art. 26 Abs. 1 B-VG), die eine gleiche, unmittelbare, persönliche, freie und geheime Wahl ermöglichen, eingehalten werden. Im jetzigen Wahlsystem werden diese Punkte weitgehend erfüllt. Neue Wahlmethoden, bei denen zumindest ein Teil des Wahlvorganges, jedoch nicht zwangsweise die gesamte Wahl, elektronisch abgewickelt wird, werden unter dem Begriff E-Voting zusammengefasst. Diese Art der Stimmabgabe, unterstützt durch elektronische Medien, wird immer populärer. Aufgrund des Mangels technischer Möglichkeiten ist der Prozess jetziger Wahlsysteme intransparent. Es existiert eine sogenannte BlackBox, die den größten und wichtigsten Teil des Wahlsystems verhüllt.

Die Abbildung unten zeigt den jetzigen

Wahlprozess. Jede Wählerin und jeder Wähler muss sich im Wahllokal authentifizieren, um die Stimme abzugeben. Was anschließend mit der Stimme geschieht, ist jedoch nur mehr für sehr wenige Personen (z.B. Wahlhelfer) nachvollziehbar. Immer wieder wird in Zeitungen über verschwundene Wahlzettel und Wahlbeteiligungen von über 100 % berichtet. Diese und andere Meldungen zeigen, dass es beim jetzigen Wahlsystem Probleme gibt. David Chaum stellte fest, dass zwar die Sammlung der Wahlzettel und ihre Auszählung klar nachvollziehbar wären, jedoch andere Schritte im Rahmen der Ermittlung des Wahlergebnisses wenig durchsichtig seien und Möglichkeiten der Manipulation böten.

Neue elektronisch unterstützte Wahlsysteme erlauben es hingegen, den Schritt von der abgegebenen Stimme, zum Auszählungsergebnis transparent zu machen.

Abstract

Electronic-Voting (E-Voting) stellt eine junge Entwicklung im elementarsten Bereich der Demokratie dar: den Wahlen. Nach den ersten „in-vivo"-Einsätzen wird Bilanz über Vor- und Nachteile gezogen.

In meiner Diplomarbeit stelle ich die Grundlagen und den Aufbau bekannter E-Wahlsysteme dar. Der Fokus liegt hierbei auf end-to-end-verifizierbaren Wahlsystemen. Diese bieten Wählerinnen und Wählern die Möglichkeit, die korrekte Zählung ihrer abgegebenen Stimme nachzuverfolgen und zu überprüfen. Gleichzeitig wird das Wahlgeheimnis gewahrt, um die Wählerinnen und Wähler vor Stimmenkauf zu schützen. Zur Erhöhung der Transparenz bei Wahlen können end-to-end-verifizierbare Wahlsysteme unterstützend sowohl bei Präsenz- als auch bei Internet-Voting-Wahlsystemen eingesetzt werden.

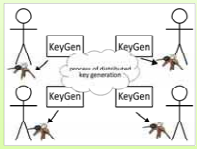
Vertiefend gehe ich auf die end-to-end-Wahlsysteme Punchscan, Threeballot und Scantegrity ein.

Der praktische Teil umfasst die Implementierung des von Ben Adida entwickelten end-to-end-verifizierbaren Wahlsystems Scratch & Vote. Es wurde zu diesem Zweck mit einer Threshold-Entschlüsselung erweitert. Bei der Abfassung der Arbeit ließ ich mich davon leiten, das gesamte Wissen, das für die Implementierung eines solchen Wahlsystems notwendig ist, verständlich und anhand von Beispielen zu vermitteln.

Wahlprozess

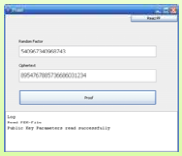
1

Generierung der geheimen verteilten Schlüssel
Generierung und Verteilung des öffentlichen Schlüssels
Drucken der Wahlzettel



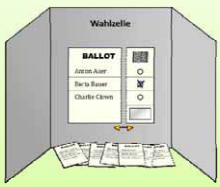
2

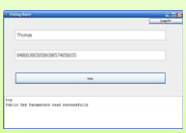
Aufrubbeln des Rubbelfeldes
Eingabe der Zahlen
Verifikation ob Stimme korrekt verschlüsselt wurde



3

Kandidatin/Kandidat ankreuzen
Linken Teil abtrennen
Mit rechtem Teil und unversehrtem Rubbelfeld Wahlzelle verlassen

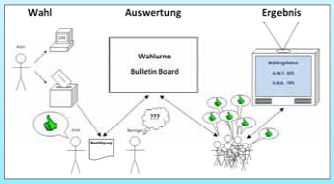




Informationen zu Scratch & Vote

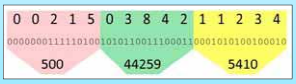
Open-Audit-Voting

Bei Open-Audit-Votings kann der gesamte Prozess der Wahl von allen Beteiligten mitverfolgt und überprüft werden.



Scratch & Vote

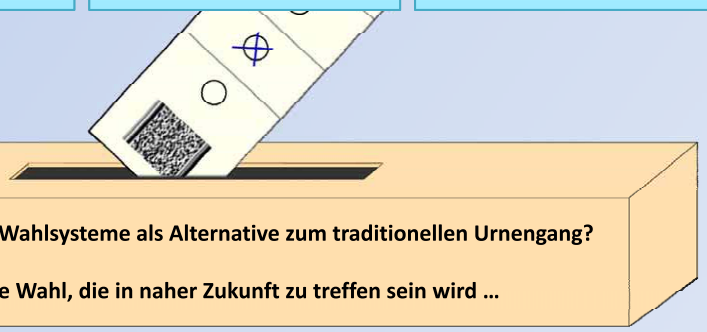
Scratch & Vote ist ein end-to-end-verifizierbares Wahlsystem. Die Stimmen aller Wählerinnen und Wähler werden in einer verschlüsselten Zahl gespeichert. Kommt eine neue Stimme hinzu, wird die Zahl mit der neuen verschlüsselten Stimme multipliziert und ergibt das neue verschlüsselte Ergebnis.



Der Wahlzettel

Der Wahlzettel kann entlang einer Perforation in drei Teile geteilt werden. Die Reihung der KandidatInnen in der linken Hälfte des Wahlzettels variiert. Unter der Rubbeloberfläche sind Zahlen versteckt, die ohne Kenntnis des Private-Keys ein Entschlüsseln der Positionen der KandidatInnen auf der linken Seite ermöglichen.

BALLOT	
Anton Auer	○
Berta Bauer	○
Charlie Clown	○



End-to-end-verifizierbare Wahlsysteme als Alternative zum traditionellen Urnengang?

Bald eine weitere Wahl, die in naher Zukunft zu treffen sein wird …

4

Kontrolle und Vernichtung des unversehrten Rubbelfeldes

5

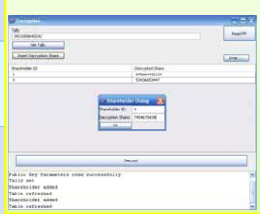
Überprüfung am Bulletin Board

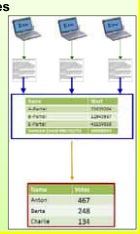
6

Einzelentschlüsselungen der Parteien

7

Berechnung des Endergebnisses





Kontakt: student@kalchgruber.com