erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Angel Tchorbadjiiski

FIfF-Studienpreis 2012
3. Preis

Liquid Democracy

Konzept zur kryptographischen Absicherung

Das Liquid-Democracy-Konzept ist in letzter Zeit durch verschiedene Institutionen (Enquête-Kommission, Munich Open Government Day) und auch durch den Einsatz bei der Piratenpartei Deutschland bekannt geworden. Die beiden meistverbreiteten Software-Implementierungen des Konzepts sind LiquidFeedback *und* Adhocracy*, welche ihren Nutzern verschiedene Diskussionsmöglichkeiten anbieten. Es können Vorschläge gemacht werden und über diese lässt sich abstimmen. Das Augenmerk beider Implementierungen liegt auf der Diskussion. Das führt zu verschiedenen Problemen bezüglich der Anonymität und Geheimhaltung der Abstimmungen und der Sicherheit der Systeme.*

Anforderungen an das System

Das Liquid-Democracy-Konzept bietet eine sehr aktuelle und interessante Grundlage. Aus diesem Grund habe ich es mir zum Ziel meiner Diplomarbeit gesetzt, ein Wahlsystem zu entwerfen, welches auf dem Konzept basiert und folgende Anforderungen erfüllt:

- **Wahl über das Internet** – Die Abstimmung kann über ein unsicheres Netzwerk durchgeführt werden.
- **Anonymität** – Die im System vorhandenen Informationen erlauben es nicht, Wähler zu identifizieren oder eine Korrelation zwischen Wählern und Stimmen herzustellen.
- **Geheimhaltung und Integrität** – Die übertragenen Daten sollten nicht von Dritten gelesen oder unbemerkt manipuliert werden können.
- **Öffentliche Wahlergebnisse** – Nach der Wahl sollen die Ergebnisse in einer Form vorliegen, die es den Wählern erlaubt, die eigene Stimme zu überprüfen.
- **Authentifizierung und Autorisierung** – Es soll sichergestellt werden, dass jede Stimme von einem gültigen Wähler abgegeben worden ist.
- **Wahlberechtigungen nur an gültige Wähler** – Das System darf nur bei aktiver Mitwirkung von gültigen Wählern Wahlberechtigungen erstellen können. Anderweitig erstellte Berechtigungen werden mit einer hohen Wahrscheinlichkeit aufgedeckt.
- **Delegation –** Im System ist es möglich, die eigene Stimme einfach oder mehrfach (priorisiert) zu delegieren. Zusätzlich ist jederzeit eine Überstimmung/Zurücknahme der eigenen Stimme wieder möglich. Eine Zeit- oder Bereichsdelegierung sollte auch möglich sein.
- **Nichtabstreitbarkeit** – Jede Entität (Wahlregister, Wahlcomputer, Wähler), die an einer Aktion teilgenommen hat, kann das nicht abstreiten, weil Daten vorhanden sind, die das belegen. Bei einer Manipulation soll dadurch feststellbar sein, welche der Entitäten genau daran beteiligt war.

Obwohl die gemeinsame Entscheidungsfindung sicherlich einen sehr wichtigen Punkt darstellt, fand ich es persönlich spannender, ein sicheres System zu entwickeln, dass anonyme und geheime Abstimmungen über das Internet ermöglicht. Es ist dabei sehr wichtig, dass die zwischen Wähler, Wahlregister *(Voting Register, VR)* und Wahlcomputer *(Voting Computer, VC)* ausgetauschten Daten für Dritte nicht einsehbar oder manipulier-

bar sind. Weiter sollte sicher gestellt werden, dass alle Benutzer des Systems wirklich dazu berechtigt sind, an einer Wahl teilzunehmen, und jeweils nur einmal abstimmen können. Die Wahlergebnisse sollten veröffentlicht werden, was es jedem Benutzer ermöglicht, zu überprüfen, ob die eigene, abgegebene Stimme der entspricht, die in der Datenbank des VCs gespeichert ist. Dafür sollte bei Stimmenabgabe eine Quittung vom VC generiert werden, die von den ausgetauschten Daten abhängt und nicht von Dritten erratbar ist. Zu guter Letzt, aber nicht minder wichtig, sollte das System auf dem Liquid-Democracy-Konzept aufsetzen, wobei aber nicht nur Einfach-, prioritätbasierte Mehrfachdelegierung und Rücknahme einer Delegierung möglich sind, sondern auch Weitergabe des Stimmrechtes basierend auf Zeit oder Themengebiet. Dies würde den Wählern eine größere Flexibilität ermöglichen.

Systemarchitektur

Das im Laufe meiner Diplomarbeit entstandene System ist in Abbildung 1 dargestellt.

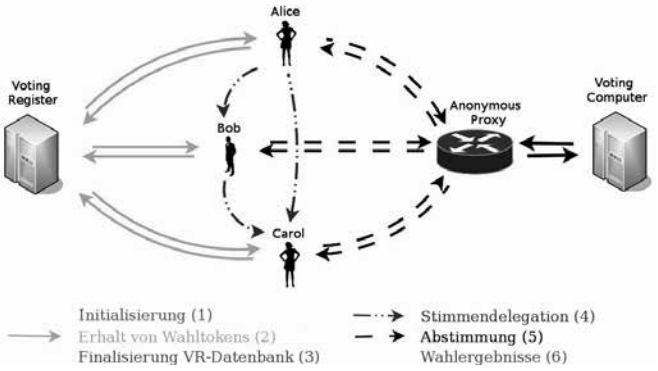


Abbildung 1: Systemarchitektur

Die VR-Instanz trägt Verantwortung für die Überprüfung der Wähleridentität, die Wahlberechtigung und die Vergabe von anonymen Wahltokens. Die Vergabe der Wahltokens ist physikalisch von der VR-Instanz getrennt, die anhand der Wahltokens entscheidet, ob ein Wähler zur Abstimmung berechtigt ist, die Stimmen speichert und die Wahlergebnisse öffentlich macht. Im Fall einer Manipulation ist es so möglich festzustellen, welche der Instanzen sich nicht an das Protokoll gehalten hat.

Der Abstimmungsprozess ist in sechs Phasen unterteilt (siehe Abbildung 1), wobei die folgenden Phasen eine Interaktion des Wählers erfordern:

Abstimmungsprozess

Phase 1 – Initialisierung

In dieser Phase werden die Datenbanken der Server (VR und VC) reinitialisiert und neue RSA-Schlüssel generiert. Dies entwertet explizit alle in der Vergangenheit vergebenen Wahltoken. Zusätzlich holt sich VR eine signierte aktuelle Liste der Wahlberechtigten (im weiteren WBL), die unter Anderem einen öffentlichen Schlüssel zu jeder der Personen enthalten muss. Diese werden in der nächsten Phase benötigt, um sicherzustellen, dass der VR nicht in der Lage ist, ohne Mitwirkung eines Wahlberechtigten gültige Wahltokens zu generieren.

Phase 2 – Erhalt von Wahltokens

Nachdem die Initialisierung abgeschlossen ist, kann jeder Wahlberechtigte mit dem VR in Verbindung treten und ein anonymes Wahltoken erhalten. Die Identität des Wählers wird mittels einer *Challenge-Response-Authentifizierung* bestimmt, basierend auf den in Phase 1 erwähnten öffentlichen RSA-Schlüssel. Die Response ist dabei mit dem privaten Schlüssel des Wählers signiert, sodass eine aktive Teilnahme nachgewiesen werden kann.

Um die Anonymität des Systems zu gewährleisten, muss jeder Wähler eine eigene *Hash-Kette* (wird anhand eines Beispiels in Phase 4 erklärt) generieren. Das letzte Element dieser Kette wird vom VR über blinde Signatur mit dem privaten RSA-Schlüssel des VR-Servers unterschrieben. Dies ist das Wahltoken, welches die Berechtigung für die spätere Abstimmung darstellt.

Phase 3 – Finalisieren der VR-Datenbank

Es muss sichergestellt werden, dass VR die Wählerliste nicht nachträglich verändern kann. Um dies zu gewährleisten, wird die Identität der Person, der dazugehörige öffentliche Schlüssel, die von VR gesendete Challenge (zum Beispiel Zeitstempel) und die vom Benutzer signierte Response veröffentlicht. So kann jede/r überprüfen, ob jede in der Liste aufgeführte Identität ein Token erhalten hat. Ist die Signatur der Response ungültig, hat eine Manipulation stattgefunden.

Phase 4 – Stimmendelegation

Will beispielsweise die Wählerin Alice ihre Stimme mit unterschiedlicher Priorität an die Personen Bob und Carol weitergeben, muss sie in Besitz einer Hash-Kette sein. Diese wird, wie in Abbildung 2 dargestellt, durch iteratives Anwenden einer kryptographischen Hash-Funktion $h()$ auf ein nur Alice bekanntes Element h_S generiert.

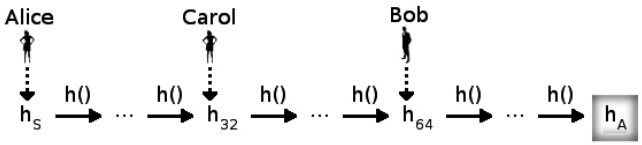


Abbildung 2: Verwendung von Hash-Ketten zur priorisierten Delegierung

Erhält Carol das Tupel (h_{32}, h_A) und Bob (h_{64}, h_A), so können sie beide anstelle von Alice abstimmen. Je weiter das erste Element des Tupels von dem Anker (letztes Element) entfernt ist, desto höher ist die Priorität. Da Alice in Besitz der Elemente h_S bis h_{31} ist, kann sie jederzeit mit einem dieser Tupel überstimmen, was als Rücknahme der delegierten Stimme anzusehen ist.

Um Zeit- oder Bereichsdelegierung zu ermöglichen, kann anstelle einer einfachen Hash-Kette auch ein Merke-Baum (Hash-Baum) verwendet werden. Dabei wird die Wurzel des Baumes, wie oben dargestellt, als Wahltoken verwendet, und die Blätter sind Hash-Ketten. Auf diese Weise kann zum Beispiel die eine Seite des Baumes verwendet werden, um verschiedene Delegierungsperioden zu definieren und die andere Seite, um Delegierungsbereiche vorzugeben.

Phase 5 – Abstimmung

Nach Abschluss der Delegierungsphase können alle Personen, die in Besitz einer gültigen Wahlberechtigung sind, beim VC eine Stimme abgeben.

Um die Identität des Wählers zu verschleiern, können anonyme Proxys eingesetzt werden. Dabei muss eine verschlüsselte Verbindung zwischen Wähler und VC hergestellt werden, die einerseits die Prüfung der Serveridentität ermöglicht, andererseits die Integrität und Geheimhaltung der übertragenen Daten gewährleistet.

Mit Hilfe des signierten Wahltokens kann VC feststellen, ob ein Wahlberechtigter vorliegt oder nicht. Mittels *Diffie-Hellmann-Key-Exchange* wird benötigtes Zufallsmaterial generiert, sodass sowohl VC als auch Wähler aktiv an diesem Prozess beteiligt sind.

Die eigentliche Stimmenabgabe erfordert ein kompliziertes kryptographisches Protokoll. Zuerst wird ein Commitment seitens des Wählers generiert, in dem die Zufallszahl und die Stimme enthalten sind. Diese werden mit einem Element der Hash-Kette verändert und dem VC zur blinden Unterschrift weitergegeben. Nachdem das Commitment unterschrieben worden ist, wird das verwendete Element dem VC verraten, damit die Stimme aufgenommen werden kann. Als letztes generiert der VC eine kryptographische Quittung, die von den ausgetauschten Daten und der vorherigen Server-Quittung abhängt. Diese kann bei einer erkannten Manipulation dazu verwendet werden, die Wahlergebnisse anzuzweifeln.

Phase 6 – Veröffentlichung der Wahlergebnisse

Der VC generiert zwei getrennte Listen. Die erste enthält die Wahltokens und die Elemente, die zum Maskieren der Wahl verwendet worden sind. So kann die Signatur des VRs und die Hash-Kette jedes einzelnen Wählers überprüft werden. Die zweite Liste enthält die Zufallszahl und die eigentliche Stimme. Da die Zufallszahl nur dem Wähler bekannt ist, kann kein anderer die Stimme mit der Identität des Wählers verbinden. Hat eine Manipulation stattgefunden, hängt die Wahrscheinlichkeit ihrer Entdeckung davon ab, wie viele Personen ihre Stimme überprüfen. Bei Wahlen mit mehr als einer Million Teilnehmern reicht etwa ein Prozent, um eine hundertprozentige Wahrscheinlichkeit einer Manipulationsentdeckung zu gewährleisten.

Nachteile

Wie bei jeder Wahl, die nicht in überwachten Wahllokalen stattfindet, ist es auch hier möglich, dass Stimmenkauf oder Erpressung von Wählern stattfinden. Da das System die Überprüfung der eigenen Stimme ermöglicht, kann das auch einem Käufer/Erpresser zu Gute kommen. Um dem entgegen zu wirken, können vertrauenswürdige Entitäten (trusted third parties) verwendet werden, die die Ergebnisse anstelle der Wähler überprüfen.

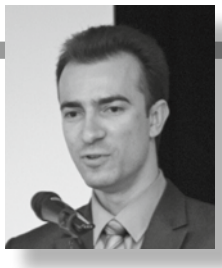
Ein weiterer Punkt betrifft die Sicherheit der Systeme, die von den Wählern verwendet werden. Ist das verwendete System unter der Kontrolle eines Angreifers, kann nicht sichergestellt werden, dass die abgegebene Stimme der gewollten Wahl entspricht. Um solche Angriffe zu verhindern, können Smartcards verwendet werden, die alle kryptographischen Operationen völlig autonom durchführen, sodass keine Manipulation auf der infizierten Maschine stattfinden kann. Weiter könnten Wähler eine CD mit einem bootfähigen Betriebssystem verwenden, das aktuell ist und mit sehr hoher Wahrscheinlichkeit nicht infiziert, um an einer Wahl teilzunehmen.

Um ein System zu erschaffen, das ein Augenmerk auf Sicherheit, Anonymität und Vertraulichkeit von Wahlen setzt und die oben aufgeführten Anforderungen erfüllt, habe ich verschiedene kryptographische Basisblöcke zu komplexen Protokollen kombiniert. Dadurch wirkt das System sehr undurchsichtig und erfordert Kenntnisse in Kryptographie, um den Abstimmungsprozess zu verstehen.

Fazit

Das während meiner Diplomarbeit entstandene System ermöglicht es, eine anonyme und geheime Wahl über das Internet durchzuführen. Ich habe mich mit Hilfe verschiedener kryptographischer Protokolle darum bemüht, die Sicherheit des Systems zu gewährleisten und jede Manipulation entdeckbar zu machen. Wegen der öffentlichen Wahlergebnisse ist jeder in der Lage, diese auf Korrektheit zu überprüfen, und falls eine Manipulation vorliegt, kann sichergestellt werden, welche Entität sich nicht an das Protokoll gehalten hat.

Angel Tchorbadjiiski



Angel Tchorbadjiiski hat an der Rheinisch-Westfälischen Technischen Hochschule (RWTH) Informatik auf Diplom studiert. Sein starkes Interesse an IT-Sicherheit wurde zum Studienschwerpunkt. Nebenbei nahm er mit einem Team von RWTH-Studenten regelmäßig an verschiedenen Capture-The-Flag-Wettbewerben wie Cipher *(http://www.cipher-ctf.org)*, iCTF *(http://ictf.cs.ucsb.edu/)* und RuCTFE *(http://ructf.org/e)* teil. Während und nach Abschluss seines Studiums arbeitete er als Penetrationstester.