Civitas: ein modernes Computerwahlsystem

Eine Lösung für das Dilemma der Online-Wahl?

9. April 2015

Inhalt

Inhaltsverzeichnis

Definition

- IT-Sicherheit ist, wenn Computer das tun, was Benutzer wünschen bzw. erwarten.
- Spezielles Problem bei Wahlen: frei, gleich, geheim

Probleme

- gefälschte Wahlzettel
- wie kann die Auszählung überprüft werden?
- Geheimhaltung? Post-Snowden?

typische Probleme früherer Systeme

Wahlcomputer

- Hochgradig belastet
- Allesamt offensichtlich (vgl. letzte Folie)
  $\rightarrow$ IT-Sicherheitsprobleme sind nicht offensichtlich
- Zentralisierung
- Konzeptionell (Geheime Wahl konzeptbedingt unmöglich)

$\rightarrow$ scheinen unüberwindbar

Kryptographie

Zielsetzung

Daten “verschlüsseln” oder “chiffrieren”, so dass sie nicht mehr verstanden werden können (idealerweise: nicht unterscheidbar von Rauschen).

- Statt eines Klartextes wird chiffierter Text übertragen, Buchstabensuppe
- Angriff “teuer”: braucht tausende Jahre Rechenzeit o.Ä.
- Computer werden schneller, dh. irgendwann in der Zukunft verfällt die Sicherheit
- In der Realität nicht anders

Public-Key-Krypto

- Problem bei gewöhnlicher Verschlüsselung: jedes Sender-Empfänger-Paar benötigt einen (geheimgehaltenen Schlüssel)
- über sogenannte “Falltürfunktionen” lässt sich eine asymmetrische Verschlüsselung konstruieren: Verschlüsseln mit Schlüsselteil, entschlüsseln mit gesamtem Schlüssel.
- Verwaltung der Schlüssel enorm vereinfacht
- Abhängig z.B. von der Komplexität der Primfaktorzerlegung

Komplexität der Primfaktorzerlegung

Primfaktorzerlegung gilt als schwieriges Problem. Bislang nur langsame Algorithmen. Quantencomputer? Derzeit nicht realistisch (max. 5 qbit, “Annealing” scheint keinen Vorteil zu bringen).

Inhaltsverzeichnis

Geheimhaltung und Sicherheit

- Wahlleiter muss sicherstellen, dass jeder nur einen Wahlschein erhält
- am Stimmzettel darf für dritte nicht erkennbar sein, welche Wahl getroffen wurde
- Fälschungen sollen unmöglich sein
- Wahllokal kann im Allgemeinen nicht überwacht werden

Estland

Estland führt Wahlen für Volksvertretungen per Internet durch, verwendet aber kein System vergleichbar mit Civitas

Bei Papier-Wahlen treten solche Probleme ebenfalls auf.

Überprüfbar durch Wähler (voter-verifiability)

Zu überprüfende Tatsachen:

- Stimmzettel wurde empfangen und verarbeitet
- Alle Stimmzettel wurden gezählt
- kein ungültiger Stimmzettel wurde abgegeben
- Auszählung ist korrekt
- das bekanntgemachte Ergebnis stimmt

vgl. Anwesenheit bei der Auszählung
Civitas stellt fast alle dieser Eigenschaften sicher

Schiebung unmöglich (non-Coercability)

Ungültige Wahlscheine sind beliebig erhältlich und funktionstüchtig, dh. können verwendet werden, eine Stimme abzugeben, die aber nicht gezählt wird.

- Äußerlich nicht unterscheidbar von den echten Wahlscheinen
- Verwenden, wenn jemand beobachtet oder versucht, Stimme zu kaufen
- können verworfen werden, wenn der Angreifer Enthaltung verlangt
- können verkauft werden
- Wähler muss aktiv werden
- Führt dazu, dass der Versuch aussichtslos ist, wird nicht versucht (zumindest nicht von klugen Menschen)

Inhaltsverzeichnis

Rollen

(Behörden, Personen mit Parteiämtern)

Supervisor

Stellt den Stimmzettel zusammen, Autorisiert andere Rollen, bestimmt Start- und Endzeitpunkt

Registrar

Autorisiert Wähler

Registrationsbeamter

Erzeugt Stimmzettel

Tabulationsbeamter

Zählt Stimmzettel aus

Bestandteile der Software

- öffentliches nur-schreiben “Log”
- Registration
- Wahlurne
- Tabulation
- Stimmabgabe

Aufruf zur Wahl

- ein leeres “Log” wird erzeugt
- der Registrar veröffentlicht dort eine Wählerliste, dh. eine Liste, die Identifikationen (Namen, Nummern) und öffentliche Schlüssel einander zuordnet
- die Tabulationsbeamten erzeugen gemeinsam einen Schlüssel und veröffentlichen dessen öffentlichen Teil
- die Registrationsbeamten erzeugen gemeinsam für jeden Wähler eine Urkunde, die aus so vielen Teilen besteht, wie es Registrationsbeamten gibt

Wahl

- Wähler beschaffen von den Registrationsbeamten unter Benutzung zweier Schlüssel jeweils einen Teil ihrer Urkunde
- Sie kombinieren diese Teile, um ihre (dann geheime) Urkunde zu erzeugen
- Wähler schicken ihre Urkunden zusammen mit der Wahlentscheidung (verschlüsselt) an wenigstens eine Wahlurne
- Wähler können jederzeit falsche Urkunden erzeugen (s.o.)

Tabulation

- Supervisor beendet die Wahl
- Eingesandte Stimmen werden überprüft[1]
- Doppelte Stimmen werden verworfen
- Ein Mixnet wird verwendet, um Stimmen und Urkunden zu anonymisieren
- *rightarrow* alle verbleibenden Stimmen sind anonym, autorisiert und korrekt
- Die Stimmen werden entschlüsselt, der Klartext wird veröffentlicht

[1] Das ist viel komplizierter, als es hier den Anschein hat

Sicherheit durch Redundanz

- Es gibt mehr als eine Wahlurne, möglicherweise sogar verschleierte Wahlurnen.
- Alle Tabulationsbeamten müssen kooperieren, um das Ergebnis zu entschlüsseln
- Alle Registrationsbeamten müssen kooperieren, um auch nur eine gültige Stimme herzustellen

Sicherheit durch Konstruktion

Non-coercibility: s.o.

Voter verifiability

- Veröffentlichtes Ergebnis wird von den Tabulationsbeamten signiert
- Tabulationsbeamten veröffentlichen Beweise über die verwendeten Mixnets (waren Permutation, es liegt kein Betrug vor)
- Ungültige (oder doppelte) Stimmen werden nachweisbar ausgeschlossen

Sicherheit durch Konstruktion II (geheime Wahl)

- Urkunden könnten veröffentlicht werden
  rightarrow Alle Registrationsbeamten müssen die Urkunden, die an die Tabulationsbeamten geschickt werden, anonymisieren.
- (wirksamer) Zwang ist ausgeschlossen
- geheime Beobachtung des Wahlvorgangs *rightarrow* Paranoia
  Gegenmaßnahme: mehrere ungültige Stimmen abgeben

Enter the void

- kleiner Wermutstropfen: Keine Vorkehrung für den Wähler vorhanden, die überprüft, ob seine Stimme gezählt wurde - technisch ist das allerdings möglich
- Alternative (einfacher, aber nicht so ausgefeilt): Helios

Quellen

Civitas geht zurück auf Arbeiten von Michael R. Clarkson, Stephen Chong und Andrew C. Myers.

Civitas

`https://www.cs.cornell.edu/andru/papers/civitas-tr.pdf`

Moderne Online-Wahlsysteme

`http://www.mathematik.hu-berlin.de/~schliebn/dl/Diploma-thesis-Schliebner-INF.pdf`

Helios

`http://static.usenix.org/events/sec08/tech/full_papers/adida/adida.pdf`