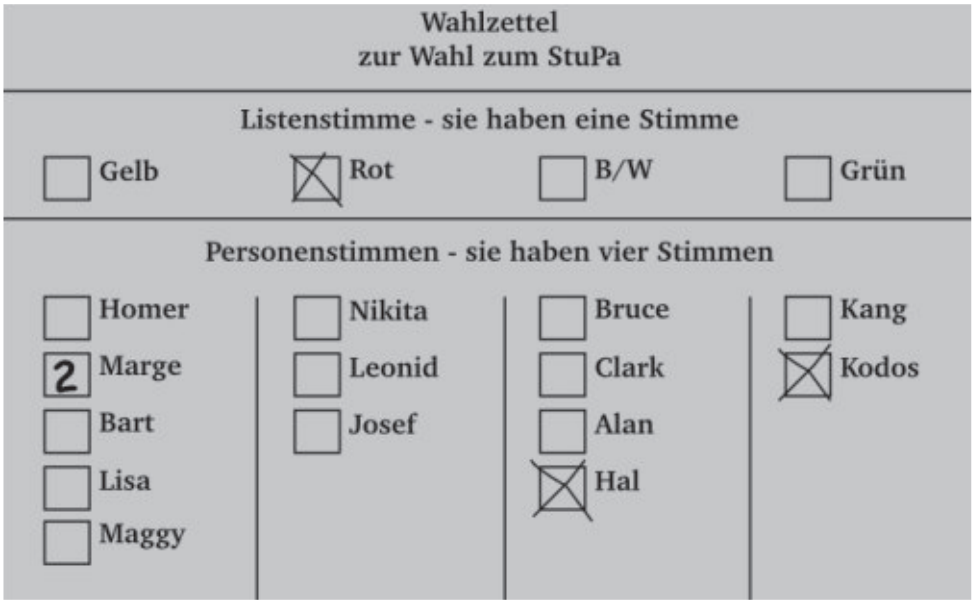

Wahlzettel
zur Wahl zum StuPa

Listenstimme - sie haben eine Stimme

☐ Gelb ☒ Rot ☐ B/W ☐ Grün

Personenstimmen - sie haben vier Stimmen

☐ Homer	☐ Nikita	☐ Bruce	☐ Kang
2 Marge	☐ Leonid	☐ Clark	☒ Kodos
☐ Bart	☐ Josef	☐ Alan	
☐ Lisa		☒ Hal	
☐ Maggy			

Musterwählerin Susi Sonnenschein hat das Prinzip verstanden und richtig ihre Kreuzchen gesetzt: Ihre Erststimme ging an eine Liste, die übrigen Zweitstimmen hat sie auf verschiedene Kandidaten verteilt. Dabei hat sie sowohl Hal als auch Kodos jeweils eine Stimme gegeben und auf Marge zwei Stimmen vereint.

hat man am letzten Freitag in der Wahlwoche die Chance, im UStA-Büro ohne Datenübermittlung zu wählen.

Für weitergehende Informationen, was der UStA, die autonomen Referate und das StuPa machen, gibt einige Wege: Das Umag zu lesen ist natürlich immer ein guter Anfang. Weitere Informationen findet man unter www.usta.de, dort kann man sich auch für den Email-Newsletter an- oder abmelden. Zudem kann man natürlich auch die öffentlichen UStA- und StuPa-Sitzungen besuchen. Das StuPa tagt zur Zeit alle zwei Wochen im Raum 214 im Gebäude 20.12 (Kolleg am Schloss).

Vom Holzkasten zum Siliziumchip

Zum ersten Mal ein elektronisches Wahlsystem auf dem Campus im Einsatz

Von Björn Tackmann

Bei den Unabhängigen Wahlen vom 14. bis zum 18. Januar wird neben der üblichen Papierwahl zum ersten Mal ein elektronisches Wahlsystem zum Einsatz kommen. Das dabei verwendete System Bingo Voting wurde am Europäischen Institut für Systemsicherheit (EISS) der hiesigen Fakultät für Informatik entwickelt. Die Wahlordnung wurde bereits durch das StuPa für den Einsatz dieses neuen Systems angepasst.

In der letzten Zeit gab es turbulente Entwicklungen im Bereich elektronischer Wahlen. Zunächst waren Wahlmaschinen auf dem Vormarsch: In den Niederlanden war bereits eine breite Abdeckung erreicht, auch in Deutschland wurden vereinzelt Wahlmaschinen eingesetzt (z.B. Nedap in Cottbus) und weitere Verfahren geplant (elektronischer Wahlstift in Hamburg, mittlerweile soll er nicht mehr eingesetzt werden). Jedoch wurde nach der Aufdeckung eklatanter Sicherheitsmängel die Zulassung vieler Wahlmaschinen zurückgezogen. Warum soll nun also ausgerechnet bei den Wahlen zum Unabhängigen Modell ein neuer Anlauf mit einem elektronischen Wahlsystem gestartet werden? Woran scheitern die herkömmlichen Verfahren, und was macht Bingo Voting besser?

Hardwarefehler?

Einige Probleme des Nedap-Verfahrens lassen sich getrost auf die Hardware schieben. So lässt etwa die Abstrahlung der Wahlmaschine Rückschlüsse auf den Inhalt des Bildschirms zu. Mit ähnlichen Problemen haben aber alle Wahlverfahren zu kämpfen, und sie lassen sich etwa mit einer trickreichen Kamerainstallation in einer herkömmlichen Wahlkabine vergleichen.

Der gravierende Mangel der Nedap-Maschinen liegt jedoch im Zählsystem: Der Wähler kann den Vorgang der Auszählung nicht kontrollieren, da er nicht "in den Speicher schauen" und herausfinden kann, ob seine Stimme für Kandidat A wirklich für Kandidat A gezählt wurde. Nach der Wahl gibt die Wahlmaschine einfach das Ergebnis der Wahl aus. Ist die Wahlmaschine manipuliert, kann sie dem von ihr bevorzugten Kandidaten B also einfach Stimmen zumogeln - dem Wähler kann sie ja trotzdem anzeigen, dass sie seine Stimme für Kandidat A gezählt hätte.

Der Chaos Computer Club und die holländische Initiative "Wij vertrouwen Stemcomputers niet" haben die Software der Wahlmaschine sogar so geändert, dass sich das Ergebnis der Wahlmaschine mit jeder zusätzlichen Stimme einem Wunschergebnis an-

nähert. So ein Angriff ist schlimmer als eine Fälschung des Wahlergebnisses bei einer Papierwahl: am Ende der Wahl gibt es ja nur das Ergebnis im Speicher der Wahlmaschine, bei einer Papierwahl kann wenigstens eine erneute Auszählung erfolgen. Wie kann ein elektronisches Wahlverfahren also sicher sein? Es gibt kryptographische Wahlverfahren (Bingo Voting, Neffs Verfahren, Prêt-à-voter), die dem Wähler erlauben, die korrekte Zählung seiner Stimme zu prüfen.

Die Quittung bringt's!

Bei Bingo Voting erhält der Wähler eine Quittung über den Wahlvorgang. Außerdem wird nach der Wahl ein Protokoll der Auszählung veröffentlicht. Mit der Quittung und dem Protokoll kann ein Wähler nun überprüfen, ob seine Stimme korrekt bei der Auszählung berücksichtigt wurde. Dabei sind alle Informationen kryptographisch gesichert, so dass das Wahlgeheimnis nicht beeinträchtigt wird.

Eine Wahlmaschine kann nun zwar die Wahl verfälschen, geht dabei aber das Risiko ein, dass die Manipulation von einem Wähler entdeckt wird. Wenn so viele Stimmen manipuliert werden, dass es sich im Wahlergebnis niederschlägt, fällt es auf. Dies ist sogar der Fall, wenn nur ein geringer Teil der Wähler die Quittungen prüft. Mit der Ausgabe der Quittung entstehen allerdings neue Probleme: Kann der Wähler einem Dritten mit Hilfe der Quittung seine Stimme offenlegen, ermöglicht dies Erpressung und Stimmenkauf.

Zufallszahlen? Bingo!

Das Wahlverfahren muss also sicherstellen, dass die Quittung dem Wähler zwar die korrekte Zählung der Stimme nachvollziehbar macht, sie jedoch für alle anderen nicht von einer Quittung für eine andere Stimme zu unterscheiden ist. Bingo Voting löst dieses Problem, indem Stimmen als Zufallszahlen kodiert

Diese Kartenleser werden mit einer fest eingebauten Chipkarte die Zufallszahlen für das Bingo Voting erzeugen.

werden. Gibt der Wähler seine Stimme an der Wahlmaschine ab, erhält er eine Quittung, bei der für jede mögliche Stimme eine Zufallszahl steht. Die Stimmen, die nicht vom Wähler stammen, werden durch vor der Wahl festgelegte Zufallszahlen repräsentiert.

Die Korrektheit der Wahl hängt nun also davon ab, dass in der Wahlkabine ein vertrauenswürdiger Zufallszahlengenerator zur Verfügung steht. Für die Unabhängigen Wahlen erhalten wir dazu von der Firma Reiner SCT speziell modifizierte Chipkartenleser. Eine fest eingebaute und für Sicherheitsanwendungen zertifizierte Chipkarte generiert dabei die Zufallszahlen.

Die Überprüfung der Wahl findet in drei Schritten statt:

1) Der Wähler prüft in der Wahlkabine, dass die neue Zufallszahl an die korrekte Position auf der Quittung geschrieben wurde.
2) Der Wähler prüft nach der Wahl, ob seine Quittung mit dem Auszählungsprotokoll korrekt veröffentlicht wurde.
3) Jeder kann die Korrektheit der Wahl anhand der veröffentlichten Quittungen, des Auszählungsprotokolls und vor der Wahl veröffentlichter Informationen zu den Zufallszahlen prüfen.

Der dritte Schritt kann aufgrund der Anzahl der Stimmen nur mit einem Computer geschehen. Eine Software hierzu wird vom EISS bereitgestellt, die Prüfung mit weiteren unabhängigen Implementierungen ist erwünscht und stärkt natürlich das Vertrauen in die Korrektheit des Ergebnisses.

Sollte eine Wahlmaschine manipuliert werden, kann diese natürlich das Wahlgeheimnis angreifen. Sie kann jedoch das Ergebnis der Auszählung nicht verfälschen, ohne dass es entdeckt wird. Außer den üblichen Argumenten für elektronische Wahlsysteme (schnellere Auszählung, Unterstützung der Wähler bei der Abgabe der Stimme) liefert ein kryptographisches Wahlverfahren im Gegensatz zu einer Papierwahl zusätzlich also eine individuelle Verifizierbarkeit des Wahlergebnisses.

Einen Vortrag zum elektronischen Wahlsystem und dem Einsatz bei den Unabhängigen Wahlen gibt es am Dienstag, den 8. Januar 2008, um 17:30 Uhr im Hörsaal -101 im Informatik-Gebäude.

Bingo Voting

- Bei den unabhängigen Wahlen vom 14. bis zum 18. Januar wird das Wahlverfahren "Bingo Voting" eingesetzt.
- Bisherige elektronische Wahlverfahren (Niederlande, Hamburg) sind unsicher.
- Bingo Voting gibt dem Wähler eine Quittung, die die korrekte Zählung seiner Stimme zeigt. Trotzdem ist der gewählte Kandidat für Dritte nicht an der Quittung zu erkennen.
- Am 8. Januar 2008 um 17:30 Uhr findet im Hörsaal -101 im Informatik-Gebäude ein Vortrag zu Bingo Voting bei den unabhängigen Wahlen statt.