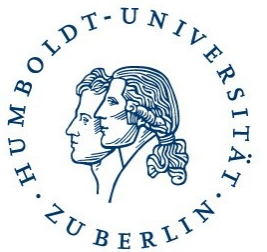
Humboldt-Universität zu Berlin
Institut für Informatik
Informatik in Bildung und Gesellschaft



Ergebnisse der Irish Commission on Electronic Voting und der Nedap-Hack

12. Dezember 2007

Sebastian Debray, Marco Schöpl

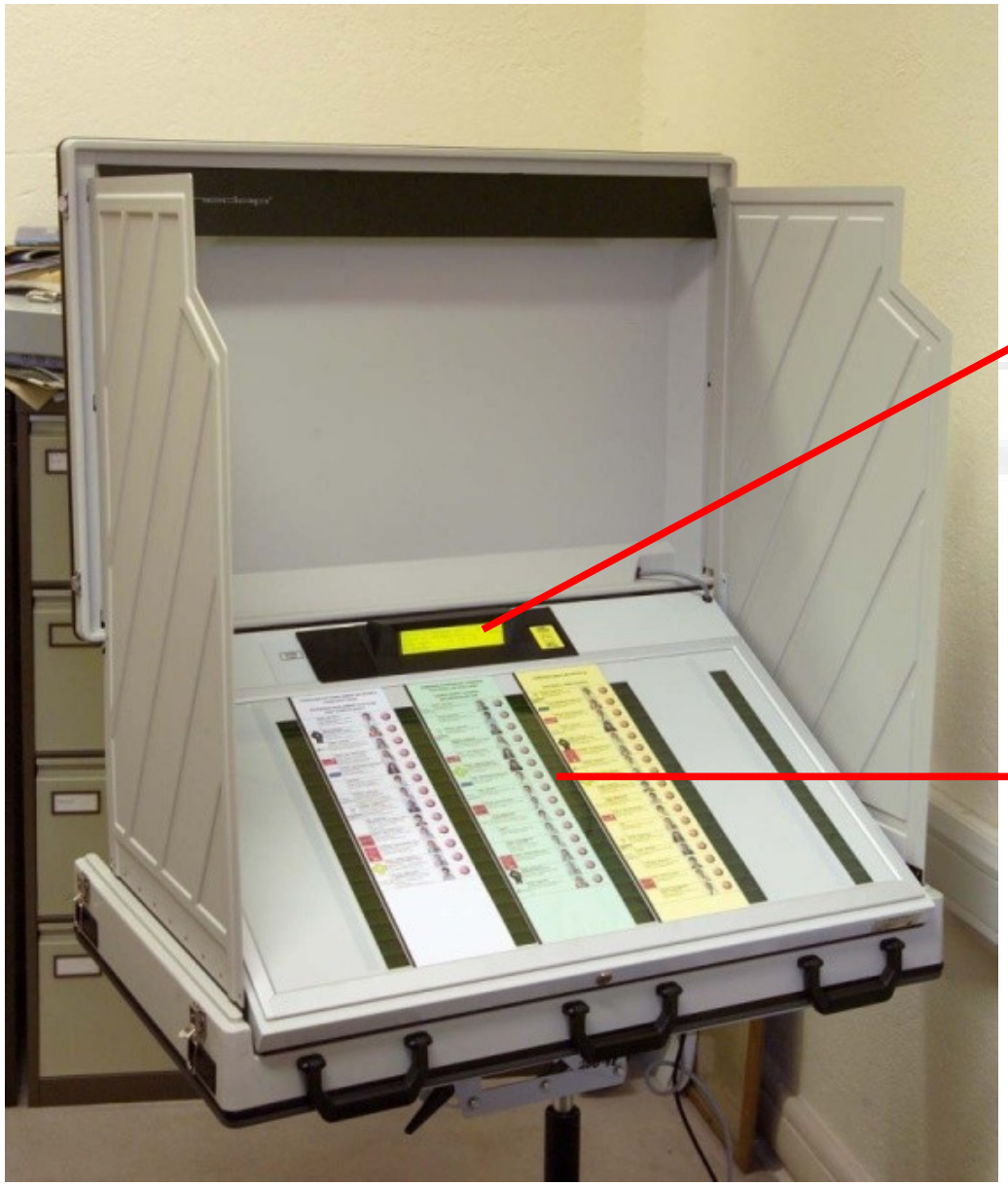
Gliederung

1. Der Nedap ES3B & ESI1/ESI2
2. Probleme aus Sicht der Irish Commission
3. Probleme aus Sicht der Niederländischen Aktionsgruppe „wijvertrouwenstemcomputersniet“ und des Chaos Computer Club
4. Reaktion der Öffentlichkeit
5. Quellen

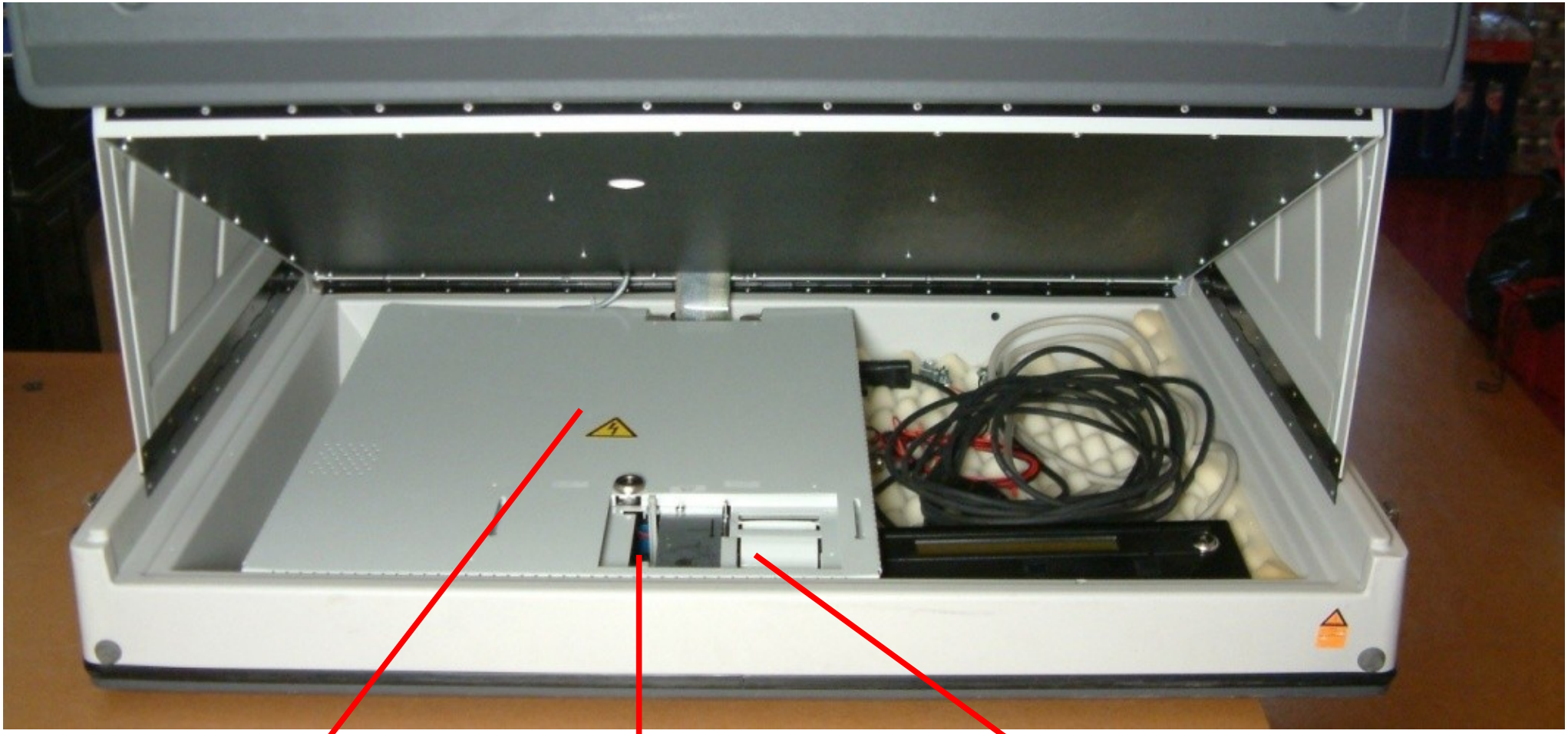
1. Nedap ES3B & ESI1/ESI2

Der Wahlcomputer

Vorderansicht



Rückseite – Abdeckung 1 entfernt



Rückseite – Abdeckung 2 entfernt

(E)PROMs Prozessor Drucker

Die Software

Aufgaben

➔ Stimmabgabe und Stimmspeicherung

➔ Berechnung des Endergebnisses, Ausdrucken

Umsetzung

➔ einfache Struktur („elektronische Strichliste“)

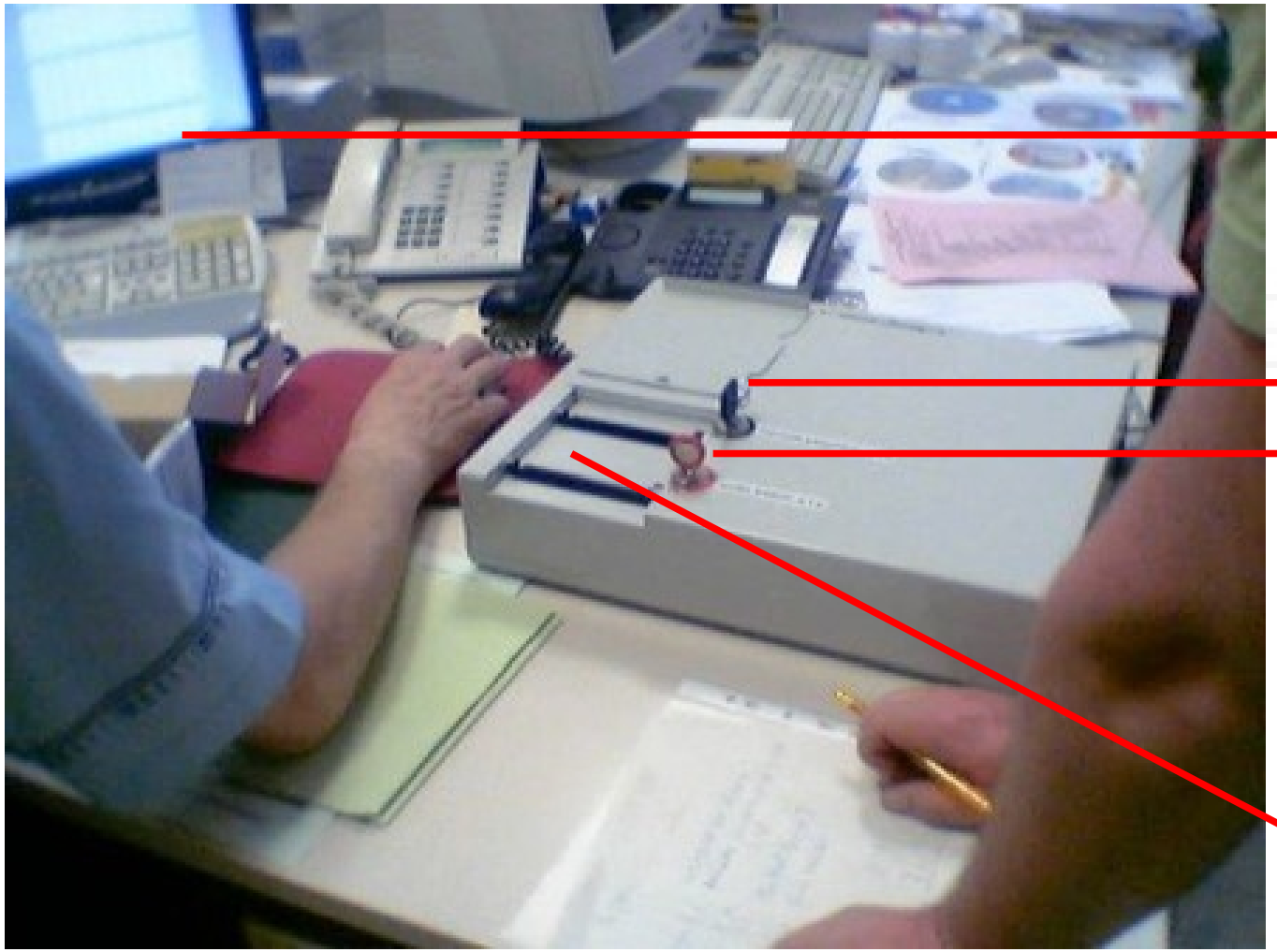
➔ Sicherheit?

- Redundanz (Stimmen mehrfach abgespeichert)
- Speichermodule nur Schreibbar, nicht Löschbar
- Schreiben an pseudo-zufälliger Position im Modul

1. Nedap ES3B & ESI1/ESI2

Die Programmiereinheit und das Zubehör

Auslese- und Programmiereinheit

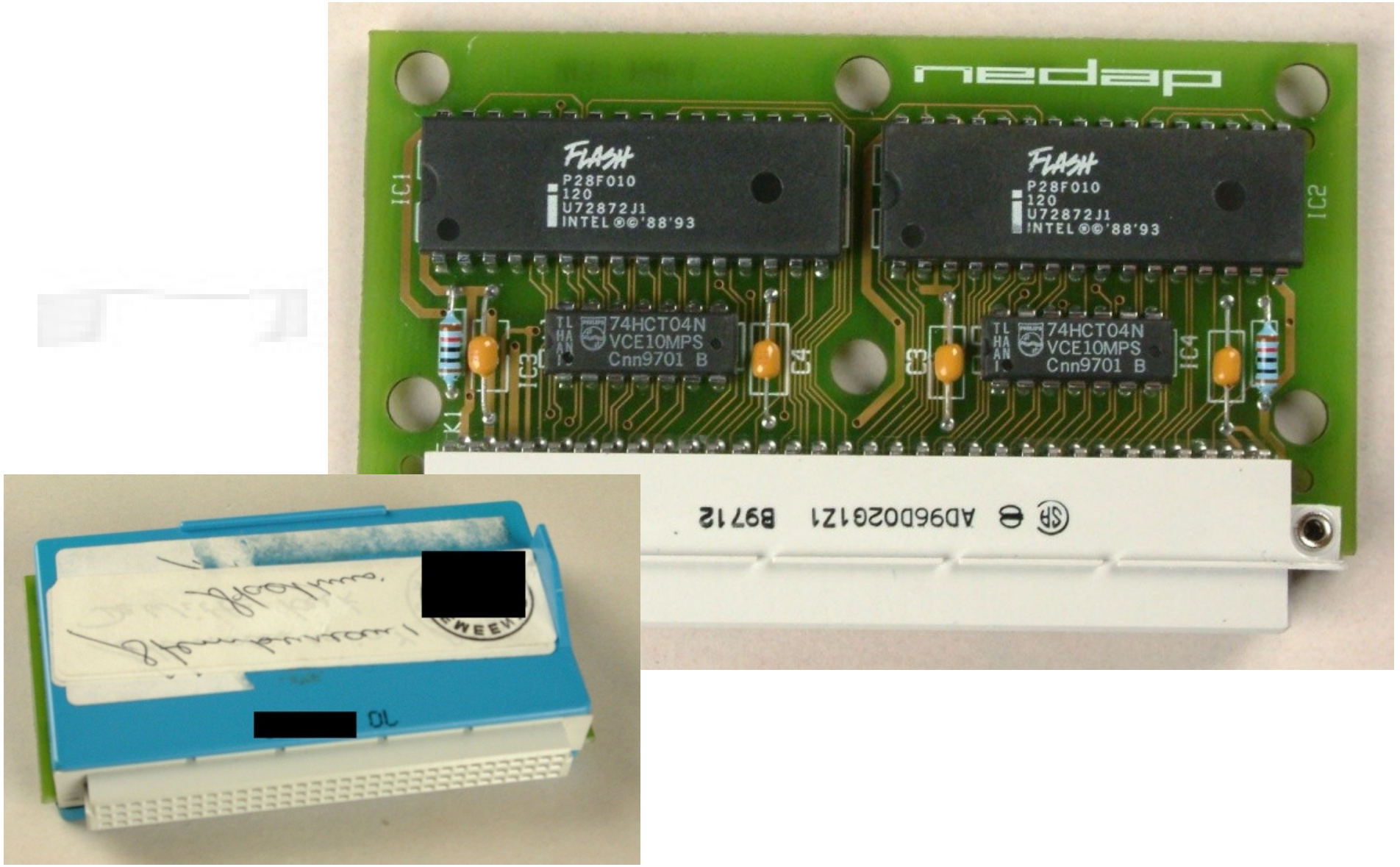


Normaler Windows-PC

Lese- und Schreib-schlüssel
(C&K YL Series 4 Tumbler Camlock, A126 Best.-Nr: 115140126)

Steckplätze

Die Speichermodule



„Integriertes Wahl System”

Aufgaben

- ➔ Programmierung der Stimmspeichermodule
- ➔ Auslesen der Stimmen
- ➔ Berechnen des Gesamtergebnisses

Sicherheit?

- ➔ Stichwort: ältliches Windows mit Internetanbindung
- ➔ Maintenance Mode - „GEHEIM” / „SERVICE ”

2. Irish Commission

Irish Commission on Electronic Voting

Hintergrund

- Reports von 2004 und 2006
  - sollte die Benutzung von Wahlcomputern überprüfen
  - Im Report von 2004: Keine Empfehlung
  - Im Report von 2006: Empfehlung unter Vorbehalt von Verbesserungen

Ergebnisse der Irish Commission

Hardware

- Wahlmaschine
  - gute Qualität und Design
  - Zugriff auf Hardware zu einfach
  - bessere Geräteidentifizierung
  - Elektromagnetische Strahlung egal
- Management-PC
  - Sicherheit der Hardware ist inadäquat

Ergebnisse der Irish Commission

Software

- Management-PC
  - Quellcode in Delphi nicht nach allgemeinen Standards der Wirtschaft entwickelt
  - Fehlerhaft
  - Kann relativ günstig nochmals entwickelt werden
  - System anfällig für Hackerangriff (ermöglicht Netzwerkverbindung...)

Ergebnisse der Irish Commission

Software

- Wahlmaschine
  - Quellcode in C nach allgemeinen Standards der Wirtschaft entwickelt
  - Muss vor der Benutzung nochmals eingehend überprüft werden (Analyse des Quellcodes)

Ergebnisse der Irish Commission

Datentransport

- Inadäquate Sicherheitsmaßnahmen zur Sicherung der Daten
  - „ballot modules“ für Transport der Daten vom Wahlcomputer zum Management-PC, Rest CDs
  - Verbesserung der Sicherheit durch Verschlüsselung der Daten und digitale Signaturen

Ergebnisse der Irish Commission

Sicherung

- Wahlcomputer sind nicht adäquat gegen Zugriff geschützt
  - Sicherung der Wahlcomputer zu jeder Zeit durch äußere Sicherheitsmaßnahmen notwendig

Ergebnisse der Irish Commission

Sicherung

- Verbesserungen durch
  - einheitliche Sicherheitsstandards
  - garantierte Sicherung der Geräte nach der Programmierung unmittelbar vor der Wahl
  - Sicherung des Datentransports per CD / „ballot modules”
  - Geräteregistrierung mit Identität, Position, Bewegungen und Dokumentation der Benutzung

Ergebnisse der Irish Commission

Sicherheit

- Papierwahl ist (noch) sicherer
- elektronische Wahl hat Potential, das Sicherheitsniveau der Papierwahl zu erreichen

Genauigkeit

- Max. Genauigkeit ist bei Wahlcomputer höher

3. Aktionsgruppe und Nedap-Hack

Wijvertrouwenstemcomputersniet

WIJVERTROUWENSTEMCOMPUTERSNIET

Initiatoren

➔ Rop Gonggrijp, Peter Knoppers, Anne-Marie Oostveen, Barry Wels

Ziel

➔ durch jeden nachprüfbare Wahlen

Motivation zum Hack

➔ Wie (un)sicher ist es wirklich?

➔ „Wahlnachrichten”

Das Schachspiel

„Den Beweis für die Aussage, dass man mit unserer Wahlmaschine auch Schach spielen kann, würde ich gerne vorgeführt bekommen.“

Statement von Jan Groenendaal, Übers. aus „Wahlnachrichten“ der HSG Wahlsysteme Deutschland

3. Aktionsgruppe und Nedap-Hack

Angriffsmöglichkeiten

Software anpassen

Probleme

➔ Austausch der Software?

- Wechseln der Speicherbausteine

➔ Prüfsummenberechnung?

- Aufgabe der Software

➔ Testwahlen?

- Erkennungslogik (schnelle Stimmabgabe, ...)
- Manipulation nur nach fester Tastendruckfolge

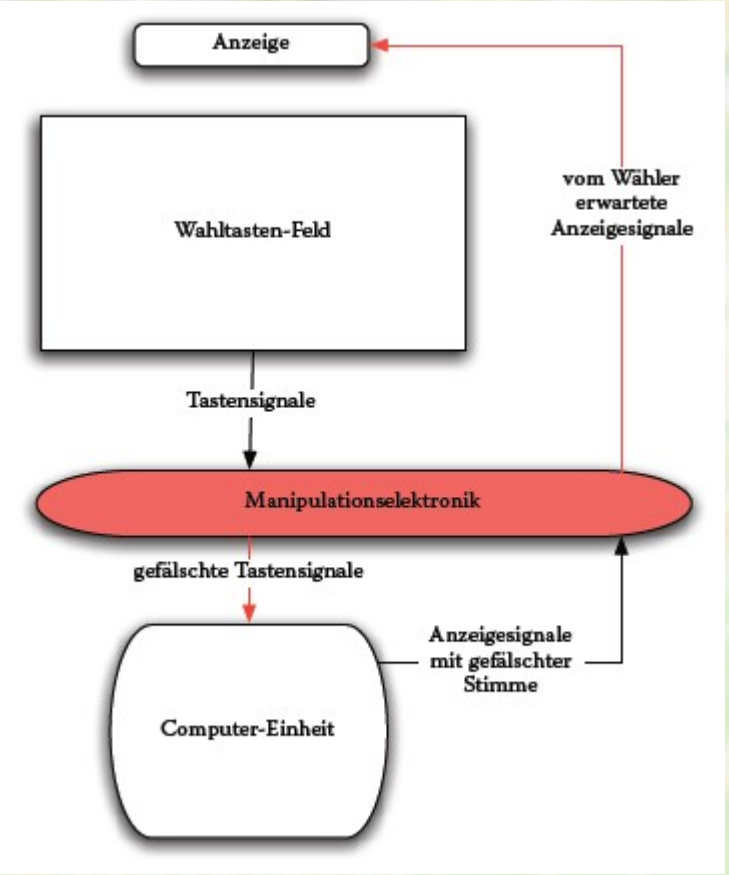
➔ Zwischenspeicherung 'gestohlener' Stimmen?

- im Konfigurations-EEPROM auf Systemplatine

Hardware anpassen

Ideen

- ➔ Austausch des Prozessors
  - Schutz: gleiches Aussehen wie Original
- ➔ hinzufügen einer Manipulationselektronik
- ➔ Speichermodul anpassen



Lauschangriff

Problem

➔ Abstrahlung nicht genügend abgeschirmt

- Display-Wiederholfrequenz normal: 72 Hz
  - bei Anzeige von Sonderzeichen: 58 Hz
- aus mehreren Metern Entfernung abhörbar

Reaktion der Öffentlichkeit

Presse und Politik

in den Niederlanden, Deutschland und anderswo

Reaktion der Presse

- ➔ generell aufgeschlossen
  - Internationale Berichterstattung
  - Hinterfragen der Technik
- ➔ erneutes Betrachten der US-Präsidentschaftswahlen

Reaktion der Politiker

Niederlande

➔ Aufhebung der Wahlcomputerzulassung

Deutschland

➔ „Ergebnisse nicht vergleichbar, weil andere Bauart”

➔ PTB-Prüfbericht und Zulassung werden verteidigt

Quellen

- Report der Irish Commission on Electronic Voting (von 2004 bzw. 2006)
- wijvertrouwenstemcomputersniet.nl – Abgerufen am 23.11.2007
- berlin.ccc.de – Abgerufen am 23.11.2007
- chaosradio.ccc.de – Abgerufen am 23.11.2007
- „Wahlnachrichten" der HSG Wahlsysteme GmbH, August 2006
- Nedap/Groenendaal ES3B voting computer – a security analysis Gonggrijp, Hengeveld et al.; 6. Oktober 2006
- Beschreibung und Auswertung der Untersuchungen an NEDAP-Wahlcomputern Kurz, Rieger, Gonggrijp; 30. Mai 2007