Irish Commission
Nedap Hack

Jonas Liepe
Oliver Stadie

Inhalt

- Nedap / ES3B allgemein
- Situation davor
- Bericht der Irish Commission
- Bericht über den Nedap-Hack
- Situation danach

Was ist der Nedap?

- Ein Wahlcomputer
- Klasse: Direct Recording Electronic
- Hersteller:
  - niederländische Firma N.V.Nederlandsche Apparatenfabriek (Nedap)
  - 1929 gegründet
  - Software teilweise von Groenendaal
- Hardware äquivalent zu einem PC der 80er

Was ist der Nedap? (2)

Funktionsweise des Wahlcomputers:

Portable Voting Machine with attached Control Unit*

=

Control Unit

Ballot Module

CD mit:
Integrated Election Management Machine and Programming/ and Counting Software

Personal Computer (PC)

Programming/Reading Unit*

* Systeme haben eingebettete Software

Was ist der Nedap? (3)

Nedap Wahlkabine von innen

Situation bisher

- **Allgemeinheit:** Grundsätzlich kritische Haltung oder Unwissenheit.
- **Presse:** Gleichgültig
- **Politiker:** Vertrauen in die Technik durch Bericht der PTB
- **Hersteller:** Vertreten ihr Produkt
- Zulassung von Nedap in Deutschland, Niederlanden und Irland

Irish Commission

Was ist die Irish Commission:

- Gegründet am 01.03.2004 durch Irische Regierung
- Aufgelöst am 04.09.2006

Wer ist die Irish Commission:

- 5 Mitglieder
- Vorsitzender: Matthew P. Smith

Aufgaben der Irish Commission:

- Testen des Nedap / Povervote Systems auf:
  - Testbarkeit (Testing)
  - Zuverlässigkeit (Accuracy)
  - Geheimhaltung (Secrecy)

Irish Commission (2)

Rahmenbedingungen:

- Nur 2 Monate Zeit für ersten Bericht, deswegen teilweise oberflächlich
- Über den Rahmen ihrer Aufgaben hinaus

Vorgehensweise:

- Befragung der Öffentlichkeit
- Tests durch unabhängige Institutionen
- Blackbox Tests der Einzelkomponenten
- Auswerten früherer Tests
- Simulieren von „Mini-Wahlen“

Irish Commission (3)

Testergebnisse – Testbarkeit:

- Zeitmangel (First Report)
- Viele Softwareupdates
- Kein Zugang zum Quellcode (First Report)
- Teilweise unangemessene Softwarequalität (Second Report)
- Fehlende Tests von Schnittstellen
- Fehlende Gesamt-Tests („end-to-end“)

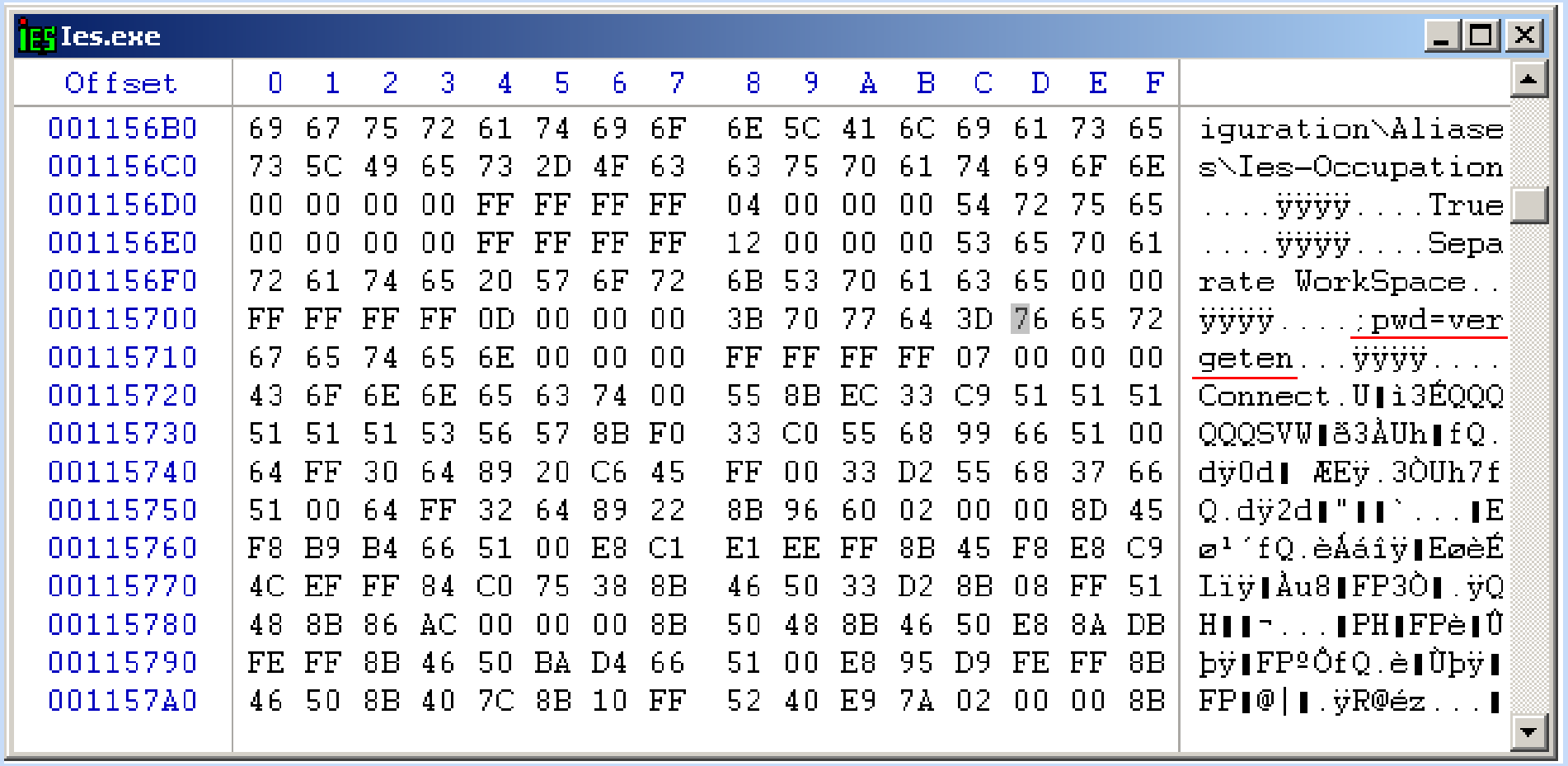
Irish Commission (4)

Testergebnisse – Zuverlässigkeit:

- Mangel an Testbarkeit
- Fehler in der „count software“
- Manipulierbare „count software“
- Manipulierbare Hardware
- MS Access 97 / Win2000 leicht zu hacken
- Handhabung durch Wahlpersonal (Aufgabenteilung)
- Keine gedruckten Dokumente
- Uneindeutige Stimmaufteilung überschüssiger Stimmen (Irisches Wahlsystem)

Irish Commission (5)

Beispiel: Das Access-Passwort ist 11 mal im Klartext in der ausführbaren election-software-Datei.



Ies.exe

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
001156B0	69	67	75	72	61	74	69	6F	6E	5C	41	6C	69	61	73	65	iguration\Aliase
001156C0	73	5C	49	65	73	2D	4F	63	63	75	70	61	74	69	6F	6E	s\Ies-Occupation
001156D0	00	00	00	00	FF	FF	FF	FF	04	00	00	00	54	72	75	65	....ÿÿÿÿ....True
001156E0	00	00	00	00	FF	FF	FF	FF	12	00	00	00	53	65	70	61	....ÿÿÿÿ....Sepa
001156F0	72	61	74	65	20	57	6F	72	6B	53	70	61	63	65	00	00	rate WorkSpace..
00115700	FF	FF	FF	FF	0D	00	00	00	3B	70	77	64	3D	76	65	72	ÿÿÿÿ....;pwd=ver
00115710	67	65	74	65	6E	00	00	00	FF	FF	FF	FF	07	00	00	00	geten...ÿÿÿÿ....
00115720	43	6F	6E	6E	65	63	74	00	55	8B	EC	33	C9	51	51	51	Connect.U‹ì3ÉQQQ
00115730	51	51	51	53	56	57	8B	F0	33	C0	55	68	99	66	51	00	QQQSVW‹ð3ÀUh™fQ.
00115740	64	FF	30	64	89	20	C6	45	FF	00	33	D2	55	68	37	66	dÿ0d‰ ÆEÿ.3ÒUh7f
00115750	51	00	64	FF	32	64	89	22	8B	96	60	02	00	00	8D	45	Q.dÿ2d‰"‹–`...ŤE
00115760	F8	B9	B4	66	51	00	E8	C1	E1	EE	FF	8B	45	F8	E8	C9	ø¹´fQ.èÁáîÿ‹Eøèɹ
00115770	4C	EF	FF	84	C0	75	38	8B	46	50	33	D2	8B	08	FF	51	Lïÿ„Àu8‹FP3Ò‹.ÿQ
00115780	48	8B	86	AC	00	00	00	8B	50	48	8B	46	50	E8	8A	DB	H‹†¬...‹PH‹FPè‹Û
00115790	FE	FF	8B	46	50	BA	D4	66	51	00	E8	95	D9	FE	FF	8B	þÿ‹FPºÔfQ.è•Ùþÿ‹
001157A0	46	50	8B	40	7C	8B	10	FF	52	40	E9	7A	02	00	00	8B	FP‹@|‹.ÿR@éz...‹

Irish Commission (6)

Testergebnisse – Geheimhaltung:

- „Beeps“ bei Eingaben
- Eingeschränktes Wahlgeheimnis für Behinderte
- Signierte Stimmenabgabe (durch Ranking)
- Umkehren der Zufallsfunktionen (Pseudozufall)
- Kein geheimer leerer Wahlzettel

Irish Commission (7)

Papier vs. Nedap:

- Pro Nedap:
  - Entfernung des Zufalls
  - Vorbeugen gegen versehentliche Falschwahlen
  - Entfernung von subjektiven Einflüssen
- Pro Papier:
  - Vermeidung von Amtsmissbrauch
  - Leere Stimmzettel
  - Transparenz
- Unentschieden:
  - Wichtige und unwichtige Auszählfehler

Irish Commission (8)

Fazit der Irish Commision:

- Finale Version nötig
- Voller Einblick in den Quellcode nötig (First Report)
- C-Code ist unter vorausgesetzten Standards
- Delphi-Code ist gar nicht zu empfehlen
- Unabhängige parallele Tests
- End-to-end Tests nötig
- Neuer Kompletter Test nach jedem Update

Wij vertrouwen stem Computers niet

- Wij vertrouwen stem Computers niet ist eine Vereinigung von Bürgern, die beunruhigt über Einsatz von Wahlcomputern bei holländischen Wahlen sind
- Wollen, dass Wahlen für jeden Bürger nachprüfbar fair ablaufen
- Nach ihrer Ansicht am Einfachsten mit Rückkehr zu Papierwahlen, deshalb Bericht

Vorbereitungen:

- Am 23.8.2006 eins geliehen, am 6.9.2006 zwei gekauft
- Aktuelle Versionen der Software
- Nur 3 Monate Zeit, da Veröffentlichung vor der Wahl

Hardwarebeschreibung

Schlüssel:

- Für $1.68 bei Allied Electronics für Voting Computer
- Schlüssel für Lese-/ Programmiereinheit immer der Gleiche

ES3B (Voting Machine):

- Motorolla 68000 8Mhz
- Programmspeicher 2*128kb EPROM
- Hauptspeicher 16kb RAM
- Ballot Slot
- Systemparameter (Device ID)/ Einstellungen 8kb EEPROM
- keine Echtzeituhr

Hardwarebeschreibung (2)

ES3B (Voting Machine) Fortsetzung:

- I/O TTL Bauweise 74 chips
- 2 serielle ports (PC und Modem)
- Drucker Port
- Wähler-Display, Wähler-Keyboard
- Manager-Display, Manager-Tasten
- Power-Taste/ Wahl-Taste

Lesegerät (Reading/Programming Unit):

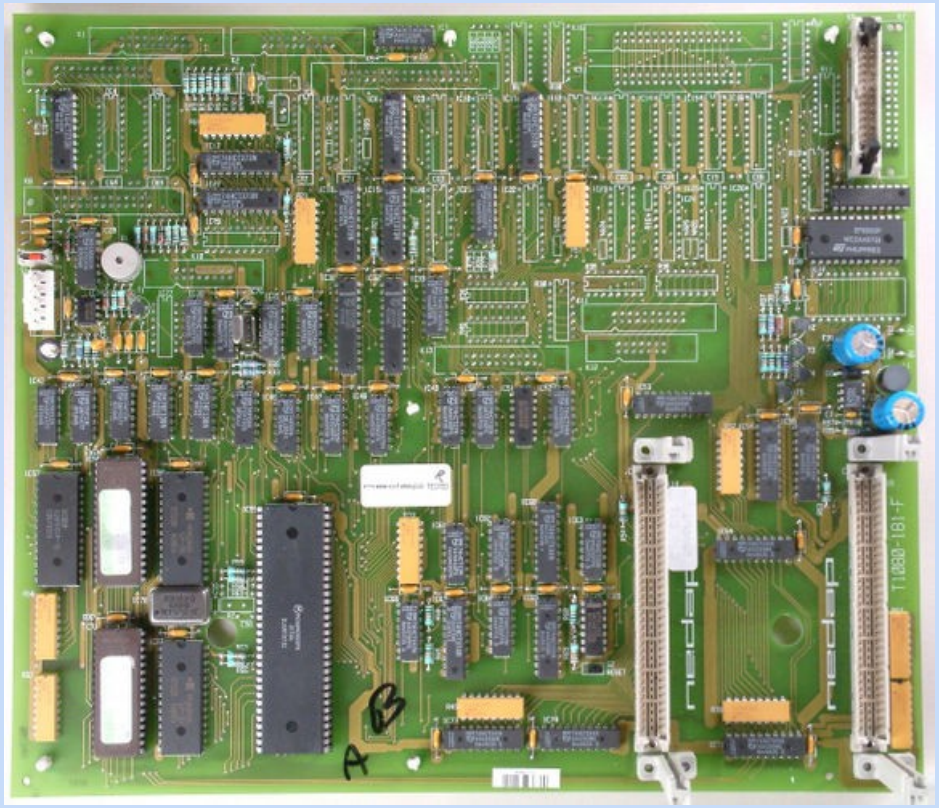
- Ähnlich mit einigen Bestandteilen fehlend

Ballot Modul :

- 2 flashchips

Hardwarebeschreibung (3)

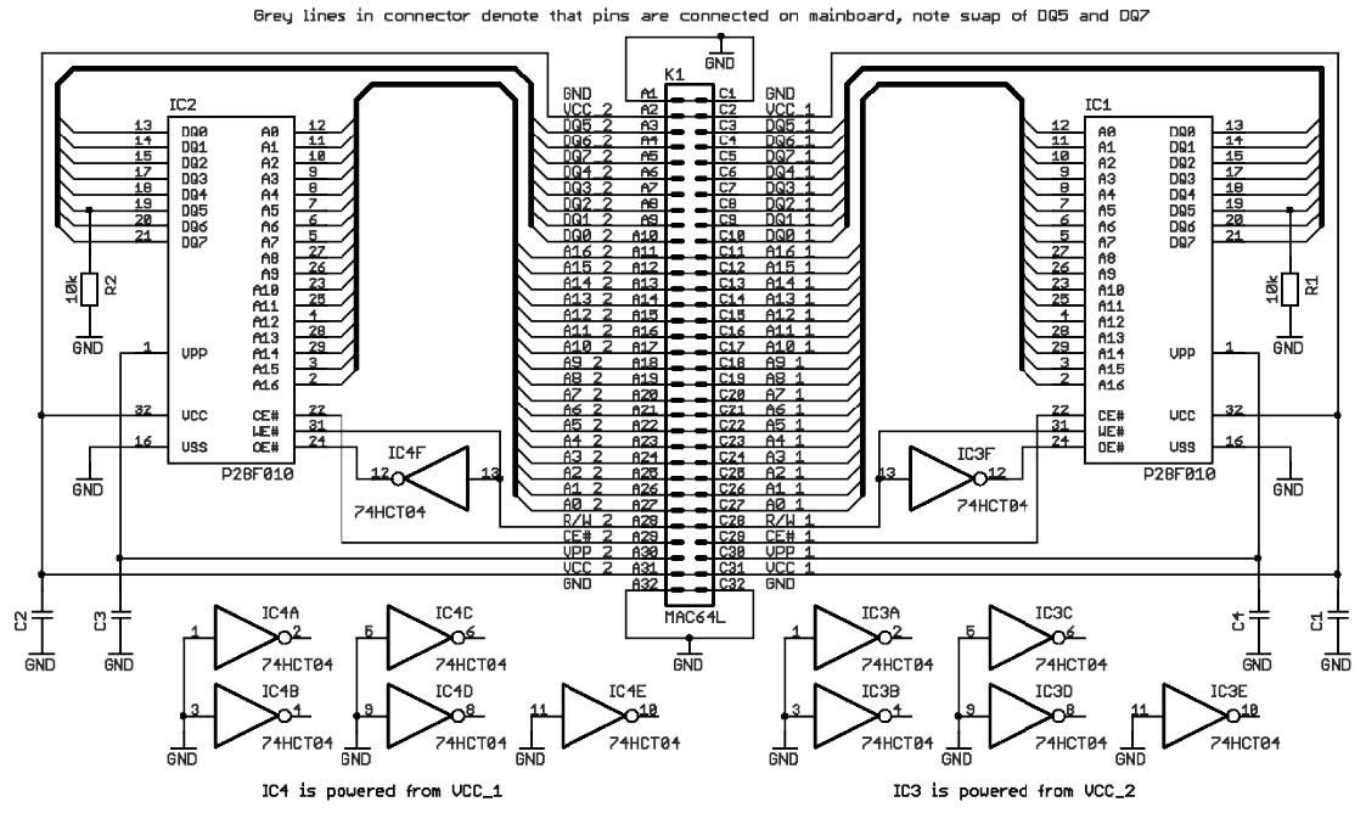
Mainboard von ES3B



- k01 manager display
- k02 voter display
- k03 voting keyboard
- k04 printer
- k06 pc serial port
- k07 modem serial port
- k08 printer port 2
- k09 power supply
- k11 voting keyboard
- k12 voting keyboard
- k13 voting keyboard
- k14 programmier slot
- k15 Lese slot
- k16 voting keyboard

Hardwarebeschreibung (4)

Schaltplan - Ballot Module



Softwarebeschreibung

- Programm auf beiden EPROMS des ES3B
- ISS (Integraal Stem Systeem) zum Laden neuer Konfigurationen (Kandidatenlisten) für MS Windows und Auslesen/ Berechnen der Ergebnisse der Ballot Module
- Maintenance Mode: Auslesen binärer Daten eines im Lesegerät steckenden Ballot Moduls

Beispielprogramm Schach

- Mittels gcc-Crosscompiler Bibliothek erstellen (lesen, schreiben, I/O Befehle, Display)
- Mit kleiner zusätzlicher Bibliothek (newlib) konnte „Tom Kerrigan's Simple Chess Program“ kompiliert werden
- 2 und 5 Cent-Münzen unterm Spielfeld zum Drücken der Tasten

Beispielprogramm Schach (2)

Manipulationssoftware ES3B

- Idee nicht neu, siehe Bericht Irish Commission
- Erase flash Kommando nicht von Voting Computer aus möglich
- Zwischenspeichern der Stimmen, die manipuliert werden sollen auf EEPROM
- Wenn durch Muster Testwahl erkannt, dann nicht manipulieren
- Zukunftsversion hat „magic button“, Tastenkombination zum Starten der Manipulationssoftware

Erkennungsmechanismen/Sicherheit erhöhen

- Kann EPROM auslesen und mit bekannter, richtiger Software vergleichen
- Checksum ungeeignet, da Addition aller Bytes im EPROM
- Serieller Port ungeeignet, da durch Programm auf EPROM gesteuert
- Programm auf Prozessor
- Sicherung der Geräte vor unbefugtem Zugriff
- Geräte sicher versiegeln

Manipulation ISS

- ISS meist an Bürorechnern mit Internet, Windows 2000
- ISS hat keine Sicherheitsmechanismen, die Manipulation zur Laufzeit verhindern
- Schutzmaßnahmen und Zugangsbeschränkungen für sensitive Systeme laut BSI (wurde hier nicht angewendet)

Hardwaremanipulation

- Zwischen Keyboard und Mainboard, Board einsetzen dass Knöpfe vertauscht
- TTL Chip gegen modernen Mikrochip austauschen, der Manipulationsprogramm hat, das mit spezieller Tastenkombination gestartet wird
- Ballot Modulhülle nachbilden, das falsche Ergebnisse speichert
- Elektromagnetische Abstrahlung mit UKW Empfänger messen (erhöhte Frequenz bei Umlauten)

Fazit der Initiative

- Kurzfristige Änderungen ergeben unzulängliche Besserungen
- Ganz gleich welches Programm, die Architektur kann keine verantwortungsvollen Sicherheitskriterien erfüllen
- Holländisches Reglement unzureichend
- Nicht genug Beachtung der Wahlmaschinen in Bezug auf Sicherheitsaspekte

Situation dannach

- NEDAP erweitert Gerät um Drucker und PROM statt EPROM
- In Irland Nedaps ausgesetzt bis 2009, nach dem Bericht der Irish Commission
- In Cottbus doch kein Kauf nach Ablehnung der Beschwerde von Thomas Langen
- Einspruch von Ulrich Wiesner abgelehnt, da keine Fehler in Vorbereitung/ Durchführung der Wahl
- Nach unabhängiger Untersuchung Dezember 2006 vorläufige Zurückziehung der Zulassung in Niederlande
- Auf kleine Anfrage Geräte hinreichend manipulationssicher

Situation danach (2)

- HSG sagt nie manipulationssicher, Sicherheitsvorkehrungen bei Wahl hinreichend
- Petition über Streichung von Zulassung von Wahlgeräten

Quellen

- First Report of the Commission on Electronic Voting (Dez. 2004)
  http://www.cev.ie/htm/report/download_first.htm
- Second Report of the Commission on Electronic Voting http://www.cev.ie/htm/report/download_second.htm
- http://www.wijvertrouwenstemcomputersniet.nl/nedap-en
  Hardwarebericht
- Nedap Hack
  http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf
- Presse & Auswirkungen des Nedap hacks
  http://www.heise.de/newsticker/meldung/98664
- ccc wiki wahlcomputer
  https://www.berlin.ccc.de/wiki/wahlcomputer
- Spektrum Informatik:
  Bericht Nedap-Wahlcomputermanipulationsmethoden an Hard- und Software