Diebold AccuVote

Alexander Baldauf
&
Andreas Prang

Gliederung

1. *Einleitung*
    1. *Die Autoren*
    2. *Was ist Diebold?*
    3. *Grundsätzliche Daten zu den Diebold-Maschinen*
2. *Aufbau der Software*
    1. *BallotStation Software*
    2. *Systemstart*
3. *Schwachstellen / Angriffsmöglichkeiten*
4. *Szenarium*
5. *Quellen*
6. *Schluss*

Prof. Aviel Rubin[Rub]

"Professor of Computer Science"

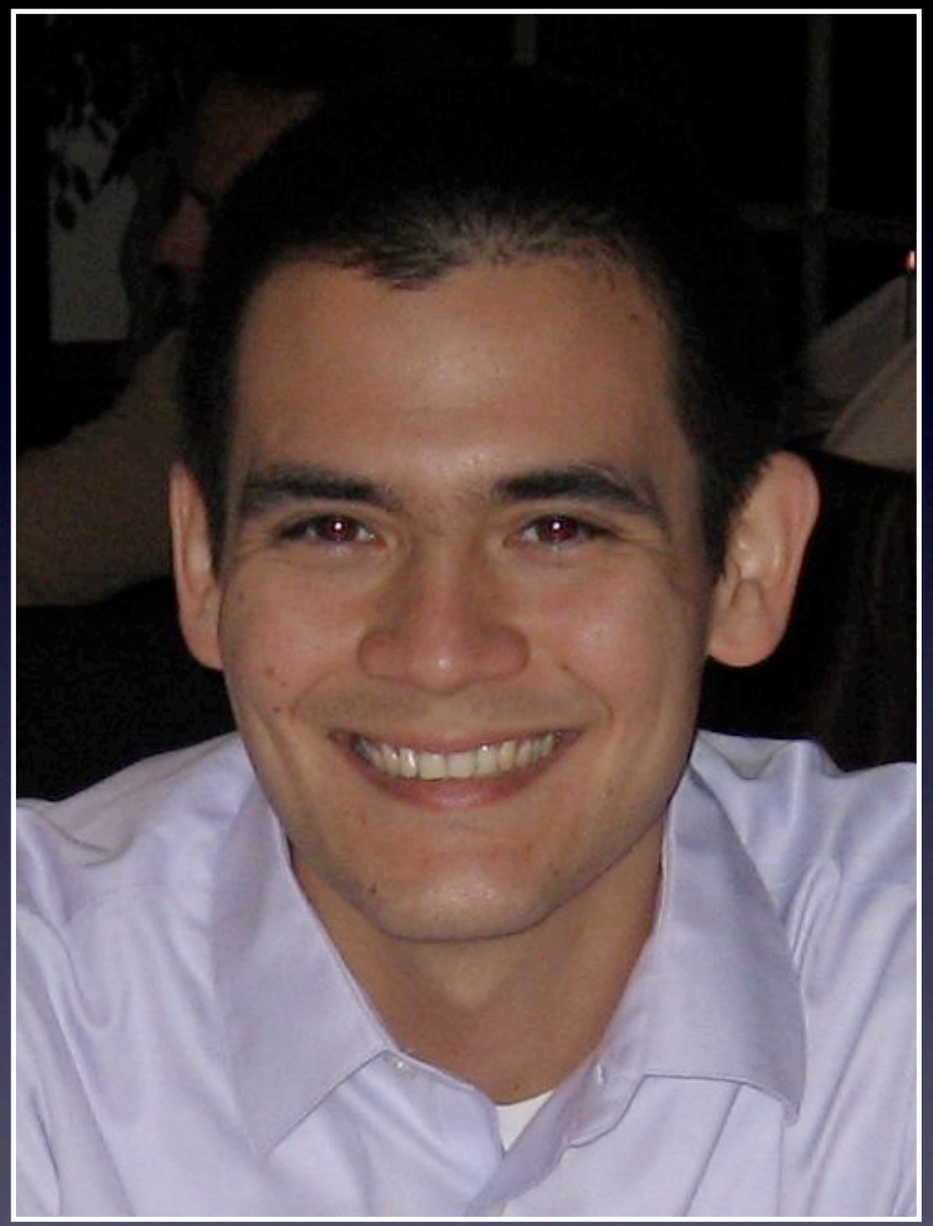
techn. Direktor des "Information Security Institute" der Johns Hopkins Univ.

preisgekrönt für die Sicherung der Integrität des Wahlprozesses

weitere Autoren [Anal]

Tadayoshi Kohno

z.Z. "Assistant Professor
Department of Computer
Science and Engineering
University of Washington" [Yosh]



weitere Autoren [Anal]

Adam Stubblefield

- z.Z. "Assistant research professor of computer science at Johns Hopkins University" [Stub]
- "cofounder of a computer security consulting company, Independent Security Evaluators (ISE)" [Stub]

weitere Autoren [Anal]

Dan Wallach

z.Z. "associate professor in the systems group at Rice University's Department of Computer Science" [Wall]

"associate director of ACCURATE" [Wall]

Diebold

"From the strength and security of the safes and vaults first manufactured by Charles Diebold in 1859,

to the technology-based integrated systems, software, and service that the Company provides today..."

Diebold

Produkte des Konzerns seit der Gründung:

- Panzerschränke
- Bürozubehör
- Mikrofilm
- Alarmsysteme
- Bankensysteme
- Rohrpost

- Panzerplatten für Fahrzeuge
- Wahlmaschinen/-service/-zubehör

==> jetzt Premier Election Solutions

- diverse Software
- Videoüberwachung

Grundsätzliche Daten

AccuVote-TS(X)

- Touchscreen
- Drucker
- Diverses

Zubehör

AccuVote OS

- Scanner
- Drucker
- SmardCard

output

Grundsätzliche Daten

AccuVote-TS(X)

Grundsätzliche Daten

AccuVote OS

BallotStation Software

BallotStation Software

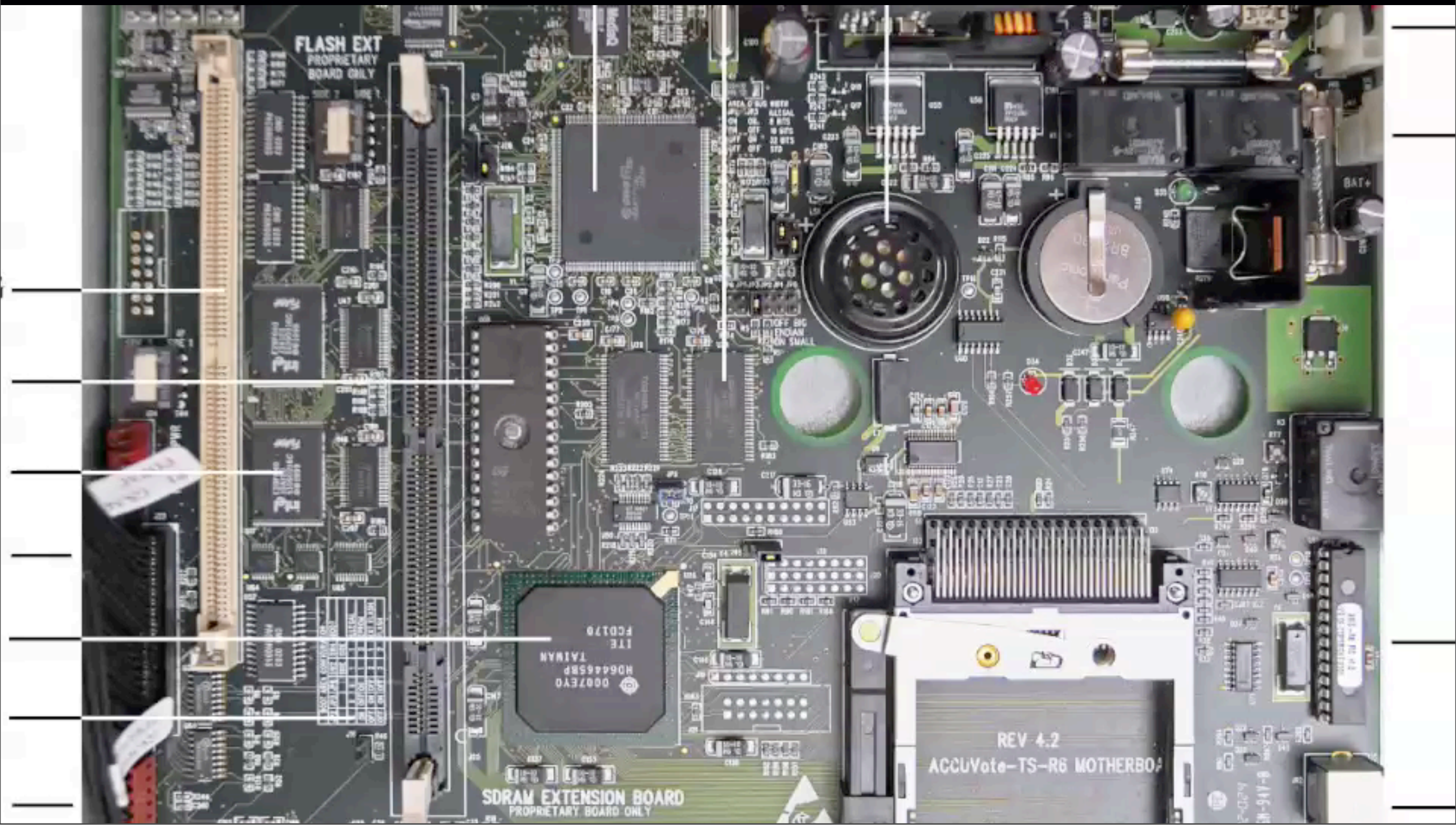
- Erkenntnisse stammen aus CVS-Logs
- vermutete Lebensdauer mindestens bis 2002
- kurz und knapp: augenscheinlich Schlampig entwickelt
- Objektorientiert C++ (keine Typensicherheit)
- von diversen Firmen entwickelt seit 1996 (DSKey)
- schlechte Kommentierung

BallotStation Software

- kurz und knapp: augenscheinlich Schlampig entwickelt
  - […]
  - kryptische Befehlsketten
- keine Verweise auf Fehlerprotokollkeine im Code ersichtliche Koordination der Kollaboration
- veralterte Verschlüsselung

BallotStation Software

Zertifizierung



Systemstart[SysS]

1. Jumper steuert Startadresse der CPU

2. Bootloader => 16MB Flash

3. Suche nach Spericherkarte auf PCMCIA Slot 1

Systemstart[SysS]

Suche nach Dateien

- fboot.nb0 neuer Bootloader
- nk.bin neues gepacktes OS => 16MB Flash
- EraseFFX.bsq Flash leeren

Systemstart[SysS]

4. OS wird in RAM geladen

5. Kernel wird gestartet

6. Erster Prozess: Filesys.exe
   Startet alle Programme aus
   HKEY_LOCAK_MASHINE\init (Windows-Module)

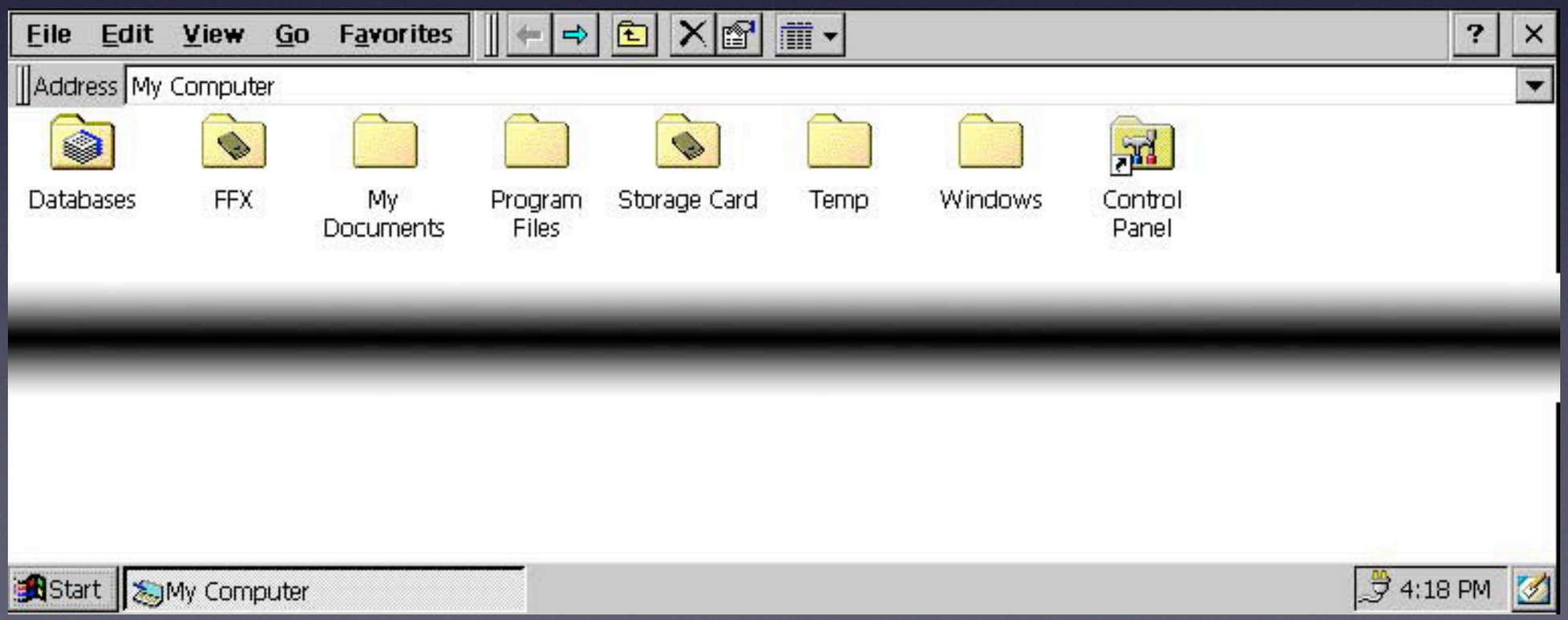
Systemstart[SysS]

Mounten der Speichermodule:

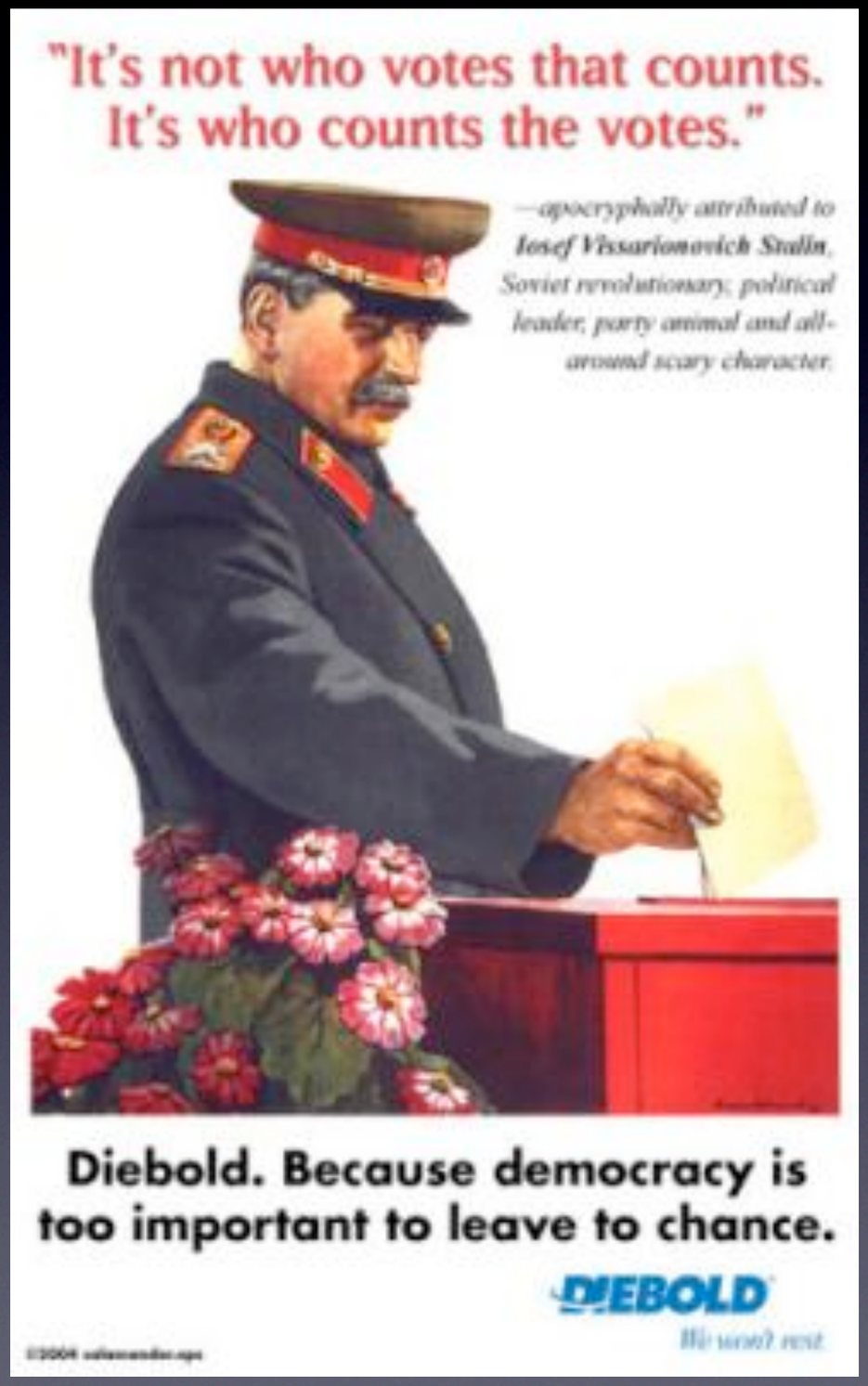
\	RAM
\FFX	16MB Flash
\Storrage Card	PCMCAI Slot1

Systemstart[SysS]

7. Starten des Taskmanagers
   If (\FFX\explorer.glb vorhanden){
     starte Explorer
   }else{
     \FFX\Bin\BallotStation.exe
   }



Schwachstellen



Schwachstellen

Allgemeine Schwachstellen

- keine Verschlüsselung der Smartcards
- election.edb in Klartext (ASCII)
- veralterte, geknackte Verschlüsselung
- Schlüssel steht in Klartext im Quellcode
- Unverschlüsselte Kommunikation über öffentliche Netze (DFÜ, www)
- Admin-/ Ender-/ Wählerwert leicht veränderbar

Schwachstellen

Sabbotage

- als Admin / Ender die Wahl vorzeitig beenden
- Seriennummer des Terminals fälschen (Registryeintrag)
- Stimmzähler manimpulieren (Integer in System.bin)
- Annehmen der Identität eines Terminals (Daten in election.edb und Registry)
- Diskrepanz zwischen gedrucktem Log und gespeichertem (Drucker abschalten)
- DoS gegen zentralen Wahlserver

Schwachstellen

Manipulation

- Veränderung der election.edb (z.B. Kanidatenreiheinfolge oder Parteizugehörigkeit)
- Veränderung der Aufzeichnungen (Redundant, aber schlecht verschlüsselt)
- Veränderung der Daten während der Übertragung (ISP oder Telefongesellschaft, Protokoll muss bekannt sein)

Schwachstellen

Wahlgeheimnis

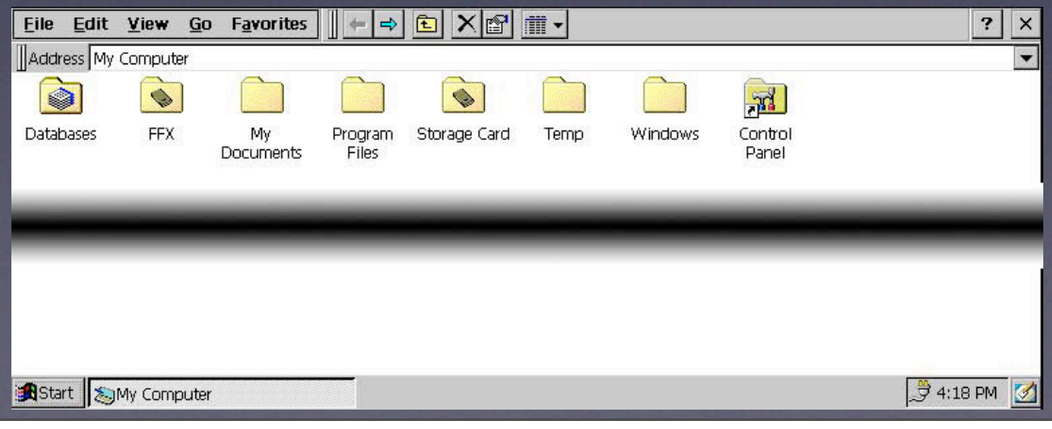
- sequentielle Speicherung in Maschine
- Zuordnung einer pseudo-pseudozufälligen Seriennummer (Generator<=Wahlstatistik)
- Zuordnung aber NICHT Sortierung VOR der Übertragung

Szenarium - Stealing Votes[SysS]

BallotStation.exe
(Hack) installieren

Restart

BallotStation.exe =>
WichtigeDatei.exe



Szenarium

Stealing Votes

Quellen

- [Anal] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach: -
  Analysis of an Electronic Voting System, Proc. IEEEt Symposium on Security and Privacy (May, 2004)
- [SysS] Ariel J. Feldman, J.Alex Halderman and Edward W. Felten -
  Security Analysis of the Diebold AccuVote-TS Voting Machine
- [Brav] Aviel D. Rubin, PhD
- [Rub] Autor unbekannt: "Professional bio" -
  http://avirubin.com/ - Stand: 17.12.2007
- [Yosh] Tadayoshi Kohno: Selbstdarstellung -
  http://www.cs.washington.edu/homes/yoshi/ - Stand: 17.12.2007
- [Stub] Adam Stubblefield: Selbstdarstellung -
  http://www.cs.jhu.edu/~astubble/ - Stand: 17.12.2007
- [Wall] Dan Wallach: Selbstdarstellung -
  http://www.cs.rice.edu/~dwallach/ - Stand: 17.12.2007

Jokaroo.com

Boom Chicago of Amsterdam made the following video in anticipation of technological advances in US elections.

It can be seen in our theater as part of our show 'Mr. America Contest' or in voting booths across Florida Nov. 2, 2004...

Diskussion

Überlegung:

Kann ein Computer mit proprietärer Software und Hardware sicher sein?

Welche Schwachstellen müssten beseitigt werden?