HUMBOLT-UNIVERSITÄT ZU BERLIN
INSTITUT FÜR INFORMATIK

Ergebnisse der Diebold-Schwachstellenanalyse von Aviel Rubin

Tugs-Erdene Erdene-Ochir

19.Dezember.2007

Inhalt

- Diebold-AccuVote-TS-System
- Wer ist Aviel Rubin?
- Einführung an die Diebold-Schwachstellenanalyse von Aviel Rubin
- Schwachstellen
- Gesamtwertung

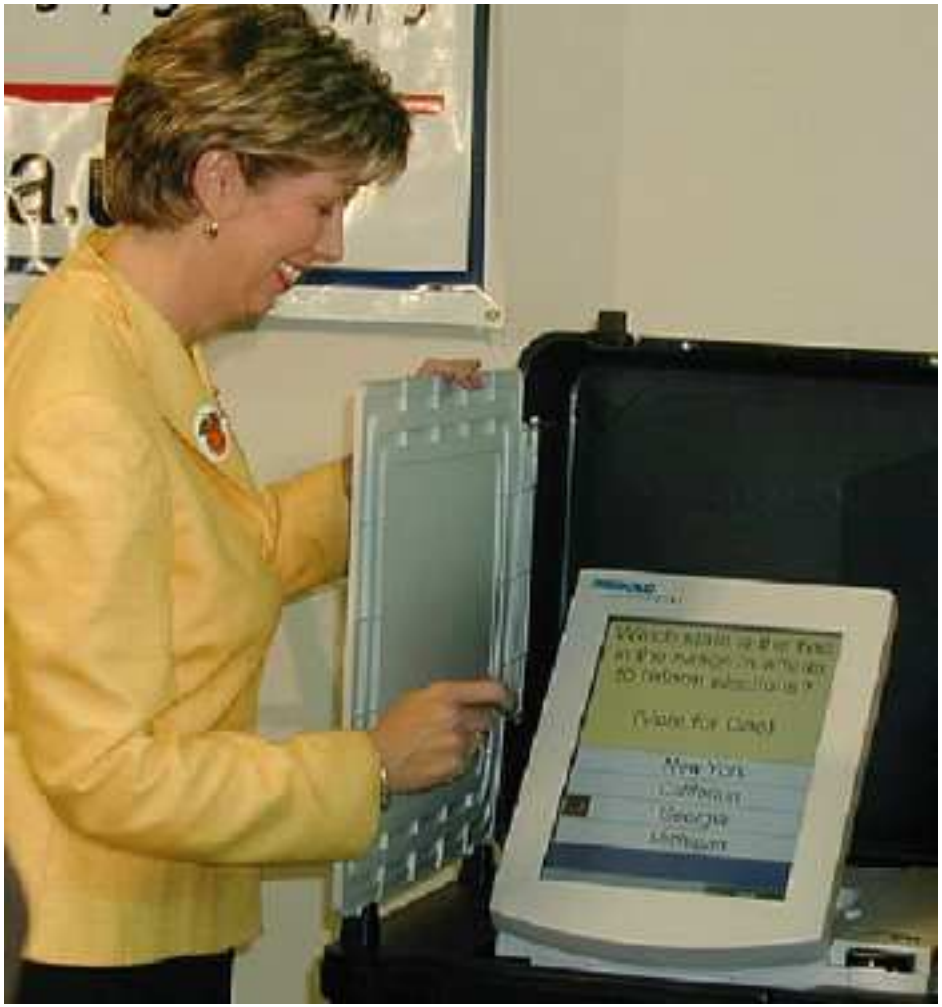
Diebold-AccuVote-TS-System

- Firmendaten
    - Ehemalige Diebold Election Systems
    - Premier Election Solutions
- Meist eingesetztes elektronische Abstimmungssystem mit AccuVote-TSx in USA
- Allgemeine Wahl im November 2006 in USA
    - In 385 Grafschaften
    - Mehr als 10% aller Stimmen
    - Mehr als 33000 AccuVote-TS-Terminals

Diebold-AccuVote-TS-Systemablauf

- Einrichten
  - Wahlgangdefinition
  - Konfiguration und Installation der Abstimmungsterminals
- Die Wahl
  - Authentifizierung der Wählerkarte
  - Wählen
  - Annullierung der Wählerkarte
- Die Ergebnisse berichten
  - Beendung der Wahl
  - Übertragung der Wahlergebnisse
    - Mit einer abnehmbaren Flashkarte
    - Über einem Ortsnetz, dem Internet und einer Telefonleitung

Diebold-AccuVote-TS-System



Wer ist Aviel Rubin?

- Informatik-Professor an der Universität Johns Hopkins
- Technische Direktor des Instituts für Informationssicherheit an der Uni Johns opkins
- Mitbegründer von „Independent Security Evaluators”
- Autor von mehreren Büchern über Sicherheit
- Baltimorean des Jahres (2004)
- Empfänger von Electronic Frontiers Foundation Pioneer Award (2004)

“Er kommt als jemand herüber, der aufrichtig glaubt, dass, was er tut, richtig ist, und er hat die technologische Tiefe um es zu unterstützen” [1]

[1]Gerald Masson, Direktor des Instituts für Informationssicherheit an der Uni Johns Hopkins, www.nytimes.com

Diebold-Schwachstellenanalyse von Aviel Rubin

- Quellcode
  - Nicht Opensource
  - Der Quellcode für AccuVote-TS gelang an die Öffentlichkeit (Bev Harris, 2003)
- Abstimmungsterminal für Test
  - Code
    - Implementier für Windows-CE-Gerät
    - Kompiliert und auch läuft auf regulären MS-Windows-Maschinen
- Weit unter den minimalen Sicherheitsstandard

Dieser Tabelle fasst einige der wichtigeren Angriffe auf das System zusammen

	Voter (with forged smartcard)	Poll Worker (with access to storage media)	Poll Worker (with access to network traffic)	Internet Provider (with access to network traffic)	OS Developer	Voting Device Developer
Vote multiple times using forged smartcard	•	•	•			
Access administrative functions or close polling station	•	•			•	•
Modify system configuration		•			•	•
Modify ballot definition (e.g., party affiliation)		•	•	•	•	•
Cause votes to be miscounted by tampering with configuration		•	•	•	•	•
Impersonate legitimate voting machine to tallying authority		•	•	•	•	•
Create, delete, and modify votes		•	•	•	•	•
Link voters with their votes		•	•	•	•	•
Tamper with audit logs		•			•	•
Delay the start of an election		•	•	•	•	•
Insert backdoors into code					•	•

Schwachstellen der Chipkarte

- Keine kryptographische Operationen
  - Keine sichere Authentifizierung der Chipkarte zum Abstimmungsterminal
  - selbst erstellte Chipkarte (Homebrew-Smarcards)
  - Authentifizierungswerte (ffi_ElectionKey, ffi_VCenter und ffi_DLVersion)
    - ffi_ElectionKey und ffi_DLVersion gleich für alle Wahlorte
    - ffi_VCenter ist leicht zu lernen

- Keine Aufzeichnung der Wählerseriennummer (ffi_VoterSN)
  - Das Abgeben vielfacher Stimmen

- Geheimzahl der Administratorkarte und Ender-karte wird zum Terminal im Klartext geschickt
  - Geheimzahl ist leicht zu finden
  - Denial-of-Service Angriff ist möglich

Schwachstellen der Wahlkonfiguration und Wahldaten

- Die ganze Konfigurationsinformation wird ohne jede Form des Integritätsschutzes gespeichert
  - In der Windows Register
  - Ein anderes Abstimmungsterminal darstellbar auf der Schirm

- nicht verschlüsselte Übertragung der Wahldefinition und Wahlergebnisse ohne Prüfsumme
  - Man-In-The-Middle Angriff möglich
  - darstellen legitimer Abstimmungsterminal

- Wahlergebnisse (einzige verschlüsselte Daten)
  - veraltete Verschlüsselungsalgorithmus „Single-DES“ seit Dezember 1998
    - leicht zu knacken
  - Schlüssel für Verschlüsselung wird in Quellcode direkt angegeben
    - #define DESKEY ((des_key*)“F2654hD4“)

Schwachstellen der Softwaretechnik

- Einige Codes stammen aus dem AccuTouch-Code von „Global Election Systems“ (1992-2001)

- Insgesamt wird der Code ziemlich uneben kommentiert
  - Unkommentierte logische Verzweigungen
  - Schwer den Quellcode zurückzufolgen und die Probleme zu beheben

- Versucht Pufferüberlaufe zu vermeiden
  - Nicht zu behaupten, dass es keine Pufferüberlaufe gibt
  - Bessere Lösung ist Java Zyklon
  - Beweisbar, dass richtige Durchführung vom Compiler und Laufzeitsystem unmöglich ist bei Angriffen
    - Pufferüberläufe
    - Typverwirrungsangriffe

Gesamtwertung

- Bedrohung
  - Wähler, die administrative Funktionalität
  - Größere Bedrohung ist Insider wie
    - Wahlbeamter
    - Softwareentwicklern
    - Hausmeistern

- Vorschlag
  - Ein angemessene Niveau und Disziplin für Programmieren
  - Verschlüsselungs-Standard (AES) benutzen

Quelle

- Aviel Rubin, Tadayoshi Kohno, Adam Stubblefield, Dan S. Wallach (2004): Analysis of an Electronic Voting System. http://avirubin.com/vote.pdf [02.Dezember 2007].

- Ariel J.Feldman, J. Alex Halderman, Edward W. Felten (2006): Diebold-AccuVote-TS-System. 1-3. http://www.usenix.org/events/evt07/tech/full_papers/feldman/feldman.pdf [02.Dezember 2007].

- Aviel Rubin's Homepage. http://avirubin.com/ [02.Dezember 2007]