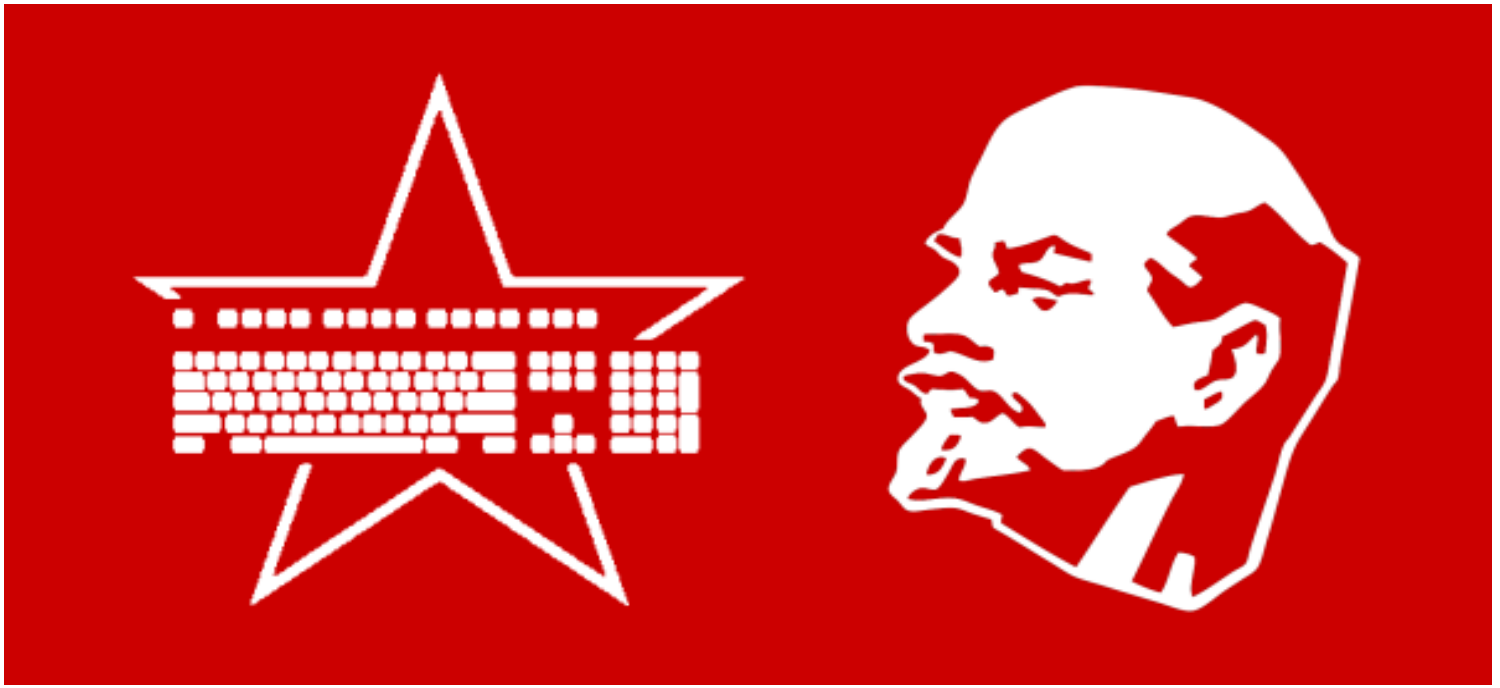


“Vertrauen ist schlecht, Kontrolle ist unmöglich!”

Wie sollten wir mit Technik umgehen, die wir nicht oder nur teilweise verstehen können?
Warum sollte dabei Ge-Wissen wichtiger sein als Fach-Wissen?

Referent: **Bernd Fix**, Hacker-Veteran des Chaos Computer Clubs
Vorstandsmitglied der Wau-Holland-Stiftung

Zu meiner Person:

- Jahrgang 1962 in Norddeutschland
- Studium Physik und Philosophie (Göttingen, Heidelberg)
- seit 1986 im Chaos Computer Club aktiv
- 1987 erste dokumentierte Viren-Bekämpfung
- 1988 Firma für Verschlüsselungs-Software (PC-DES)
- 1991 Firma im Bereich VR (CAD, 3D-Visualisierung)
- 1998 AG-Gründung in der Schweiz (Dornach)
- seit 2003 Vorstandsmitglied der Wau-Holland-Stiftung
- 2004 jetzige Firma aspector GmbH

Computersicherheit: Kryptologie, Smartcards, Netzwerke

Berater im Bereich Enterprise Security Architecture

© http://www.oe24.at

© http://www.tagesschau.de

© http://www.fireworld.at

© http://www.netzwelt.de

Vertrauen (ins Pkw-NAVI) ist schlecht, deshalb …

… ein “richtiges” und teures LKW-NAVI kaufen

… auf die Schilder hören:

(Beispiel aus England)

… am besten: **Vertrauen erschüttern!**

Vertraue Computern

nur so weit, wie Du sie
verstehen
~~werfen~~ kannst!

Wir müssen nicht jede Computer-Technik verstehen, aber wir müssen...

... ihre **Grenzen** kennen,

... ihre **Möglichkeiten** kennen,

... ihren **Nutzen** kennen,

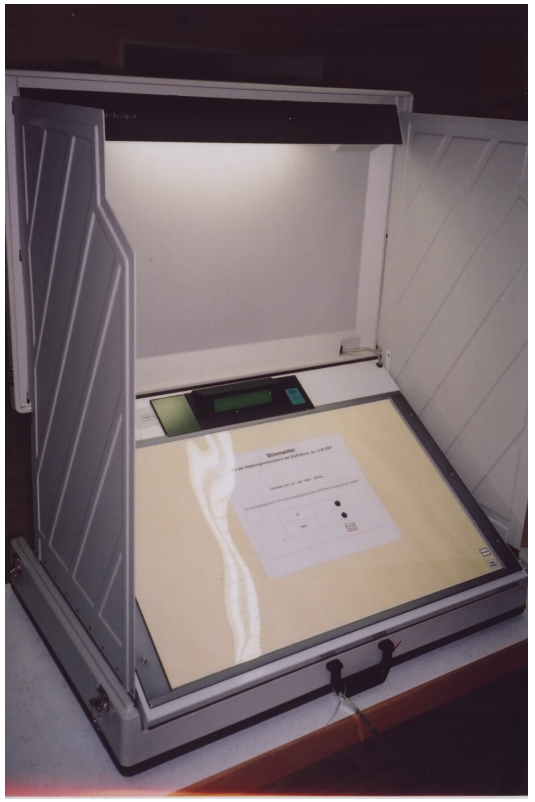
... ihre **Gefahren** kennen,

bevor wir sie **bewerten** können.

Es gibt kein **Vertrauen in Technik**, sondern nur ein **Vertrauen in die Menschen**, die die Technik entwerfen, herstellen und nutzen.

Zwei aktuelle Beispiele:

- Wahlcomputer



- Biometrischer Reisepass

Wahlcomputer -- Grenzen:

Befürworter reden von “**Wahlmaschine**”

Unterschied **Maschine** – **Computer**:

Maschine: Eine definierte Funktion mit geringer Varianz

Computer: Universalmaschine mit sehr vielen Funktionen

Wahlmaschine → enge Grenzen
→ wenig Möglichkeiten
→ nur ein definierter Nutzen
→ keine Gefahren!

Wahlcomputer → weite Grenzen
→ viele Möglichkeiten
→ mehrere Nutzen möglich
→ viele Gefahren möglich

Wahlcomputer -- Möglichkeiten / Nutzen:

- Komplettes Reverse Engineering der Original-Hard- und Software
- Entwickeln und Programmieren einer neuen Software
- “**Schach Matt**” dem Wahlcomputer!

Wahlcomputer -- Gefahren:

Entwickeln und Programmieren einer zweiten Software:

Manipulierte Wahlsoftware!

Drei Anforderungen:

- verhält sich exakt so wie das Original
- besteht die “offizielle Typenprüfung” (Testwahl)
- fälscht trotzdem gezielt das Wahlergebnis

Austausch der Software in einem realen Gerät dauert max. 60 Sekunden:

ePass -- Technik:

Hardware: RFID-Chip mit ...
... **Datenspeicher**
... kontaktloser Datenübertragung
... kontaktlose Stromversorgung

Software: Kryptoverfahren für Integritätsnachweis
(im Lesegerät integriert; standardisiert)
RFID-Betriebssystem weniger relevant

Sicherheit: Basiert wesentlich auf der Sicherheit der verwendeten Algorithmen und Verfahren
(kein Hardware-Schutz!)

ePass -- Technik:

Gespeicherte Daten (vereinfacht):

- Alle im Pass gedruckten Informationen
- Passbild
- optional: Fingerabdrücke, Irisabbild, ...

Digitale Signatur der Daten ist alleiniges vorgeschriebenes Sicherheits-Merkmal!

Jedes Land unterhält dafür eine eigene PK-Infrastruktur, die mindestens zweistufig ausgelegt sein muss.
Es gibt keine übergeordnete Authorisierungs-Instanz; jedes Land ist souverän in Bezug auf seine Schlüssel.

ePass -- Grenzen und Möglichkeiten:

ePass -- Nutzen: Fälschungssichere Dokumente

ePass -- Gefahren:

- Unbemerktes Auslesen von Daten durch Dritte

ePass -- Gefahren:

- Unbemerktes Auslesen von Daten durch Dritte
- Überall dort wo Daten gesammelt werden, werden sie auch missbraucht, gehen verloren oder tauchen an den unmöglichsten Stellen wieder auf.
- ePass-Zwang per Gesetz (keine Wahlmöglichkeit)

"Achten Sie darauf, dass ihr biometrischer Reisepass niemals in eine eingeschaltete Microwelle gerät..."