Die Gefahren von RFID, TPM/TC & Co.

Franz Pletz
<fpletz@phidev.org>

Chaos Computer Club München e.V. (MuCCC)

26. Juni 2008

Fahrplan

Zum CCC

- galaktische Gemeinschaft von Lebewesen, unabhängig von Alter, Geschlecht und Abstammung sowie gesellschaftlicher Stellung
- Einsatz für Informationsfreiheit und Menschenrecht auf zumindest weltweite, ungehinderte Kommunikation
- Beschäftigung mit Auswirkungen von Technologie auf die Gesellschaft und das einzelne Lebewesen
- technische Forschung, Entwicklung von technischen Hilfsmitteln, die Diskussion technischer Sachgebiete sowie öffentliche Demonstrationen
- Forum der Hackerszene: Instanz zwischen Hackern, Systembetreibern und der Öffentlichkeit

Zum CCC - konrekt

Womit beschäftigen wir uns konrekt?

- Überwachung/Datenschutz
  - Vorratsdatenspeicherung (AK Vorrat)
- Wahlcomputer/Wahlsoftware
  - Hessenwahl: NEDAP-Hack
  - Bayernwahl: we need **you**!
- Geistiges Eigentum
  - DRM (Digital Rights/Restriction Managment)
- Netzzensur/Netzneutralität
- Plastikgeld und Trackingkarten
  - EC/maestro, Geldkarte
  - Kundenkarten (Payback)
  - RFID

Fahrplan

RFID?

- RFID: Radio Frequency Identification
- Einsatzgebiete
  - berührungslose Identifizierung und Lokalisierung von Gegenständen und Personen
  - automatische Erfassung und Speicherung von Daten
- Bestandteile
  - Transponder am Objekt (Tag, Karte, . . .)
  - Lesegerät mit Schnittstelle zu anderen EDV-Systemen

Lesegerät

- erzeugt elektromagnetisches Feld geringer Reichweite, in der Regel mit Induktionsspulen
- benutzte Frequenzen
  - normalerweise 13,56 MHz
  - selten auch 125kHz/134kHz
- Anbindung an weitere EDV-Anlagen, z.B. ein Server der die empfangenen Daten verarbeitet und Antworten sendet

Lesegerät

Abbildung: Portal als Lesegerät zur Authentifizierung oder Diebstahlsicherung

Lesegerät

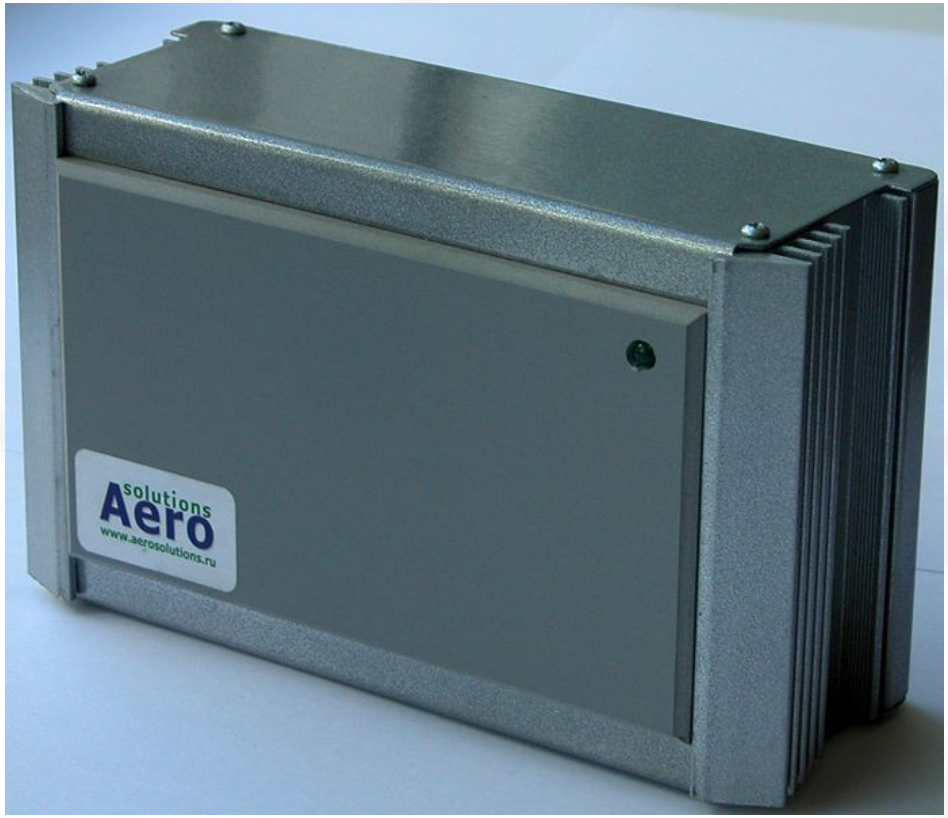

Abbildung: RFID-Leser als kompakter, unauffälliger Kasten

Transponder

- Bestandteile
  - Antenne (Spule)
  - Transceiver: analoger Schaltkreis zum Empfang
  - digitaler Schaltkreis (Chip)
  - permanenter Speicher
- Arten
  - passiv: Stromversorgung durch induzierten Strom
  - halb-aktiv: Batterie zur Versorung des Chips
  - aktiv: Batterie zur Versorgung von Chip und Speicher (z.B. für beschreibbaren Speicher)

Transponder

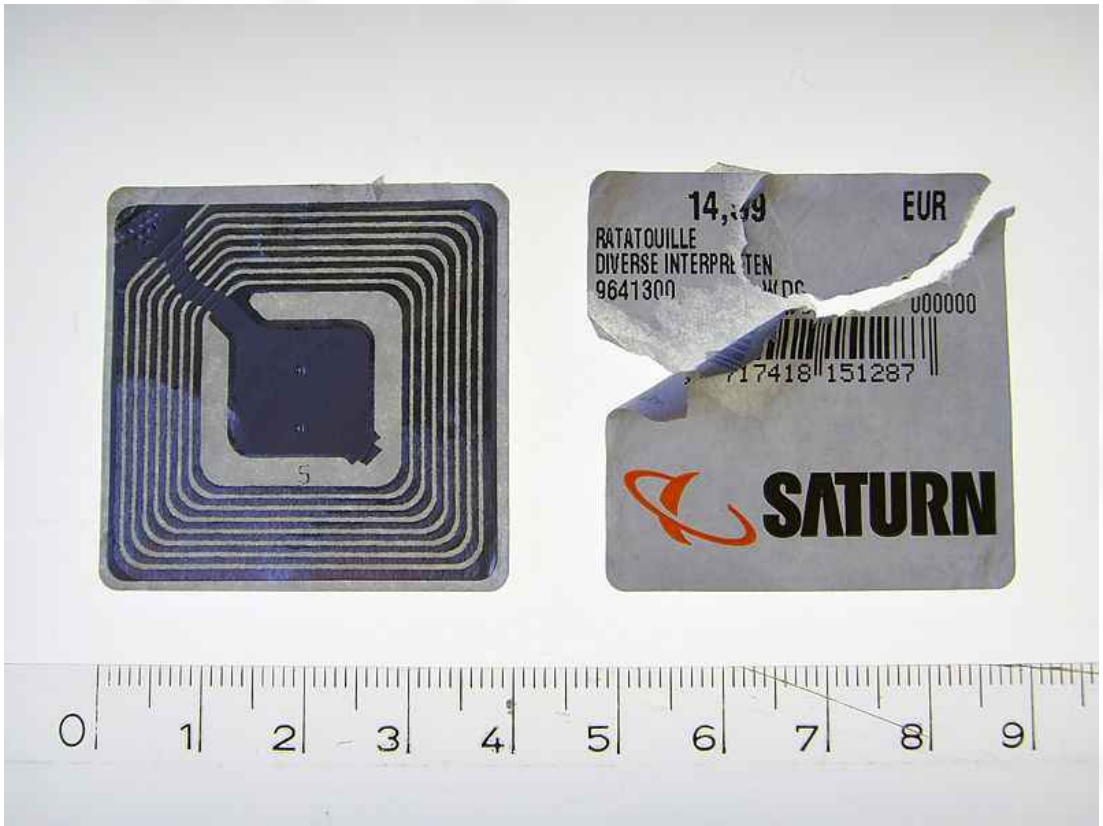

Abbildung: RFID-Tag als Diebstahlsicherung

Transponder

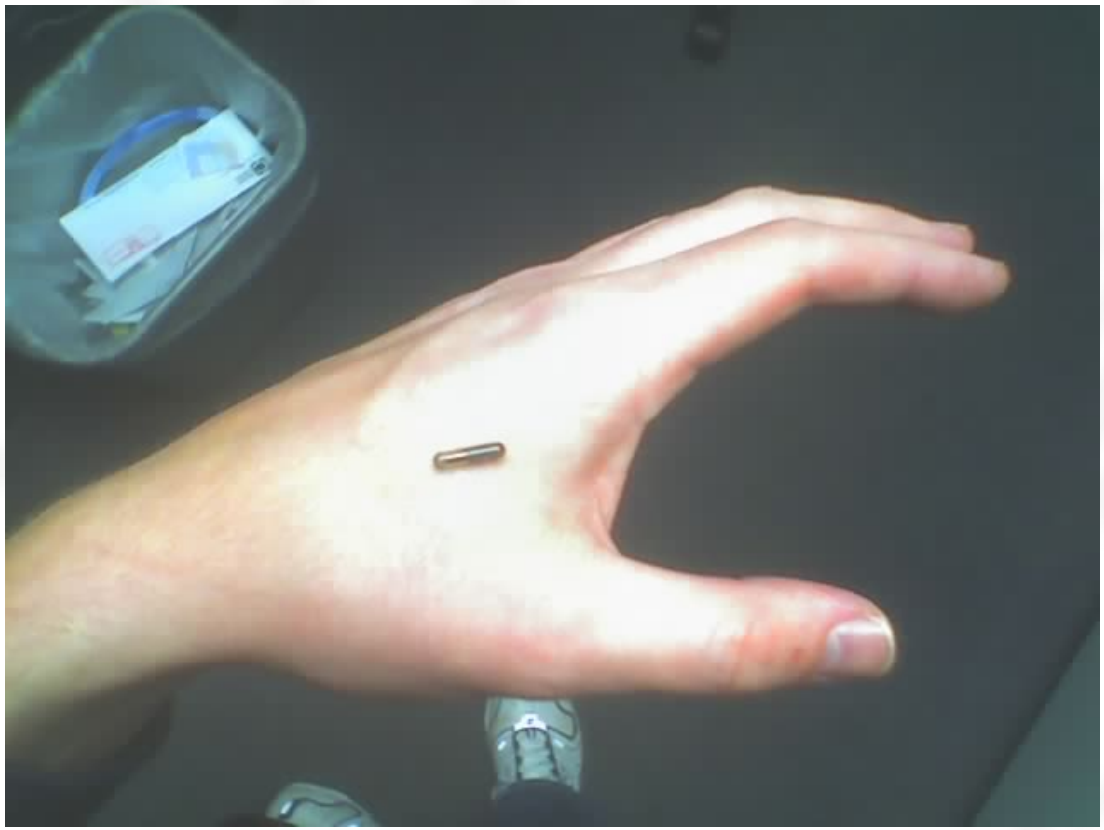

Abbildung: RFID-Tags zur Implantion unter die Haut (`http://amal.net/rfid.html`)

Transponder

Abbildung: RFID-Tags zur Implantion unter die Haut (`http://amal.net/rfid.html`)

Transponder

Abbildung: RFID-Tags zur Implantion unter die Haut (`http://amal.net/rfid.html`)

Wo finden wir RFID-Chips?

- Tickets (WM)
- Zugangskontrollsysteme
- Bezahlsysteme/Micro-Payment (Mensa)
- Ersatz des Autoschlüssels
- Ausweise (neuer Reisepass, bald Personalausweis?)
- Tagging von Konsumgütern (Ersatz des Barcodes)

Probleme?

- Datenschutzbedenken
  - Tracking von Personen ohne Kontrollmöglichkeit
  - Unbemerktes Auslesen von gespeicherten Daten
  - Nicht immer klar welche Daten gespeichert werden
- meist schwache Verschlüsselung
  - Security by Obscurity
  - Eigenschaften machen starke Verschlüsselung sehr schwer
- Gerade in den Nachrichten: RFID-Chips können medizinische Geräte lahmlegen oder stören

OpenPCD/OpenPICC

- freie Hardware und Software 13,56 MHz Lesegerät- und Transpondersimulatoren
- Beteiligte: Milosch Meriac, Harald Welte
- `http://www.openpcd.org/`

Abbildung: OpenPCD

Sputnik

- Besuchertracking auf 23C3, CCCamp, 24C3
- aktiver Tag auf dem 2.4GHz ISM Band

Abbildung: Sputnik-Tag

MiFare Classic

- am meisten eingesetzte RFID-Lösung in der Welt für Authentifizierung und Micro-Payment
- Beteiligte: Karsten Nohl, Henryk Plötz, starbug
- Vorstellung auf dem 24C3
- Benutzte Hardware: OpenPCD
- durch Analyse der Schaltkreise: Crypto-Algorithmus
- Algorithmus trival:
  - 16-bit RNG auf Basis der Zugriffszeit
  - strukturelle Schwächen
  - dadurch kein Brute-Force nötig!
- Cracking mit $100 Device in einer Woche

MiFare Plus

- angekündigter Nachfolger der Classic (Q4/2008)
- mittlerweile: Cracking von Crypto-1 (Classic) in 200 Sekunden nach Abhören von 50 Bit unabhängig von RNG
- Plus mit 2 Cryptoverfahren zur Auswahl
  - „verbessertes“ Crypto-1: crackbar
  - 128-bit AES: sicher

Für weitere Informationen

- Chaosradio 135: Kundenkarten, Chips und Bankkarten - Kartenspiel im Portemonnaie (`http://chaosradio.ccc.de/cr135.html`)
- Vorträge vom 22C3 und 23C3
  - EU RFID Policy: `http://events.ccc.de/congress/2007/Fahrplan/events/2396.en.html`
  - Sputnik Analyse: `http://events.ccc.de/congress/2007/Fahrplan/events/2270.en.html`

Fahrplan

TPM?

- Trusted Platform Module
- entwickelt von der Trusted Computing Group (TCG)
- Spezifikation eines Cryptoprozessors, der kryptographische Schlüssel generieren und speichern kann
- Remote Attestation: Generierung eines eindeutigen Hashes von Hard- und Software (Signatur)
- Sealing: Verschlüsselung mit Passwort
- Binding: Verschlüsselung mit chipeigenem, eindeutigem RSA Schlüssel

Einsatz von TPM

- Verifikation der Konfiguration bzw. Identiät von Systemen
- Verschlüsseln von Festplatten/Partitionen
- DRM (Digital Rights/Restriction Management)
- Erzwingen einer Softwarelizenz
- Trusted Computing

Trusted Computing (TC)

- eigentlich: Treacherous Computing (geprägt von RMS)
- Sichere Ein- und Ausgabe (Trusted Path)
- Abgesichere Speicherregionen, Programmausführung in sicherem Speicher
- Erweiterung von TPM (Remote Attestation, Binding)

Anwendung von Trusted Computing

- Verhindern von Cheating bei Onlinespielen
- Schutz vor Viren und Malware
- Schutz von wichtigen Daten, z.B. biometrische Daten zur Anmeldung an PCs
- Grid Computing (Authentifizierung, Verifizierung)

Unterstützung

- seit 2004 werden TPM-Chips von allen grossen Herstellern in PCs verbaut, manuelle Aktivierung im BIOS
- Linux Kernel seit 2.6.13 Support für TPM-Module, freier TC-Software-Stack TrouSerS
- limitierte Unterstützung in Windows mit Software von Drittanbietern
  - Plan von Microsoft: Next Generation Secure Computing Base (NGCSB), früher Palladium

Probleme von TPM/TC

- starke Opposition von Sicherheitsexperten und EFF/FSF
- Spezifikationen sind frei, aber nicht die Implemtierung dieser in kommerziellen Produkten (Firmen machen Fehler!)
- Unternehmen bzw. TCG hat die Kontrolle was und wer vertrauenswürding ist
  - Zensur
  - Softwarewahl eingeschränkt
  - keine Modifikation von Software möglich
- TCG hat einen „user override“ abgelehnt

Probleme von TPM/TC

- DRM (Digital Rights/Restriction Management)
- Verlust von Anonymität (Zwangsregistrierung von PCs), jedoch DAA (direct anonymous attestation) möglich
- Praktikabilität: Ausfall des TPM-Chips fatal (interner Schlüssel kann verloren werden)
- Interoperabilität (zur Zeit etwa bei Software-Stacks)

Fahrplan

Vielen Dank für die Aufmerksamkeit!

Folien vermutlich morgen unter `http://franz-pletz.org/` herunterladbar! ;-)