Bewertung des Sicherheitsniveaus einiger Mechanismen zur Vertraulichkeit, Verfügbarkeit und Pseudonymität von Transpondern (RFID)

Erlangen 4. Juli 2006

Hartmut Pohl und Norbert Jung, Fachhochschule Bonn-Rhein-Sieg,
Torsten Roth, Evidian GmbH Köln

Sachziele der Informationssicherheit

- **Vertraulichkeit** – **confidentiality**
  Eigenschaft eines Systems, nur berechtigten Subjekten den Zugriff
  auf bestimmte Objekte zu gestatten und unberechtigten Subjekten
  den Zugriff auf alle Objekte zu verwehren. [Auch: Kennzeichnung des Schutzniveaus.]

- **Integrität** – **integrity**
  Eigenschaft eines Systems, die Korrektheit der Objekte sicherzustellen:
  Die Daten sind auf dem aktuellen Stand.
  Objekte sind gg. unberechtigte Modifikation (und/oder Zerstörung) geschützt.

- **Verfügbarkeit** – **availability**
  Wahrscheinlichkeit, ein System zu einem vorgegebenen Zeitpunkt,
  in einem funktionsfähigen Zustand anzutreffen [DIN 40042].

- **Verbindlichkeit** – **liability**
  Eigenschaft eines Systems, authentische, rechtsverbindliche Kommunikation zu unterstützen –
  syn.: Zurechenbarkeit. Geschützt gegen Täuschung, Abstreiten (non-repudiation).

- **Pseudonymität** – **pseudonymity**
  Zuordnung zu einem Identifikator (ID, Aliasname) möglich.

Berücksichtigte Sachziele

- **Vertraulichkeit** – **confidentiality**
  Eigenschaft eines Systems, nur berechtigten Subjekten den Zugriff auf bestimmte Objekte zu gestatten und unberechtigten Subjekten den Zugriff auf alle Objekte zu verwehren. [Auch: Kennzeichnung des Schutzniveaus.]

- ...

- **Verfügbarkeit** – **availability**
  Wahrscheinlichkeit, ein System zu einem vorgegebenen Zeitpunkt, in einem funktionsfähigen Zustand anzutreffen [DIN 40042].

- ...

- **Pseudonymität** – **pseudonymity**
  Zuordnung zu einem Identifikator (ID, Aliasname) möglich.

Eigenschaften der Komponenten (ATMEL)

Reader U2270B

125 kHz, 2/5 kBaud

Antenne

Parallel-Resonanz-Kondensator >= 2 nF
Antennenkreis L = 735 uH (Ferrospule), C = 2,2 nF

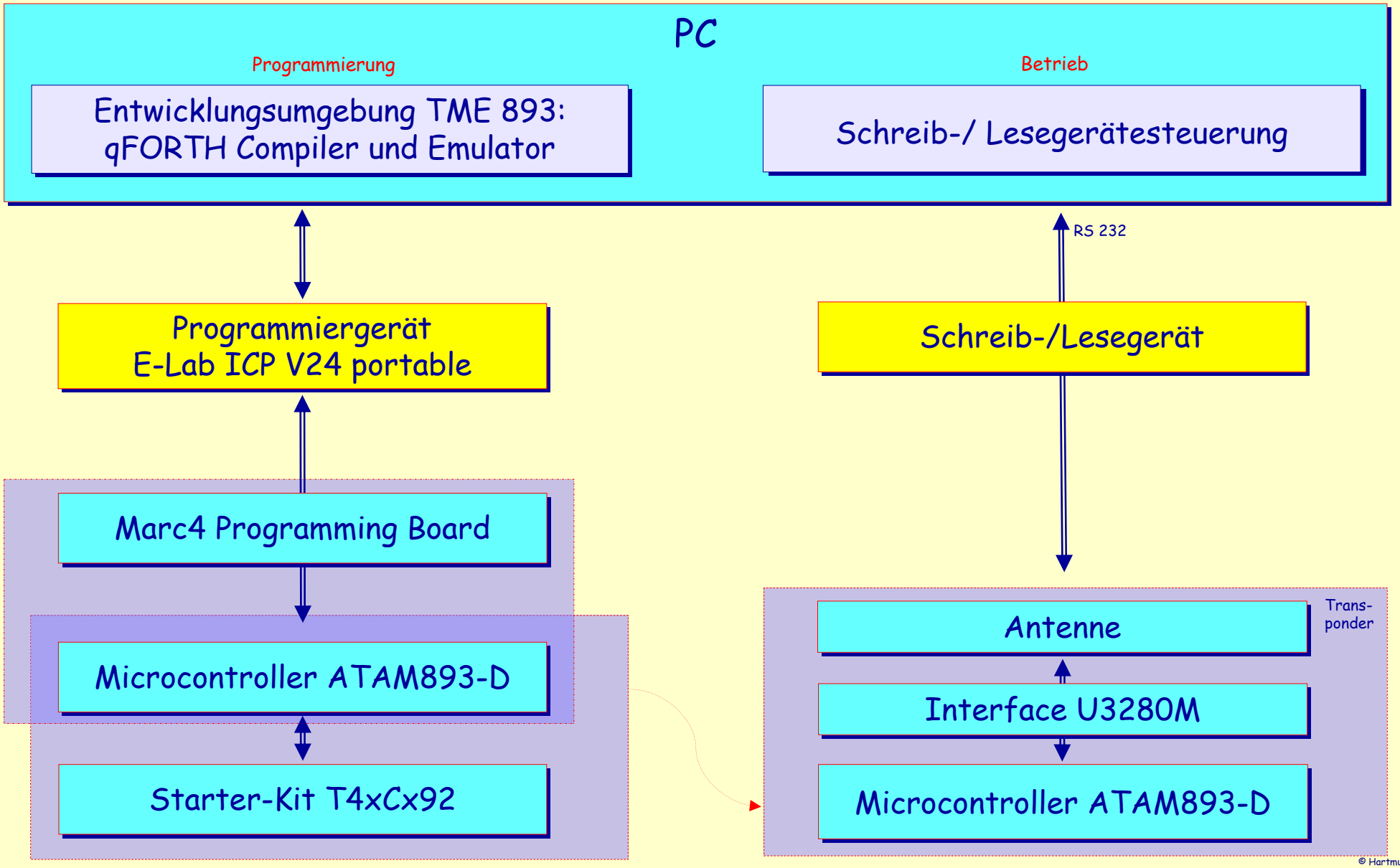
Transponder-Interface U3280M

Sende-/Empfangsfrequenz 125 KHz
32 x 16 Bit EEPROM

Mikrokontroller ATAM893-D

CPU-Typ M48C893B – 250 KHz getaktet
4 K Byte EEPROM Program Memory
256 x 4 Bit RAM Data Memory

Mechanismen-Implementierung



Vorgehensplan Mechanismen-Implementierung

1. Dokumentation des gesamten Verfahrens
2. Algorithmus auswählen
3. Algorithmus in qForth implementieren
4. Auf dem PC übersetzen (Entwicklungsumgebung)
5. Im Programmiergerät speichern
6. Auf Microcontroller speichern
7. Microcontroller mit Interface und Antenne verbinden
8. Lesegerät einrichten (U2270B), Treiber für PC, Antenne
9. Transponder vom PC/Lesegerät auslesen und nutzen
10. Dokumentation, Prüfung der Ergebnisse

Angriffe

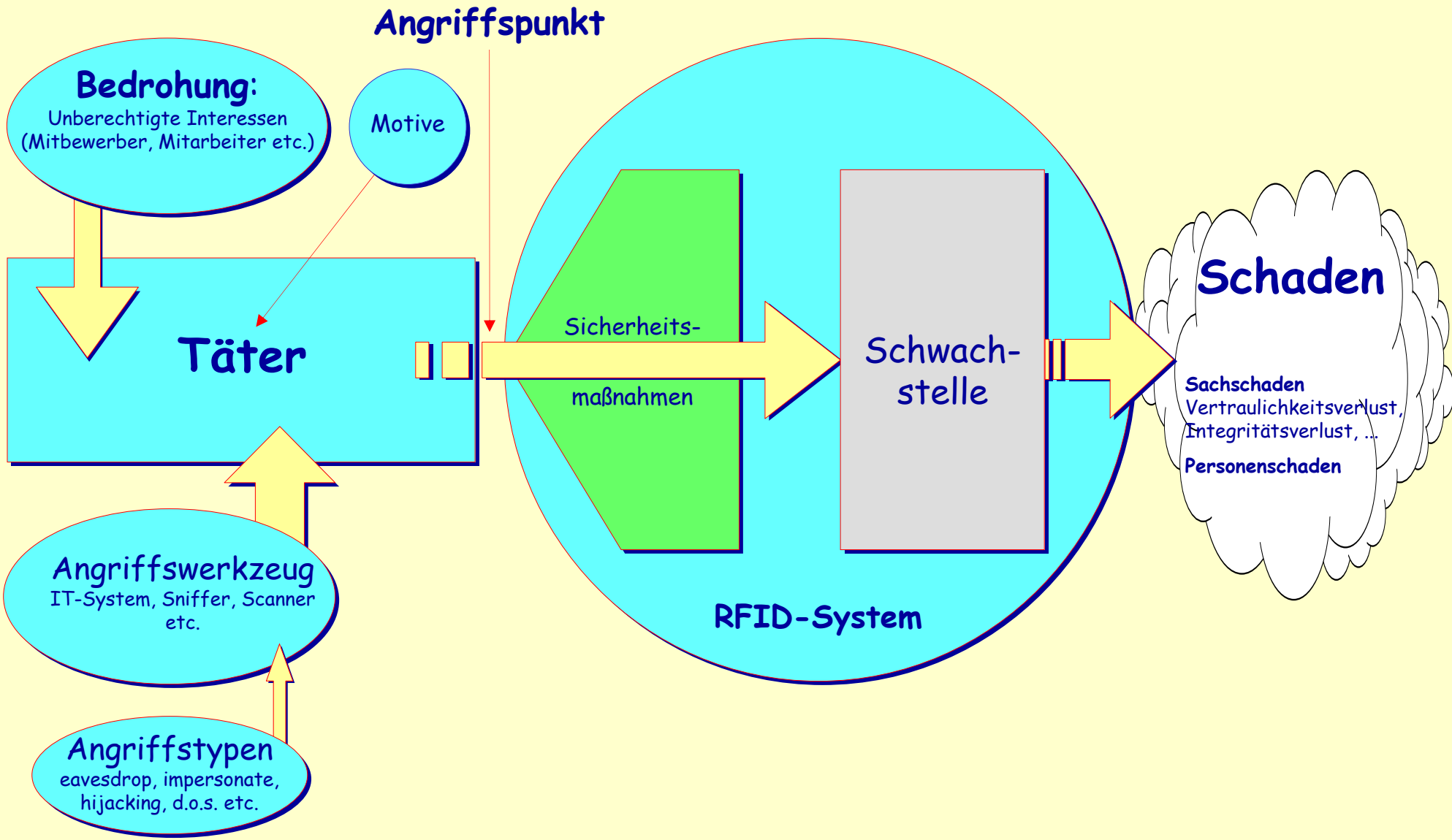
- Eavesdropping
- Traffic Analysis
- Spoofing
- Denial of Service
- Session hijacking
- Replay Attacks
- Read/Write (delete)
- ...

Angriffsklassen

	Abhören	Schreiben/Verändern
Kommunikation	Spionage	Sabotage
Gespeicherte Daten	Spionage	Sabotage

Nutzdaten und Steuerdaten

Generisches Angriffsmodell



Sachziel Verfügbarkeit

Transponder in der Medizin

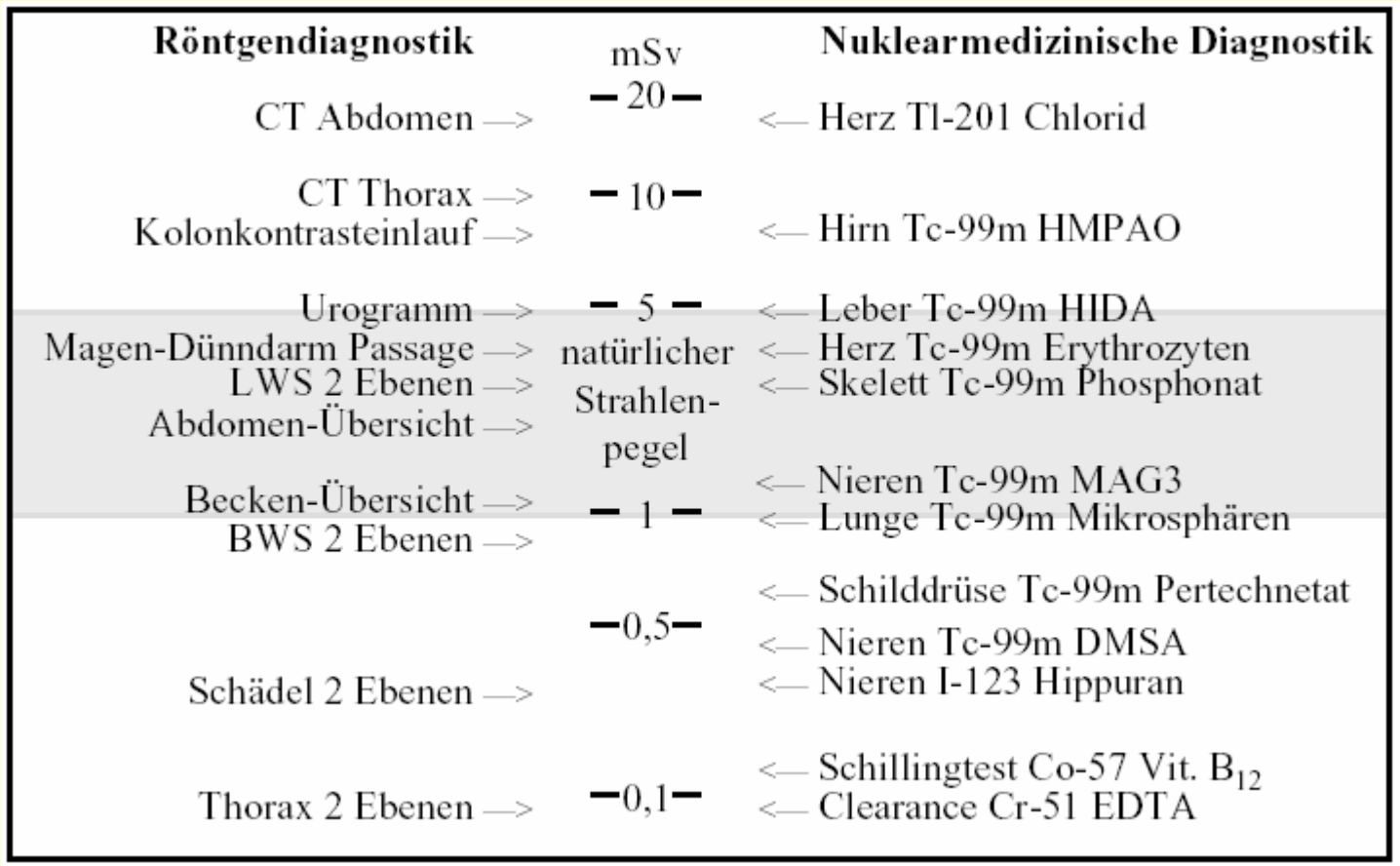
- Kontaklose Kommunikation der Patientenkarte (?)
- Identifizierung/Authentifizierung im Krankenhaus

Ionisierende Strahlung

- Relevante Veränderungen gespeicherter Daten
  bei extrem hohen Energiedosen:
  Dosisäquivalent im Bereich kSv (1000 Sievert)

- Dosisäquivalente im medizinischen Umfeld bei etwa 10 mSv
  - häufige Untersuchungen, Akkumulation:
  Gespeicherte Daten, bleibende Schäden am Chip

Radiation Dose



Eingesetzte Dosiswerte

Bestrahlungs-versuch	Grundwert in mSv	Anzahl	Dosisäquivalent in mSv
1	1	1	**1**
2	1	3	**3**
3	5	1	**5**
4	5	3	**15**
5	10	1	**10**
6	10	3	**30**

Ergebnis experimenteller Untersuchung

- Arbeitsweise: Fehlerfrei
- Gespeicherte Daten Fehlerfrei

  auch nach wiederholten Bestrahlungen

⇨ Unbeabsichtigte oder gezielte Manipulation
durch Röntgenstrahlung kann ausgeschlossen werden

Sachziel Vertraulichkeit

Maßnahmen zum Datenschutz (Vertraulichkeit)

- **Faradayscher Käfig**
  Abschirmung elektromagnetischer Felder durch leitfähige Hülle.

- **Jammer**
  Störsender.

- **Blocker**
  Antwort auf jede Anfrage eines Schreib-/Lesegeräts mit dem Ziel von Kollisionen.
  Verhinderung der Kommunikation mit anderen Transpondern in der Umgebung.

- **Kill Befehl**
  Nach Ausführung keine Reaktion auf weitere (auch andere) Befehle:
  Transponder ist nicht mehr verfügbar. Reaktivierung nicht ausgeschlossen.

- **Zugriffskontrolle**
  Rechteverwaltung, Überprüfung/Autorisierung und Protokollierung/Auswertung.

Mechanismen zur Vertraulichkeit

- Back-Office Verschlüsselung – Steuerbefehle (log-in)
- Verschlüsselung der Kommunikation: Symmetrisch/asymmetrisch
- Silent Tree Walking - Verschlüsseltes ID-Auslesen (bei Kollisionen)
- Pseudonymisierung der ID: Meta-IDs, …
- Zugriffskontrolle mit Passwörtern

Simulation von Brute-Force-Angriffen

- Transponder Hitag2: 4 Bytes Passwort
- Antwortzeit 52 ms (vergleichsweise kurz)
- Etwa 19,2 Logins pro Sekunde

---

1. Lexikonattacke
2. Angriff mit allen Zeichen eines eingeschränkten Alphabets
3. Angriff mit allen Zeichen des vollständigen Alphabets

Brute Force Attack

Test	Zeitaufwand	Zeiteinheit
Wörterbuch Attacke	25,4	Minuten
Großbuchstaben	8,5	Stunden
Alle Buchstaben	5,6	Tage
Alle Buchstaben und Zahlen	11,4	Tage
Alle Zeichen eines Alphabets	9,1	Jahre

Aber: Abhören der Luftschnittstelle

Passwortverfahren

- Geringe Anforderungen an tags: Einfache read-only-tags

- Billige tags wählen ⇨ Antwortzeit dann groß

Aber: Implementierung nur einfacher Verschlüsselungsverfahren möglich.

Sachziel Pseudonymität

Randomized Hash Lock

- **Hash Lock**
  Tag sendet Meta-ID := f(ID)
  Lesegerät sucht in einer Backend-Datenbank die Meta-ID gehörende ID und überträgt zum tag

- **Randomized Hash Lock**
  Dynamischen Generierung einer neuen Meta-ID bei jedem Auslesevorgang
  Dazu hashen der ID des tags zus. mit Zufallszahl
  Tag sendet Zufallszahl mit Hash-Wert an Lesegerät
  Zur Berechnung der wahren ID des Tags generiert das Lesegerät die Hash-Werte der übertragenen Zufallszahl mit allen gespeicherten IDs, bis ein übereinstimmender Hash-Wert gefunden ist

Randomized Hash Lock

- Rechenzeit-aufwändig bei sehr großer Anzahl von tags
- Geringe Implementierungskosten: Hashfunktion, RNG

Chained Hashes

tag: Zweimaliges hashen der aktuellen Meta-ID

Lesegerät: Hash gespeicherter IDs bis zur Übereinstimmung

Vorteil: Unempfindlichkeit gegenüber wiederholtem Ausspähen übertragener Meta-ID

Randomized Hash-Lock: Berechnug der Meta-ID

Anzahl ID	Zeit in ms
500	1
750	2
1000	8
1500	23
2000	32
3000	57

- Erfassungsgeschwindigkeit von 35 Transpondern/Sekunde: ID-Berechnung in max. 28 ms
- Abhängig von Lesegerät und Back-office-System: AMD Athlon XP 2000+ CPU, 512 MB RAM (266 MHz)
- Rechenzeitaufwand steigt linear mit der Anzahl erfolgter Request-Befehle

Resumee

- **Verfügbarkeit**
  Im medizinischen Bereich eingesetzte Strahlungsquellen schädigen nicht

- **Vertraulichkeit**
  Passworte besitzen einen sehr hohen Widerstandswert
  Vor: Transponder mit einfachen Prozessoren und langen Antwortzeiten
  - ggf. mit Timer verlängern

- **Pseudonymität**
  Auf Hash-Funktionen basierende Meta-ID-Verfahren können sehr viele IDs bearbeiten und erscheinen daher nutzbar

Weitere Arbeiten

- **Authentifizierung**
  Implementierung einer lightweight PKI

- **Fälschungsschutz**
  Überlange Passworte
  Geschützte Speicherbereiche

Prof. Dr. Hartmut Pohl

Informationssicherheit – Fachhochschule Bonn-Rhein-Sieg - ISIS – InStitut für InformationsSicherheit

- **Management Consulting**: Absicherung von Intranets und Extranets, Mobilkommunikation in großen und mittleren Unternehmen: Chemie, Pharma, Energieversorger, Kommunikation, Sicherheitsbehörden
- **Coaching** von Sicherheitsbeauftragten und Beratern. **Projektmanagement**
- **Begutachtung** von Sicherheitsprojekten – Bewertung und Auswahl von Produkten
- **Sicherheitsstrategien** und Richtlinien, Sicherheits-Benchmarking, Risk-Management, Implementierung von Standards: ISO 27000 Familie, Grundschutzhandbuch. Securing Outsourcing, Outsourcing Security - Managed Security, Trust Infrastructures (PKI)
- **Fälschungschutz** von und mit Transpondern (RFID), cloning

Max-Pechstein-Str. 4 - 50858 Köln
Tel.: 0221 - 4847 - 553. Fax.: - 529
Hartmut.Pohl@sang.net
http://www.inf.fh-bonn-rhein-sieg.de/Pohl.html