Die Sicherheitsarchitektur des digitalen Tachographen

Arbeitsgruppe 4 <Applied Cryptography & Security Engineering>

29.09.2009

Furgl / Lemke - A Review of the Digital Tachograph

Lieberknecht – Seitenkanalresistente symmetrische Verschlüsselung für digitale Tachographen

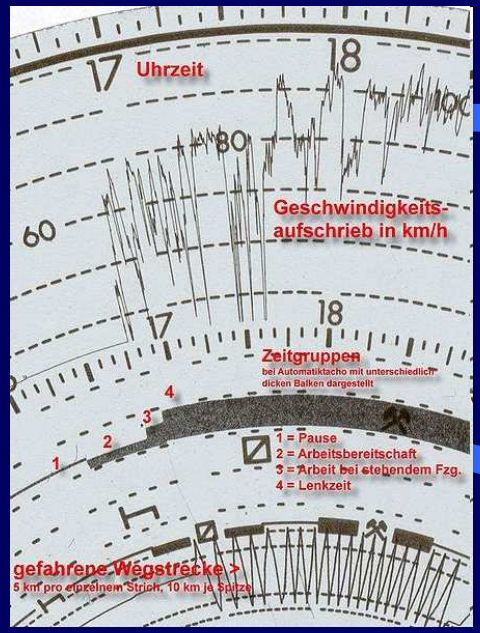
Gliederung

1. Einführung
2. Überblick Architektur
3. Sicherheitsmerkmale - Beispiele
4. PKI (Public Key Infrastruktur) und Protokollübersicht
5. Kommunikation zwischen Fahrzeugeinheit und Tachographkarten
6. Kommunikation zwischen Sensor und Fahrzeugeinheit
7. Stärken / Schwachstellen der Sicherheitsarchitektur
8. Zusammenfassung / Ausblick

1. Einführung

Hintergrund

Ersetzt analogen Tachograph für neue LKWs und Busse (nach europäischer Verordnung) ab 2006



Funktionen:
Aufzeichnung und Speicherung von Wegstrecke, Geschwindigkeit und Fahrerdaten (Lenk- und Ruhezeiten)

Hohe Sicherheitsanforderungen an die Architektur

- Kryptographisch gesicherte Verbindungen vorgeschrieben (zwischen Sensor und VU sowie VU und Karten)
- Manipulationssicherheit / Seitenkanalresistenz

Manipulation des analogen Tachographen

Angriffe auf die Technik

- Impulsübertragung zwischen Impulseinheit (Getriebe) und Fahrzeugeinheit über ungesichertes Kabel
- Wegbegrenzung des Zeigers / Veränderung der Federspannung (invasiv)

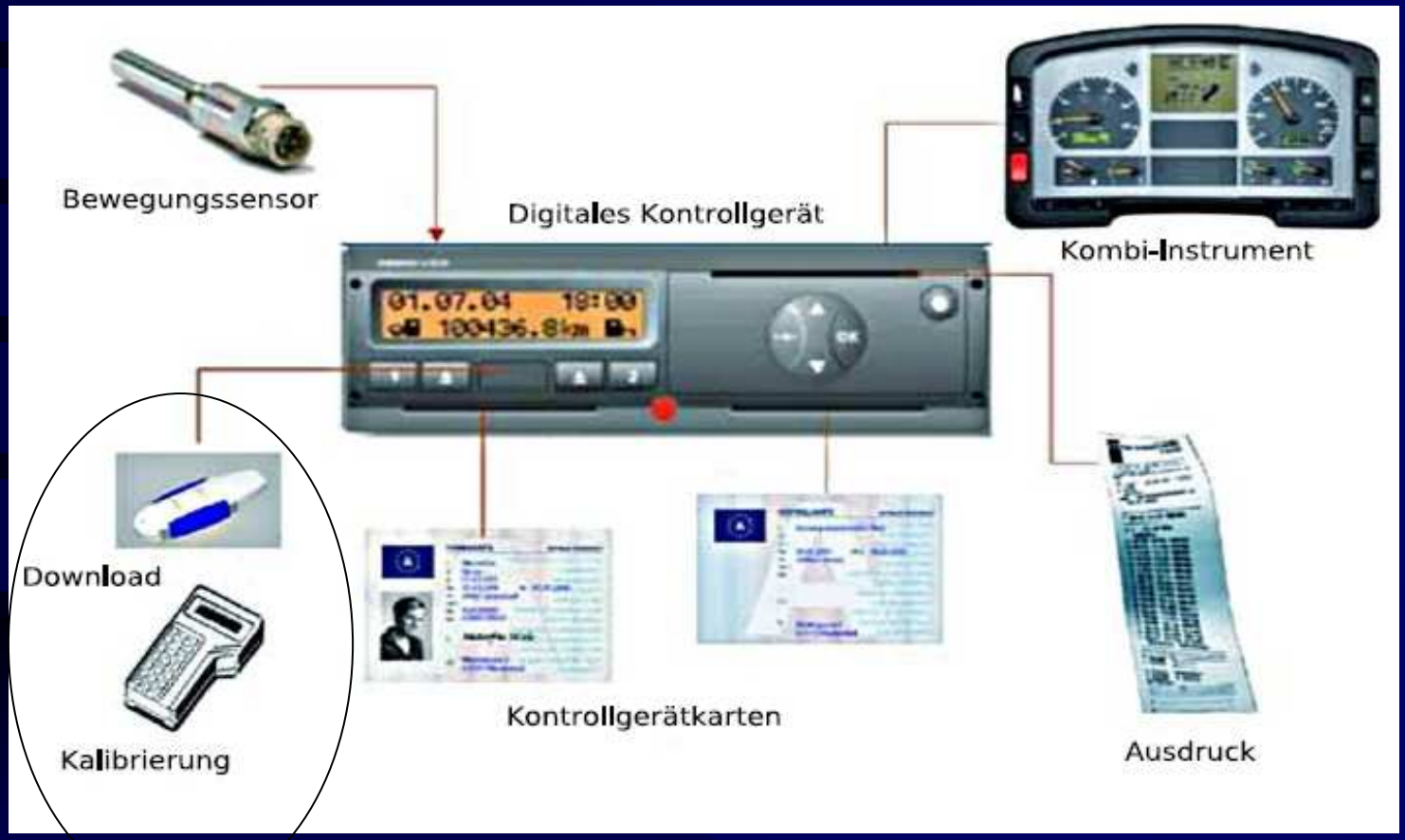
Prozedurale Angriffe

- Willkürliches „Vergessen“ und Tauschen von Tachoscheiben

PLACEHOLDER (ANDERSON ITALIAN DEV.)

2. Überblick Architektur des digitalen Tachographen

Architektur



Sicherheitsanforderungen

- Gespeicherte Schlüssel dürfen nicht ausgelesen werden können
- Daten in Fahrzeugeinheit und Karten dürfen nicht unautorisiert ausgelesen oder modifiziert werden können
- Kontrollgerätkarten bzw. Impulsgeber und Fahrzeugeinheit müssen sich gegenseitig authentifizieren
- Integrität und Authentizität aller übertragenen Daten muss sichergestellt werden
- Jegliche Sicherheitsverletzungen müssen in Audits abgespeichert werden

- *Sicherheitszertifizierung nach ITSEC E3 hoch oder Common Criteria EAL4+ vorgeschrieben*

3. Sicherheitsmerkmale - Beispiele

Verbindung Impulsgeber / Fahrzeugeinheit

- Korrekte Übertragung aller Impulse wird sichergestellt:

  2 Zähler jeweils in FE und Impulsgeber

  Impulsgeber übermittelt regelmäßig Zählerstand (verschlüsselt) an FE

  Bei **Übereinstimmung** ist von korrekter Übertragung auszugehen.

Dennoch sind Manipulationen am Impulsgeber weiterhin möglich (Hardwareänderungen und z.B. mechanische Einwirkungen), allerdings zu einem hohen Preis

Tachographkarten - Sicherheitsmechanismen

- Jede Karte hat eigene Schlüssel und Zertifikate (für die gegenseitige Authentifizierung)
- Je nach Typ werden verschiedene Datenzugriffsrechte erteilt
- Alle Karten werden von einer Behörde (in DE Kraftfahrtbundesamt) ausgestellt und in einem Zentralregister gespeichert
- Kartendaten können nur nach erfolgreicher Authentifizierung mit einer Fahrzeugeinheit verändert werden

-Karten/Fahrerdaten
-Fahrhistorie / Ereignisaudits

Kartentypen:

a) Fahrerkarte
b) Werkstattkarte
c) Kontrollkarte
d) Unternehmenskarte

Table 1. Data to be stored by the tachograph cards

Data to be stored	Card type			
	driver	workshop	control	company
Card identification and security data (initialisation data)				
application identification	x	x	x	x
chip identification	x	x	x	x
IC card identification	x	x	x	x
standard security elements	x	x	x	x
specific security elements	-	x	-	-
Card personalisation data				
card identification	x	x	x	x
card holder identification	x	x	x	x
driving licence information	x	-	-	-
Activity data				
vehicles used data	x	x	-	-
driver activity data	x	x	-	-
daily work periods start and/or end	x	x	-	-
events and faults data	x	x	-	-
control activity data	x	x	x	-
company activity data	-	-	-	x
card session data	x	-	-	-
specific conditions data	x	x	-	-
calibration and time adjustment	-	x	-	-

Tachograph-karten

gespeicherte Daten

4. PKI (Public Key Infrastruktur) und Protokollübersicht

*The **Public Key Infrastructure** (**PKI**) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates.[1]*
[Wikipedia; PKI]

Anforderungen an das Keymanagement

a) asymmetrische Kryptographie für Kommunikation zwischen Fahrzeugeinheit und Tachographkarte ---> **systemweite PKI**

b) symmetrische Kryptographie für Kommunikation zwischen Fahrzeugeinheit und Tachographkarte (Secure Messaging) ---> Sitzungsschlüssel werden über Schlüsseleinigungsprotokolle mit Hilfe von a) etabliert

c) symmetrische Kryptographie für Kommunikation zwischen Fahrzeugeinheit und Motion Sensor (Pairing und Betrieb) ---> *splitting key technology*

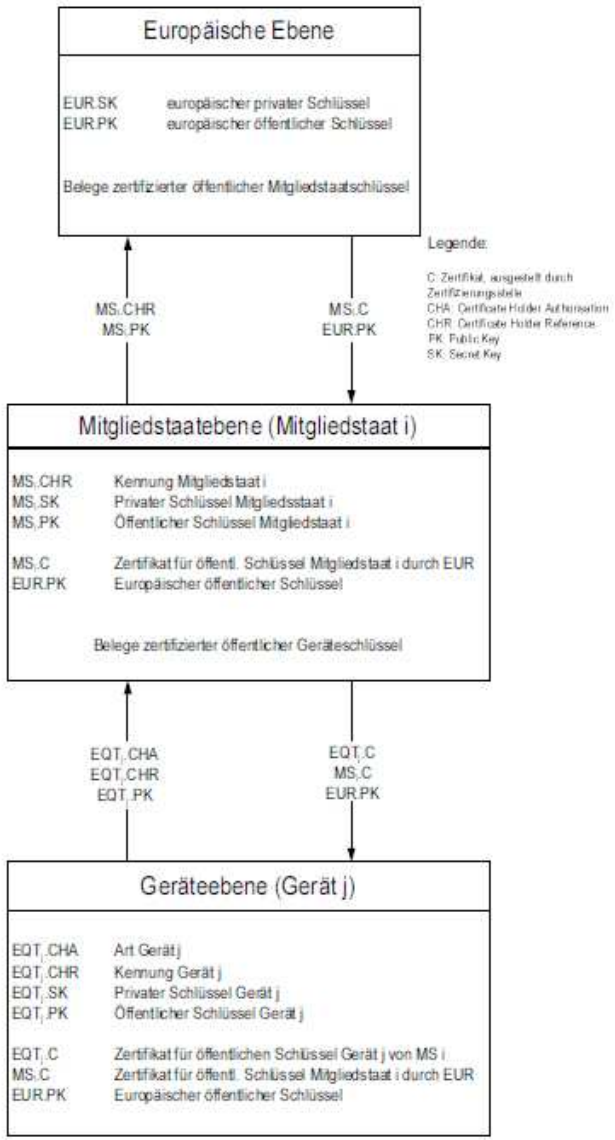


Abbildung 3.1: Hierarchie der Public-Key-Infrastruktur der digitalen Tachographen

PKI

Keylänge: RSA 1024 Bit

Europäisches Schlüsselpaar (SK zertifiziert Mitgliedsstaatsschlüssel)

Mitgliedsstaatschlüsselpaar (SK zertifiziert Geräteschlüssel)

Geräteschlüsselpaar

(Authentifizierung, dig. Signatur von Daten, Transport von Sitzungschlüsseln)

Übersicht der verwendeten Protokolle

Kommunikation zwischen Bewegungssensor und Fahrzeugeinheit:
(DES) bzw. Two-Key Triple-DES

- Integritätsschutz (Verschlüsselung des Impulsprüfwertes)
- Pairing-Protokoll

Kommunikation zwischen Fahrzeugeinheit und Karten:
Two-Key Triple-DES

Secure Messaging nach ISO7816-4, d.h. Integritätsschutz und Vertraulichkeit durch CBC-Encryption mit Two-Key Triple-DES

RSA Signatur

RSA Signatur für signierten Download der Kartendaten

- Key Management Protokolle

5. Kommunikation zwischen Fahrzeugeinheit und Tachographkarten

Asym. Kryptografie - RSA

- Verwendung: gegenseitige Authentifizierung von VU und Tachographkarten, digitale Signatur von Daten zum Download, Transport von Session Keys zwischen VU und Tachographkarten

- Schlüssellängen:

  Public Key 64 Bit, Private Key 1024 Bit, n (Produkt zweier geheimer Primzahlen) 1024 bit

- Schlüsselmanagement:

  Standard Public-Key-Infrastruktur (PKI)

Operationsphasen

Gegenseitige Authentifizierung

- Zertifikate der Kommunikationspartner werden geprüft (mittels einem Challenge-Response Verfahren)
- Ein gemeinsamer symmetrischer Sitzungsschlüssel (für die nachfolgende Kommunikation) wird etabliert

Betrieb

Unverschlüsselte oder verschlüsselte Kommunikation je nach Bestimmungen in europäischen Gesetzen

6. Kommunikation zwischen Sensor und Fahrzeugeinheit

Symmetrische Kryptografie – Two Key Triple DES

- Verwendung:

  Vertraulichkeit der Kommunikation in Sessions (z.B. zwischen Fahrzeugeinheit und Karten)

- Schlüssellänge:

  2T DES (2x 56 Bit)

- Erzeugte Schlüssel: (sog. ‘Splitting Key Technology‘)

  k_{mwc}: 112 Bit;
  sicher an Hersteller übermittelt -> Werkstattkarte (wc)

  k_{mvu}: 112 Bit;
  sicher an Hersteller übermittelt -> Fahrzeugeinheit (vu)

Schlüsselverwaltung für Sensor-VU Kommunikation

Fahrzeugeinheit:

Teilschlüssel k_{mvu}

Werkstattkarten:

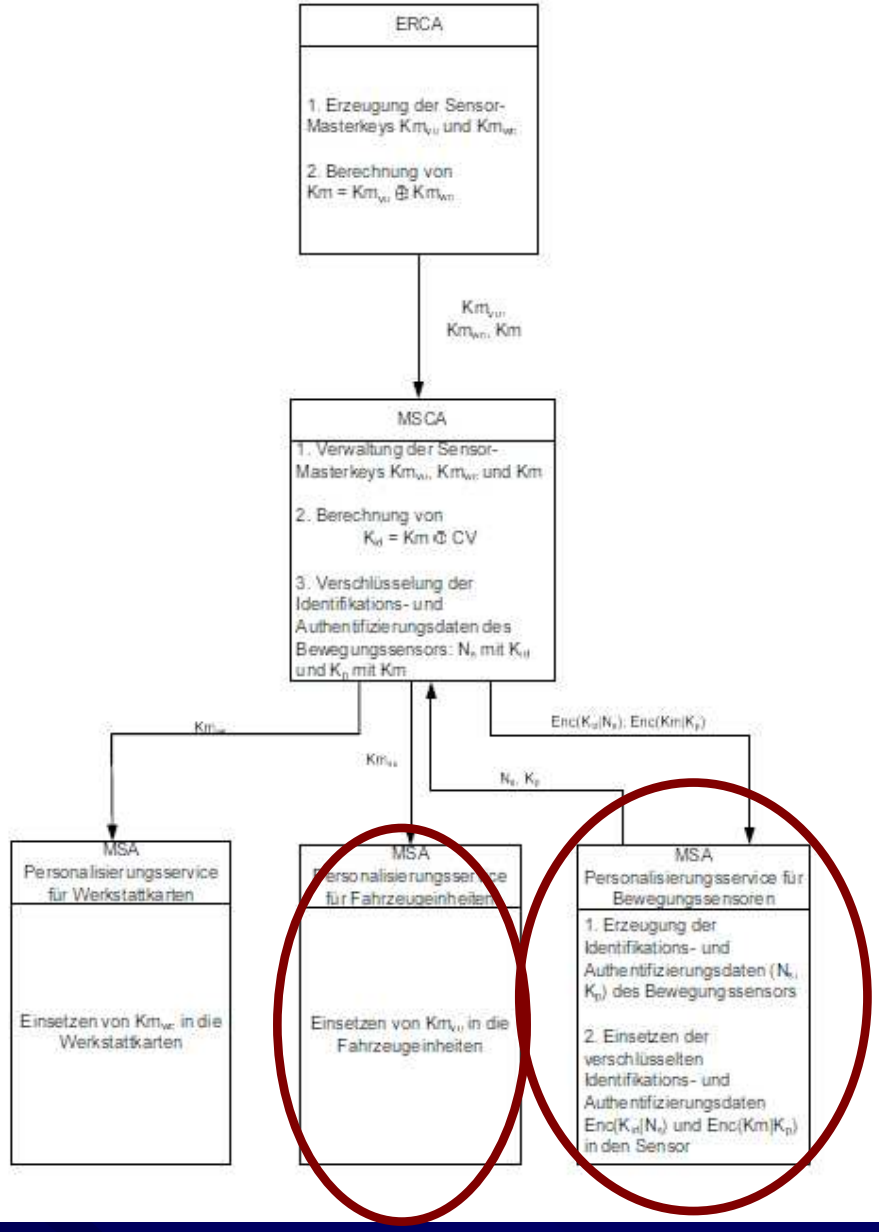
Teilschlüssel k_{mwc}

Sensor:

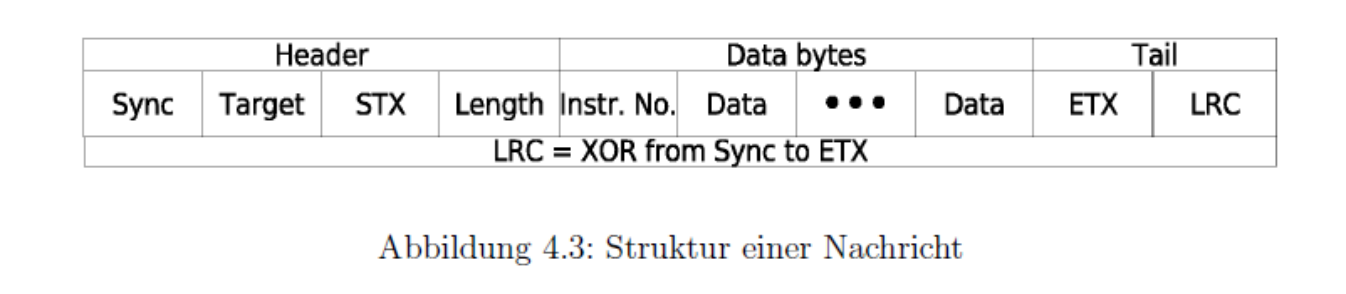
Erweiterte Seriennummer N_s

Pairingkey K_p

Enc



Kommunikationsprotokoll VU ⇔ MS



Header				Data bytes				Tail	
Sync	Target	STX	Length	Instr. No.	Data	•••	Data	ETX	LRC
LRC = XOR from Sync to ETX									

Abbildung 4.3: Struktur einer Nachricht

-seriell

-asynchron

- Fahrzeugeinheit ist aktiv, gibt Befehle an Sensor
- Korrekte Übertragung einer Instruktion wird sichergestellt, dann Ausführung der Instruktion

Unterscheidet zwischen Pairing- und Betriebsphase

Phase A: Pairing (1)

Ziel: gemeinsamer Two-Key 3DES Sitzungschlüssel

1. K_{mwc} von VU aus Werkstattkarte eingelesen / Generierung von Schlüsseln

$K_m = K_{mvu}$ XOR K_{mwc}

$K_{id} = K_m$ XOR CV

2. Challenge-Response Verfahren

a) Sensor sendet N_s an VU (Klartext)

b) VU verschlüsselt N_s mit K_{id} und schickt Chiffrat an Sensor

c) Sensor vergleicht „Response“ mit intern gespeicherten Chiffrat

Phase A: Pairing (2)

Ziel – gemeinsamer Two Key 3DES Sitzungschlüssel

3. Sensor sendet verschlüsselten Pairingkey K_p an VU
4. Fahrzeugeinheit generiert zufälligen Sitzungsschlüssel K_s und sendet diesen mit K_p verschlüsselt zurück an den Sensor

---

<u>Eigentliches Pairing:</u>

1. VU sendet mit K_p verschlüsselte Pairinginformation P_d an Sensor
2. Sensor entschlüsselt P_d und verschlüsselt mit Sitzungsschlüssel
3. VU vergleicht entschlüsseltes K_s-Chiffrat mit Klartext – Pairinginformation

Phase B: Betrieb

- Bewegungsimpulse werden unverschlüsselt zwischen Sensor und Fahrzeugeinheit übertragen
- Regelmäßig überträgt der Sensor seinen Zählerstand (vgl. Folie 2) verschlüsselt mit K_s sowie seine erweiterte Seriennummer N_s an die Fahrzeugeinheit
- Fahrzeugeinheit vergleicht Zählerstand sowie Seriennummer
- Austausch von Dateien erfolgt ebenfalls verschlüsselt mit K_s

7. Stärken / Schwachstellen der Sicherheitsarchitektur

Stärken der Architektur

- Architektur komplett offengelegt, standardisiert
- Sicherheitsmechanismen / Implementierung mit ITSEC3 Hoch evaluiert
- (Two-Key 3DES zum jetzigen Zeitpunkt als sicher anzusehen)

Prozedurale Schwächen

- Lange Einführungsphase
- Keine gemeinsamen europäischen Richtlinien für die Auslieferung der Systemkomponenten
- Keine genauen Richtlinien für den Austausch der Komponenten (Fahrzeugeinheit und Tachographkarten zwischen Designer, Hersteller, MSA etc.
- Austausch des europäischen Schlüsselpaars nicht spezifiziert (-> logistische Probleme)
- Regelmäßige Kontrolle der Daten durch Behörden kann nicht in allen Ländern garantiert werden

Schwächen der Architektur 1

- Bewegungssensor – Fahrzeugeinheit Protokolle sind nicht auf Höhe der Zeit (-> elliptische Kurven etc.)
- RSA-Schlüssellänge (1024 Bit nicht zukunftssicher)

Table 2. RSA, Length of modulus

		period		
		till end of 2007	till end of 2008	till end of 2009
length of modulus	at least	1024	1280	1536
	recommended	2048	2048	2048

- Schwachstellen im sym. Keymanagement
  - Masterkeys sind zwei Jahre gültig (was passiert, wenn sie kompromittiert sind?)

Schwächen der Architektur / Faktor Mensch

- Sicherheit des Systems hängt von den potentiell nicht vertrauenswürdigen Eingangsdaten des Bewegungssensors ab
- Speicherplatz auf Smart Card zu gering, um noch detaillierte Sitzungsinformationen, Alarmevents zu speichern

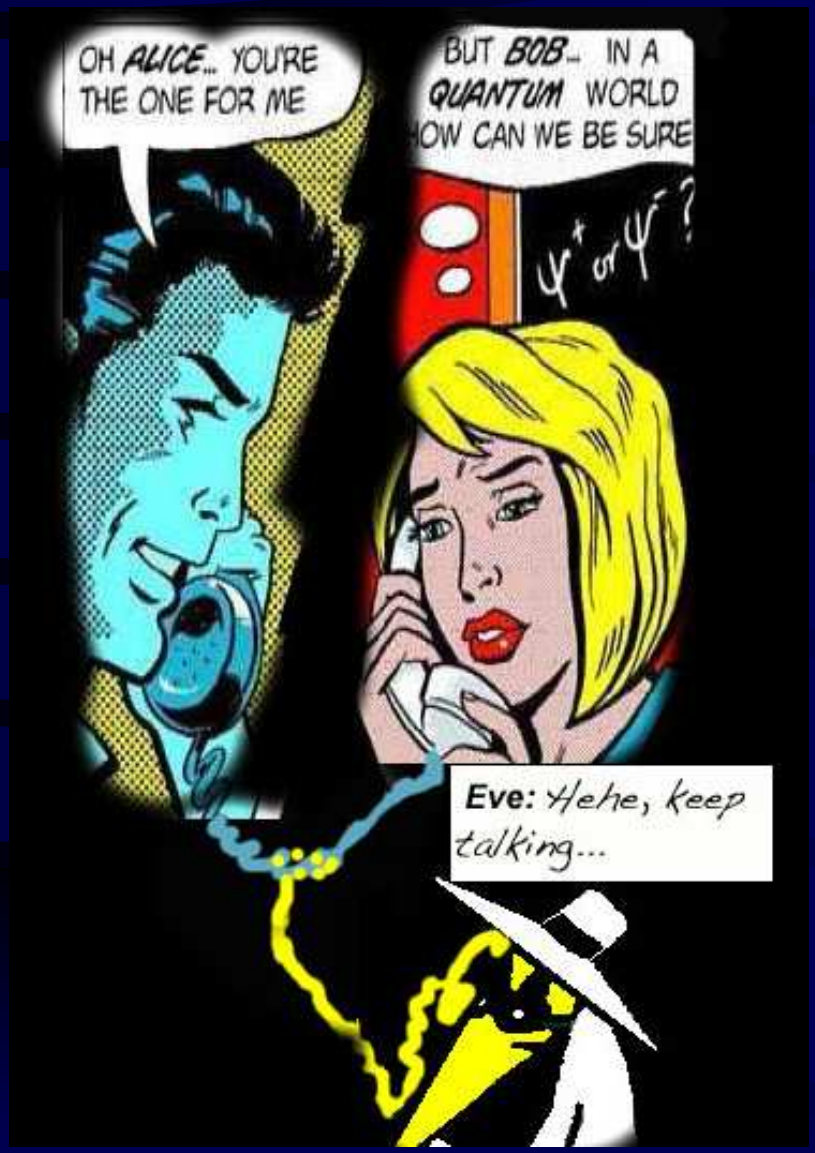
---

- Werkstattarbeiter müssen zwingend vertrauenswürdig sein (Installation, Kalibrierung)
- Fahrer als interner Angreifer; vielerlei Anreize das System zu umgehen (möglich: mehrere Karten, Kartenzerstörung)

8. Zusammenfassung / Ausblick

Ausblick

- Schritt vom analogen zum digitalen Tachograph ist als Fortschritt anzusehen, da die Manipulation deutlich erschwert wird (wg. fester kryptographische Bindung zwischen Komponenten)
- Weiterhin sind zahlreiche prozedurale - 70 % aller – Angriffe möglich


OH ALICE... YOU'RE THE ONE FOR ME
BUT BOB... IN A QUANTUM WORLD OW CAN WE BE SURE
Eve: Hehe, keep talking...

Vielen Dank!

Quellen

- Nora Lieberknecht. Seitenkanalresistente symmetrische Verschlüsselung für digitale Tachographen. Diplomarbeit, Universität Karlsruhe, 2007.
- I. Furgl and K. Lemke. A review of the digital tachograph system. In K. Lemke, C. Paar, and M. Wolf, editors, *Embedded Security in Cars*, pages 69–94. Springer, 2006.
- Ross Anderson. Security Engineering (Cambridge University Press)