maintech GmbH

Angreifbare Mobilität

Wie „online“ ist ein modernes Auto?

Kommen die Security-Erfahrungen aus dem Internet-Zeitalter demnächst auch ans Lenkrad?

Christian Daniel

Angreifbare Mobilität
Gliederung

maintech GmbH

Funkschlüssel

Reifendruck-Sensoren

GPS

RDS/TMC

Bluetooth Freisprechen

Internet

Funkschlüssel

Funkschlüssel

maintech GmbH

Funkschlüssel

- Schlüssel sind heutzutage plattgeklopfte Nägel – mechanisch uninteressant
- Die meisten Schlüssel arbeiten über Funk (433MHz, 868MHz)
- Ältere System haben Infrarot-Licht verwendet (wie TV-Fernbedienung)

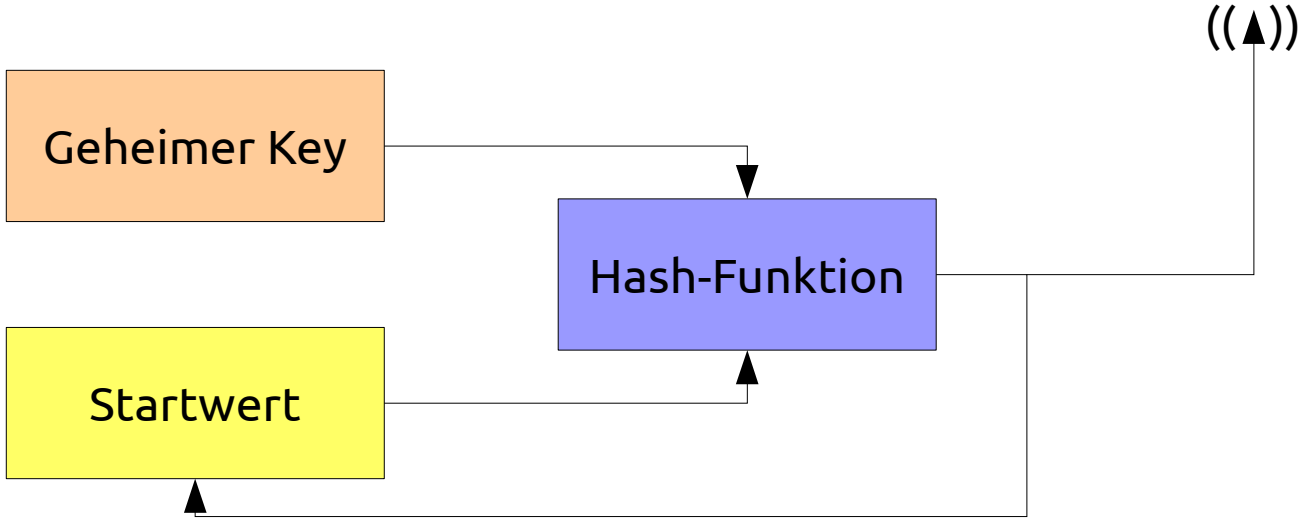
Funkschlüssel

Sicherheit: Rolling Code

Der Schlüssel berechnet aus einem Startwert und einem geheimen Key einen Hash, der gesendet wird

Der gesendete Hash wird danach zum neuen Startwert

Das Fahrzeug berechnet sich bei jedem empfangenen und korrekten Hash die nächsten fünf korrekten



Funkschlüssel

Problem: Synchronisierung

Werden mehrere Hashs nicht empfangen, muß das Auto mechanisch geöffnet werden

Im Zündschloss wird der Schlüssel geladen (Induktion) und resynchronisiert

Test: Außerhalb der Reichweite ein paarmal eine Taste drücken und dann prüfen, ob das Auto den Schlüssel noch über Funk akzeptiert

maintech GmbH

Problem: Sicherheit bei Keeloq

Keeloq ist ein Verfahren mit proprietären Algorithmen

Verfahren im März 2008 durch die Ruhr-Uni-Bochum geknackt:

Zwei Hashs müssen mitgesnifft werden, um den geheimen Schlüssel zu berechnen – danach kann der Schlüssel geklont werden

http://www.pm.ruhr-uni-bochum.de/pm2008/msg00087.htm

Angreifbare Mobilität
Reifendruck-Sensoren

maintech GmbH

Angreifbare Mobilität
Reifendruck-Sensoren

maintech GmbH

Reifendruck-Sensoren

- Technischer Name: „Tire Pressure Monitoring System“ - TPMS
- Im Autoreifen befinden sich Sensoren und Funkchips, die den Druck messen und ans Fahrzeug melden
- Hauptproblem der Technik: Energiemangel im Reifen
- Energie wird über eine kleine Unwucht aus der Rotation gewonnen und in einem Kondensator/Akku gesammelt
- Fahrzeug fragt Daten periodisch ab (Sensor wird mit 125kHz-Puls aktiviert, Antwort kommt auf 433MHz)
- Datenprotokoll ist unverschlüsselt und unsigniert

Reifendruck-Sensoren

maintech GmbH

Problem: Fremder Empfänger

Jeder Sensor hat eine eigene, eindeutige ID, die in jedem Paket mitgesendet wird

Reichweite ca. 40m

Empfänger in der Straße (z.B. Bodenwelle) können Autos eindeutig erkennen und so z.B. Bewegungsprofile erstellen

Erkennungsrate ist deutlich höher als bei Nummernschilderkennung per Kamera

Reifendruck-Sensoren

maintech GmbH

Problem:
Fremder Sender

Board-Elektronik übernimmt Meldungen direkt

Kaum Plausibilitätskontrollen in der Software

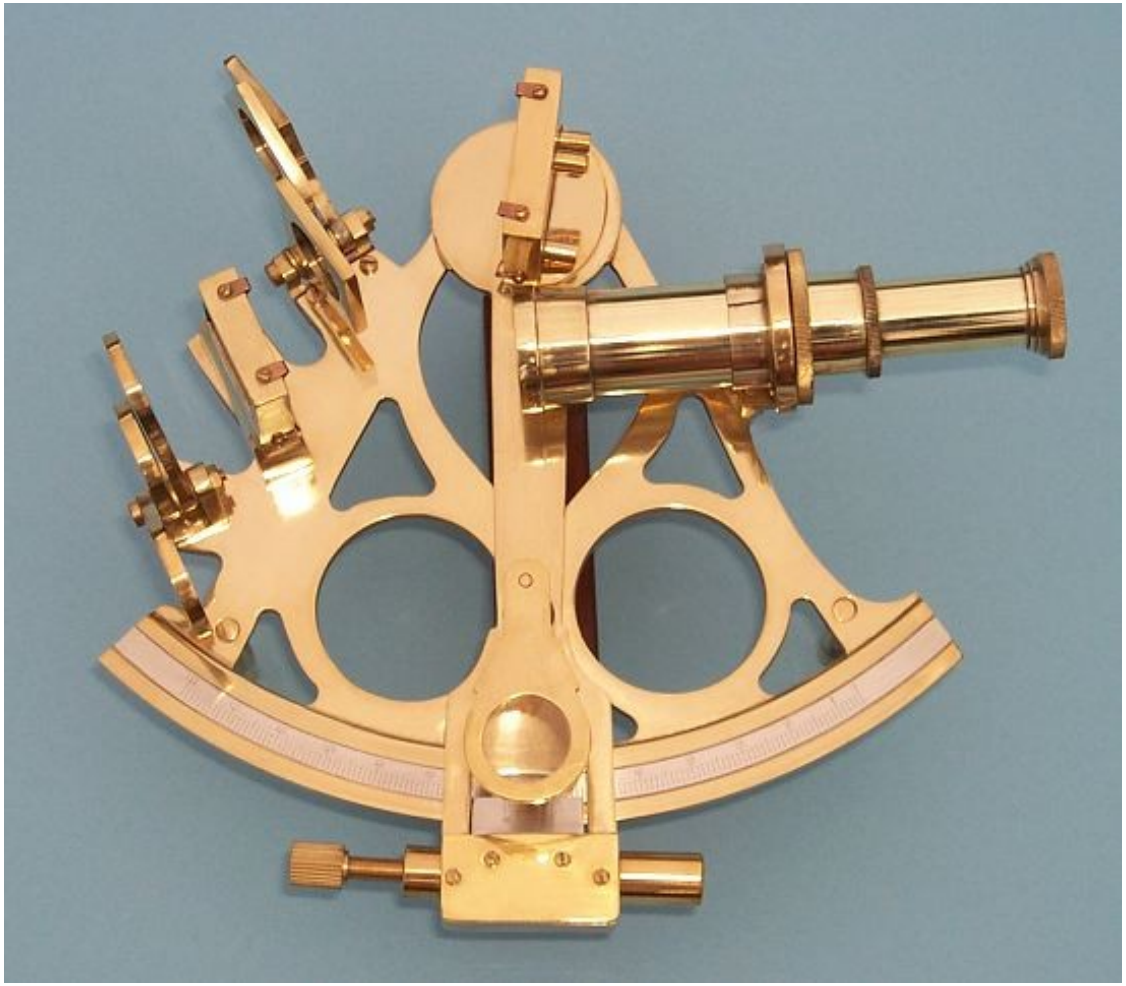
ein Fremder Sender kann jederzeit den Reifendruck-Alarm auslösen – er muß allerdings mit einer der vier bekannten und hinterlegten IDs senden

http://www.golem.de/1008/77111.html

http://www.winlab.rutgers.edu/~Gruteser/papers/xu_tpms10.pdf

GPS

maintech GmbH



Angreifbare Mobilität
GPS

maintech GmbH

GPS

- Navigation
- Elektronisches Fahrtenbuch (Steuerrechtlich relevant)
- Flottenmanagement (Arbeitsrechtlich relevant)
- Blackbox (bei Unfällen als Beweismittel zugelassen)

Sie befinden sich hier...

GPS

50Bit/s Datenrate

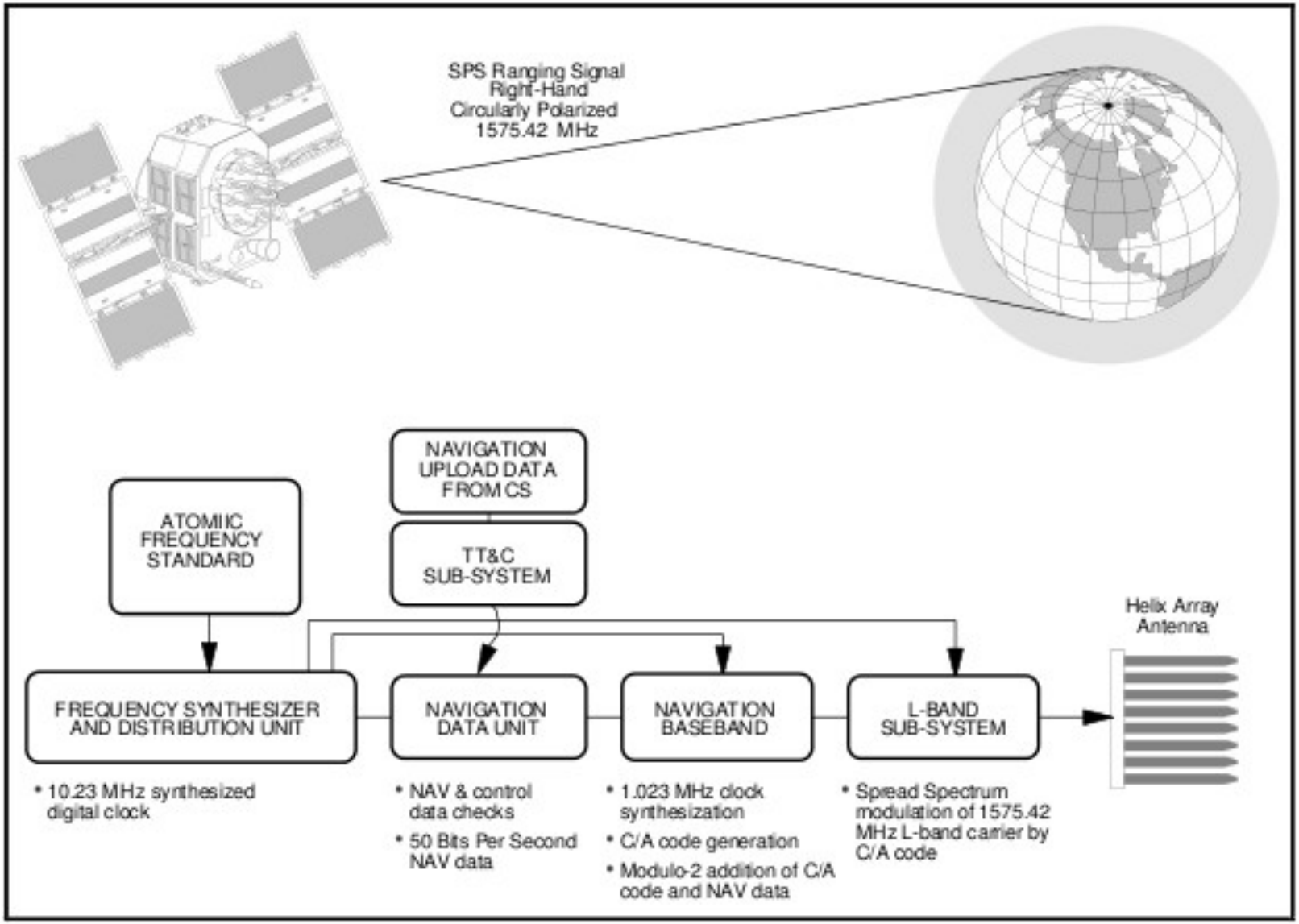
Datenrate wird mit einem Gold-Code aufgeweitet auf 1023kBit/s

Alle Satelliten senden gleichzeitig auf 1575.42 Mhz, moduliert wird mit BPSK

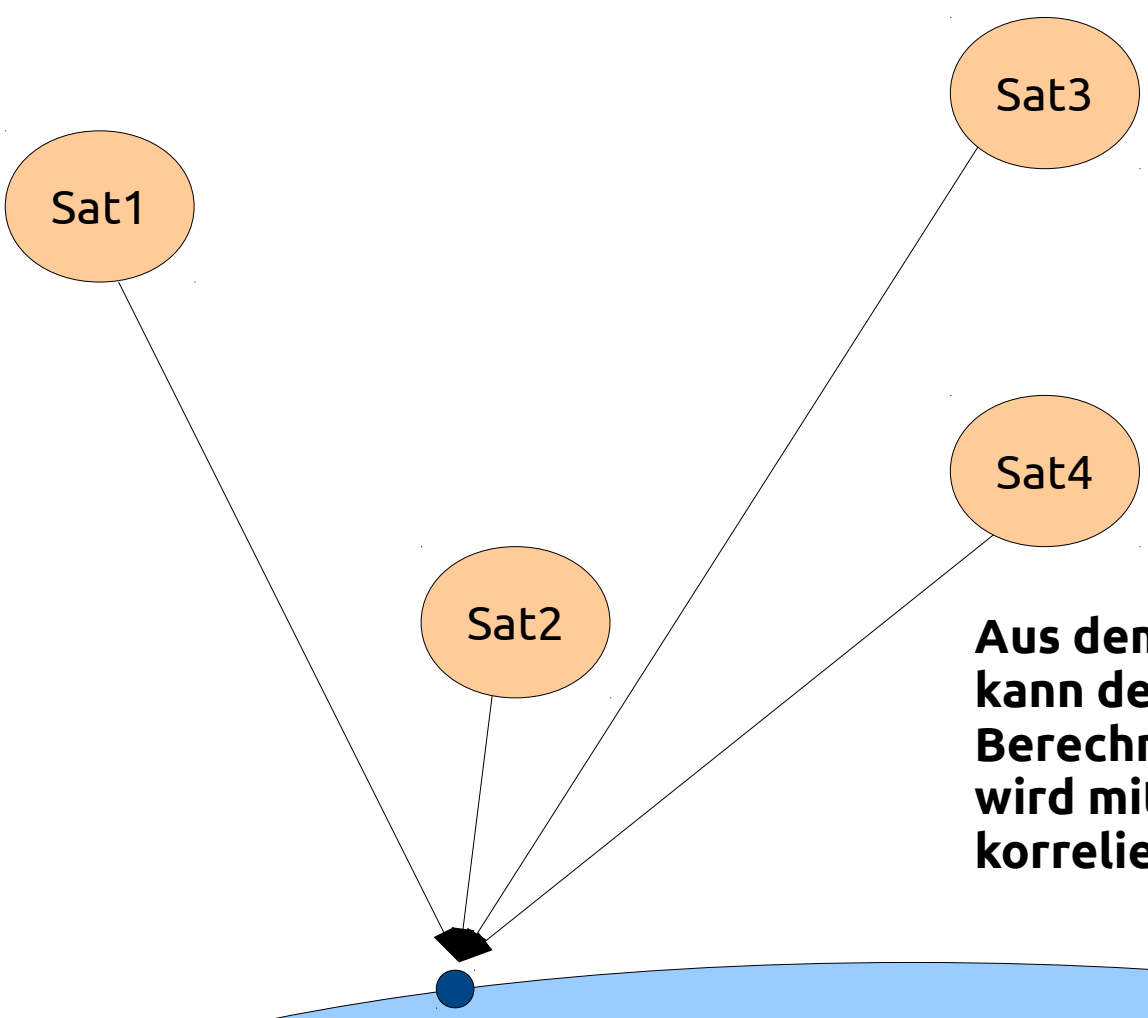
Die Signale addieren sich in der Luft

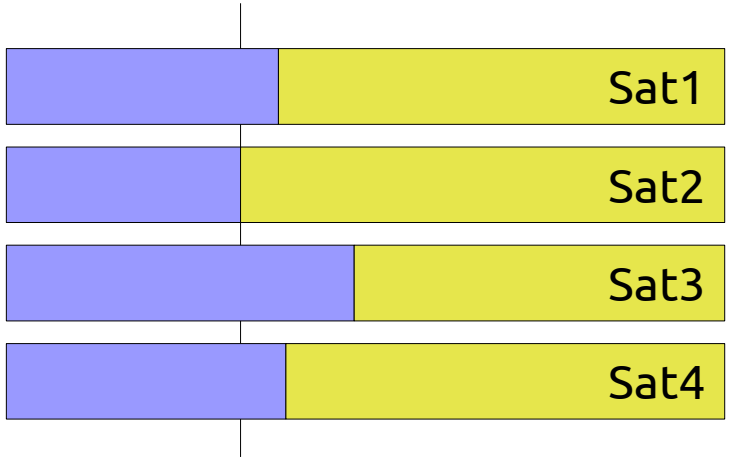
Am Boden wird immer ein Empfangspegel von -136dBm garantiert

GPS


SPS Ranging Signal
Right-Hand
Circularly Polarized
1575.42 MHz
NAVIGATION
UPLOAD DATA
FROM CS
ATOMIIC
FREQUENCY
STANDARD
TT&C
SUB-SYSTEM
Helix Array
Antenna
FREQUENCY SYNTHESIZER
AND DISTRIBUTION UNIT
NAVIGATION
DATA UNIT
NAVIGATION
BASEBAND
L-BAND
SUB-SYSTEM
• 10.23 MHz synthesized
digital clock
• NAV & control
data checks
• 50 Bits Per Second
NAV data
• 1.023 MHz clock
synthesization
• C/A code generation
• Modulo-2 addition of C/A
code and NAV data
• Spread Spectrum
modulation of 1575.42
MHz L-band carrier by
C/A code

Angreifbare Mobilität
GPS





Aus dem Laufzeitunterschied der Signale kann der Empfänger die eigene Position Berechnen (der aufgeweitete Bitstrom wird mit der einer Referenzsequenz korreliert)

maintech GmbH

Grundsätzliche Probleme und Lösungen

Problem: Der Bestimmung der eigenen Position muß die Position der Satelliten mit der gleichen oder höherer Genauigkeit bekannt sein.

Lösung: Im 50Bit/s-Datenstrom wird der Almanach gesendet – eine Liste mit Bahndaten für jeden Satelliten. Der Almanach ist 12 Minuten lang.

Problem: Um aus den Bahndaten auf die Position zu schließen, wir die aktuelle Uhrzeit benötigt. Genauigkeit ist wichtig, da die Satelliten sehr schnell fliegen.

Lösung: Die aktuelle Uhrzeit wird besonders häufig gesendet. Daher geht beim GPS-Empfänger die Uhr immer zuerst. Außerdem haben die Satelliten eine besondere Bahn und bewegen sich vom Boden aus gesehen eher langsam.

GPS

Sicherheitsrisken

Die Daten werden unverschlüsselt und unsigniert gesendet

Eigene Generatoren sind leicht aufzubauen oder günstig zu kaufen (http://www.labsat.co.uk – ca. 8000 Euro)

Erzeugung mit dem GNURadio/USRP ist möglich – es wird allerdings ein stabilerer Referenzoszillator gebraucht (http://code.google.com/p/clock-tamer)

http://www.navcen.uscg.gov/pubs/gps/sigspec/default.htm

Angreifbare Mobilität
RDS/TMC

maintech GmbH

RDS/TMC

maintech GmbH

Datenübertragung brutto 1187.5 Bit/s

Nachrichten werden in 64-Bit-Gruppen zerlegt, gesendet werden 104Bit (Netto-Rate = 725.2Bit/s)

Pro Gruppe sind die ersten ~30Bit fest (PI-Code, PTY, TP, Gruppen-Code)

Die restlichen 32 Bit können für Nutzdaten verwendet werden:

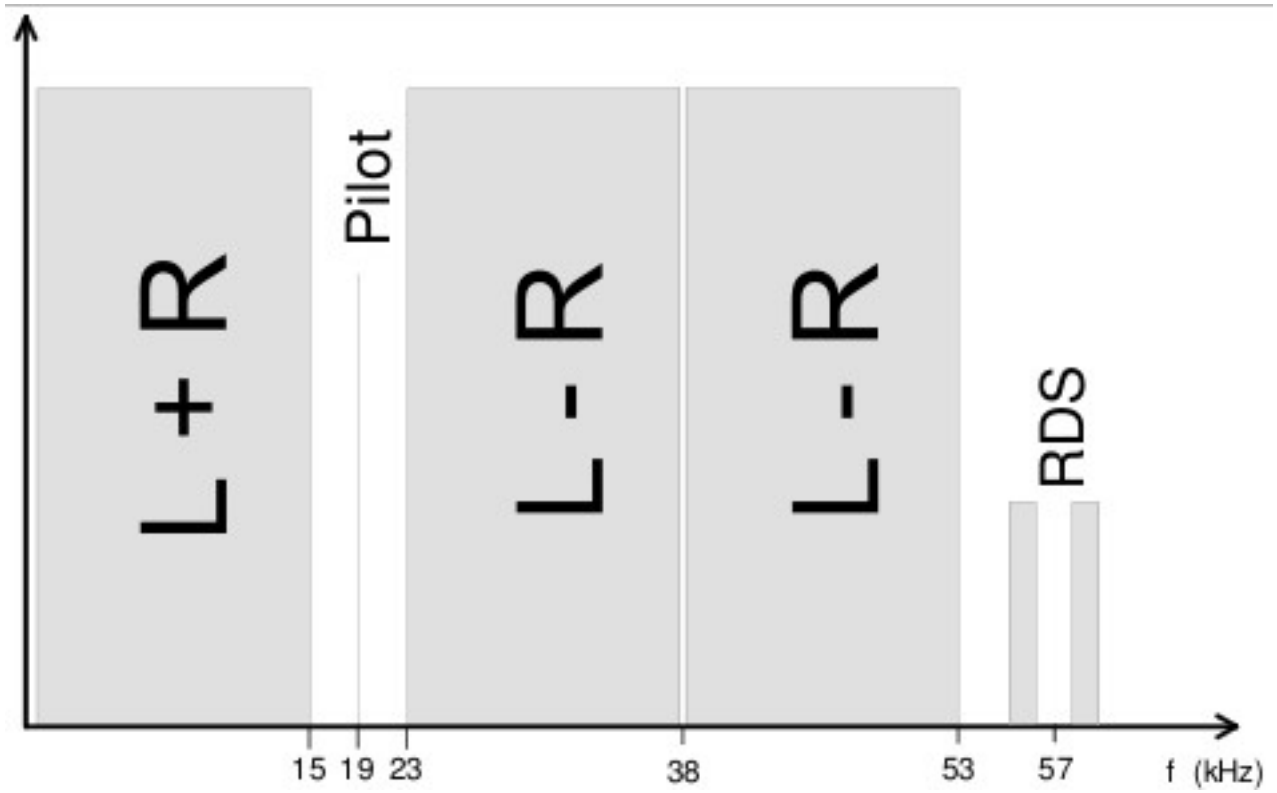
- Stationsname
- Alternative Frequenzen
- Umschaltung für Verkehrsfunk
- RadioText und RadioText+ (Liedtitel, etc.)
- TMC

Übertragung ist unverschlüsselt und unsigniert

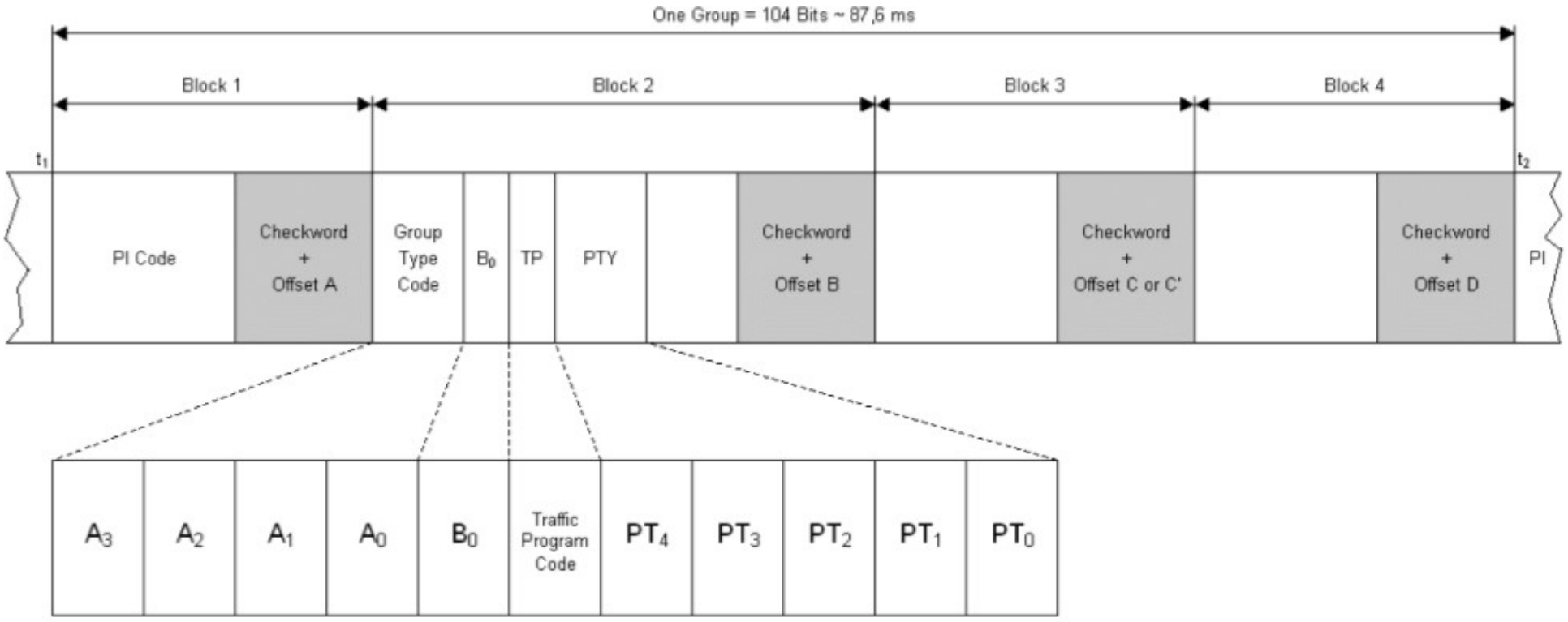
maintech GmbH

FM-Spektrum

Das Datensignal wird auf einen Träger aufmoduliert, der sich aus dem verdreifachten Stereo-Piloten ergibt. Der Träger selber wird allerdings nicht übertragen.



Struktur einer Gruppe



- PI-Code = Stations-ID (wird bei Programm-Anmeldung vergeben)
- Group-Type-Code = Bezeichnung der restlichen Daten
- TP = Verkehrsfunk
- PTY = Programmtyp (Musik, Dokumentation, Nachrichten, etc.)

Problem: EON-TP

(Verkehrsfunk auf anderer Frequenz im gleichen Sender-Netz)

Meldung: Auf einem anderen aber verwandten Programm kommt gerade eine Verkehrsfunkdurchsage

Radio: Wechselt Frequenz.

Realität: Auf der anderen Frequenz ist doch kein Verkehrsfunk.

Radio: Wechselt wieder zurück.

...Beginne von vorne...

Beispiel: Bayern 2 verwendet den Verkehrsfunk von Bayern 3 mit.

RDS/TMC

maintech GmbH

Problem: RadioText(+)

Übertragung von Zusatzinformationen zum Programm, z.B. Liedtitel, Interpret, etc.

Felder für URLs, Email-Adressen, SMS-Nummern vorgesehen: Cross-Radio-Site-Scripting-Attacken im Auto. Gerne auch in Verbindung mit HTML-basierten Klimaanlagen-Interfaces.

RadioText+ verwendet Unicode – die üblichen Probleme mit fehlenden Zeichen in Schriftarten, von rechts-nach-link-Schreiben, etc. treten auf.

maintech GmbH

Problem:
RadioText(+)

maintech GmbH

Problem: TMC TMC-Nachrichten enthalten folgende Informationen:

- Event-Code (Stau, Unfall, etc.)
- Location-Code (Liste mit Nummern für jede Kreuzung, Autobahnauffahrt, etc. Gepflegt von der Bundesanstalt für Straßenwesen) – Regelmäßige Radio-Updates notwendig.
- Dauer (bei Sperrungen z.B.)
- Gültigkeit

Die Daten werden in einem Loop gesendet. Ein Durchlauf dauert an einem Ferienanfang auch gerne eine halbe Stunde.

maintech GmbH

Problem: TMC

http://www.heise.de/security/meldung/Hacker-schicken-falsche-Meldungen-an-Navigationssysteme-170089.html

Angreifbare Mobilität
Bluetooth Freisprechen

maintech GmbH

Bluetooth Freisprechen

maintech GmbH

Bluetooth Freisprechen

Das Fahrzeug baut nicht nur eine Audio-Verbindung auf:

- SIM-Access-Profile zum Verwenden der SIM-Karte mit einem im Auto eingebauten GSM-HF-Teil
- Telefonbuch, SMS-Liste

Eine Vielzahl von Protokollen und Fallstricken ist beteiligt. Im Prinzip könnte man von einem gepaarten PC (der sich als Handy mit SAP ausgibt) bis hinunter ins GSM im Auto Attacken fahren...

Eigene Erfahrung: Paaren eines Nokia-Telefons mit dem 3er Navi führt zum Total-Crash des Telefons...

Zur Bluetooth-Security haben andere schon Telefonbücher vollgeschrieben...

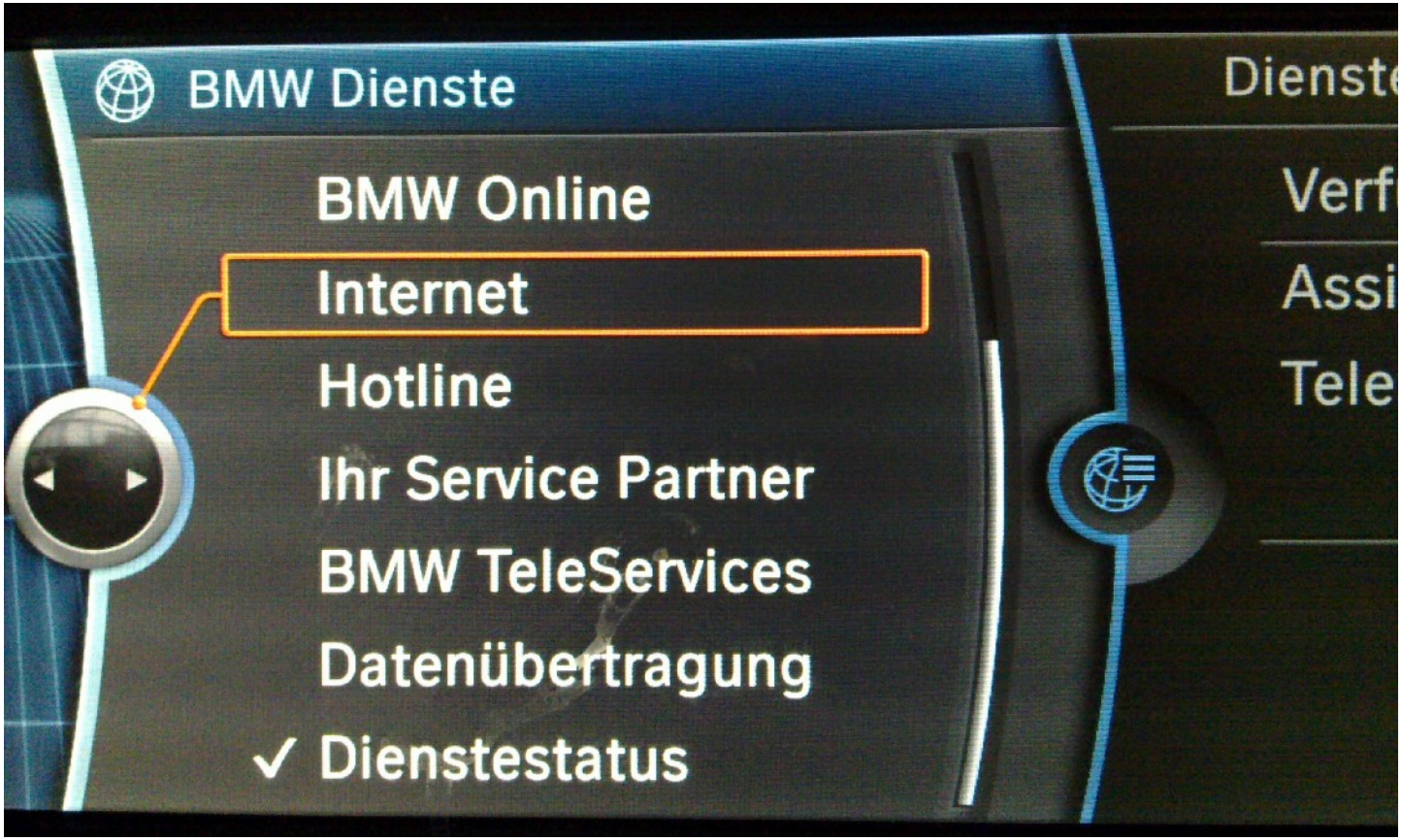
Angreifbare Mobilität
Internet

maintech GmbH

maintech GmbH

Es war unvermeidlich:

Internet



maintech GmbH

Problem: Datenschutz

Was wird wann wohin übertragen?

Ist das Fahrzeug identifizierbar?

Im Fahrzeug ist ein eigenes GSM-Modem + SIM-Karte eingebaut. Ein eigener Provider-Vertrag wird nicht abgeschlossen. Alle Kosten sind mit dem Fahrzeugkauf beglichen.

Fallen Vorratsdaten an? Verkehrsdaten? Wer bekommt diese Daten? Liegen die evtl. bei BMW in einem RZ? Dort würden sie nicht dem Fernmeldegeheimnis unterliegen.

maintech GmbH

Problem: Datenschutz

Unsere liebste Datenkrake ist auch schon da:

maintech GmbH

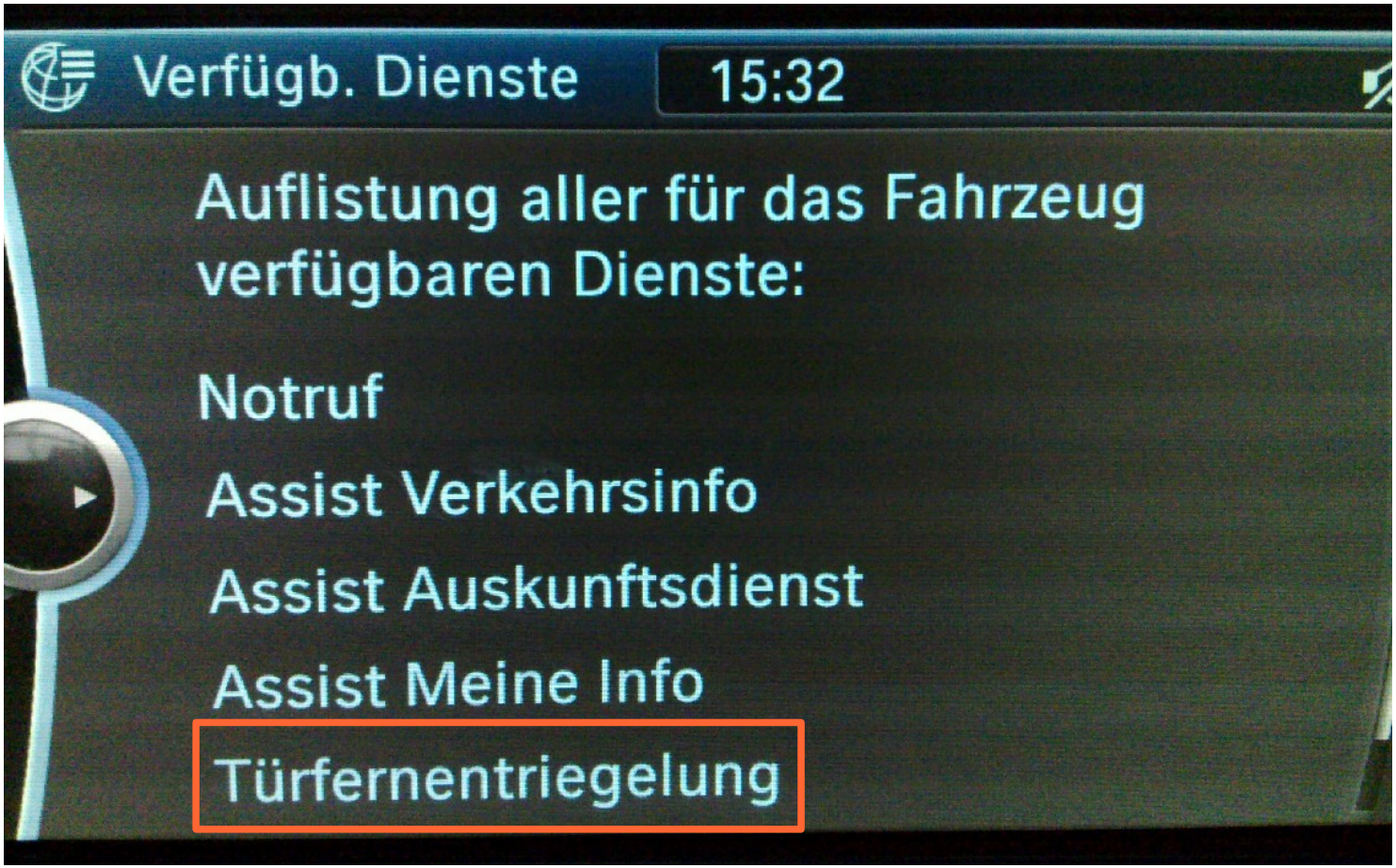
Problem: Datenschutz

Der grüne Marker sind wir – d.h. Google hat den Auto-Standort erfahren

maintech GmbH

Problem:
Datenschutz

...es wird noch lustiger...



maintech GmbH

Problem: Datenschutz

Parken Sie dieses Auto nicht vor der Sparkasse in Liechtenstein...

maintech GmbH

Problem: Sicherheit

Apple kann Anwendungen installieren, entfernen, verändern, etc. Nach dem Jailbreak haben iPhones gerne auch mal ein bekanntes root-Passwort...

Angreifbare Mobilität
Fazit

maintech GmbH

Fazit? Fazit!

Christian Daniel

Angreifbare Mobilität
Zusammenfassung

maintech GmbH

Funkschlüssel	Im Prinzip sicher, proprietäre Verfahren wurden aber geknackt
Reifendruck-Sensoren	Im Auto können Alarme ausgelöst werden; das Auto kann besser überwacht werden als mit Kennzeichen-Kameras
GPS	Empfänger vertrauen dem Signal vollkommen; ein eigenes Signal kann günstig erzeugt werden. Neben falschen Positionsdaten können auch falsche Hilfsdaten, etc. gesendet werden.
RDS/TMC	Eigenbau-Sender zum Senden falscher Nachrichten sind günstig im Internet zu bestellen. Das Protokoll enthält ettliche Lücken.
Bluetooth Freisprechen	Angriffe über Telefonbuchdaten, SIM-Access, etc. denkbar. Bluetooth ist an sich nur bedingt sicher.
Internet	Auto übers Internet oder mittels Smartphone-App auf- und zuschließen? Wie krank geht's...

maintech GmbH

Vielen Dank!

Fragen? Anregungen?
Diskussion!