Sicherheit in Mobilfunknetzen

DEEPSEC

Worum geht's?

DEEPSEC

- Mobilfunknetzwerke (GSM)
- Sicherheit
- Schwachstellen & Risiken
- Schadensbegrenzung

Sicherheit?

DEEPSEC

- *Integrität* der Verbindungs-/Gesprächsdaten
- *Vertraulichkeit* der Verbindungs-/Gesprächsdaten
- *Identität* der Gesprächsteilnehmer
- *Verfügbarkeit* der Infrastruktur

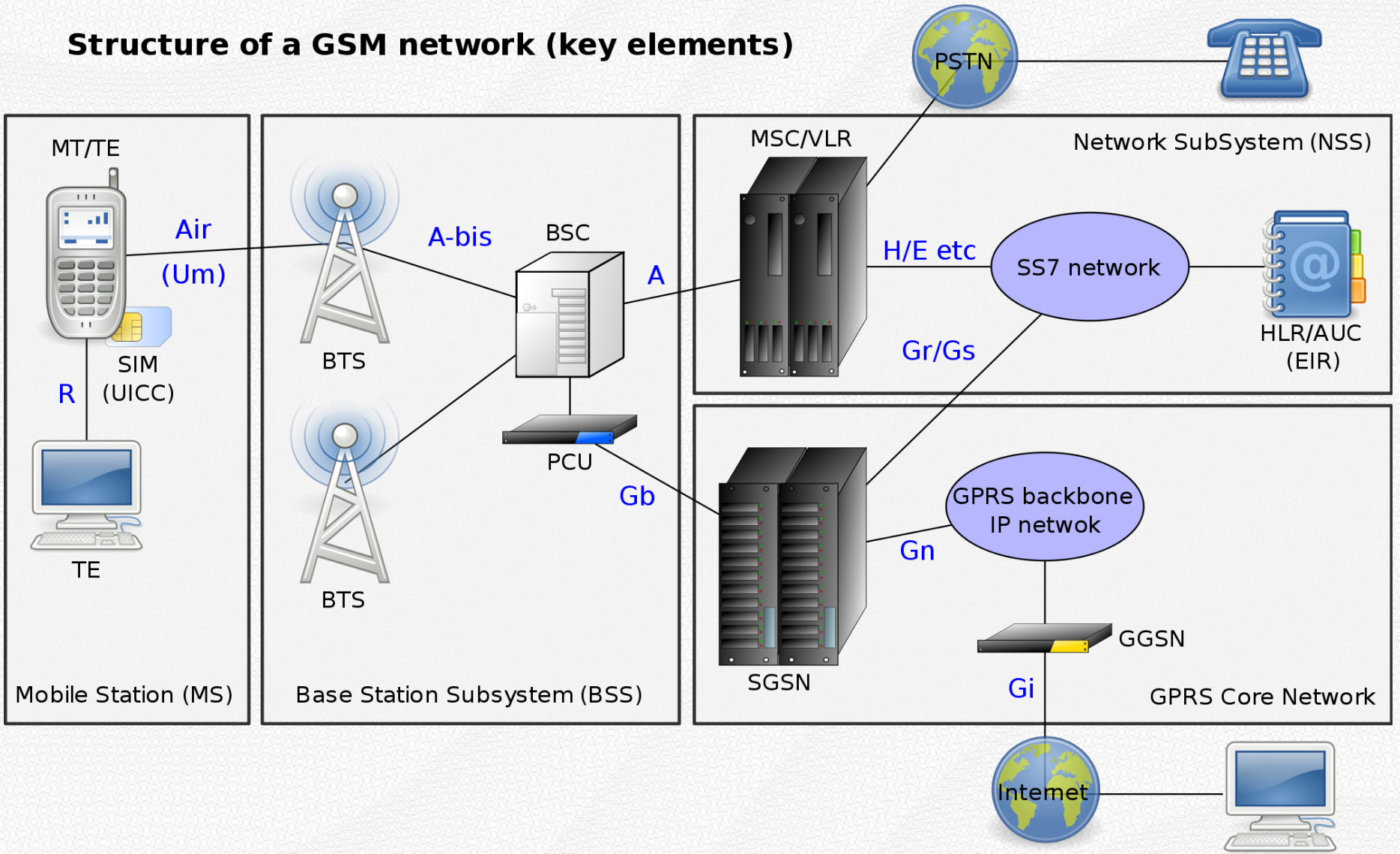
Mobilfunkwelt

DEEPSEC

- GSM Standards sehr komplex
- Oligopol weniger Hersteller, viel Geheimhaltung
  - Mobilfunkbetreiber betreiben weder Netzwerk noch Clients
  - Outsourcing und NDAs
- mangelnde Qualitätskontrolle
  - *Security by Obscurity* - Verschleierung
  - keine Sicherheits-/Kryptoanalysen
- Patches schwer bis unmöglich
  - Algorithmen teilweise in Hardware implementiert
  - Firmware-Upgrades durch Outsourcing begrenzt („packaged“/SLA)

Netzwerkübersicht

DEEPSEC



Identifikation der Clients

DEEPSEC

- International Mobile Equipment Identity (IMEI)
  - Geräteadresse
  - 14 bis 16 Stellen
- International Mobile Subscriber Identity (IMSI)
  - 64 Bit Subscriber-Identifikation
  - gespeichert auf SIM-Karte
- Temporary Mobile Subscriber Identity (TMSI)
  - temporäre Identifikation im Netzwerk
  - generiert beim Einbuchen/Anmelden

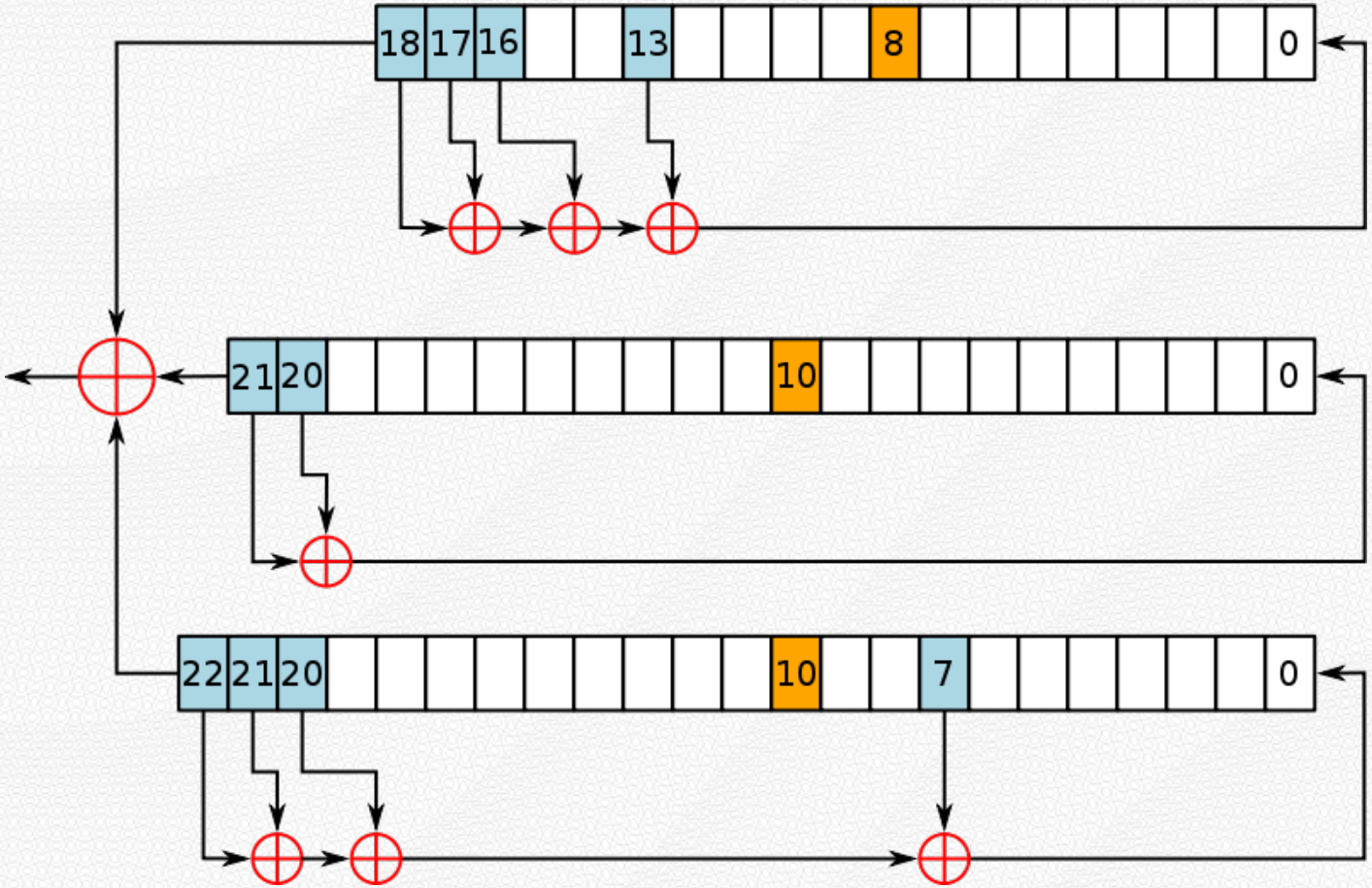
Vertrauensmodell

- Alle Netzwerke & Komponenten sind vertrauenswürdig
- Mobilfunkbetreiber vertrauen einander
  - über Staatsgrenzen hinweg (Roaming)
- Keine gegenseitige Authentisierung (2G)
  - Mobilfunknetz authentisiert sich nicht
  - Clients müssen sich authentisieren
- Mobiltelefon Teil des Netzwerks
  - Zugriff auf SIM-Karte
  - Senden von Kommandos an Mobiltelefon

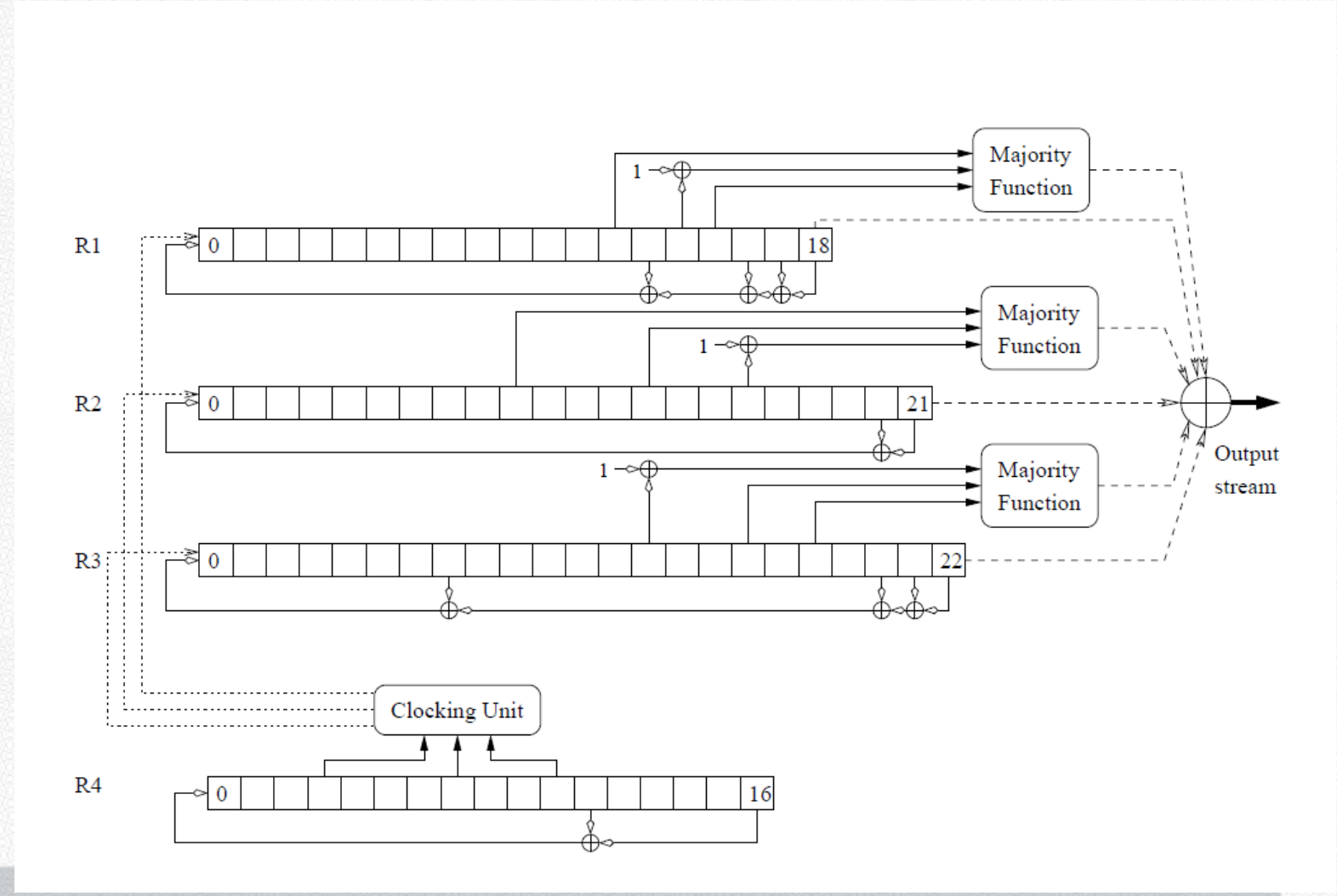
Verwendete Krypto-Algorithmen

- A5 Serie
  - Varianten A5/0, A5/1, A5/2, A5/3, A5/4
  - Verschlüsselung (A5/0 ist Klartext)
- A3 Hash
  - Authentisierung des Users
- A8 Verschlüsselung
  - Schlüsselgenerierung

- PRNG mit XOR



- Ähnlich wie A5/1 schwächer für Export



A5/3 ("Kasumi")

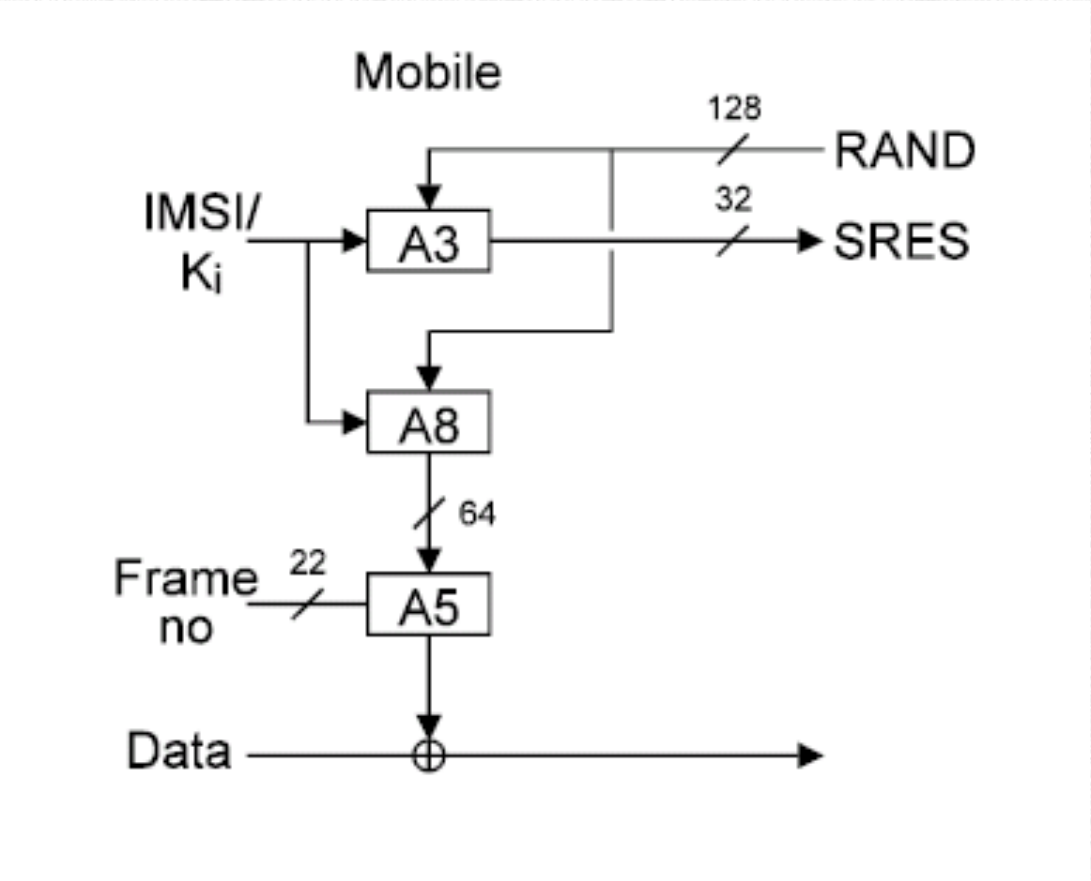
- Block-Verschlüsselung
  - Wird als Stream-Cipher eingesetzt
  - Codename "MISTY"
  - Mitsubishi

Authentifizierung

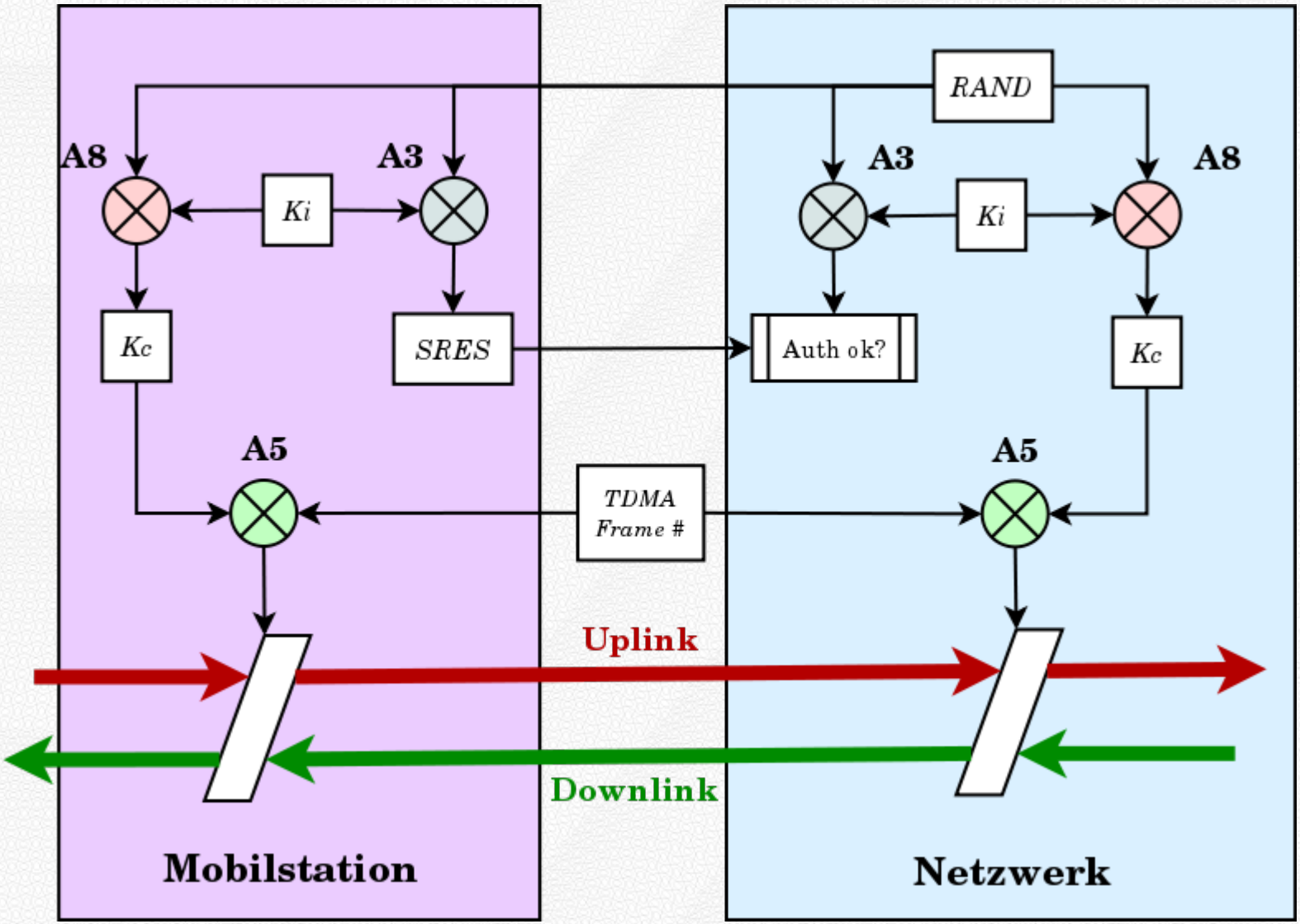
- 128 Bit *Ki* auf SIM-Karte und in Authentication Centre (AuC)
- 128 Bit Zufallszahl *RAND*
- 32 Bit Signed Response *SRES*
  - berechnet durch A3
- 64 Bit *Kc* Sitzungsschlüssel
  - berechnet durch Algorithmus A8 aus *Ki* und *RAND*
- Verschlüsselung durch Algorithmus A5
  - A3, A5 und A8 sind Standards, Implementationen verschieden
  - COMP128 ist eine Implementation von A3/A8

A3/A8 (COMP128)

- Zwei Algorithmen
- Authentisierung & Schlüsselgenerierung



Authentisierung (2)



COMP128 / A3 / A8

- Security through obscurity
  - COMP128 / A3 / A8 im Rahmen von Standard wählbar
  - A3 / A8 nicht publiziert
- COMP128 auf SIM-Karte implementiert
  - COMP128-1 gebrochen (<60s)
  - COMP128-2 nicht kryptoanalysiert
  - COMP128-3 nicht kryptoanalysiert

Verschlüsselung

DEEPSEC

- A5/0 – keine Verschlüsselung
- A5/1 – Verschlüsselung für Europa/USA
- A5/2 – schwache Variante von A5/1 für Export
- A5/3 / GEA3 – stärkerer Algorithmus (von Mitsubishi)
- A5/4 / GEA4 - dito

Verschlüsselung?

DEEPSEC

- A5/2 in Echtzeit knackbar
- 64 Bit Schlüssel!
  - Angriffe auf A5/1 seit 2007
  - A5/1 mit Rainbow Tables knackbar (2009/2010)
  - Aufwand im Sekunden-/Minutenbereich
- A5/3
  - verwendet denselben Schlüssel wie A5/1
  - kann durch Downgrade Attacke umgangen werden

Halbaktive Angriffe

DEEPSEC

- Mitschneiden von Kommunikation
- Key Replay-Attacke
- Hardware z.B. wie aktive Angriffe

start_cipher(**A5/3**, *rand*)
Gespräch aufzeichnen

BTS

Selber RAND = Selber Key

start_cipher(**A5/1**, *rand*)
Schlüssel brechen

BTS

Ich verwende 3G! Und?

- 2G, 3G, *n*G Netzwerke werden parallel betrieben
  - völlige 3G Abdeckung unrealistisch
  - 3G für Daten, 2G für Gespräche und SMS
- GSM wird lange bleiben
  - sehr viele Endgeräte (Alarmanlagen, Smart Grid, …)
  - Abdeckung abseits Ballungsräumen

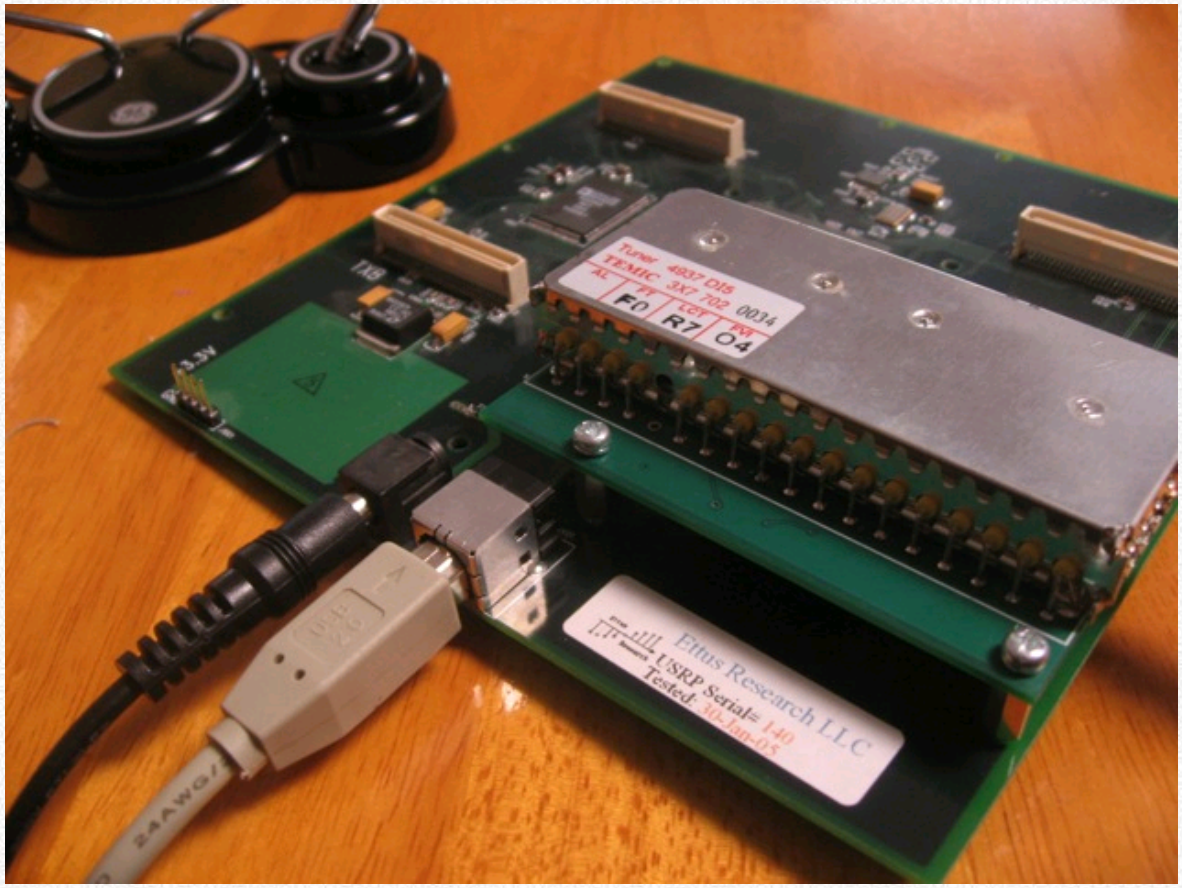
Passive Attacken

DEEPSEC

- Universal Software Radio Peripheral™ (USRP™)
- Calypso Digital Base Band Chipsatz
  - Dokumentation versehentlich publiziert
  - Motorola C123/C115/C140
  - Sony Ericsson J100i
- OsmocomBB
  - Open Source GSM Baseband Software
  - GSM Anrufe & SMS mit Freier Software

USRP (Universal Software Radio Peripheral)

- Open Source Hardware
- Eigenbau
- Relativ Günstig
- FPGA
- PC-Software



Verwendete Mobiltelefone (u.A.)

- OsmocomBB
  - Motorola C115
  - Motorola C140
  - SonyEricsson J100i

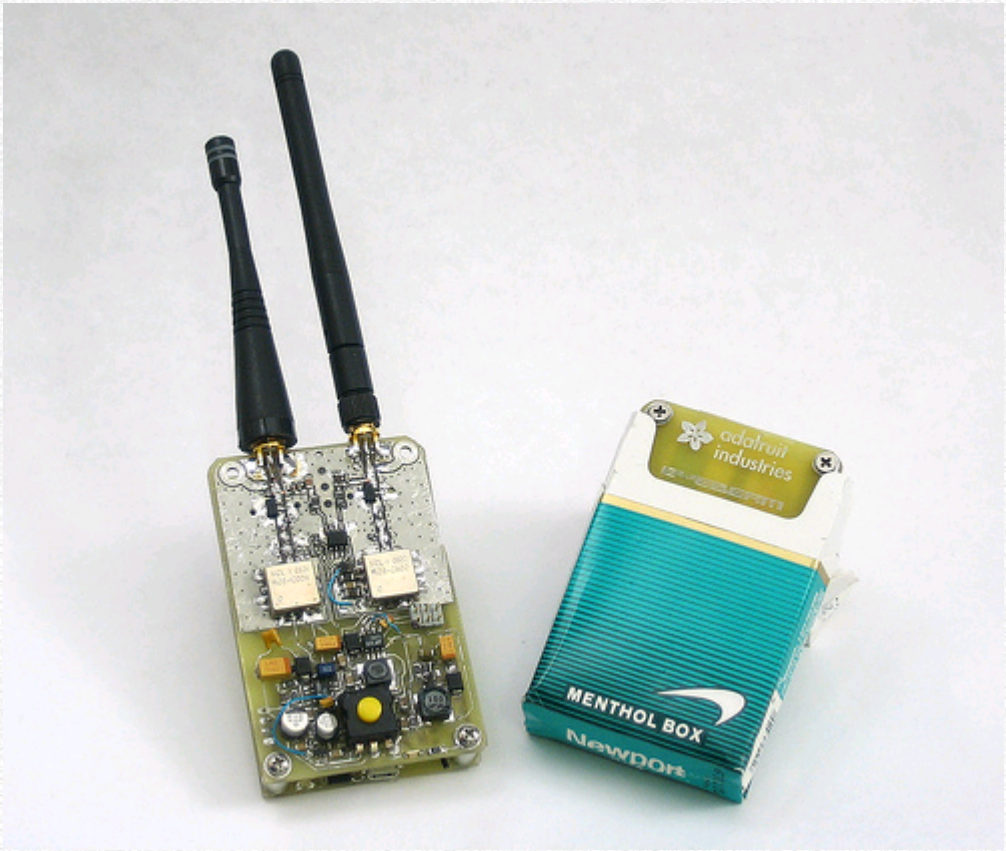
Aktive Attacken

- Basisstation aufbauen
  - OpenBTS + Asterisk™
  - Netzwerk muß sich nicht authentisieren
- mehrere Basisstationen
  - OpenBSC
- Stören der Frequenzen (Jamming)
  - (D)DoS
  - zumeist illegal (da Frequenzen verkauft/verpachtet wurden)

Eigenbau Jammer

DEEPSEC

- Z.B. Wave-Bubble
- Breitband
- Alle GSM/3G Bänder
- Billig
- Leicht zu verstecken



Verwendung von Störsendern

DEEPSEC

- Kommunikation unterbinden
- Kommunikation auf 3G verhindern
  - 3G (UMTS etc) robust und sicher
  - Mobiltelefon weicht auf 2G aus (GSM)
  - Angriffe auf 2G leichter

Deaktivieren von Zellen

DEEPSEC

- „Data driven attack“ auf Basisstationen
  - kein Jamming, kein Fluten
  - Ausnutzen von Fehler in Implementation oder Protokoll
- Demonstration auf DeepSec Konferenz 2009
  - Generieren von ungültigen Daten mit Mobiltelefon
  - DoS gegen Basisstation(en)
  - wenige Datenpakete ausreichend
- (fast) alle Basisstationen anfällig (laut Sicherheitsforschung)

Aktive Attacken

DEEPSEC

- Client verlangt keine Authentisierung vom Netz
  - Aufbau von „rogue base stations“
  - stärkste Basisstation gewinnt
  - Man-In-The-Middle
  - Lokalisierung für gezielte Attacke notwendig
- Störsender
  - rein physikalische Attacke
  - Sendeleistung/Frequenzen problematisch

SMS Attacken

- SMS weit verbreitet
  - nahezu alle Endgeräte unterstützen SMS
  - SMS Nachrichten schnell/leicht zu übertragen
- SMS Fuzzing
  - Implementationen empfindlich gegenüber falschen Daten
  - modifizierte Basisstation + Code
  - Ergebnisse präsentiert am 27C3

SMS Fuzzing Ergebnisse

DEEPSEC

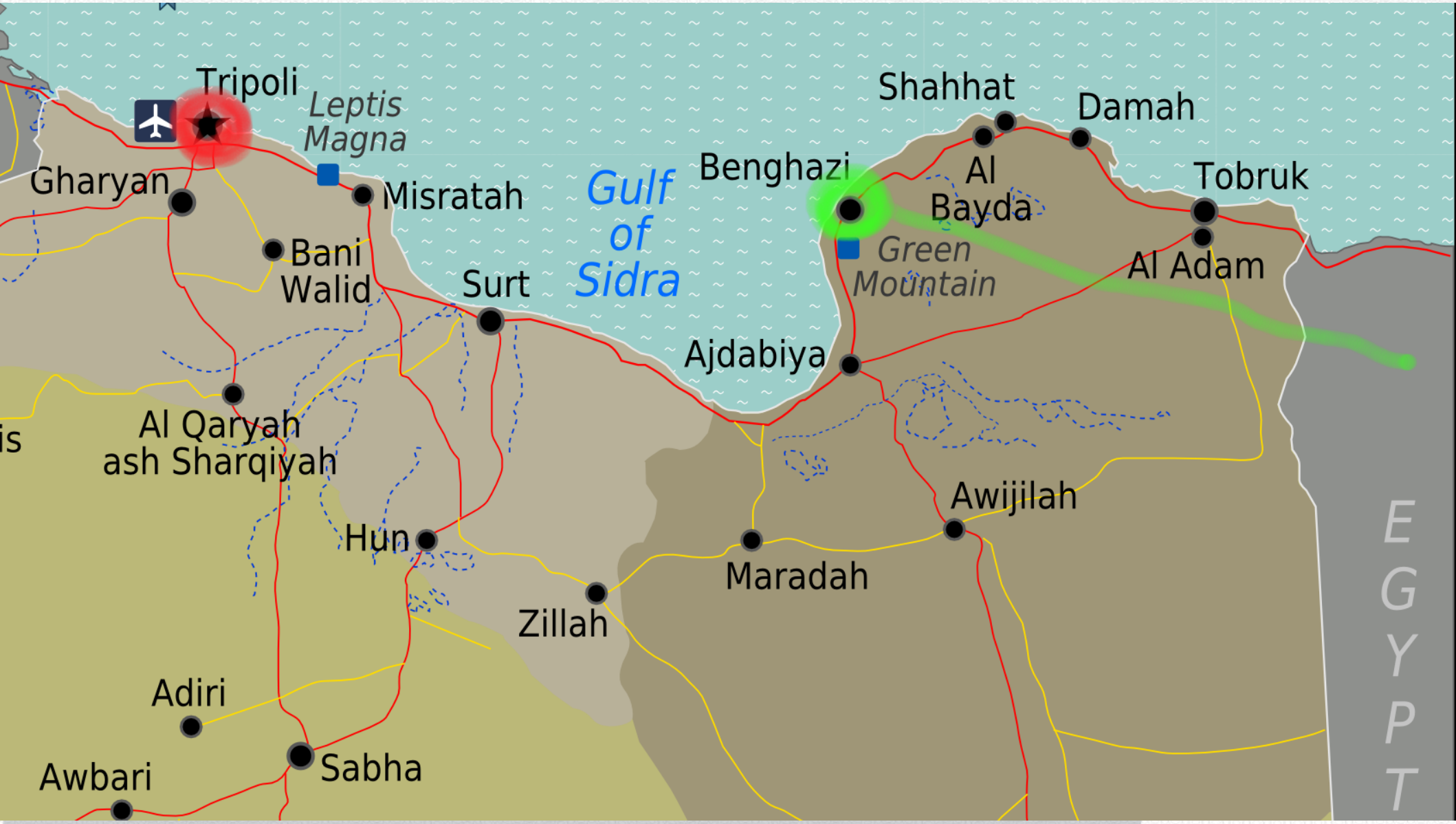
- *Nokia White Screen of Death*
- *Black Screen of Death*
- Reboot / Shutdown / Absturz
- Abmelden von Netzwerk
- SMS nicht sichtbar
- Zerstörung („bricked phone“)
- Ablehnen folgender SMS
- Apps auf Telefon starten nicht
- Watchdog Shutdown
  - Ausschalten nach 3 SMS
- Telefon sendet kein ACK
  - Netz denkt SMS nicht angenommen
  - Netz sendet SMS wieder und wieder
  - Effekt wiederholt sich stetig
  - Fix: SIM-Karte in anderes Telefon stecken…

Übernehmen von Netzwerken

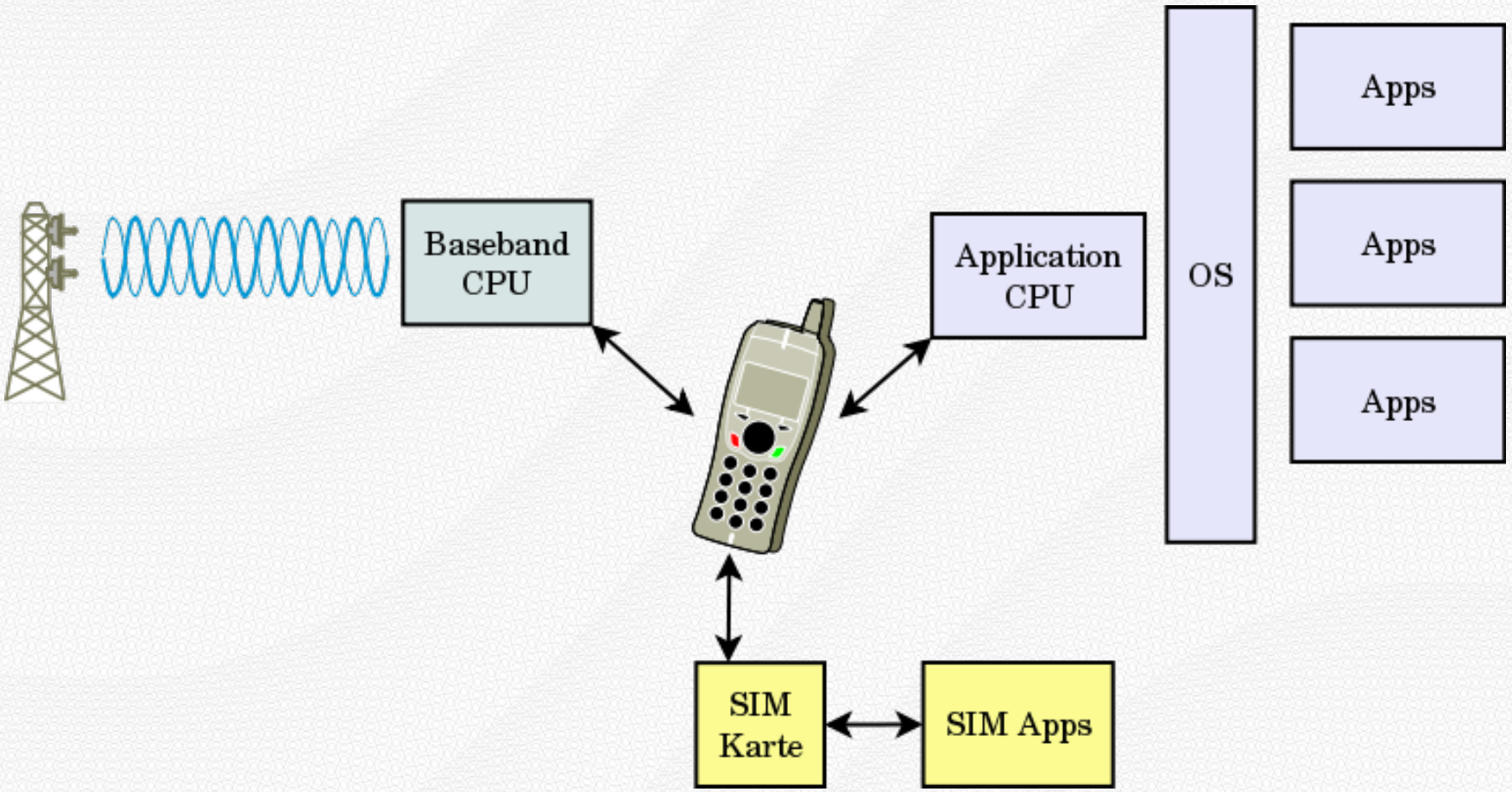
- HLR und angeschlossene MSCs sind Ziele
  - HLR enthält Schlüssel und Rufnummern
  - MSCs erlauben das Steuern der BSCs
- Übernehmen von Infrastruktur inkl. SIM-Karten
- Routen der Gespräche über eigene/fremde Anbindungen
- Beispiel: *Free Libyana* (libysches Rebellennetzwerk)

Free Libyana

DEEPSEC



Komponenten im Mobiltelefon



Baseband Attacken

DEEPSEC

- Angriff auf den Baseband Prozessor
  - Ausnutzen von Bugs/Firmware
  - Attacke mit „rogue base station“
  - vorgeführt auf DeepSec 2010 durch Ralf-Philipp Weinmann
- Aktionen begrenzt, aber
  - Einschalten von Auto-Answer – mobile Wanze
  - Rootkits/Infektion möglich, Verbreitung wie Virus ebenso
  - Zerstören von Mobiltelefonen

SIM Applikationen

- SIM-Karte kann Applikationen haben
  - Native Code oder Embedded Java
  - nicht notwendigerweise sichtbar/zugänglich
  - Provider kann SIM Apps ändern (Over-the-air Programming)
- SIM-Apps können Mobiltelefon Anweisungen geben
  - SIM Application Toolkit (STK) für 2G
  - USIM Application Toolkit (USAT) für 3G

Smartphone Applikationen

DEEPSEC

- Smartphones folgen PCs in punkto Malware
  - keine Plattform ist immun gegen Malware
- App Developer sind keine Sicherheitsexperten
  - Grafiken und Sounds sind einfach wichtiger
  - App Stores wird bedingungslos vertraut!
- Kontrolle der App Store Betreiber nicht ausreichend
  - weder iOS noch Android noch andere sind verschont
  - DRM funktioniert nicht

Reaktionen

DEEPSEC

- Mobilfunkbetreiber
  - betreiben ihre Netzwerke nicht (mehr) selbst
  - entwickeln keine Mobiltelefone / Smart Phone
  - können nichts gegen Fehler im GSM Standard tun
- Hersteller
  - beharren auf Geheimhaltung
  - reglementieren Updates
  - können nichts gegen Fehler im GSM Standard tun

Reaktionen

DEEPSEC

- Politik
  - keine Reaktionen bekannt
  - zusammengefaßt in „*Cyberwar*“ / „*Cybercrime*“
- Behörden
  - sind teilweise informiert
  - haben teilweise Richtlinien um Risiken zu adressieren
- Kunden
  - wissen nichts von den Risiken
  - fragen nicht nach Sicherheit
  - bekommen keine unverzerrten Informationen

Gegenmaßnahmen

DEEPSEC

- Mobilfunk und Endgeräte richtig klassifizieren
  - nicht für alle Sicherheitsanforderungen verwendbar
  - Sicherheit nachrüsten, wenn möglich
  - sensitive Daten löschen / nicht darüber transportieren
- Sicherheit von Herstellern verlangen
- Gespräche zusätzlich absichern
- Datenkommunikation zusätzlich absichern
  - VPN Technologien verwenden
  - verschlüsselte Container verwenden
  - Redundanz vorsehen!

Danke!

DEEPSEC

- Vortragende der DeepSec Konferenzen
  - David Burgess, Karsten Nohl, Dieter Spaar, Ralf-Philipp Weinmann , Harald Welte
- Alle Sicherheitsforscher, die nichts glauben
- Hersteller, die zuhören statt zu klagen
- Benutzer, die Sicherheit in Produkten einfordern

…as we know, there are known knowns. There are things we know we know. We also know there are known unknowns. That is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know.
– *Donald Rumsfeld, 12.2.2002, Department of Defense news briefing*

Über uns…

DEEPSEC

The DeepSec IDSC is an annual European two-day in-depth conference on computer, network, and application security. We aim to bring together the leading security experts from all over the world. DeepSec IDSC is a non-product, non-vendor-biased conference event. Intended target audience: Security Officers, Security Professionals and Product Vendors, IT Decision Makers, Policy Makers, Security-/Network-/Firewall-Admins, Hackers and Software Developers.

Web: https://deepsec.net/
Blog: http://blog.deepsec.net/