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

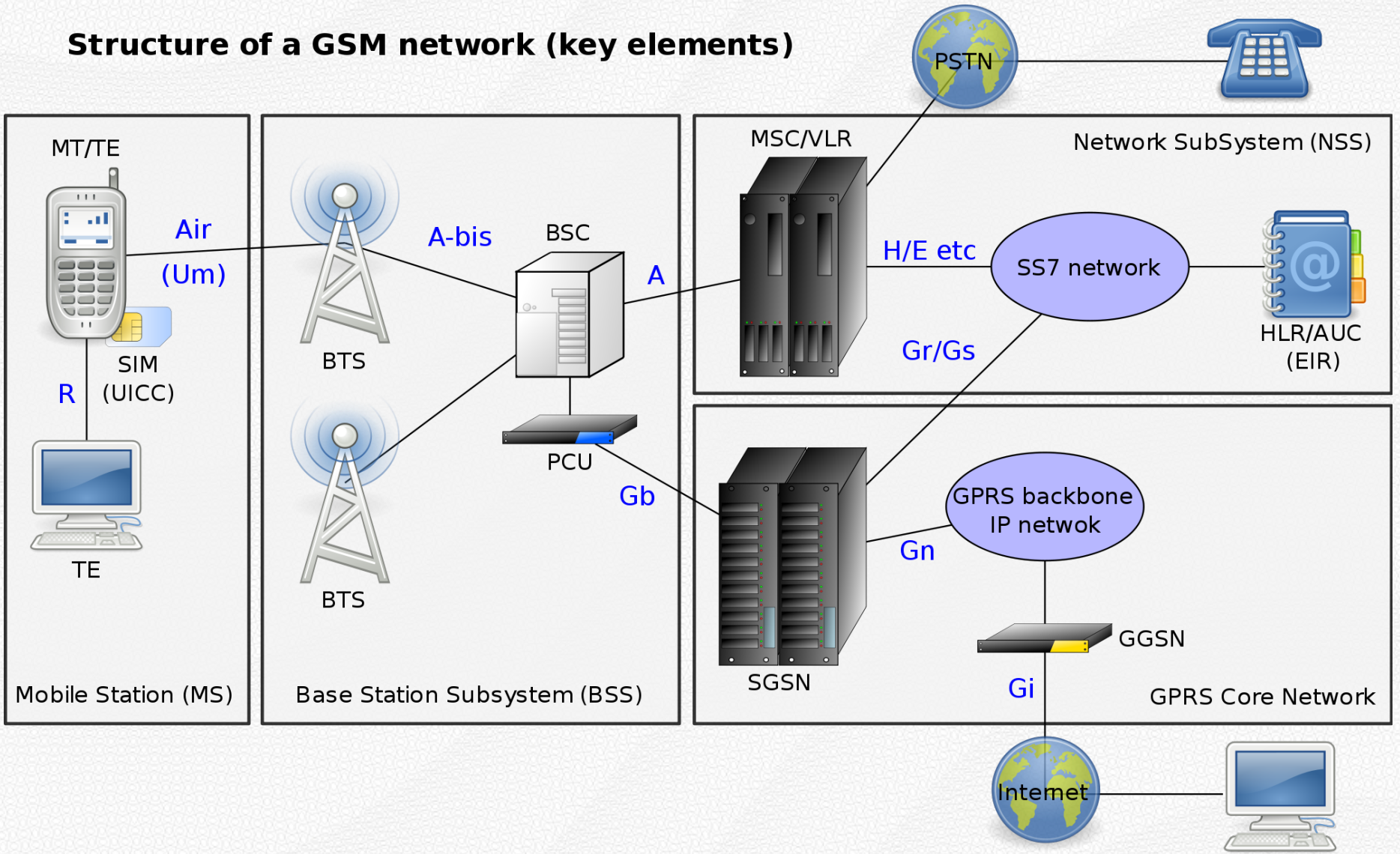
Mobilfunkwelt

DEEPSEC

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

Netzwerkübersicht

DEEPSEC



Identifikation der Clients

- 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

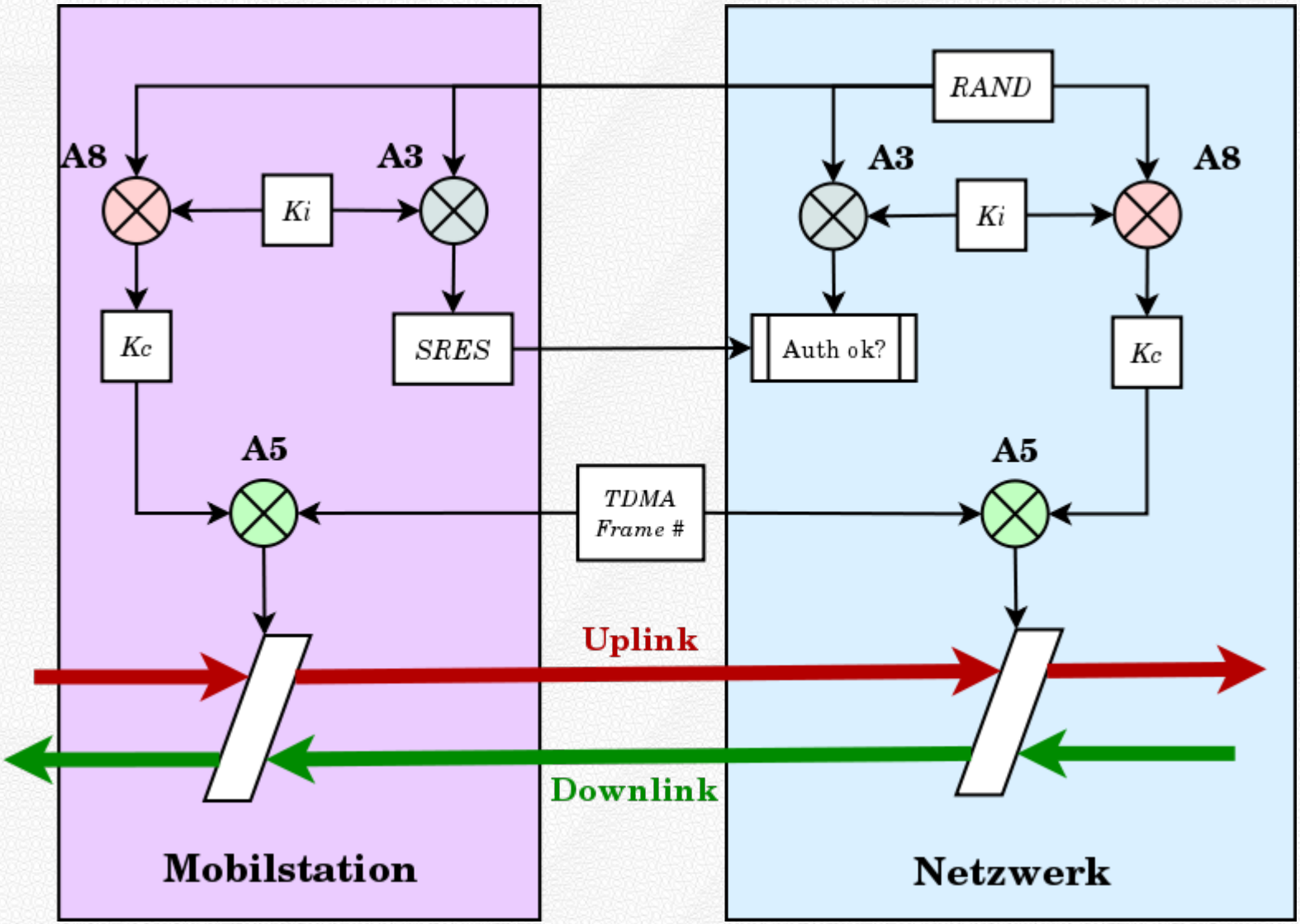
DEEPSEC

- Alle Netzwerke & Komponenten sind vertrauenswürdig
- internationale Mobilfunkbetreiber vertrauen einander
- 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

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

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

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 bleiben
  - sehr viele Endgeräte (Alarmanlagen, Smart Grid, …)

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

Aktive Attacken

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

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

- Client verlangt keine Authentisierung
  - 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

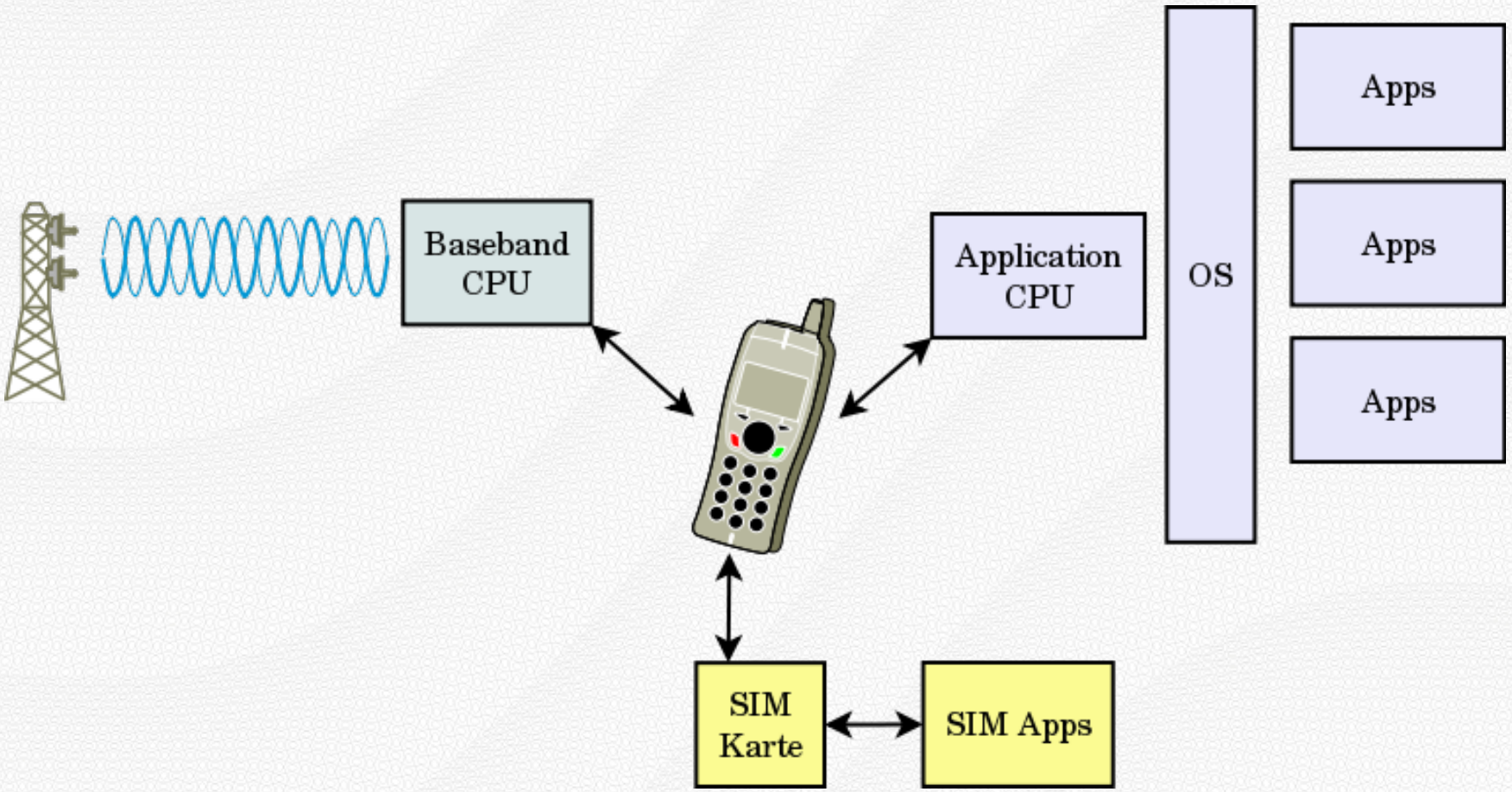
- SMS weit verbreitet
  - nahezu alle Endgeräte unterstützen SMS
  - SMS Nachrichten schnell/leicht zu übertragen
- SMS Fuzzing
  - Implementationen empfindlich gegenüber falschen Daten
  - modifizierte Basisstation + Code
  - Ergebnisse präsentiert am 27C3

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…

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

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

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

…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

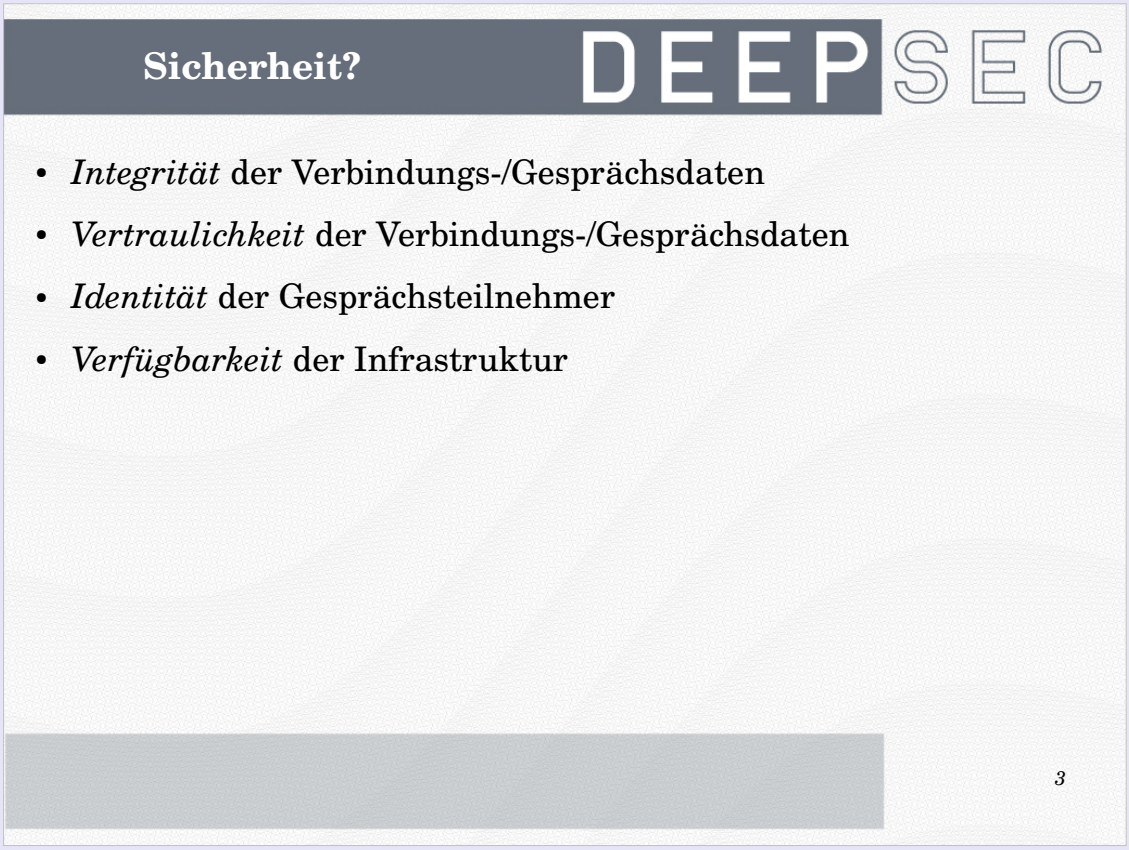
The DeepSec IDSC is an annual European two-day in-depth conference on computer, network, and application security. We aim to bring together the leading security experts from all over the world. DeepSec IDSC is a non-product, non-vendor-biased conference event. Intended target audience: Security Officers, 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/

Das Bild zeigt ein altes schwedisches Analogtelefon (kopiert von Wikipedia). Mobiltelefone gibt es seit den 20er Jahren. Ab 1950 nahmen die ersten Mobilfunknetzwerke ihren Betrieb auf (0G, 1G). Die ersten Netzwerke verwendeten Analogfunk. Die Groupe Spécial Mobile (GSM) nahm 1982 ihre Arbeit auf. Der GSM900 Standard wurde 1990 eingefroren, 1992 kamen die ersten Mobilfunktelefon auf den Markt. Alle Technologien ab 2G sind durchgehend digital.

Mittlerweile sind GSM, GPRS, EDGE, UMTS und HSDPA in Verwendung (alles 2G/3G Standards). 4G steht vor der Tür.

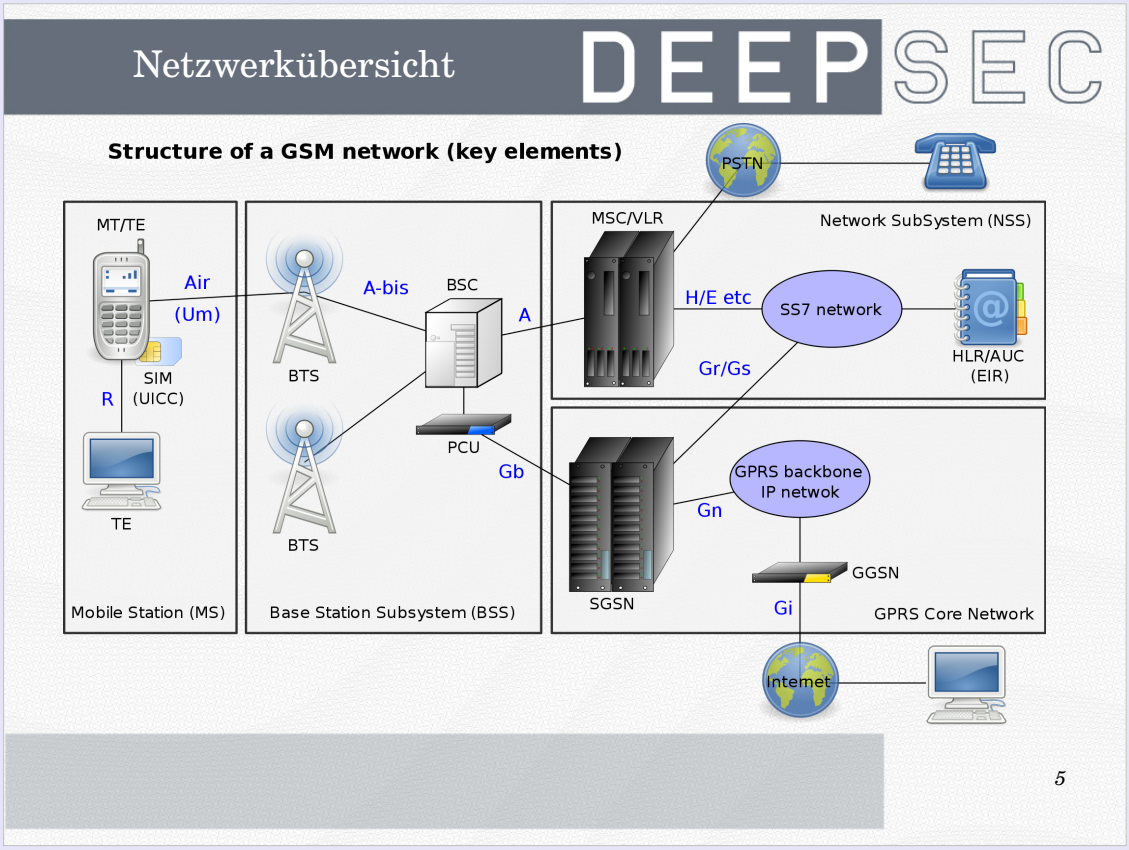
Der Schwerpunkt dieses Vortrags liegt auf GSM (2G). Neuere Protokolle werden meist nicht betrachtet, da den Sicherheitsforschern im Moment nur 2G Ausrüstung für Testzwecke zur Verfügung steht. Das wird sich ändern. Nichtsdestotrotz werden einige Konzepte betrachtet, die sich auf 3G und „intelligente“ Telefone (Smartphones) ausdehnen.



Bevor man über Sicherheit redet, sollte man immer wissen, was man damit meint.

In den seltensten Fällen werden alle Kriterien immer für alle Kommunikationen gleich wichtig sein. Es macht daher sehr viel Sinn eine Klassifizierung einzuführen und nicht alle Daten über die höchste Sicherheitsstufe zu leiten. Dieser Ansatz ist sehr verbreitet und wird auch beim Militär eingesetzt.

Die Standards in der GSM-Welt bestehen aus 1000+ Dokumenten, die jeweils 1000+ Seiten haben können. Die Standards sind prinzipiell publiziert, aber über die Implementationen ist außerhalb der geschlossenen Riege der Hersteller nichts bekannt. Alle Komponenten sind proprietär, es gibt Geheimhaltungsabkommen, und selbst die Mobilfunkanbieter haben wenig bis keinen Einblick in alle Komponenten der Infrastruktur.
Darüber hinaus sind einige Algorithmen per FPGA in Hardware implementiert, d.h. Patches sind unmöglich (es sei denn man möchte landesweit die Basisstationen tauschen, was sehr teuer ist).
Dedizierte Sicherheitsevaluierungen gibt es nicht. Geräte werden auf eine Liste von Funktionen geprüft und sind dann standardkonform.



Zu den Kernkomponenten gehören noch:

•Mobile Switching Center (MSC) – leitet die eigentlichen Anrufe zu/von Teilnehmern, führt Verrechnung durch.

•Home Location Register (HLR) – hält ein Register aller Teilnehmer mit Telefonnummern und Voreinstellungen.

•Visitor Location Register (VLR) – hält ein Register aller Roamingkunden mit deren Telefonnummern und Einstellungen

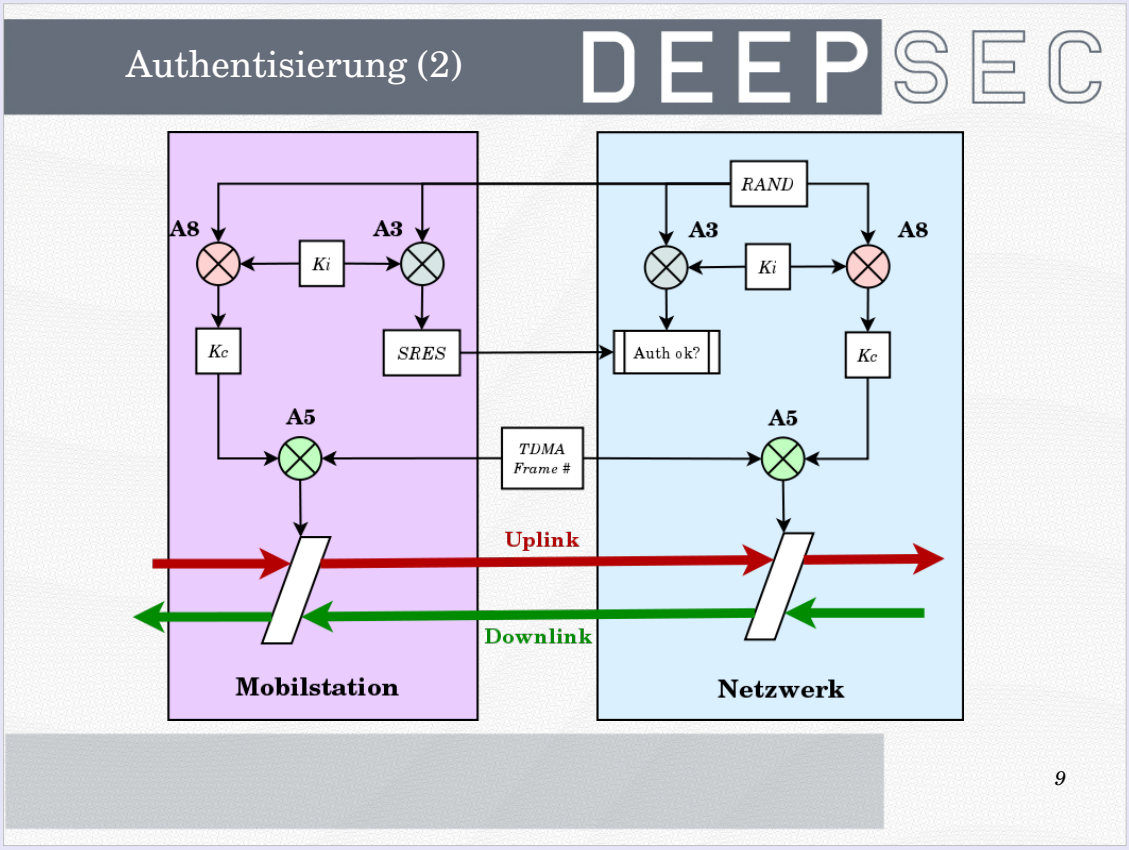
•Equipment Identity Register (EIR) – hält Listen von IMEIs geblockter Endgeräten sowie Geräte, die im Monitoring erfaßt werden (Diagnose, Anruflogs).

Dann kommen noch SMS/MMS Dienste, Mailboxen, Lawful Interception Schnittstellen und andere Subsysteme dazu.

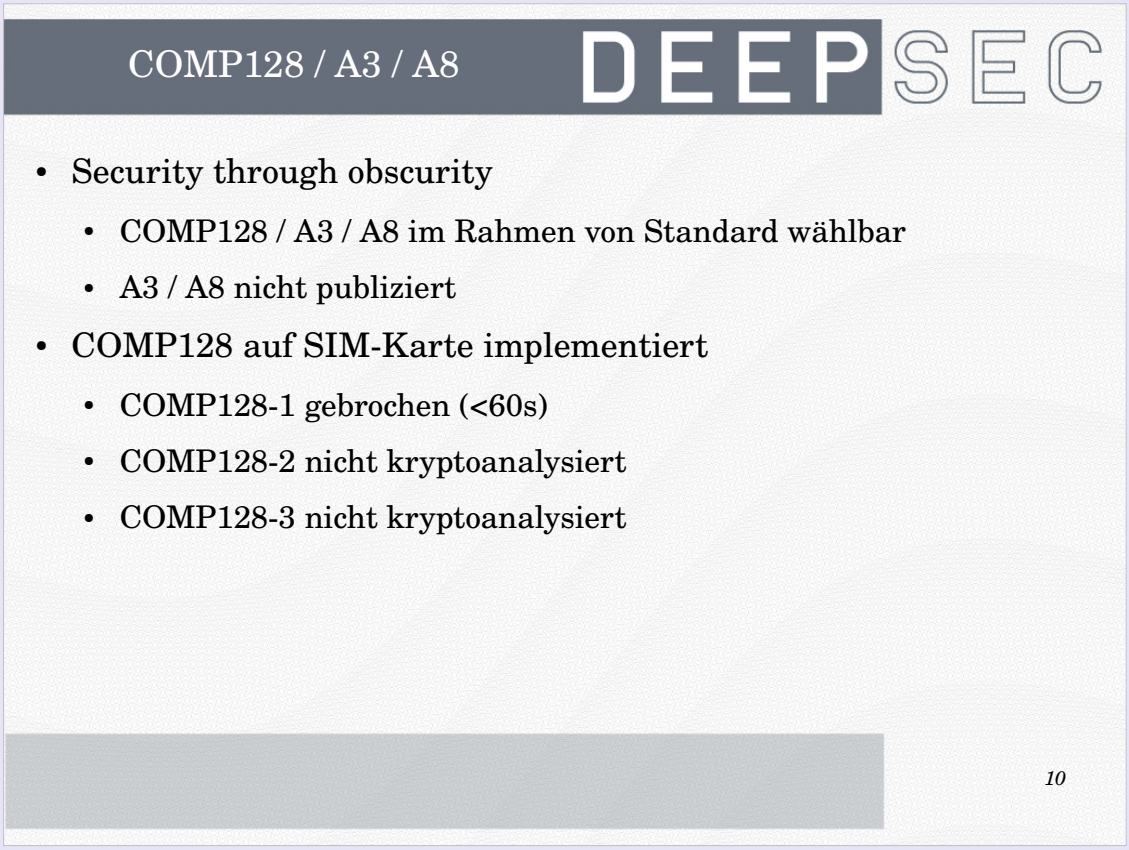
Die IMEI kann man sich so vorstellen wie die Media Access Control (MAC) Adresse von Netzwerkkarten. Sie ist dem Gerät zugeordnet. Die IMSI ist dem Netzwerkteilnehmer zugeordnet und wird so selten wie möglich verwendet, um sie zu schützen. Für den Betrieb wird die temporäre Kennung TMSI generiert und verwendet, ganz analog zu einem Sitzungsschlüssel.

Das Vertrauensmpdell stammt aus der Zeit der staatlichen Telekom-Gesellschaften. Das Netzwerk ist bedingungslos vertrauenswürdig, und alle Clients müssen dem Netzwerk gehorchen. In 2G Netzwerken bedeutet dies, daß die Authentisierung einseitig verläuft. In 3G Netzwerken ist die Authentisierung theoretisch beidseitig, aber es steht den Betreibern frei dies so durchzusetzen. Sicherheitstechnisch muß man also davon ausgehen, daß der Client Teil des Netzwerks ist und sich der eigenen Kontrolle entzieht. Das gilt speziell für alle auf SIM-Karte und Telefon abgespeicherten Daten.
Zwecks Roaming müssen die Mobilfunkbetreiber sich gegenseitig international vertrauen. Theoretisch kann jeder Betreiber bei Kenntnis der IMSI eine Anfrage an das Heimnetzwerk stellen.

Authentisierung und Verschlüsselung benötigt Schlüssel. Der Geheimschlüssel *Ki* ist auf der SIM-Karte und im AuC des Betreiber gespeichert. Der *Ki* wird selten und nie im Klartext verwendet. Stattdessen werden aus ihm Zwischenwerte wie *SRES* und der temporäre Schlüssel *Kc* berechnet. Der Kc wird periodisch geändert (meist einmal pro Einbuchung). Bei den Algorithmen läßt der Standard etwas Freiraum für die Implementation. A3/A8 werden meist als COMP128 zusammengefaßt und sind in der SIM-Karte implementiert.
Die Schlüssellänge von 64 Bit ist kryptografisch nicht mehr zeitgemäß und bezeugt das Alter des Standards.

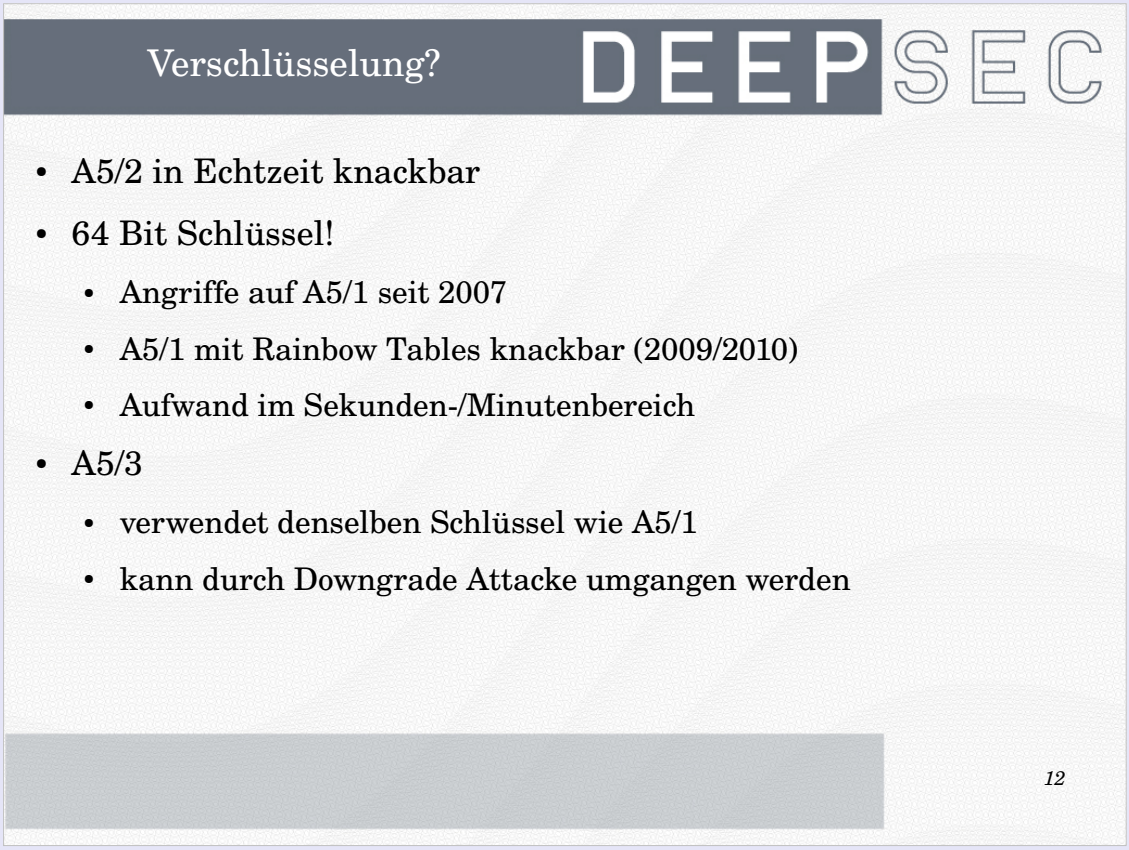


Das Diagramm illustriert welche Komponenten wie kombiniert werden, um den temporären Sitzungsschlüssel *Kc* sowie die Identifikation *SRES* zur Authentisierung zu berechnen. Bei der A5 Verschlüsselung fließt noch die 22 Bit lange Rahmennummer ein, die aus der Mobilkommunikation entnommen wird und sichtbar ist. Verschlüsselt werden beide Kommunikationsrichtungen.

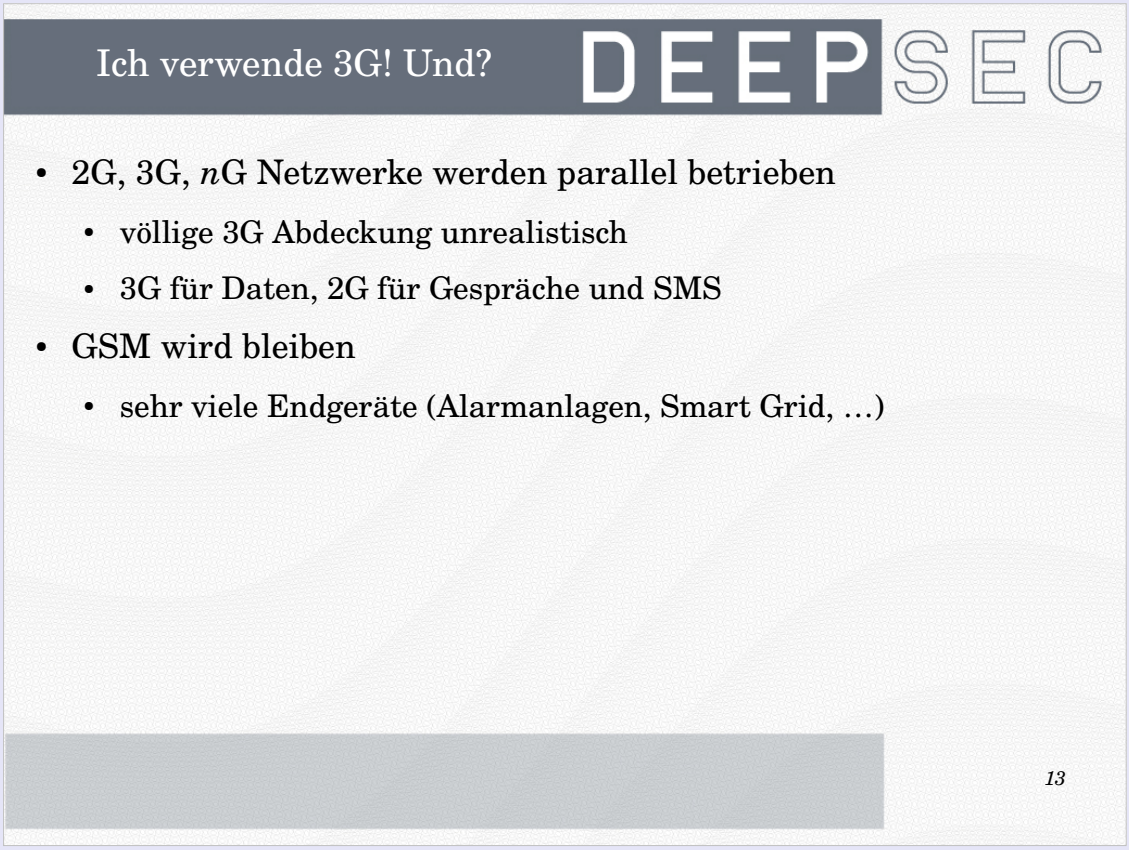


COMP128 ist nicht publiziert, daher gibt es auch keine Peer Review. COMP128-1 wurde von Sicherheitsforschern einem Reverse Engineering unterzogen und machte damit eine Kryptoanalyse möglich, die zu Ungunsten des Algorithmus ausging. Um das Klonen von SIM-Karten zu unterbinden, wurden zwei weitere Versionen des Algorithmus entworfen, die bisher nicht öffentlich untersucht wurden.

A5 stellt mehrere Betriebsmodi zu Verfügung. Der Hintergrund ist eine Auseinandersetzung um die Stärke der Verschlüsselung. Die NATO wollte 1994 eine schwache Verschlüsselung, die deutsche Regierung aufgrund der Grenze zum Warschauer Pakt einen starken Algorithmus. Es gibt daher A5/1 (für westliche Staaten) und A5/2 als Exportvariante. A5/0 bietet keine Verschlüsselung, und A5/3 stammt aus den 3G Standards. Nach wie vor ist A5/1 in Verwendung. Da neuere Telefon A5/2 nicht mehr unterstützen, kann es passieren, daß man in bestimmten Ländern A5/0 benutzen muß, wenn das Netzwerk nur A5/0 und A5/2 spricht (dies ist beispielsweise in Marokko der Fall).

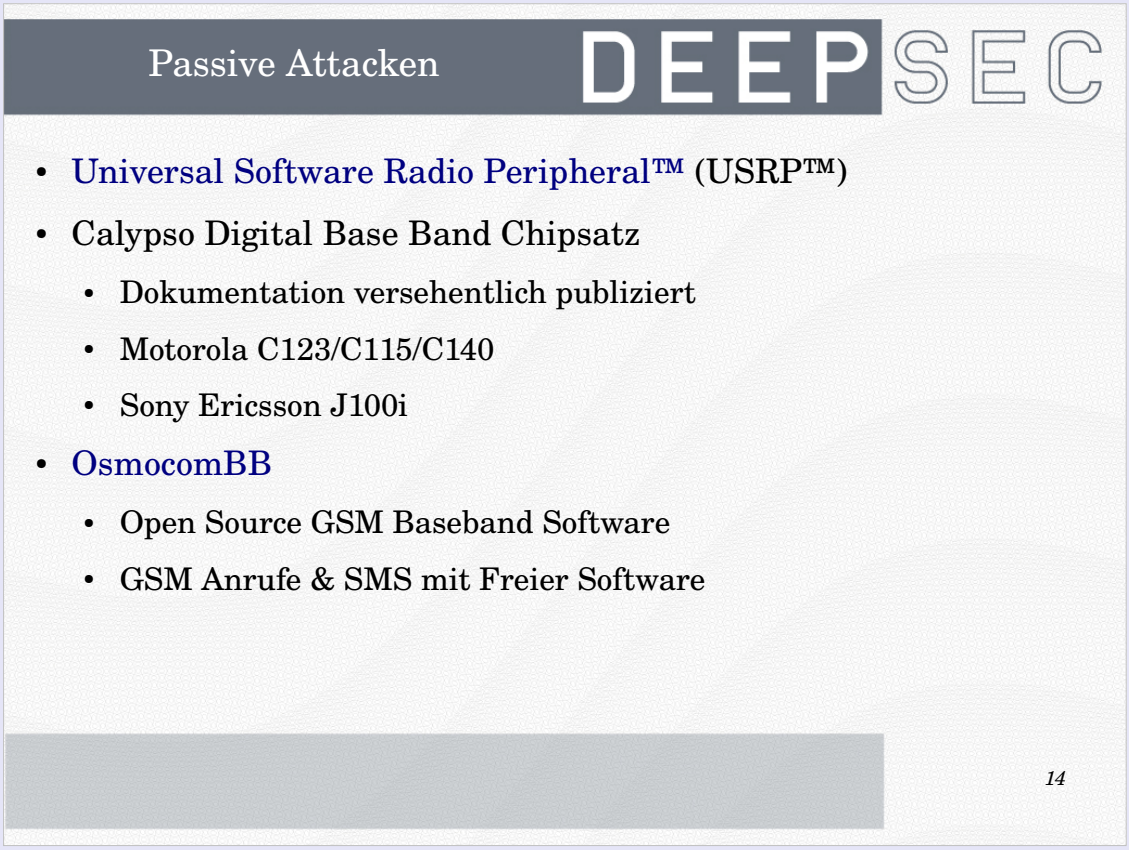


A5/2 ist per Design schwach und kann sehr leicht gebrochen werden. A5/1 wird seit einigen Jahren von Kryptografen angegriffen. Die erste DeepSec Konferenz im Jahre 2007 hatte einen Vortrag eines Sicherheitsforschers zu diesem Thema (2009 und 2010 gab es Folgevorträge). Seit 2010 existieren Rainbow Tables, die das Entschlüsseln von aufgezeichneten A5/1 Kommunikationen möglich machen. Auf modernen PCs liegt die Zeit für das Knacken der Verschlüsselung im Sekunden-/Minutenbereich.
Da A5/3 denselben Schlüssel wie A5/1 verwendet, kann man mit einer Downgrade-Attacke A5/3 auch angreifen. Da A5/3 aber noch nicht weit verbreitet ist, spielt es noch eine geringe Rolle.



2G Netzwerke werden nicht verschwinden, da es Millionen von Endgeräten gibt und geben wird. Die Mobilfunkbetreiber können es sich nicht leisten die Infrastruktur komplett auszutauschen. Darüber hinaus sind die Zellen für 3G für dichte Ballungsräume optimiert, nicht für ländliche Gegenden. 3G wird häufig für Daten eingesetzt, was dazu führt, daß die Gespräche oft auf die 2G Netzwerke geleitet werden, um Datenkapazitäten im 3G-Teil freizuhalten. Mit 4G wird dasselbe passieren, es wird einfach dazukommen.

Durch die Vielzahl der Endgeräte und Anwendungen ist Mobilfunk nun kritischer als eigentlich geplant. Man darf nicht vergessen, daß Mobilfunk nie dafür gedacht war Landleitungen zu ersetzen. Dieser Umstand wird ungerne beworben.



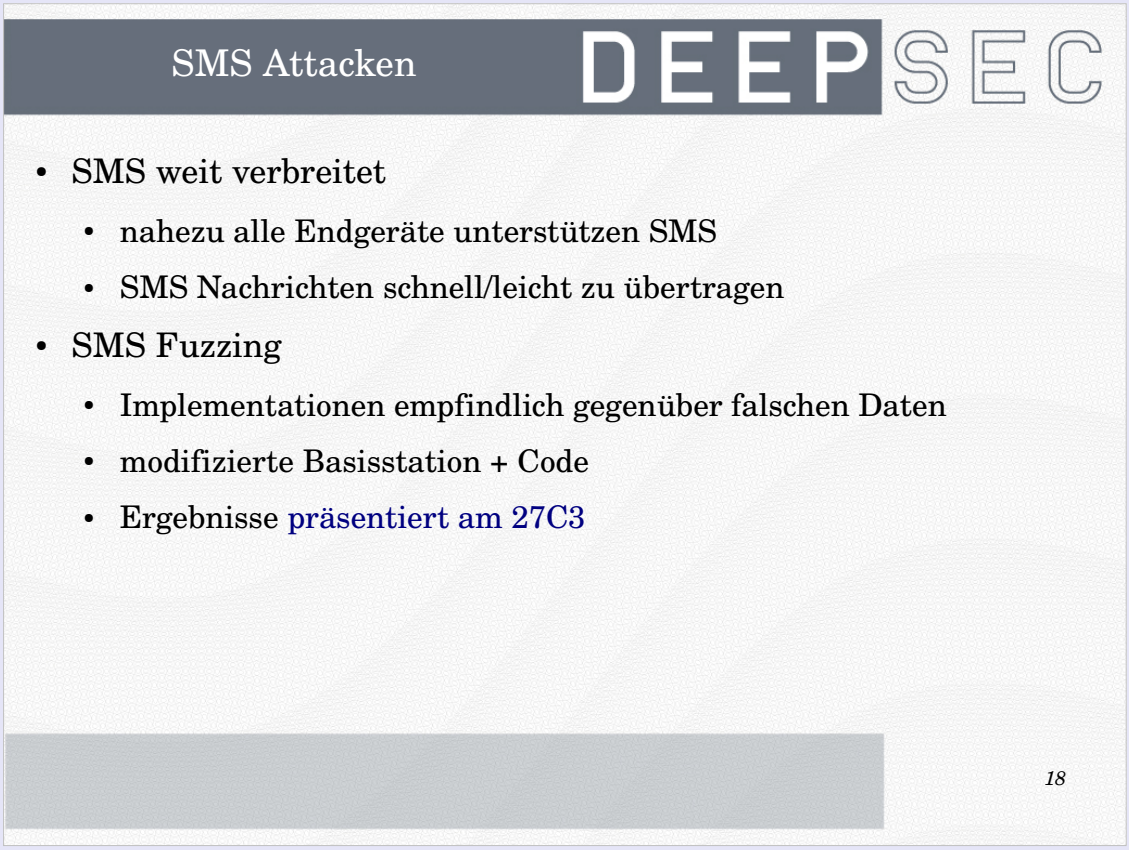
Die Sicherheitsanalyse scheiterte bisher an der proprietären Technologie. Man hat daher begonnen die Funkübertragungen mit frei programmierbaren Software-Radios wie USRP zu analysieren. Mittlerweile läßt sich der Calypso Baseband Chipsatz von Texas Instruments auch einsetzen, da die Dokumentation geleckt ist. OsmocomBB ist eine Software, mit der man eine Basisstation auf Basis Freier Software betreiben kann. Dieses Werkzeug ist sehr wichtig, und es wurden damit testweise schon GSM-Netzwerk betrieben. Die Entwicklung hat sich als sehr förderlich für Sicherheitsbetrachtungen herausgestellt, da man so auch Mobilfunkgeräten bei der Komunikation zuschauen kann.

Für aktive Attacken muß man ein GSM Netzwerk aufbauen, sei es auch nur in kleinem Rahmen. Da das mobile Endgerät das Netzwerk nicht authentisiert, sind Mittelsmenschattacken dann sehr leicht möglich. Es gilt hier auch wie bei anderen Technologien: Das stärkste Signal gewinnt. Natürlich kann man wie in jeder funkgestützten Kommunikation auch Störsender einsetzen, allerdings ist der Betrieb nicht erlaubt, und bestimmte Modulationen lassen sich nicht so einfach stören (das ist beispielsweise bei 3G der Fall).

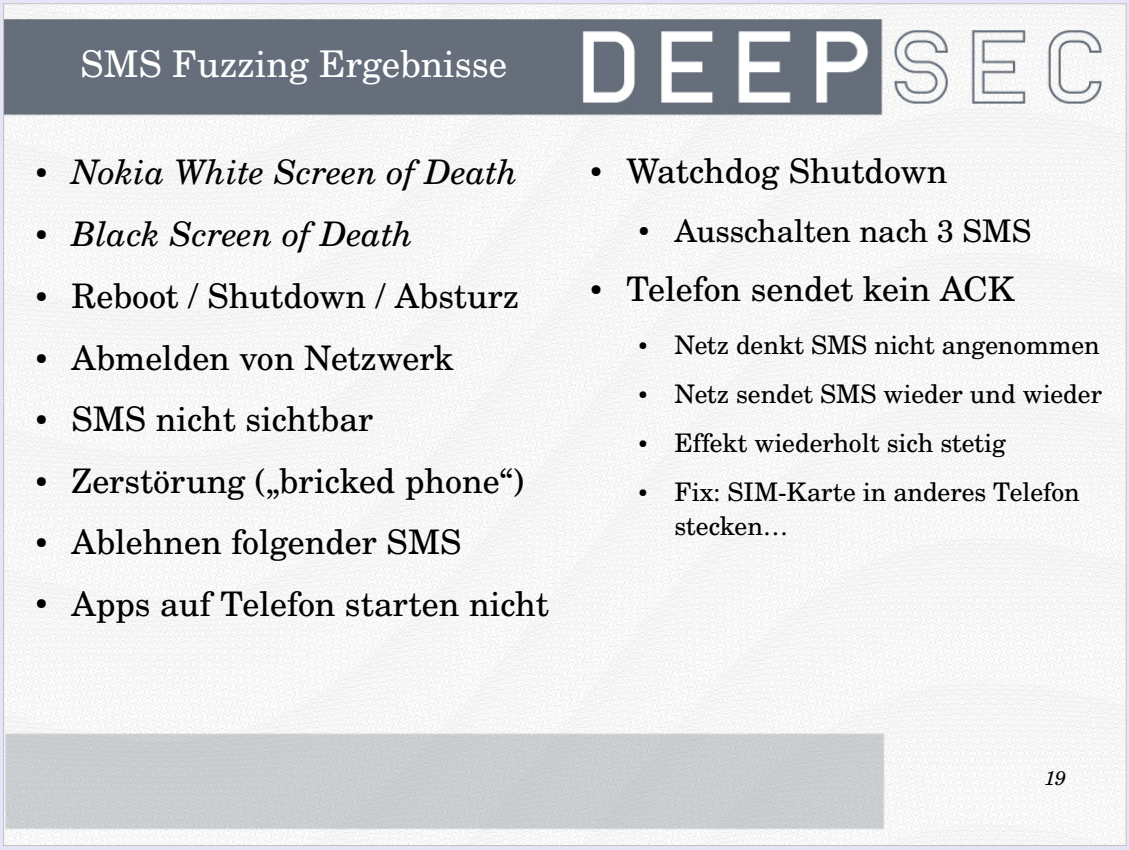
Auf der DeepSec 2009 wurde von Dieter Spaar gezeigt, daß man Basisstationen mit „unfreundlichen“ Transmissionen deaktivieren kann (Absturz/Reboot). Durchgeführt wurde dieser Angriff mit einem Mobiltelefon, welches frei programmierbar war. Diese Attacke benötigt keine Störsignale, keine große Leistung und nur wenig Zeit. Ursache ist ein Designfehler im GSM-Protokoll.
Laut Karsten Nohl betrifft der Fehler so ziemlich alle Basisstatio
. Wenn man sich jetzt vorstellt, daß man ein Bündel Telefone (eines pro Netzanbieter) per Straßenbahn oder Auto durch die Straßen einer Stadt schickt, dann wird klar wie anfällig Mobilfunknetzwerke gegenüber koordinierten Angriffen sind.

Aktive Attacken

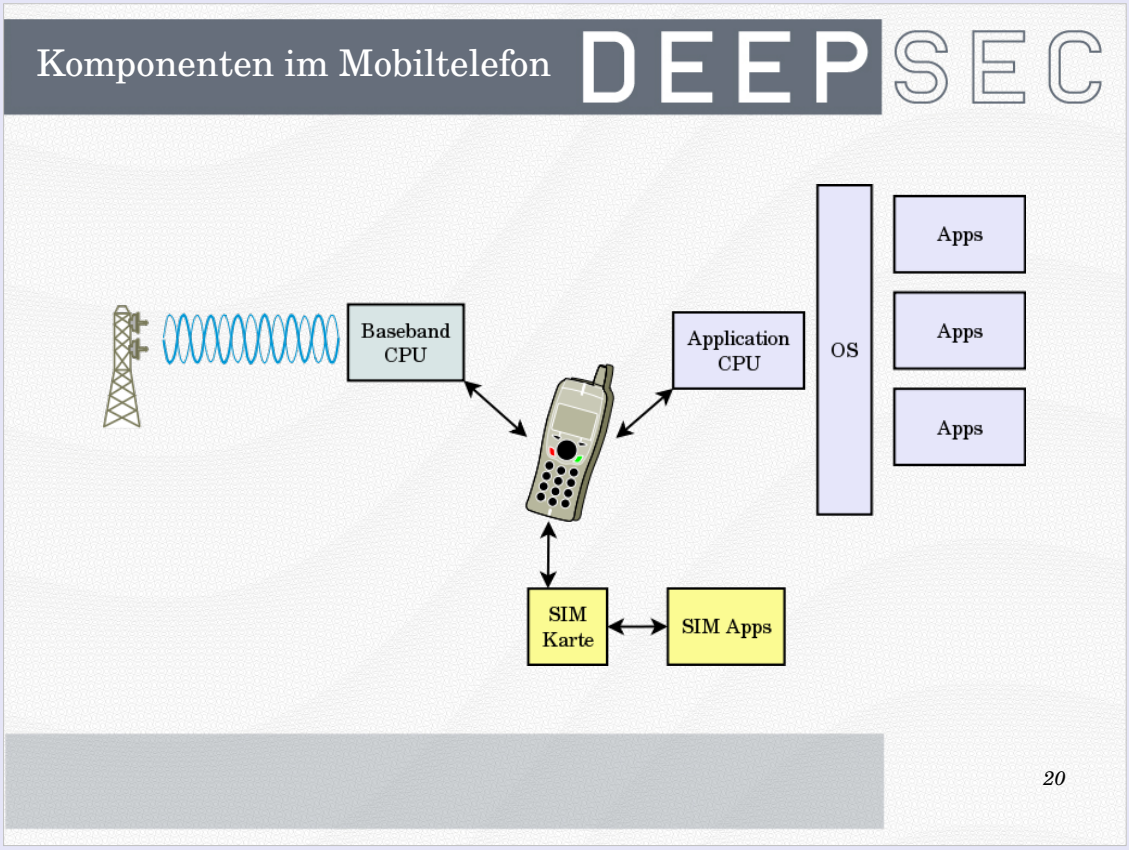
- Client verlangt keine Authentisierung
  - Aufbau von „rogue base stations“
  - stärkste Basisstation gewinnt
  - Man-In-The-Middle
  - Lokalisierung für gezielte Attacke notwendig
- Störsender
  - rein physikalische Attacke
  - Sendeleistung/Frequenzen problematisch



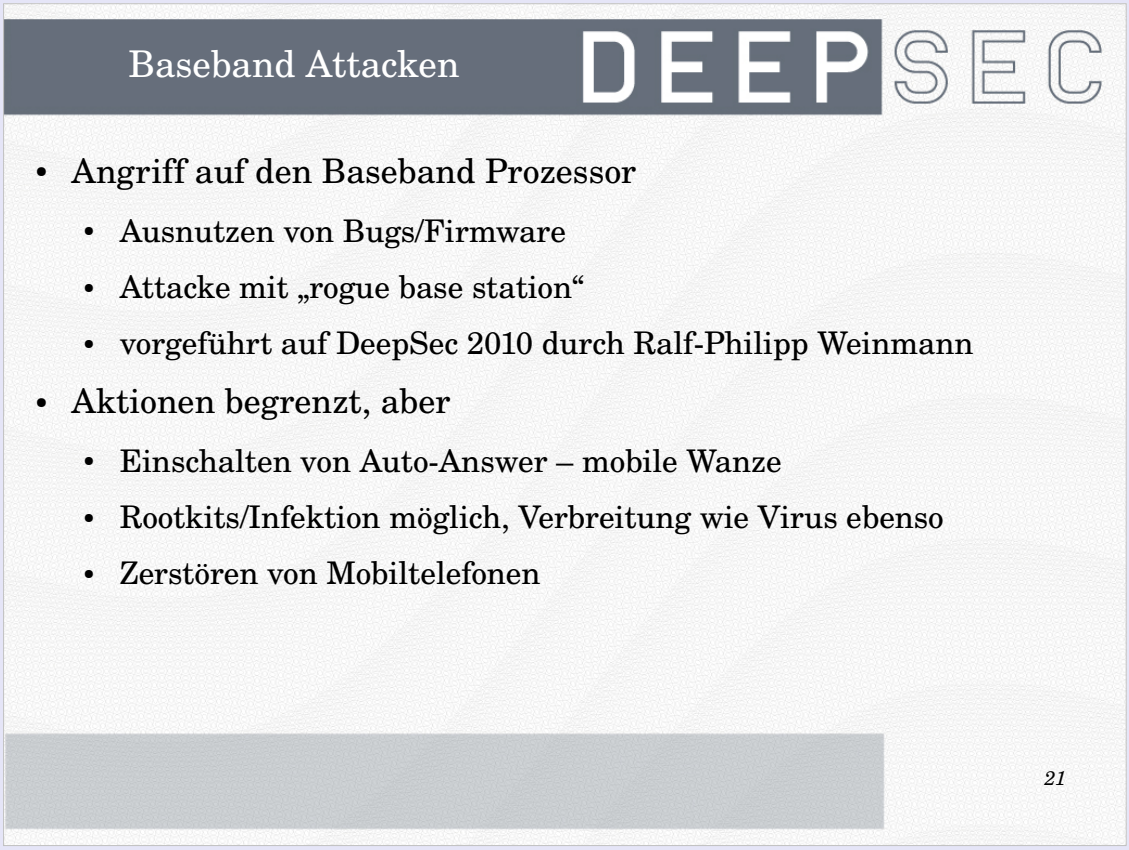
Jährlich werden Milliarden von SMS Nachrichten verschickt. Das Format ist standardisiert, aber was passiert, wenn man ungültige Sequenzen einbaut? Nicht alle Implemetation verstehen das Konzept „fail gracefully“. Durch Techniken wie „fuzzing“, dem gezielten Generieren und Abschicken von manipulierten SMS Nachrichten, kann man Fehlern in der SMS-verarbeitenden Software auf die Spur kommen. Colin Mulliner und Nico Golde haben am 27C3 die Ergebnisse ihrer Tests mit sogenannten Feature Phones (keine Smartphones) präsentiert.



Hier sind einige Effekte aufgeführt, die den Telefonen nach Annahme der Test-SMS-Nachrichten widerfahren sind. Neben völliger Deaktivierung war auch ein Fall eines „bricked phones“ dabei. Manche SMS wurden auch still empfangen, d.h. man konnte am Mobiltelefon nichts vom Empfang bemerken. Auf diese Art und Weise könnte man Telefon deaktivieren, ohne daß man davon etwas mitbekommt. Beim Effekt „Telefon sendet kein ACK“ wird das Schad-SMS vom Netzwerk wiederholt gesendet, d.h. man kann dann sein Telefon nur wieder benutzen, wenn man die SIM-Karte kurzzeitig in ein Telefon eines anderen Herstellers steckt, das SMS empfängt und dann die SIM-Karte wieder wechselt.



Man darf nicht vergessen, daß moderne Mobiltelefone aus mehreren Subsystemen bestehen, die eine eigene CPU haben. Baseband, SIM-Karte und Betriebssystem sind unabhängig. Nur wenn die Hersteller Schnittstellen einbauen, dann kann man auf diese Bereich zugreifen. Der Baseband-Prozessor ist immer abgeschirmt (es gibt auch keine verfügbare Dokumentation über den Baseband-Teil). Die SIM-Karte stellt auch eine eigene Umgebung für Embedded Java™ bzw. eigenen Code zur Verfügung (Intel® 8051 Derivat). Selbst ohne Smartphone bleibt da genügend CPU und RAM für Attacken.
Baseband und SIM-Karte zählt zur Netzinfrastruktur.



Man kann den Baseband Prozessor über die Luftschnittstelle angreifen. Auf der DeepSec 2010 wurde ein solcher Angriff demonstriert (Angriff ist für iPhones und Google Android verfügbar). Durch die geringen Resourcen in diesem Bereich kann man nicht viel tun, aber das Einschalten des Mikrofons per Anruf sowie Zerstörung und sogar das Verbreiten von Schadcode sind möglich. Letzteres wird gerade untersucht, laut Auskunft des Sicherheitsforschers ist es denkbar.

Applikationen auf SIM-Karten führen ein Eigenleben, welches vom Mobilfunknetz bestimmt wird. Nur Endgeräte, die eine Schnittstelle zu diesen Apps haben, können diese sehen und mit ihnen Daten austauschen. Manche Smartphones haben keine solche Vorkehrung. SIM Apps werden gerne von Banken verwendet, um zusätzliche Verschlüsselung einzubauen (speziell afrikanische Banken machen das). Natürlich können SIM Apps auch mißbraucht werden. Updates geschehen meist vom Besitzer unbemerkt über die Luftschnittstelle.

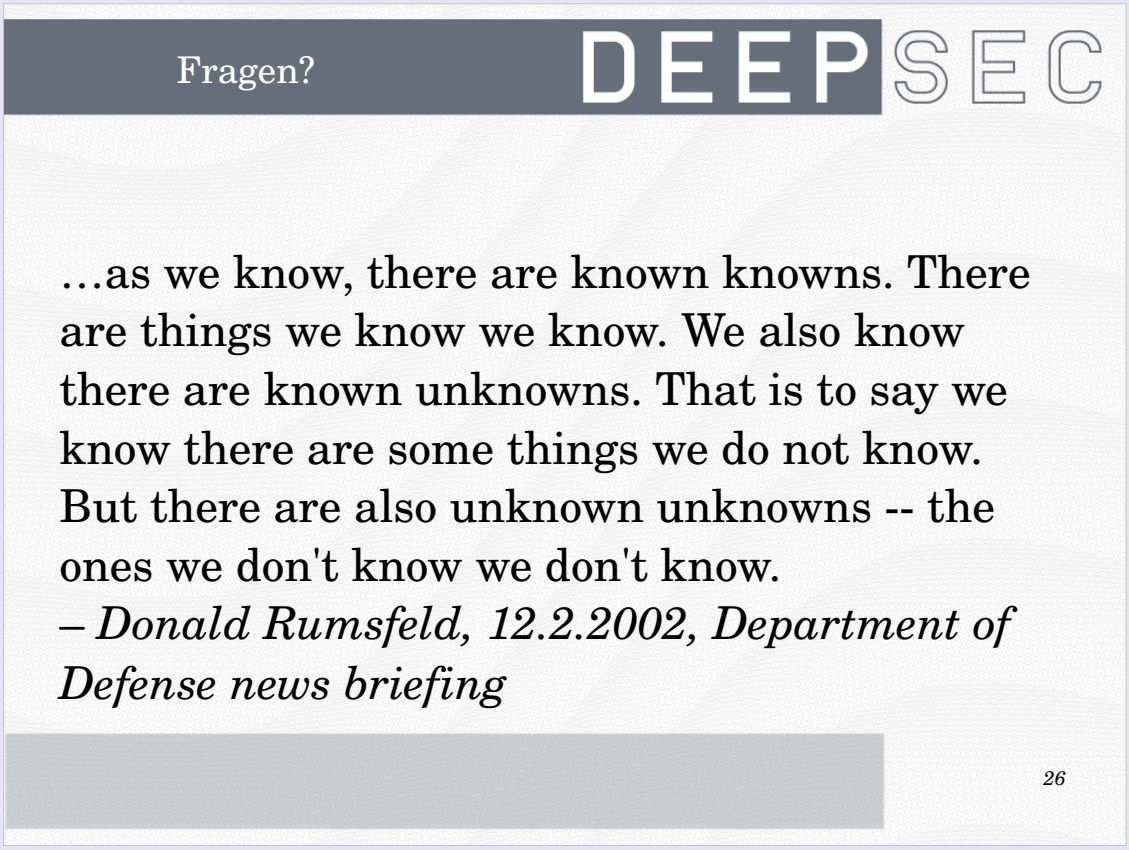
iOS und Android sowie andere Smartphone Systeme haben sich in den letzten Jahren stark verbreitet. Sie sind zwar immer noch in der Minderheit, verglichen mit den Milliarden von „dummen“ Endgeräten, aber durch die zur Verfügung stehenden Applikationen wurde schon Schaden angerichtet. Die Tendenz den App Store Betreibern zu vertrauen senkt die Hemmschwelle unbekannte Software zu installieren (das Phänomen ist von PCs bereit bekannt). Die Tatsache, daß Sicherungen periodisch geknackt werden (siehe iPhone Jailbreaking) zeigt, daß man Geräte, die man aus der Hand gibt, nicht vollständig abgesichert werden können.

Dieser Vortrag ist eine Zusammenfassung vieler anderen Vorträge, Workshops und Konferenzen, allen voran der Materialien, die auf den vergangenen DeepSec Konferenzen publiziert wurden. Wir danken allen Sicherheitsforschern, die den Schleier der Verheimlichung durchstoßen und die ganzen Sicherheitsprobleme aufgedeckt haben.

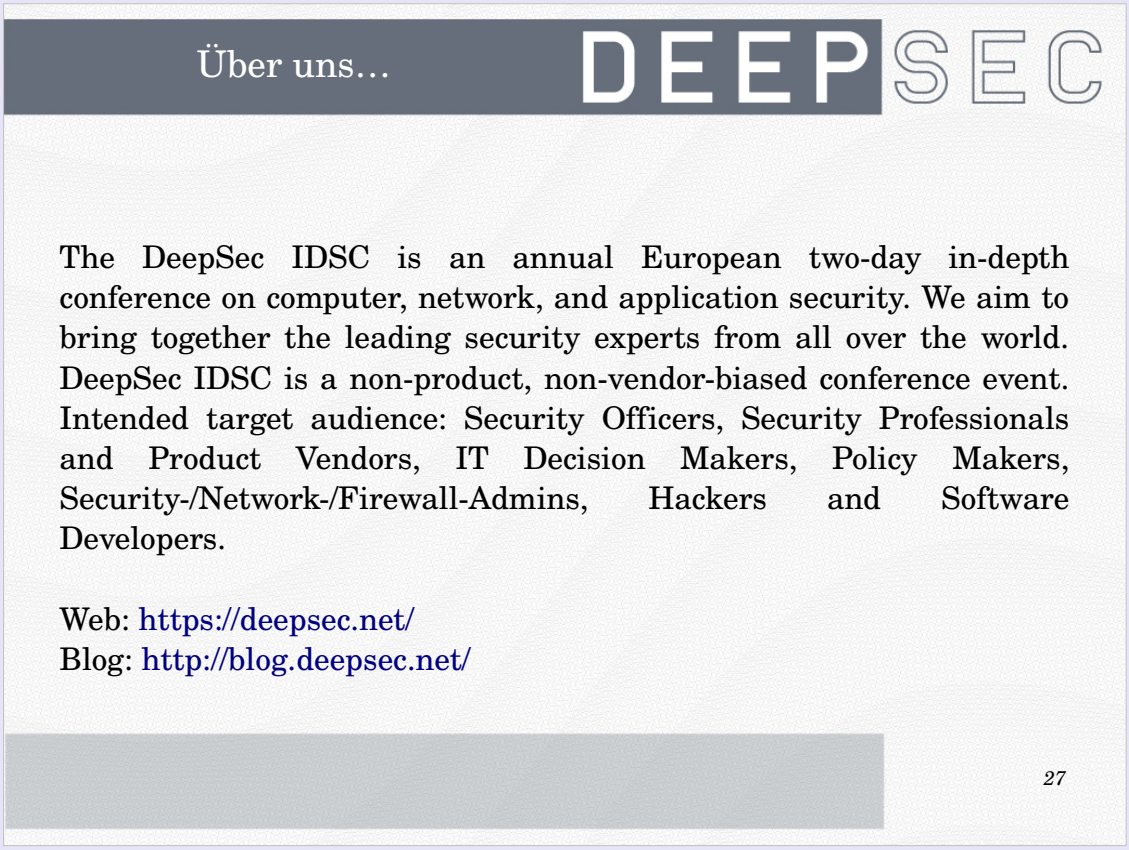
Gegenmaßnahmen

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



Herr Rumsfeld macht deutlich wie wichtig das ständige Hinterfragen von vermeintlichen Tatsachen und Fakten ist, auch wenn das Zitate aus einem anderen Kontext stammt.



Wir freuen uns über jegliches Feedback, Kommentare im Blog, interessierte Sponsoren für die jährliche DeepSec Konferenz, Teilnehmer, Anregungen für Sicherheitsthemen, eigene Erfahrungen und sonstigen regen Austausch. Wir bieten bei Anrufen keine sichere Kommunikation, man kann uns aber verschlüsselt Nachrichten via E-Mail oder Webseite zukommen lassen.

Danke für Ihre Aufmerksamkeit!