POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

rechtsstaatlich • bürgerorientiert • professionell

Nano Mobilfunkzelle in der IT-Forensik

Eine Kooperation zwischen der FH Aachen und dem LKA NRW

Inhalt

POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

- **Vorstellung**
  - Kooperation
- Aufgabenstellung / Ziele
- Das GSM Mobilfunknetz
- Marktschau
- openBSC & nanoBTS
- Software Projektarbeiten
- Fazit & Ausblick

Vorstellung

POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

- Philip Schütz, B.Sc., LKA NRW
  Cybercrime-Kompetenzzentrum,
  SG42.2 IuK-Ermittlungsunterstützung, IT-Forensik

- Rolf Stöbe, B.Sc., FH Aachen
  Studiengang: Master Information Systems Engineering

Kooperation

POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

- 2012
  - Kooperationsvertrag zwischen FH Aachen und LKA NRW
    - Praxissemester mit den ersten beiden Studenten

- 2013
  - Zwei Abschlussarbeiten beim LKA NRW
  - Eine neue Abschlussarbeit begonnen
  - Ein weiterer Student im Praxissemester

Inhalt

POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

- Vorstellung
- **Aufgabenstellung / Ziele**
  - Rechtliche Aspekte
  - Eigene Mobilfunkzelle
- Das GSM Mobilfunknetz
- Marktschau
- openBSC & nanoBTS
- Software Projektarbeiten
- Diskussion/Fragen

Aufgabenstellung / Ziele

- Malwareerkennung durch Aktivitäten im Testnetz
  - Möglichkeit 1: WLAN
    Nachteil: Geräte ohne WLAN, keine SMS
  - Möglichkeit 2: GSM-Netz Daten überwachen
    Vorteil: Alle Daten können erfasst werden

Rechtliche Aspekte

- Umsetzung mittels Überwachungsmaßnahmen
  - Testmaßnahmen müssen bei der BNetzA angemeldet werden.
  - Die probeweise Anwendung der Überwachungsfunktionen richtet sich nach § 23 TKÜV und ist auf das unabdingbare Maß zu begrenzen und nur zulässig zur Funktionsprüfung der Aufzeichnungs- und Auswertungseinrichtungen der berechtigten Stellen.
  - **Daher können Testüberwachungsmaßnahmen leider nicht zur Verfügung gestellt werden.**

Ziel: Eine eigene Zelle …

Eigene Mobilfunkzelle

POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

- Langzeitüberwachung eines Telefons
- Spioniert mein Handy mich aus?
- Verhalten von Apps analysierbar
- Reagiert das Handy auf Interaktionen von außen?
  - Eingehender Anruf / SMS …

- Alterung von Vergleichsgeräten
  - SMS / MMS mit eigenen Inhalten
  - SMSC konfigurierbar (Zeitstempel)
  - Wie sehen Daten im Netz aus

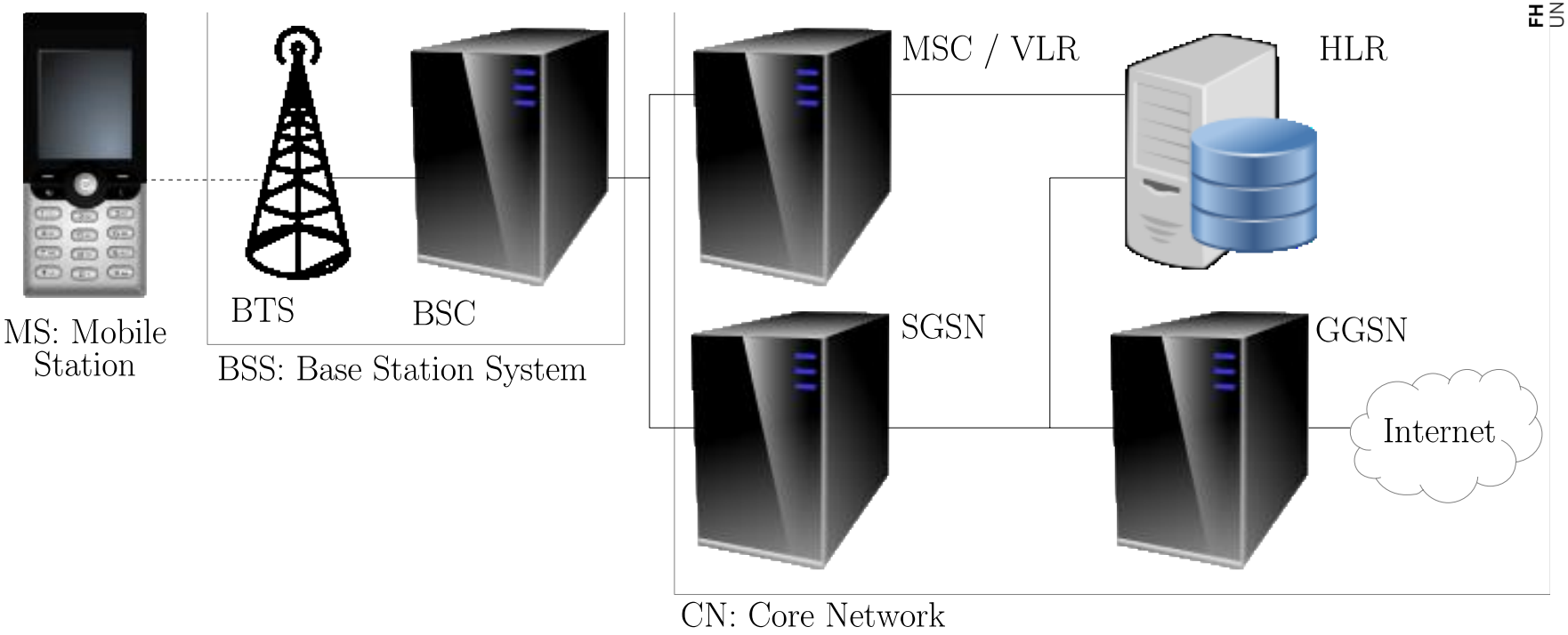
Inhalt

POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

- Vorstellung
- Aufgabenstellung / Ziele
- **Das GSM Mobilfunknetz**
- Marktschau
- openBSC & nanoBTS
- Software Projektarbeiten
- Fazit & Ausblick

Das GSM Mobilfunknetz



BTS: Base Transceiver Station
BSC: Base Station Controller

Inhalt

- Vorstellung
- Aufgabenstellung / Ziele
- Das GSM Mobilfunknetz
- **Marktschau**
  - WLAN
  - professionelle Messgeräte
- openBSC & nanoBTS
- Software Projektarbeiten
- Fazit & Ausblick

- openBTS & WLAN
- openBSC & nanoBTS

WLAN

- Einfach abzuhören
- Keine zusätzliche Hardware nötig
- Nicht alle Handys haben WLAN
- Keine GPRS/UMTS-Datenverbindung
- Nicht geeignet für Alterung von Handys
  - Keine Anrufe
  - Keine SMS

openBTS & WLAN

- Vorteile wie WLAN
- Zusätzliche BTS
  - Komplizierter Aufbau
- Anrufe und SMS sind möglich
- Kosten: ~ US$ 1.200

Quelle: http://www.ettus.com

Professionelle Messgeräte

- Zum Beispiel: Agilent 8960 oder Rohde & Schwarz CMU200
- Umfangreiche Funktionen
  - Analyse der Funkschnittstelle, Frequenzspektren, ...
- Fertiger Aufbau in einem Gerät
  - Kann Anrufe tätigen/empfangen, SMS senden/empfangen
  - GPRS-Datenverbindung
- Zugehörige Software kann Protokolle analysieren
- Kosten: ~ 100.000€

openBSC & nanoBTS

POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

- Fertige BTS (ip.access nanoBTS)
- Fertiges Network-in-the-Box (sysmoBSC)
- Trotz fertiger Hardware alles weitgehend frei konfigurierbar
- GPRS/EDGE-Datenverbindung abhörbar
- SMS senden/empfangen, SMS „abhörbar“
- Anrufe (bisher nur mit zweitem Handy)
- Kosten: ~ 8.000€

- Bezug über Fa. sysmocom GmbH (http://www.sysmocom.de)

Inhalt

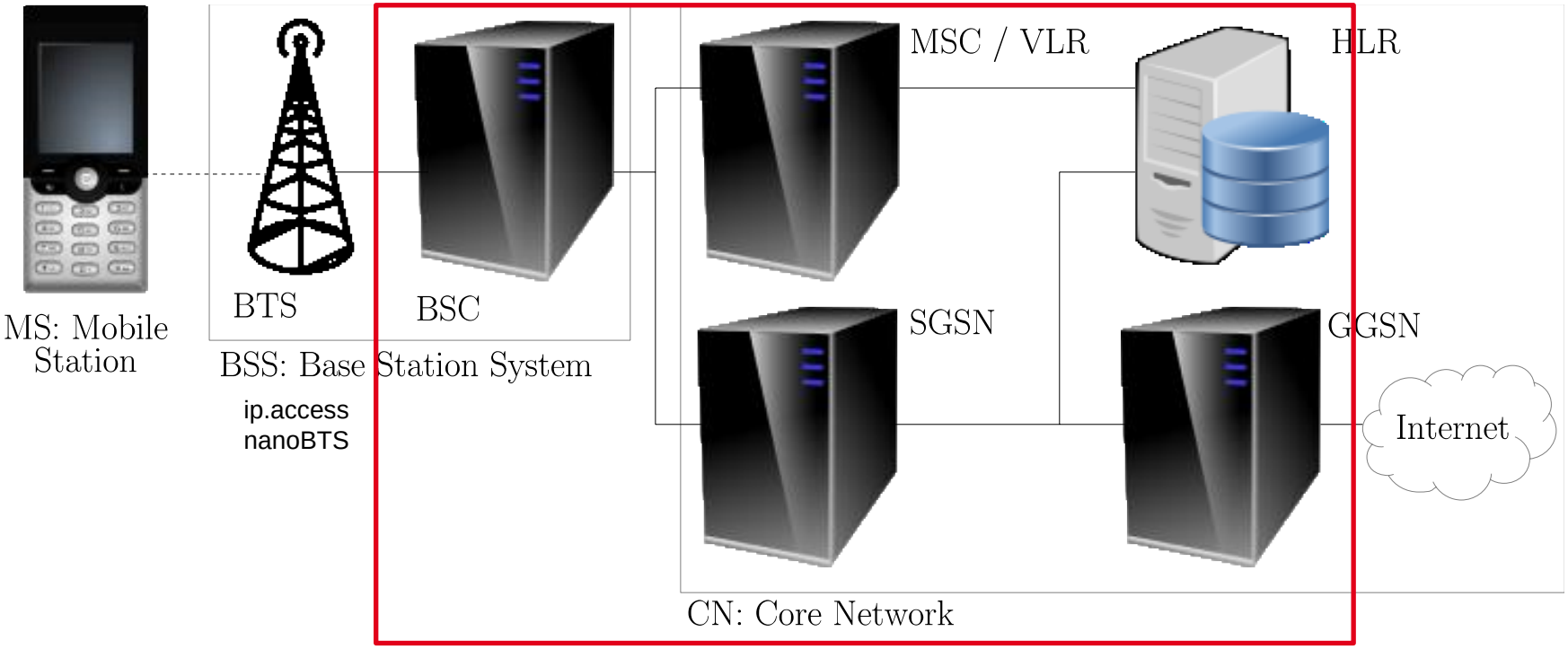
POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

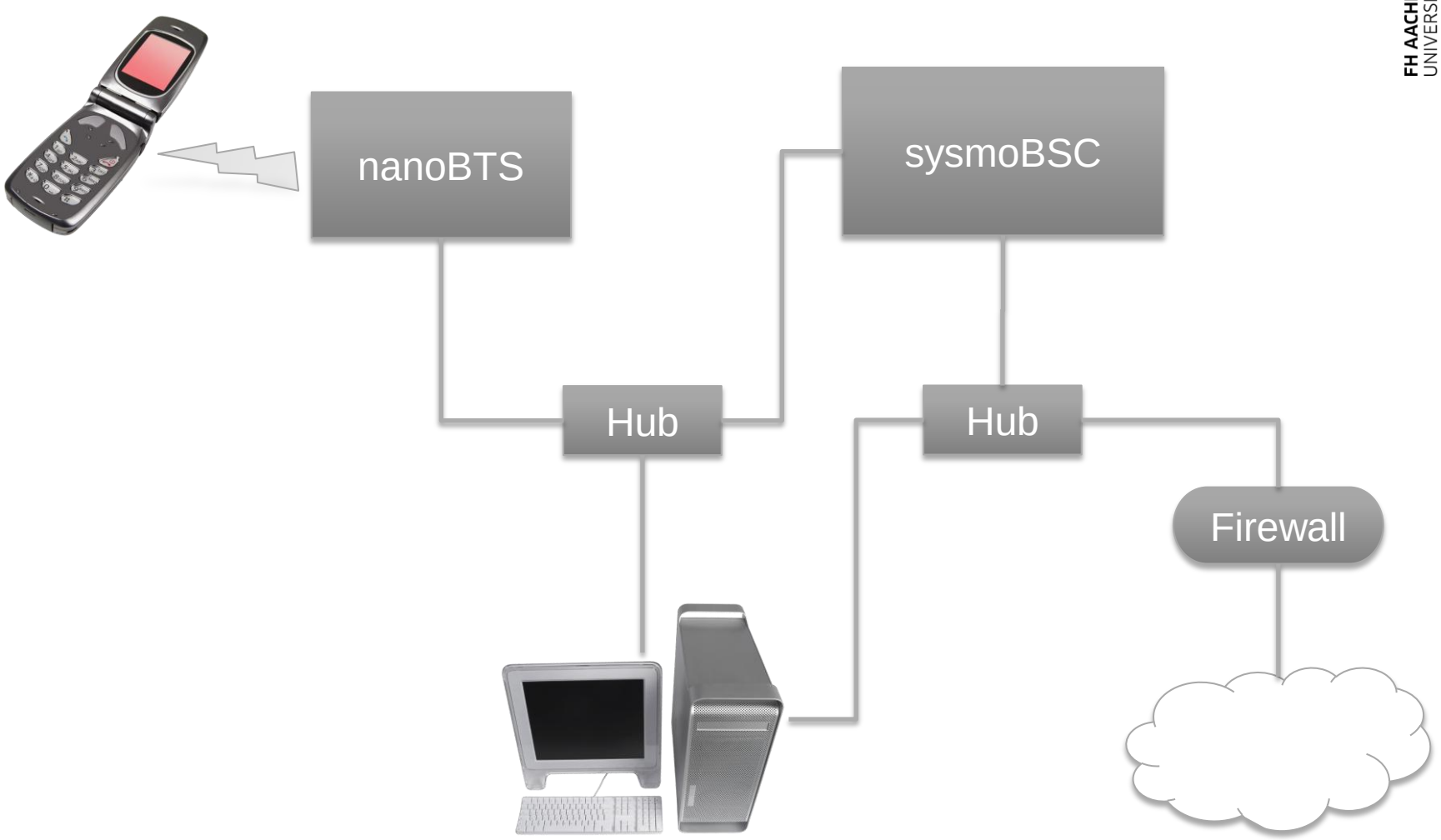
- Vorstellung
- Aufgabenstellung / Ziele
- Das GSM Mobilfunknetz
- Marktschau
- **openBSC & nanoBTS**
  - Hardwareaufbau
  - Einschränkungen
  - BNetzA Betriebsvorgaben
- Software Projektarbeiten
- Fazit & Ausblick

openBSC & nanoBTS

- sysmoBSC fungiert als NITB, beinhaltet: BSC, HLR, SMSC, SGSN, GGSN



Hardwareaufbau



Einschränkungen

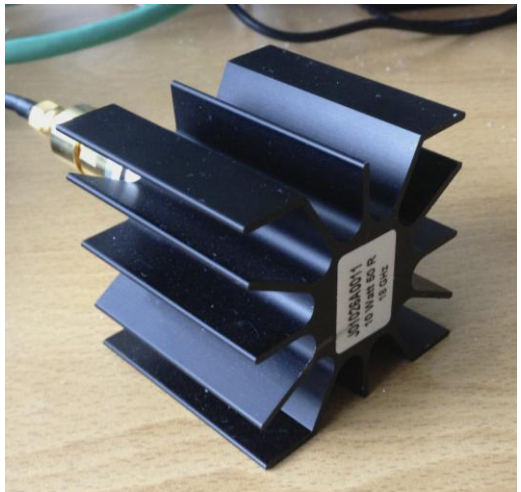
- Kein UMTS/LTE
- Keine Anrufe/SMS ins „richtige“ Netz
- Keine Anrufe/SMS aus dem „richtigen“ Netz
- Datenverkehr über SSL bleibt verschlüsselt

Betriebsvorgaben BNetzA

Bei einer Mobilfunkzelle "...*handelt es sich generell um eine ortsfeste Sendeanlage, die elektromagnetische Aussendungen in genehmigungspflichtigen Frequenzbändern durchführt*".

Aber:

„Der Aufbau und die Inbetriebnahme einer Mobilfunkzelle außerhalb der Abschirmkabine [...] kann erfolgen, wenn eine hochfrequente Aussendung durch Verwendung einer „Dummyload" (künstliche strahlungsarme Antenne) ausgeschlossen werden kann..."



Inhalt

POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

- Vorstellung
- Aufgabenstellung / Ziele
- Das GSM Mobilfunknetz
- Marktschau
- openBSC & nanoBTS
- **Software Projektarbeiten**
  - Alterung von Mobilgeräten
  - Malwaredetektion
- Fazit & Ausblick

Software Projektarbeiten

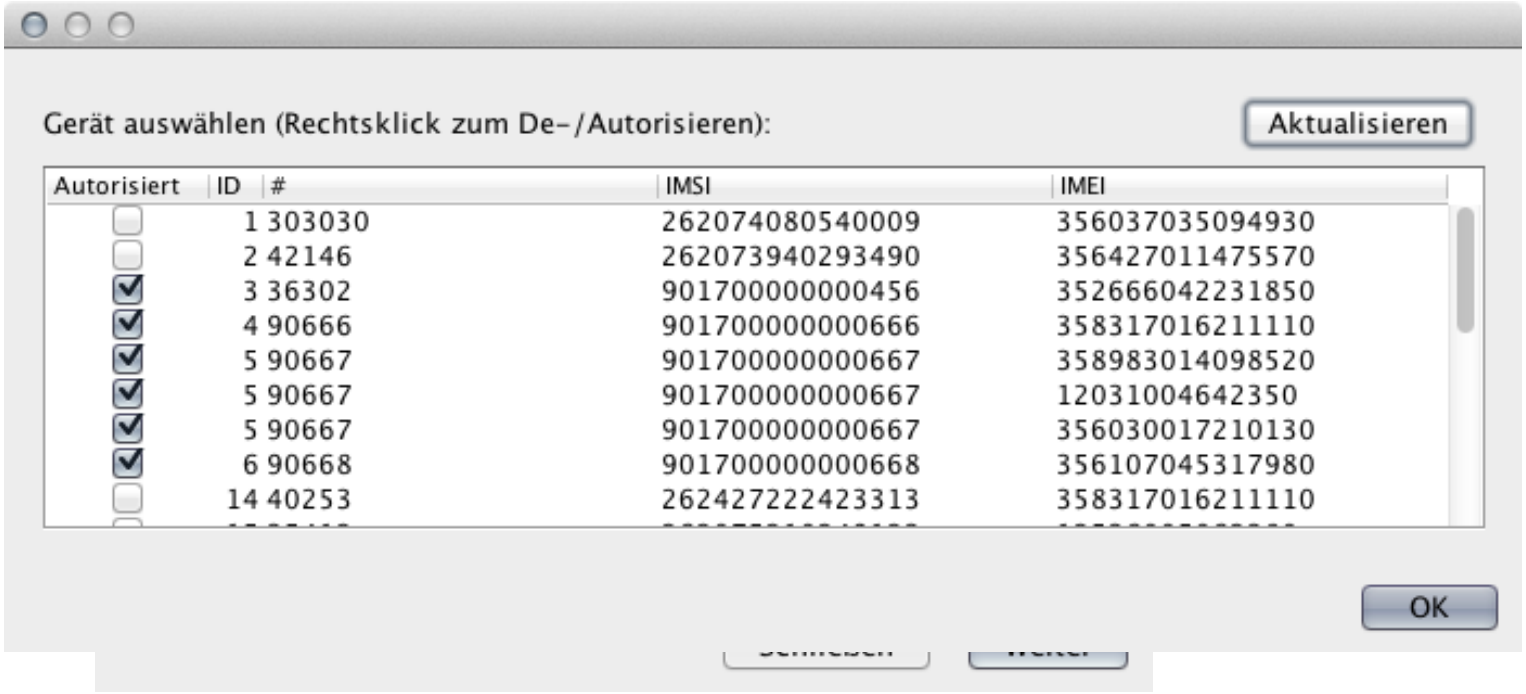
- Abschlussprojekte für Informatik Bachelor-Studium
- Praxissemester (März - September 2012)
  - Marktschau
  - Beschaffung und Aufbau Mobilfunkzelle
- Abschlussprojekte (Oktober 2012 - Februar 2013)
  - „Programm zur Alterung von mobilen Geräten zur gezielten forensischen Analyse“ (Rolf Stöbe)
  - „Programm zur forensischen Überwachung und Analyse von mobilem Datenverkehr“ (Philip Schütz)

Aufgabenstellung

- Programm zur Alterung von Mobilgeräten
  - SMS-Inhalt selbst definierbar
  - Anrufe erfassen
  - Szenarien absenden
  - Bericht über eingebrachte Daten
  - Erweiterbar
- Einsatzzwecke des Programms
  - Untersuchung von zerstörten Handys
  - Schulungsvorbereitung
  - Funktionstest für Forensik Tools

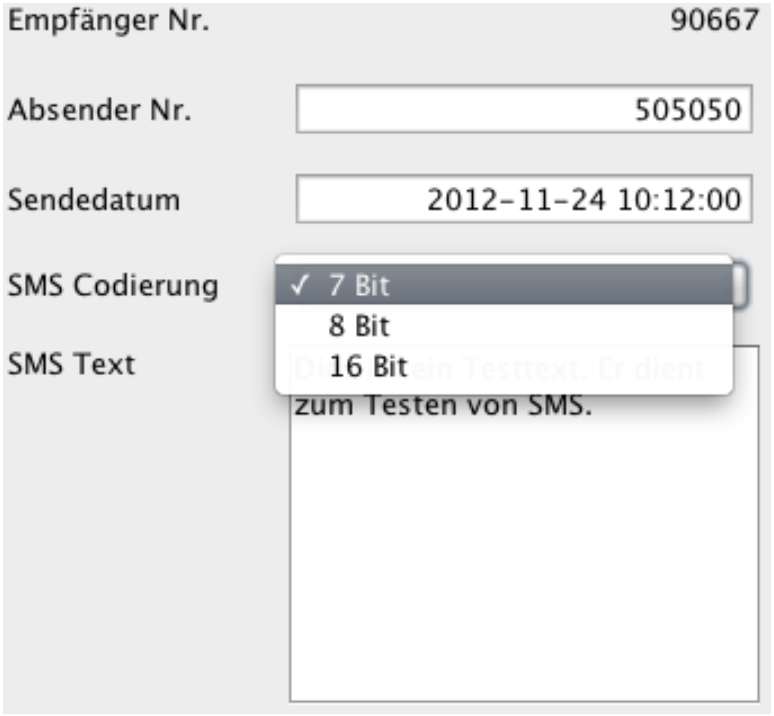
Allgemeine Programmfunktionen

- Netzwerkeinstellung anpassbar
  - MCC/MNC/Name
- Gerät für Zugriff auswählbar
  - Autorisierbar



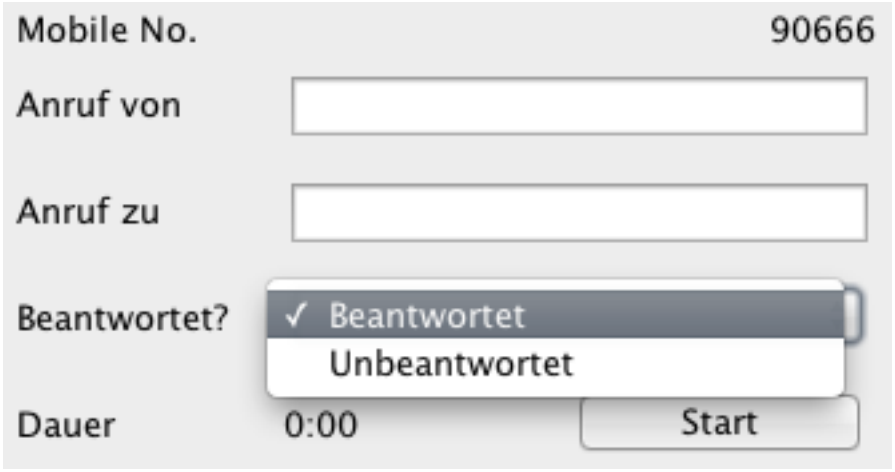
SMS & Szenarien

- Absendernummer wählbar
- Datum auswählbar
- Codierung wählbar
  - 7 Bit Standardcodierung
  - 8 Bit Binärcodierung
  - 16 Bit
- Text frei wählbar
- Szenarien
  - Viele selbstdefinierte SMS
  - Unbeaufsichtigte Zustellung



Anrufe

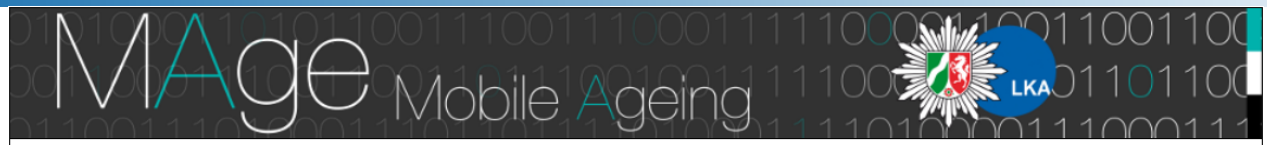
- Absender und Empfänger eintragbar
- (Un-)Beantwortet
  - Beantwortet automatischer Timer
- Anrufe von User selbst auszuführen



Berichtgenerierung

- Alle Daten die ans Mobilgerät gesendet wurden
  - In GUI Kurzbeschreibung
  - HTML Bericht erzeugt auf Anfrage
- Detailansicht zu Einträgen im Bericht
  - Anrufdauer
  - SMS Sendezeiten
  - SMS PDUs
- Handydaten einsehbar IMSI/IMEI/Rufnummer

Berichtgenerierung



Report

IMSI	901700000000668
IMEI	357913012896140
Rufnummer	32804

Calls

Type	From	To	Duration
unanswered	08154711	32804	
answered	08154711	32804	0:06 min
unanswered	32804	08154711	
answered	32804	08154711	0:03 min

Scenario SMS

Database ID	Created	Sent	Sender No.	Coding	Text	PDU
60	2012-11-24 10:12:00	2012-11-24 10:12:04	4711	7 Bit	Testdata 4711 - 7Bit	d4 f2 9c 4e 0e d3 c3 20 da 2d 16 03 b5 40 37 61 9a fe 00 00
61	2012-11-24 10:12:00	2012-11-24 10:12:05	08154711	16 Bit	SzenarioTest	00 53 00 7a 00 65 00 6e 00 61 00 72 00 69 00 6f 00 54 00 65 00 73 00 74

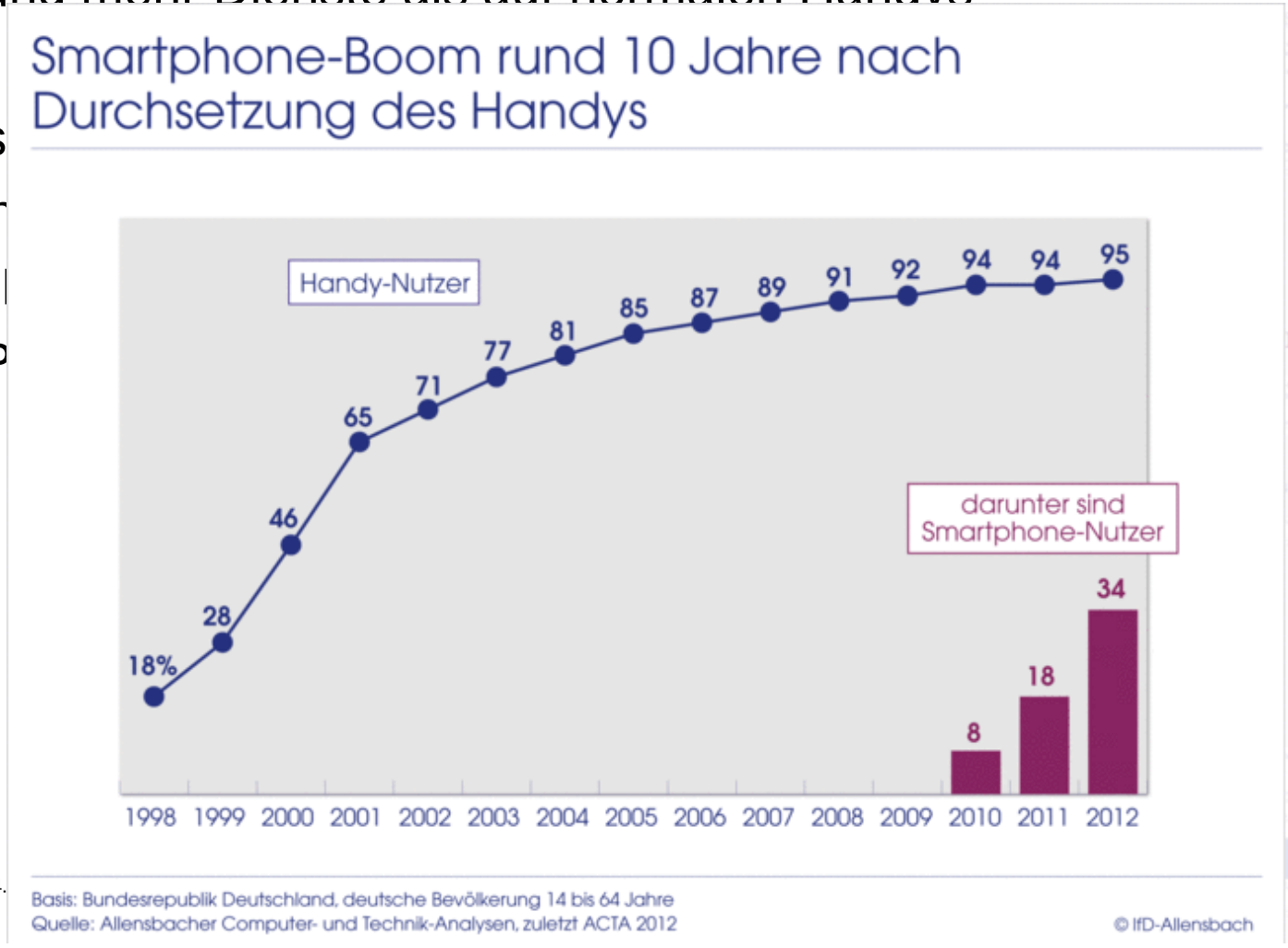
SMS

Database ID	Created	Sent	Sender No.	Coding	Text	PDU
62	2014-11-24 10:12:00	2014-11-24 10:12:05	4711	7 Bit	TestSMS!	d4 f2 9c 3e 6d 4e 43 00

Generated @ 4 Feb 2013 08:58:01

Motivation

- Smartphone Nutzung steigt
- Mehr Daten und mehr Dienste als auf normalen Handys
  - Kalender,
- Interessantes
- Unter Umstär
  - Firmen E-
  - Banking-P



Blackbox- vs. Whitebox-Analyse

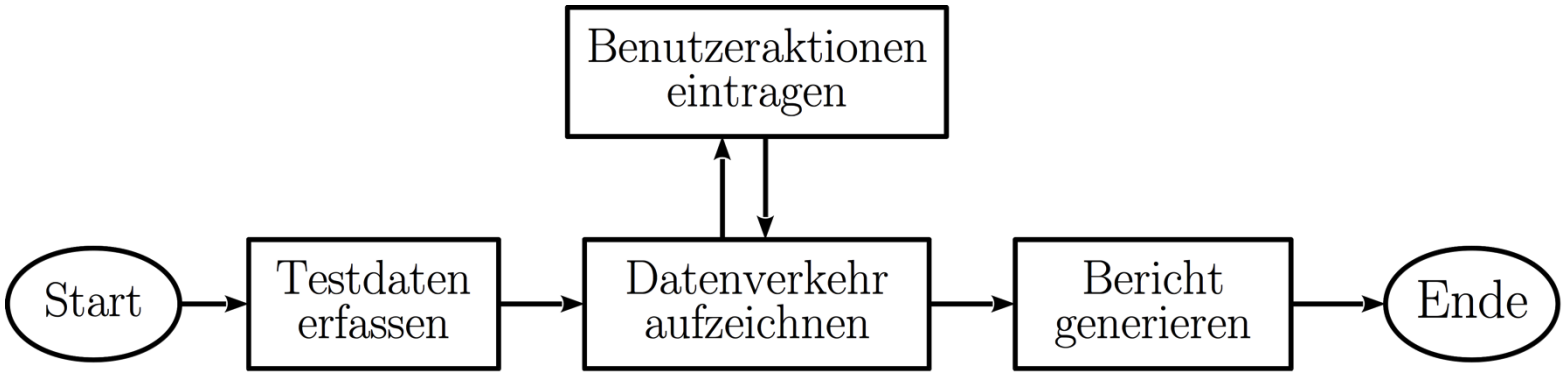
Whitebox-Analyse

- Analyse des Quellcodes auf schädliches Verhalten
- Probleme:
  - Viele Plattformen
  - Zeitintensiv
  - Erfordert Kenntnisse in Programmierung

Blackbox-Analyse:

- Verhalten der Malware beobachten
  - Veränderungen auf dem Gerät
  - **Netzverbindungen**
- Plattform-unabhängig
- Einfacher durchzuführen als Whitebox-Analyse
- Zum Teil automatisierbar

- Software soll Aufzeichnung und Analyse der gewonnenen Daten erleichtern

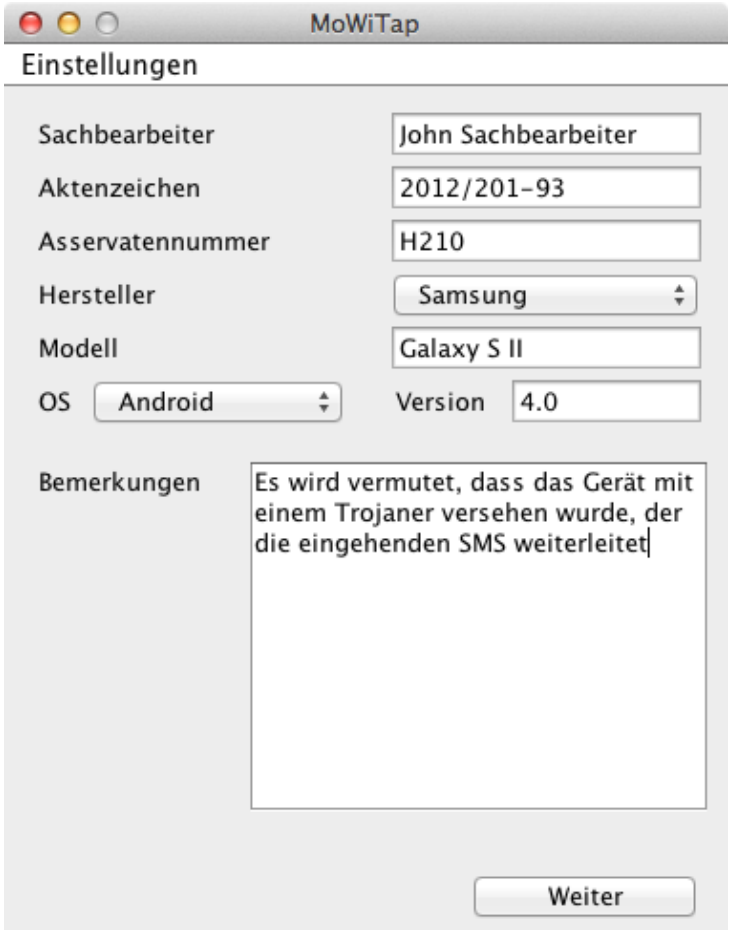


- Datenverkehr wird aufgezeichnet
- Aufgezeichnete Daten werden mit Hilfe einer Java-Bibliothek analysiert
- Bericht wird in HTML generiert

Umsetzung des Projekts

POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES



Umsetzung des Projekts

MS

se

nd der

Big ausgeblendet

Fazit & Ausblick

- Projekte heute beim LKA NRW im Einsatz
  - Zusätzlich zur Malware-Analyse auch Analyse von Wanzen
- Weiterentwicklung
  - Detektion von Anrufen
  - Simulation von Anrufen
- Weitere Abschlussarbeiten laufen/sind in Vorbereitung

Vielen Dank

POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

rechtsstaatlich • bürgerorientiert • professionell

Rolf Stöbe, B.Sc.

rolf.stoebe@alumni.fh-aachen.de

Philip Schütz, B.Sc.
Regierungsbeschäftigter

LKA NRW
Sachgebiet 42.2
Landeszentrale IuK-Ermittlungsunterstützung

philip.schuetz@polizei.nrw.de
Tel: 0211 - 939-4222