5th EUROPEAN CYBER SECURITY MONTH Anniversary

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

Der Kulturbeutel für das mobile Internet – sicher unterwegs mit Smartphone und Tablet

Dr.-Ing. Andreas Bischoff

Zentrum für Informations- und Mediendienste
Universität Duisburg-Essen

Agenda

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

- Warum Kulturbeutel?
- WLAN-Sicherheit
- Mobilfunknetze
- Schadsoftware auf dem Smartphone
- Datenkraken
- Mobile Banking
- Live-Hacking
- ECSM –WTF? Cyber?

Cyber - Cyber - Cyber

UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

WLAN - Sicherheit

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

BSI-Meldung gestern:

Was ist passiert?

Was tun?

- Don‘t panic!
- Einfach VPN verwenden

MENÜ SUCHEN

Bundesamt für Sicherheit in der Informationstechnik

Presse

Kritische Schwachstellen in WLAN-Verschlüsselung – BSI rät zur Vorsicht

Ort Bonn
Datum 16.10.2017

Der Sicherheitsstandard WPA2, der insbesondere zur Verschlüsselung von WLAN-Netzwerken empfohlen wird, ist über kritische Schwachstellen verwundbar. Betroffen sind demnach alle derzeit aktiven WLAN-fähigen Endgeräte in unterschiedlichen Ausprägungen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät dazu, WLAN-Netzwerke bis zur Verfügbarkeit von Sicherheits-Updates nicht für Online-Transaktionen wie Online Banking und Online Shopping oder zur Übertragung anderer sensitiver Daten zu nutzen.

"Nutzen Sie Ihr WLAN-Netzwerk so, als würden Sie sich in ein öffentliches WLAN-Netz einwählen, etwa in Ihrem Lieblings-Café oder am Bahnhof. Verzichten Sie auf das Versenden sensibler Daten oder nutzen Sie dazu einen VPN-Tunnel. Auch das kabelgebundene Surfen ist weiterhin sicher. Unternehmen sollten ihre Mitarbeiter sensibilisieren und geeignete Maßnahmen zur Absicherung ihrer Firmennetzwerke ergreifen.

WLAN -Sicherheit

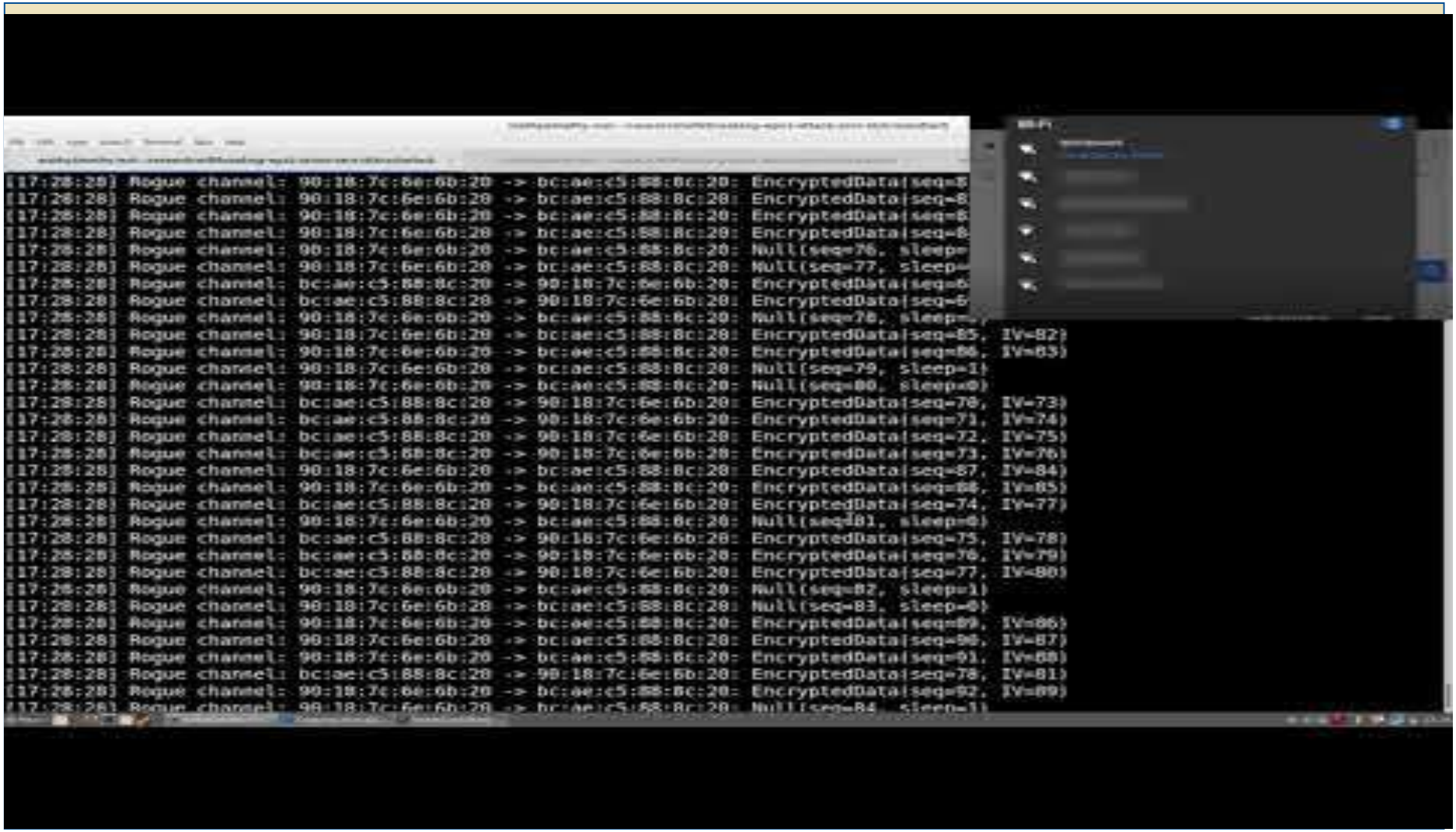
UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

- **Vertrauen schaffen – mit welchem Netz bin ich verbunden? → SSID der Name des WLANs**
- **Wer ist auf der anderen Seite? Das Internet?**
- **Wer ist dazwischen?**
- **Verschlüsselung**
- **WEP (unsicher)/ WPA (seit 2009 geknackt)/ WPA2 (gestern) / Enterprise WPA2 (gestern)**
- **Unverschlüsselt?**
- **Selbst verschlüsseln: VPN**

WLAN –Sicherheit – WPA2 KRACK

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken



Unterwegs im WLAN

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

- **Im ICE niemals ohne VPN**
- **Offene WLANs ohne VPN – no go!**
- **Auch in verschlüsselten WLAN-Netzen müssen Sie dem Betreiber des LANs dahinter bzw. dem Provider vertrauen – also auch dort besser VPN** (Vertrauen zum VPN-Provider)
- **Siehe:** https://hannover.ccc.de/~nexus/dbwifi/index.html

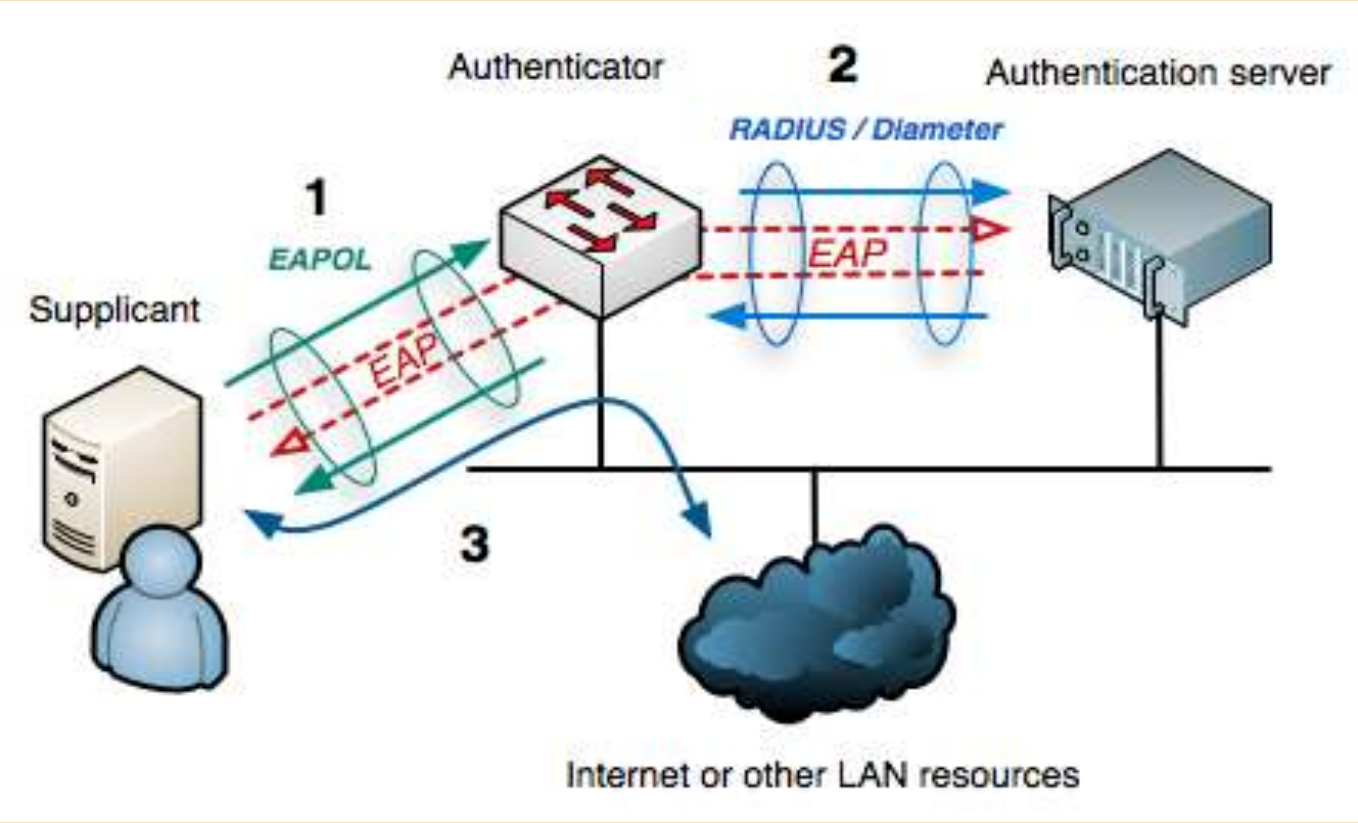
Unterwegs im WLAN

UNIVERSITÄT DUISBURG ESSEN

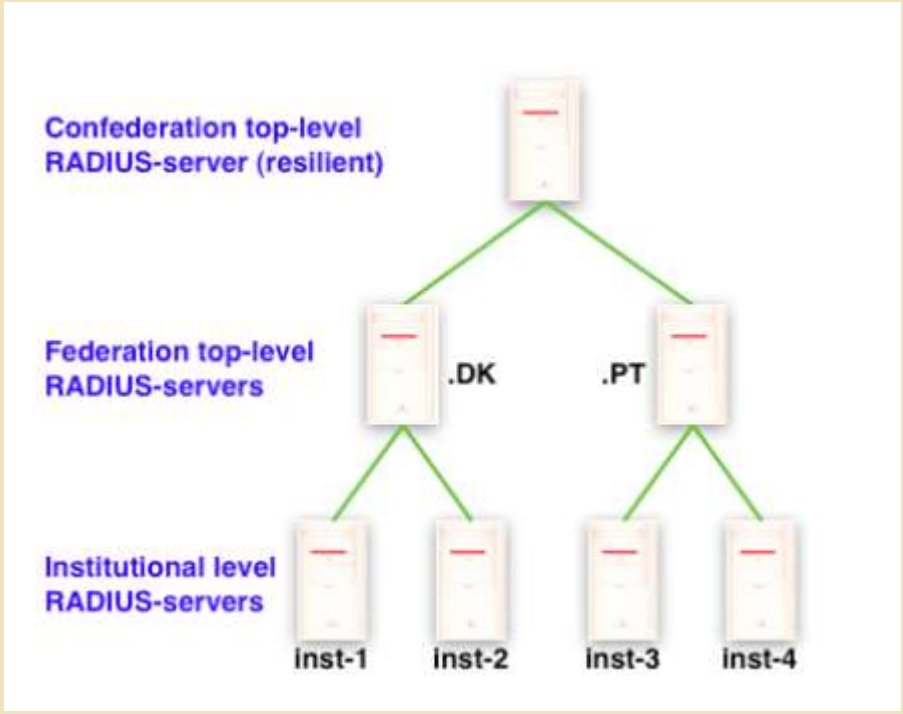
Offen im Denken

- **Warum ist eduroam (bis gestern) sicher gewesen?**
- **Enterprise WPA2 – radius – ldap - AUM**
- **Zertifikate! Wie im Web!**
- **Wer Zertifikate aufbricht…. NGF!**
- **Wenn es falsch konfiguriert ist, ist es unsicher!**

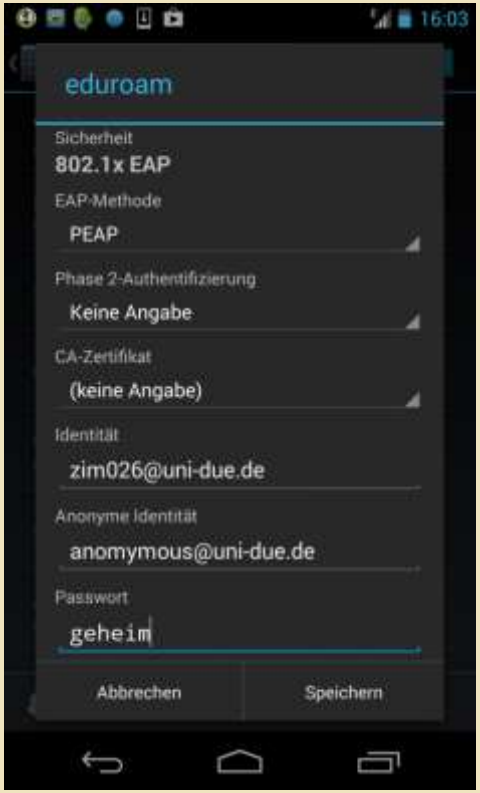
Enterprise WPA -IEEE 802.1X

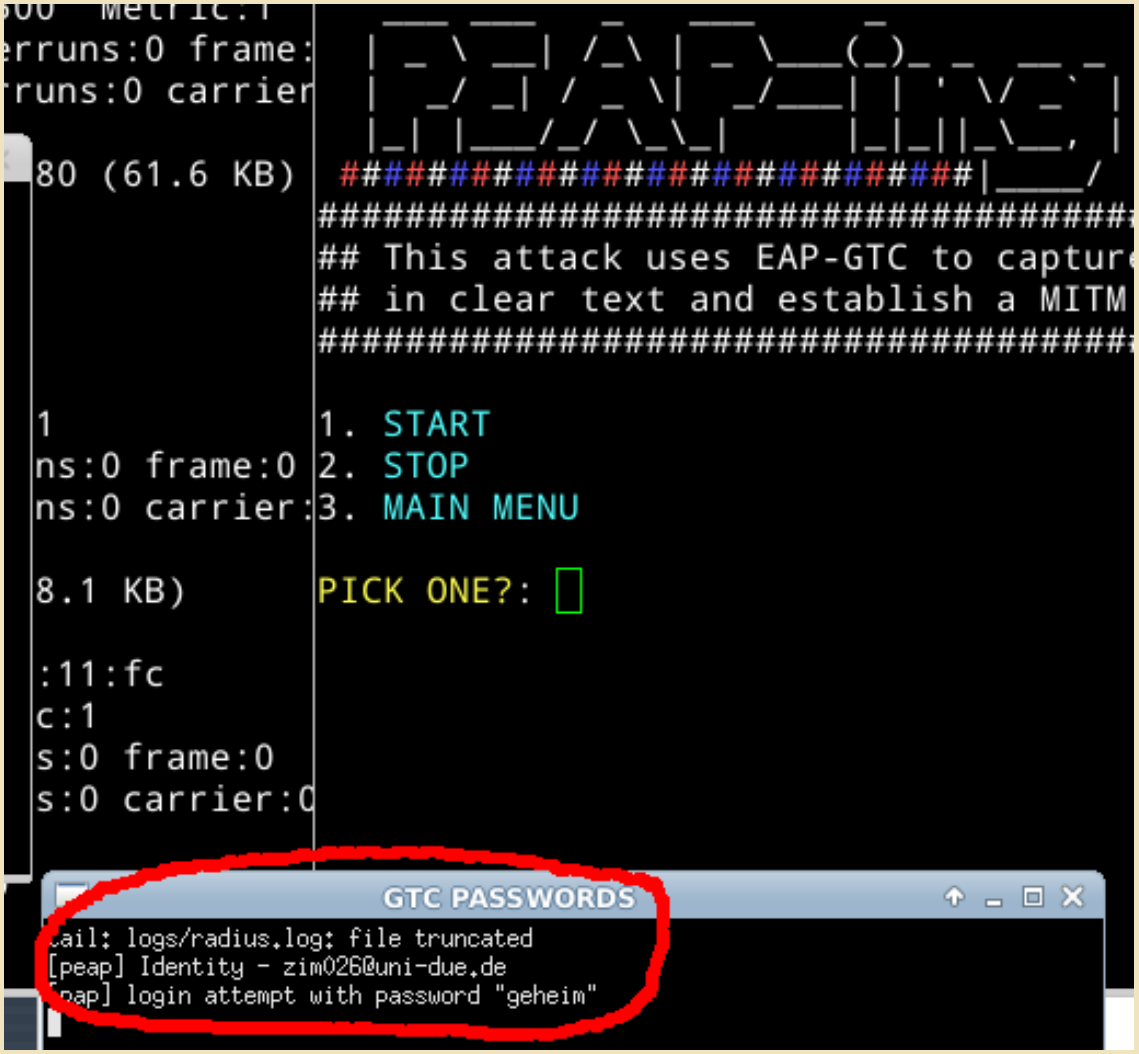


Eduroam- Infrastruktur



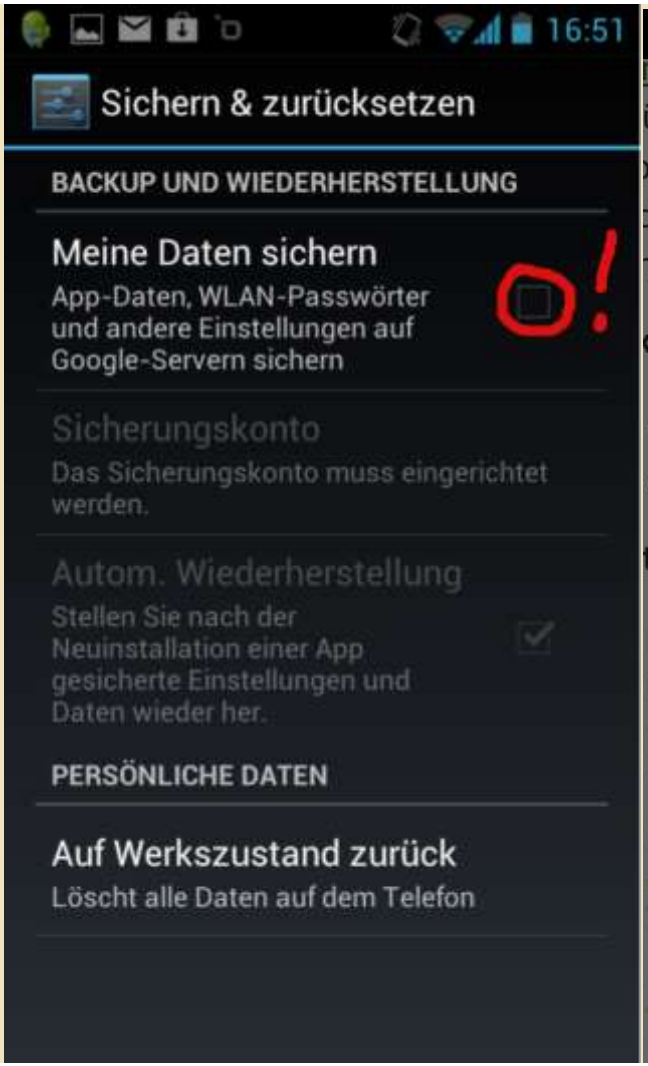
Angriffe auf Eduroam und Schutz davor

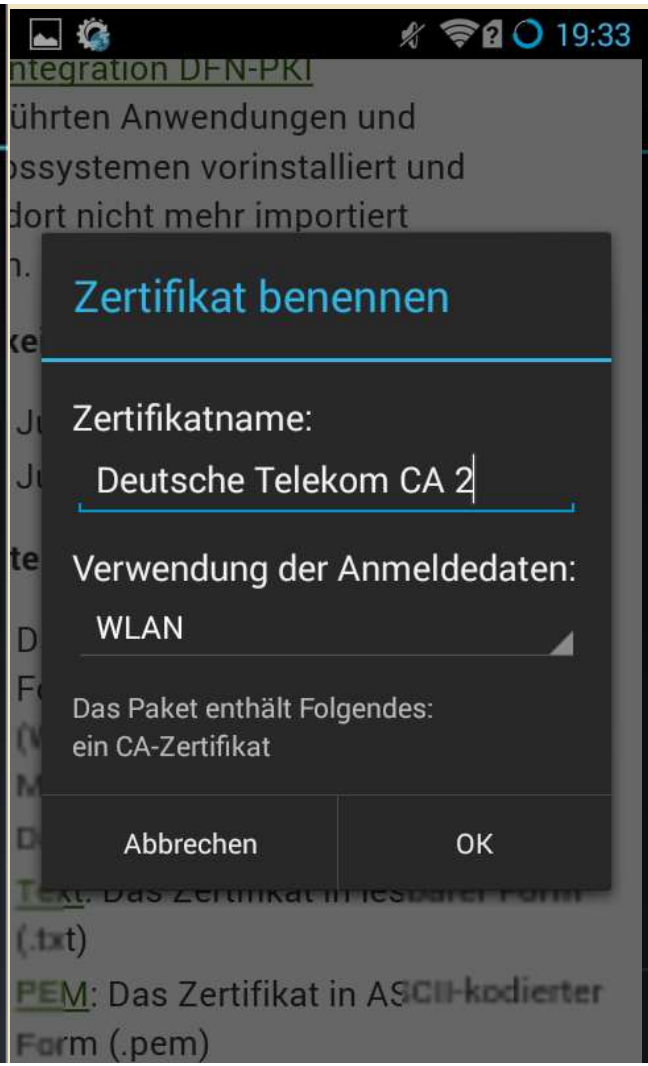


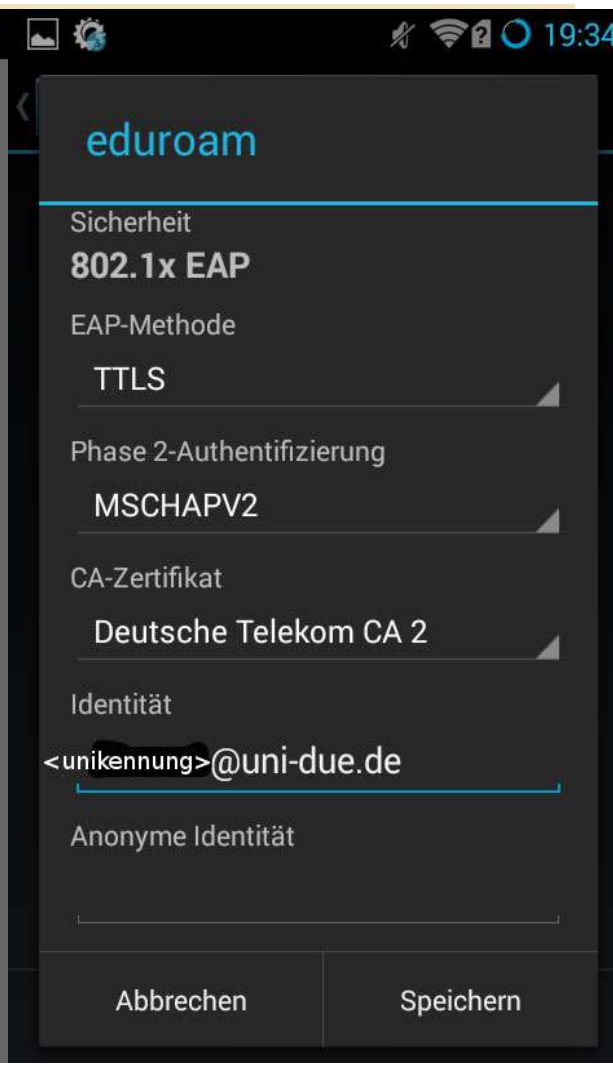


Angriffe auf Eduroam und Schutz davor

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

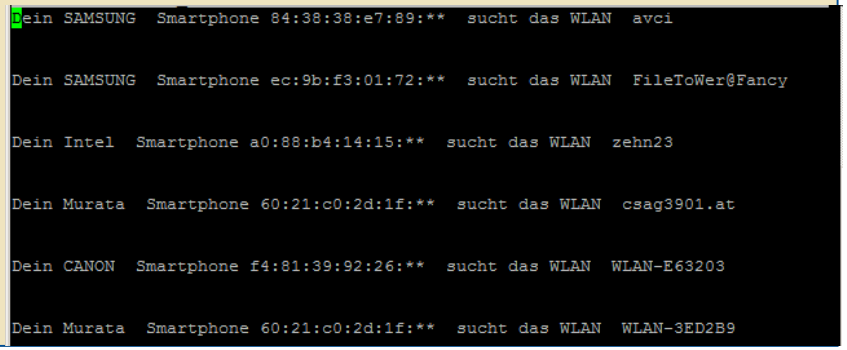




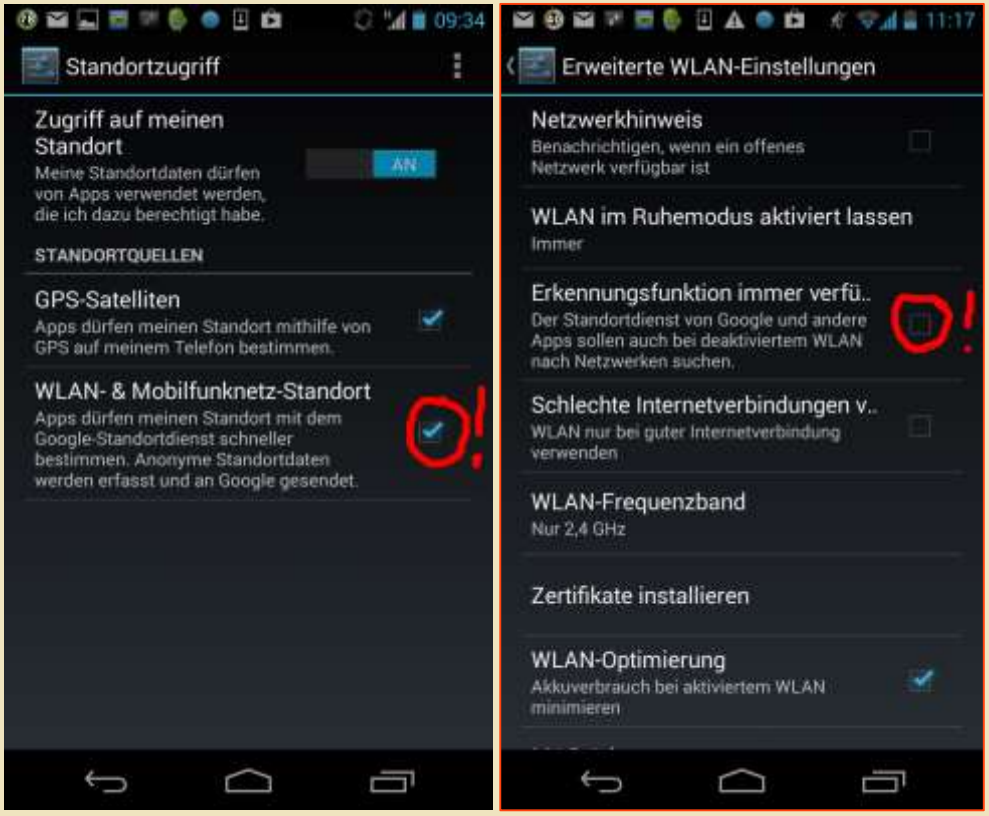


Was WLAN noch so alles macht:

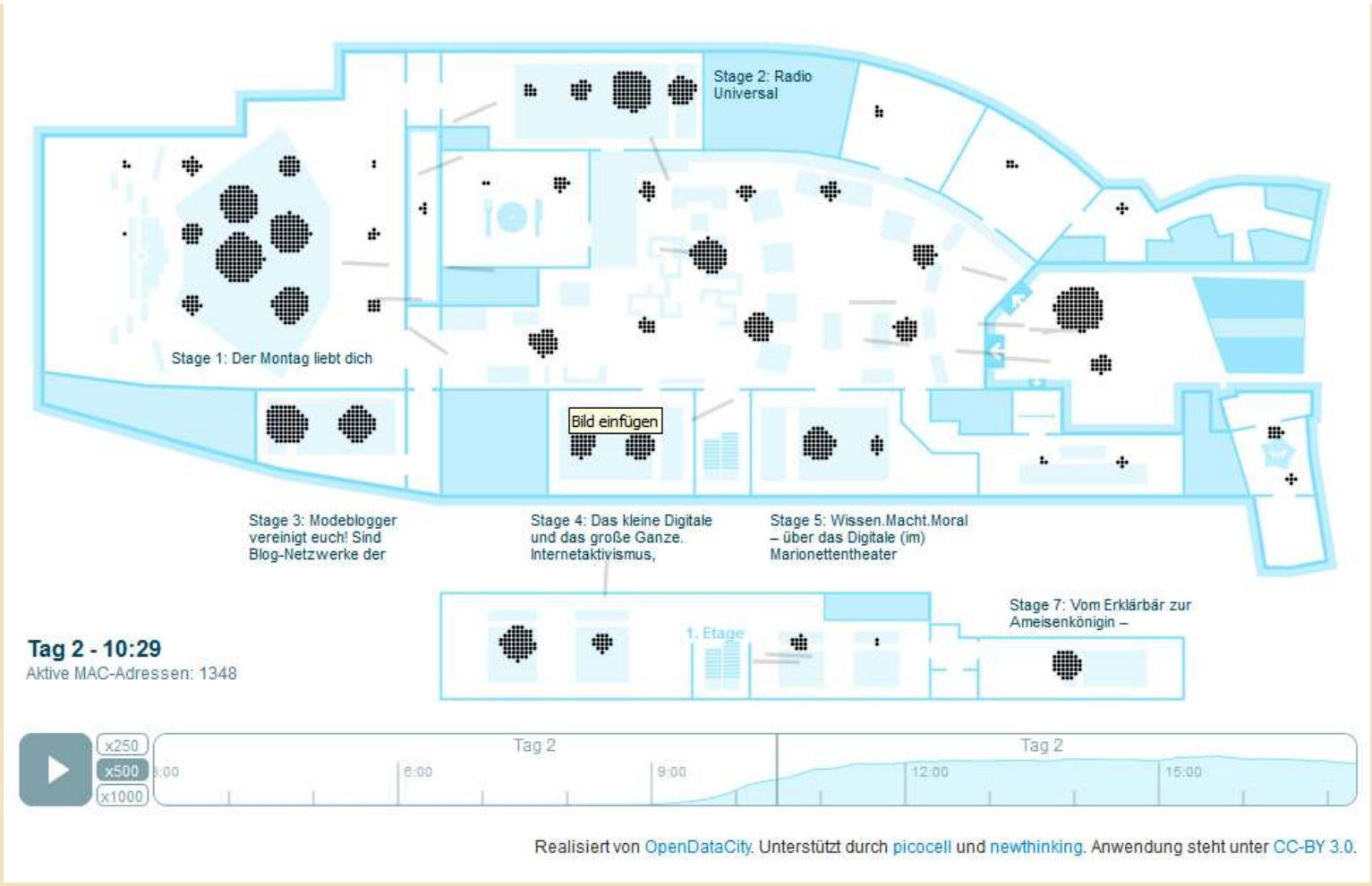
- Die Clients suchen bei eingeschaltetem WLAN immer aktiv nach bekannten SSIDs
- Ab IOS11 ist das schwierig abzuschalten
- Android: WLAN-Ortung immer aktiv, wenn nicht deaktiviert.
- Kann man abhören und tracken bzw. on the fly fake-AP aufbauen



- **WLAN-Ortung – google maps füttert seine Datenbanken mit AP-Koordinaten**
- **Sie sind WLAN-Wardriver für Google**
- **Auch bei ausgeschaltetem WLAN (default!)**



WLAN-Tracking



Quelle: http://apps.opendatacity.de/relog/

WLAN-Fazit

- **Angriffe auf Broadcom-Firmware (iPhone, und viele Android Smartphones)**
- **WLAN-Chips sind Minicomputer ohne Schutzmechanismen**

Bild: Köf3/Wikimedia Commons/CC-BY 3.0)

- **Guter Rat: WLAN immer ausschalten wo man es nicht erwartet!**
- **Kontrolle ob es wirklich aus ist (Ortung/IOS11)!**
- **Wo Netzwerkkabel sind → diese benutzen!**

UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

Mobilfunknetze

- **Mobilfunknetze – wie kommt das Internet auf das Smartphone?**
- **Lawful Interception**
  - The Great Firewall of China – oder wie Regime das Internet unterwandern
  - Next generation Firewals: NGF
  - Zurückgehaltene Sicherheitslücken
  - US-rechtssprechung / Safe Harbour
- **Metadaten - auch durch verschlüsselten https-Verbindungen**

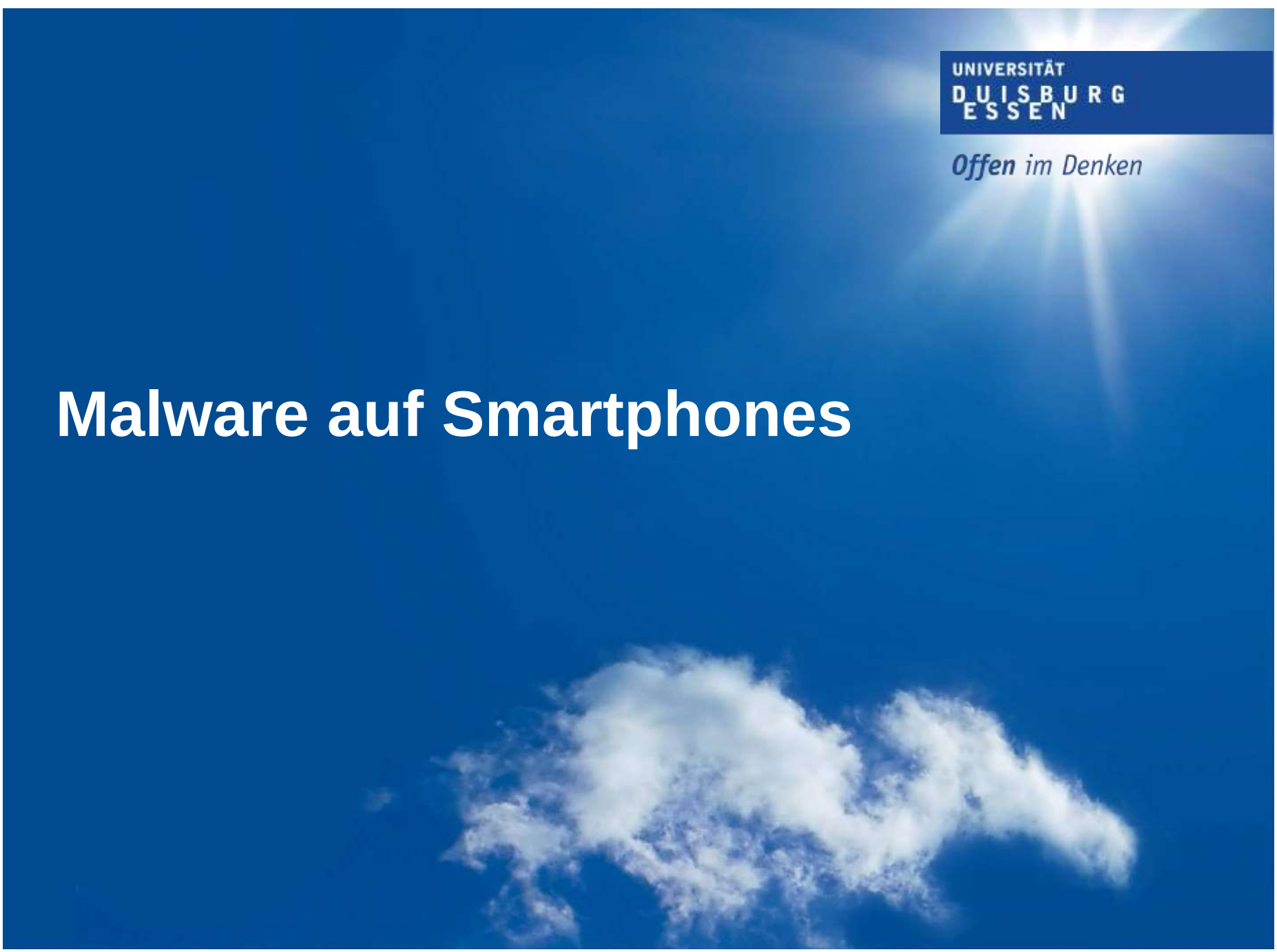
Mobilfunknetze

- **GPRS, 2G, 3G (UMTS), 4G (LTE)**
- **Provider – Vertrauen (Vodafone?, Telekom?)**
- **Hacks, GSM (Rainbow Tables), SMS (Klartext in der Mobilfunkzelle), usw.**
  - Femtocell
  - seltsame Mobilfunkmasten
  - OSMOCOM osmocom.org
  - IMSI Catcher (IMSI Catcher Catcher)
- **Lawfull interception (Snowden)**
- **Auch in Mobilfunknetzen schadet VPN nicht!**

UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

Malware auf Smartphones



Agenda:

- **Apps**
- **Angriffsvektor Browser**
  - Drive-by-Download
  - PopUps
- **Mobile Mail**
- **Was tun wenn Malware auf dem Smartphone gefunden wird**

Malware auf Smartphones

- **Wie erfahren wir davon?**

```
Meldungstyp: Bot/HTTP
Zeitpunkt: 2017-07-27 20:06:57 +0200
Beschreibung: Auf dem System scheint eine Bot-Software betrieben zu werden,
die versucht, einen HTTP-basierten Bot-Netz Control-Server zu erreichen. Zu
den unterschiedlichen Malwaretypen finden Sie unter der folgender Webseite
mehr Informationen: http://www.cert.dfn.de/index.php?id=bot

Zeitpunkt                 | Verbindung                                  | Protokoll | Reque
--------------------------------------------------------------------------------
2017-07-27 20:06:57 +0200  |132.252.*.***:n/a => http://init.icloud-analysis.com:80
2017-07-27 20:06:57 +0200  | 132.252.*.***:2375 => n/a:80                | TCP       | POST
```

- **Wie erfahren Sie davon?**
  - Auf Ihrem nächsten Kontoauszug
- **Hilft ein Virenscanner?**

Wie kommt die Malware auf das Smartphone?

- **Sie installieren Sie selbst**
  - App-Rechte - Vorsicht auch bei Apps aus alternativen App-Stores wie z.B. AndroidPit (Android) oder Cydia (für IOS-Geräte mit Jailbreak). Wir beobachten z.B. XhostGhost (manipulierte Entwicklungsumgebung für iPhone-Apps)
- **Die schädlichen Apps sind schon beim Kauf installiert (China-Smartphones)**
  - (aktuell: das One Plus übermittelt private Daten)

Wie kommt die Malware auf das Smartphone?

- **Drive-by-Downloads (mobile Browser == Browser)**
  - Werbeanzeigen, Malware in Anzeigen
  - Seltsame (HTML-) PopUps mit Aufforderung zum Download
  - PopUps mit Kennwort-Aufforderung: Tipp: Einfach mal falsches Kennwort eingeben!
- **Phishing-Mails (Der Fluch der einfachen Benutzeroberfläche)**

Ist mir doch egal! Was kann so eine Infektion schon anrichten?

- **Schadsoftware kann Geräte / Nutzer tracken, persönliche Kontaktdaten und Passwörter abgreifen oder das Telefon als Abhörwanze (auch mit Videoüberwachung) betreiben.**
- **Accounts (Zugangsdaten zu Kreditkarten, Banking-Apps, Uni, SAP, Google Play, iTunes, fb, twitter, Instagram, etc) Identitätsdiebstahl für Phishing, Spamattacken usw.**

UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

Live Hacking

Smartphone fernbedienen

Kameras in Smartphones und PCs Aufkleber

oder Blink:

Quelle: https://soomz.io

Malware auf dem Smartphone verhindern

- **App-Rechte**
  - Wenn eine App mehr Rechte verlangt, als es Ihnen sinnvoll erscheint, suchen Sie nach einer Alternative!
- **Benutzen Sie einen aktuellen Browser**
  - Android: Vermeiden Sie Chrome! Google hat kein Interesse am Schutz Ihrer Privatsphäre. Apple: Sie sind auf die Updates von Apple angewiesen.
- **Verwenden Sie einen Werbeblocker**
  - für Android und IOS mobile Addblocker: (Adblock Browser)

Wie Malware auf dem Smartphone verhindern?

- **PopUps**
  - PopUp vom Betriebssystem oder vom Browser?
  - im Browser → PopUp von der Webseite
  - Ignorieren Sie solche PopUPs
  - meiden Sie solche Webseiten!
- **Verwenden Sie aktuelle Betriebssysteme**
  - Apple: Einfach, Android: LineageOS oder Hersteller mit regelmäßigen Sicherheitsupdates (Nokia!)
  - Geben Sie Smartphone mit veralteten Android/IOS-Versionen und bekannten Sicherheitslücken nicht an Ihre Kinder weiter!
  - Vor Verkauf oder Außerbetriebnahme → immer zurücksetzen auf Werkszustand

Was tun, wenn es schon zu spät ist und Malware auf dem Smartphone installiert ist?

- Fragen Sie uns!
- Daten sichern
- Alles zurücksetzen
- Alle Passwörter wechseln

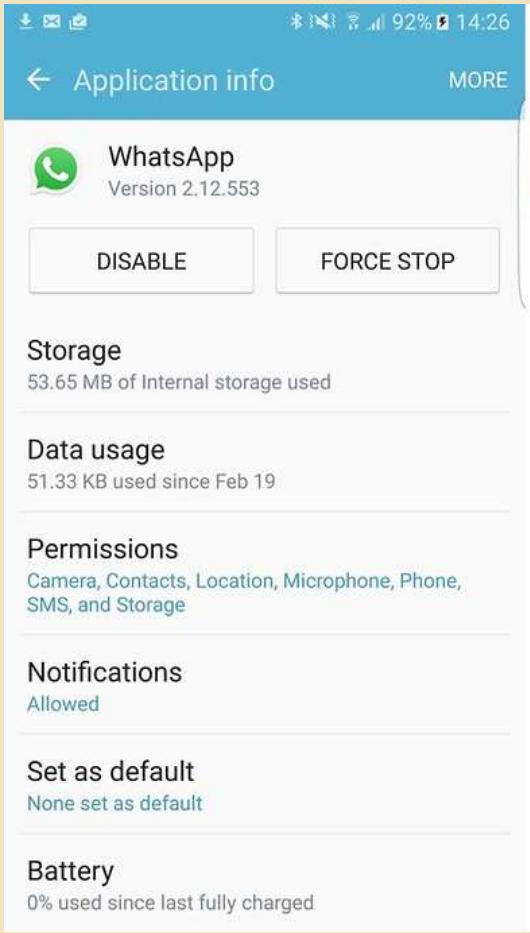
UNIVERSITÄT
DUISBURG
ESSEN

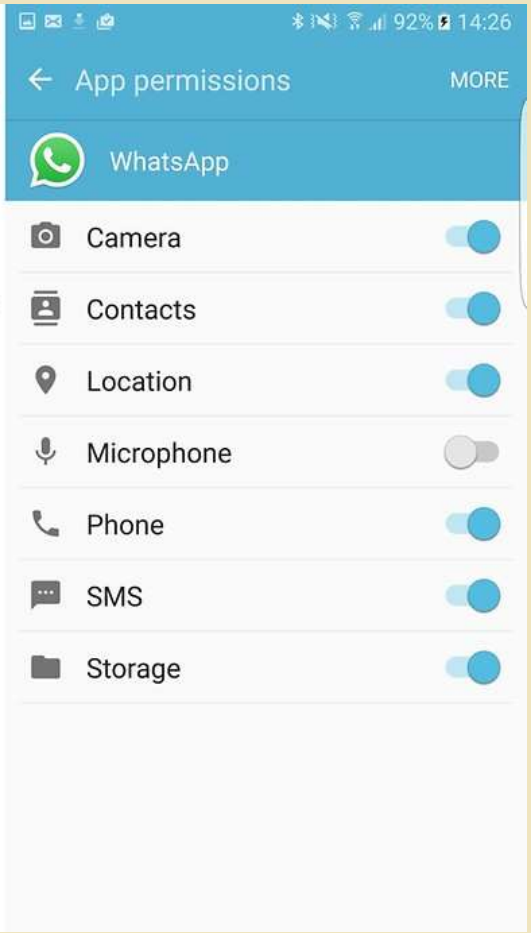
Offen im Denken

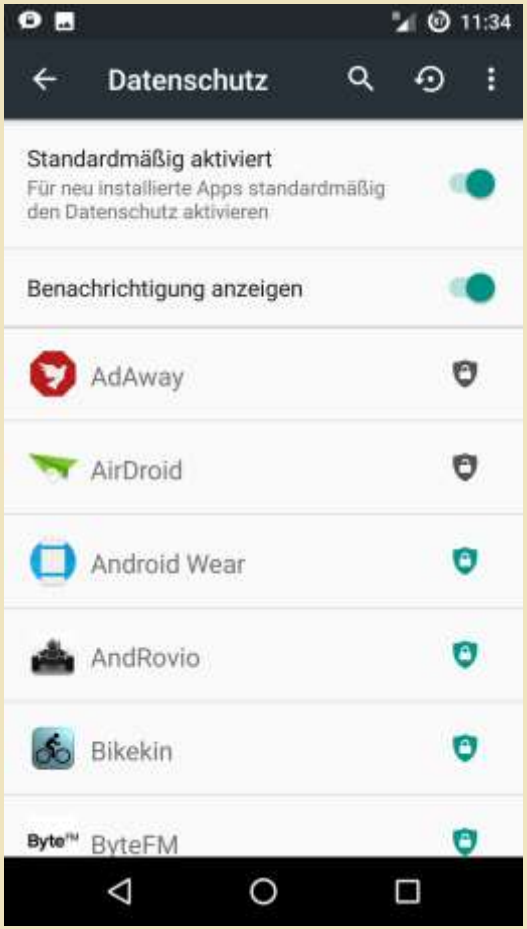
The Good the Bad and the Ugly

Darum sind App-Rechte gefährlich!

APP-Rechte einstellen - Android: Ab Android 6 bzw. ab Cyanogenmod 11 bzw. einzelne Hersteller Huawei und Gigaset

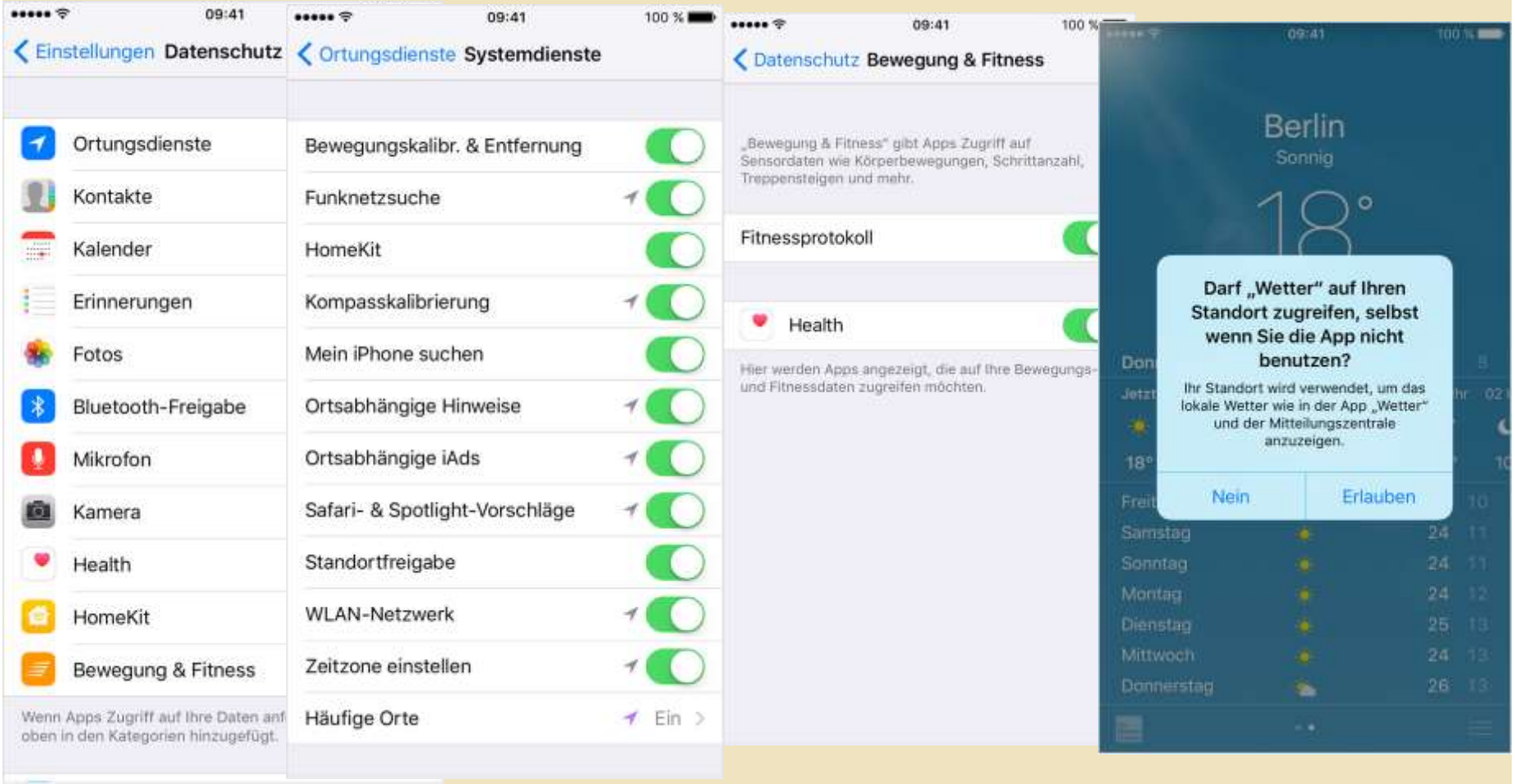






Tipp: „Einstellungen“ „Apps“ – „mehr“ bzw. „ Einstellungen" > „Datenschutz"

APP-Rechte einstellen – iPhone unter Einstellungen Datenschutz:



Tipp: "Einstellungen" > "Allgemein" > "Zurücksetzen", und tippen Sie auf "Standort & Datenschutz"

UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

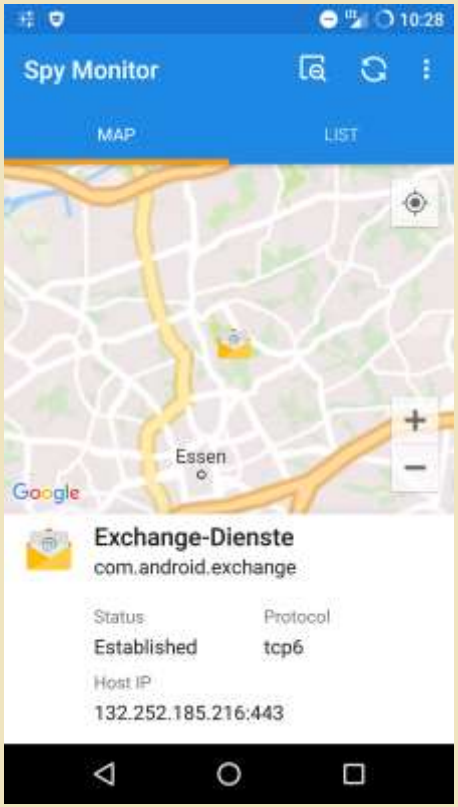
Kleiner Exkurs Exchange mobil an der UNI

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

Dos and don‘ts - Echange-Client

- Dienstliche Smartphones: WhatsApp, fb und Konsorten – no go!
- Wegen Weitergabe der dienstlichen Kontakte!
- Wenn aktuelles IOS oder Android > 6 → App-Reche einschränken
- Alternativ OWA oder OWA-nutzende APP

Testen mit wem der Email-Client kommuniziert



Spy Monitor

- zeigt an welche Server kontaktiert werden
- geht mit allen APPs
- USA == nicht gut!

UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

Mobile banking

2-Faktor-Authentifizierung

- vom Smartphone unabhängiger Kanal
- smsTAN nicht auf dem selben Telefon
- chipTAN manuell/optisch/smsTAN/pushTAN
  - https://media.ccc.de/v/32c3-7360-un_sicherheit_von_app-basierten_tan-verfahren_im_onlinebanking
  - https://media.ccc.de/v/33c3-7969-shut_up_and_take_my_money
- mobileTAN/SecureAPP, etc.

Rat: KISS

extra Gerät + Kabel!

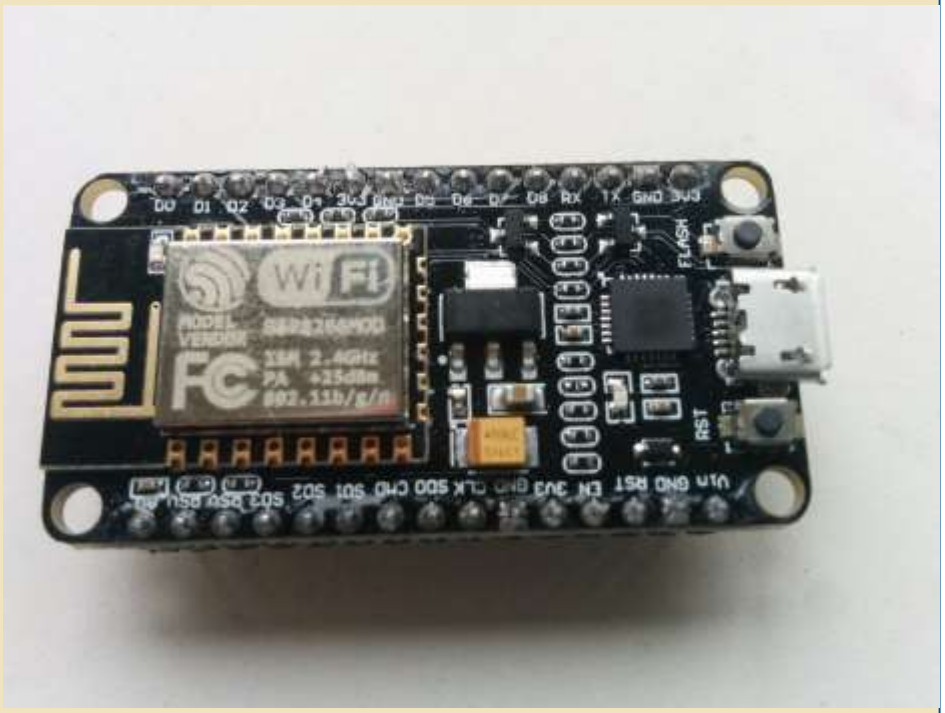
UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

Live Hacking

- **Ein kleines Biest: NodeMCU ESP8266 mit „Spacehuhn Deauthenticator“**
- **Sendet allen für WLAN-SSIDs in Reichweite Deauth-Pakete an alle Klienten!**
- **ALLE fliegen raus!**

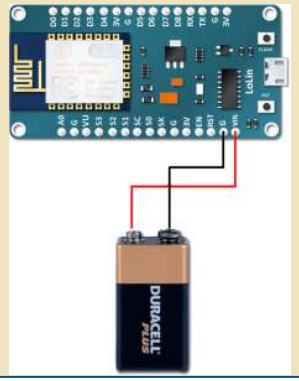
(nur 2,4GHz)

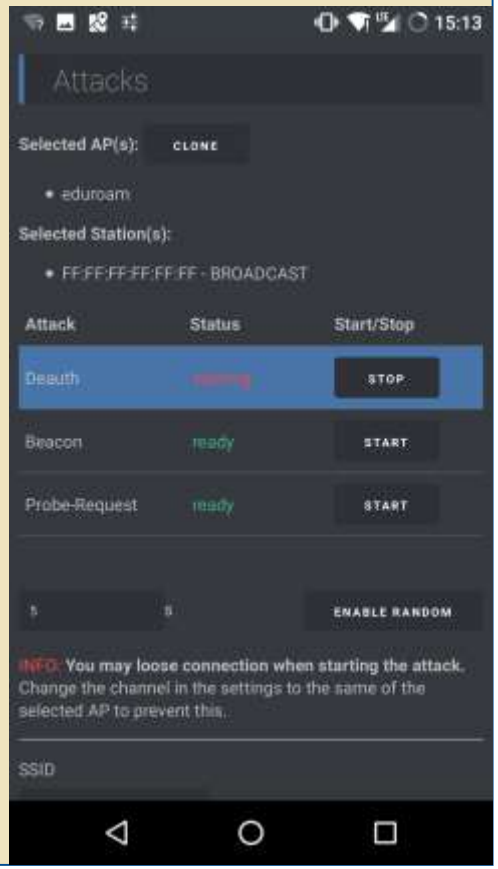


https://github.com/spacehuhn/esp8266_deauther

„Spacehuhn Deauthenticator“

- schönes GUI
- HW aus China: 3$ incl. Versand
- mit 9V Batterie < 4€
- 2 Tage fun





- **Eigener – AP mit SSID eduroam und falschen Zertifikaten**
- **Alle Smartphones die sich damit verbinden sind falsch konfiguriert!**
- **Wall of shame**
- **Wir helfen im Anschluss bei der richtigen Konfiguration!**

Der ECSM – Unsere Vorträge

- 10.10.2017 - Andreas Michels
  Mit Sicherheit am Windows-Rechner - aber wie?
- 13.10.2017 – Rainer Pollak
  Security-Check „E-Mail“
- 17.10.2017 – Dr. Andreas Bischoff
  Der Kulturbeutel für das mobile Internet – sicher unterwegs mit Smartphone und Tablet
- 20.10.2017 – Dr. Marius Mertens
  Phishers Fritze phisht...