Chat und Sprachsteuerung sicher und privat

Dr.-Ing. Andreas Bischoff
Zentrum für Informations- und Mediendienste
Universität Duisburg-Essen

Why again?

Agenda

- Wie alles begann – die Geschichte des Online Chats – Früher ™
- IRC, ICQ & Co → heute WhatsApp?
- Datenschutzfreundliche Alternativen
- Live-Hacking
- Sprachassistenten, Alexa, Siri, Cortana, Google Now & Co
- WLAN Hacks
- Hacking Gadgets

In einer fernen Galaxis…

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

Es war einmal vor langer Zeit in einer weit, weit entfernten Galaxis….

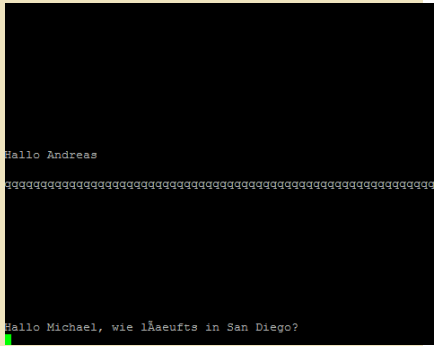
1997 - Ein einsamer Diplomand arbeitet an einer SUN-Workstation an der Fernuni in Hagen und sein Betreuer ist für ein Jahr als Gastwissenschaftler in San-Diego unterwegs….

Telefonieren war teuer! 90‘er: 2,40 DM für 30 Min Ortsgespräch Inland!

Auslandsgespräche in die USA waren horrend teuer!

Also → Unix Talk

Dieses Werk wurde von seinem Urheber Lamune in der Wikipedia auf Englisch als gemeinfrei veröffentlicht. Dies gilt weltweit.



In einer fernen Galaxis…

Es war einmal v
einer weit, weit
Galaxis….

- 1997 - Ein einsa
  an einer SUN-W
  Fernuni in Hager
  für ein Jahr als G
  San-Diego unte
- Telefonieren war
  für 30 Min Ortsg
- Auslandsgesprä
  horrend teuer!
- Also → Unix Talk

In einer fernen Galaxis…

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

Es war einmal v
einer weit, weit e
Galaxis….

1997 - Ein einsam
an einer SUN-Wo
Fernuni in Hagen
für ein Jahr als Ga
San-Diego unterv

Telefonieren war t
für 30 Min Ortsge

Auslandsgespräch
horrend teuer!

Also → Unix Talk

```
Hallo Andreas
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq

Hallo Michael, wie lÃaeufts in San Diego?
```

Aber viel früher IRC – *Internet Relay Chat*

- Entstand im BITNET unter dem Namen *Relay Chat*
- 1988 Übertragung auf das Internet von Jarkko Eikarinnen
- RFC 1459 (1993)
- RFC 2810–2813 (2000)
- Wird heute noch sehr aktiv genutzt von „Profis“ und „Hackern“.
- Rein textbasiert
- Aktuelle Clients z.B. Xchat, mIRC
- Große IRC-Netze sind: QuakeNet, EFnet, IRCnet, Undernet und Freenode
- Heute auch verschlüsselt über SSL oder OTR

Die große ICQ-Welle - Instant Messaging

- ICQ wurde im Jahr 1996 von der israelischen Firma Mirabilis gegründet
- Ab 1998 übernommen von AOL
- Ab 2010 Digital Sky Technologies, später Mail.ru Group
- Für viele Nutzer ist ICQ *„I seek you“* Erstkontakt für IM gewesen.
- Später AOL-Messenger, MSM-Messenger und ab ca. 1999 Jabber!
- An der FernUni im Jahr 2004: Versuch IM (Jabber) als dienstliche Kommunikation zu etablieren → scheitert am Verständnis der Nutzer (gegenseitige Autorisierung nötig)
- An der UDE 2008 Guido Kerkewitz Jabber
- Neuer UDE-Jabber-Dienst ab 2014 (Verbreitung nur viral)

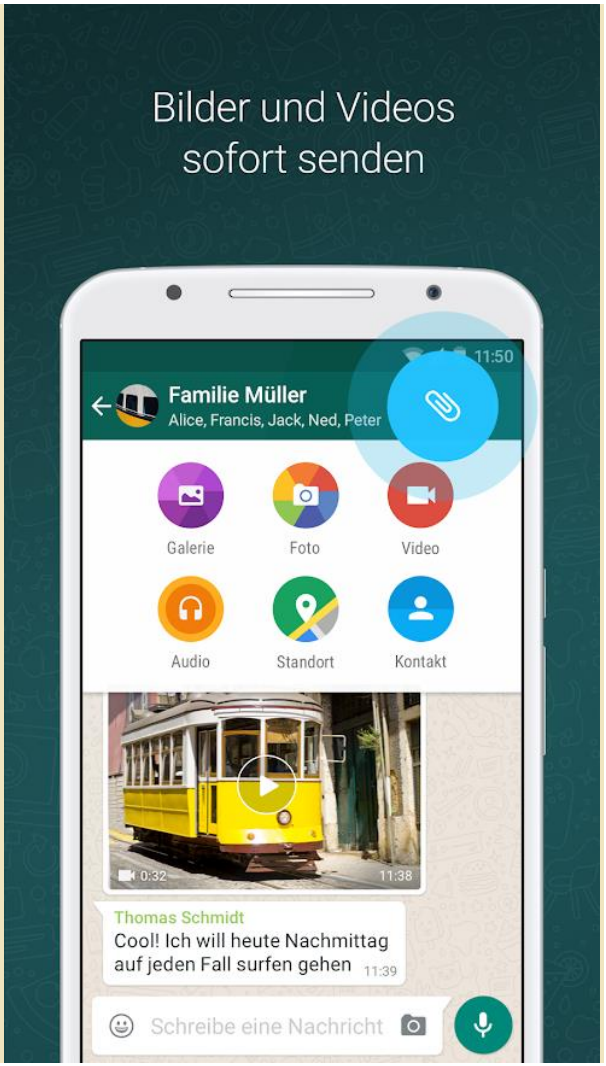
Chat mobil

- SMS war teuer (zum Vergleich: 500mB 3€ vs. SMS 80 Byte=19 Cent, d.h. 6€ /GB vs. 2.500.000€/GB)
- D-Gesamtumsatz mit SMS war mal > 5 Milliarden €
- WAP-IRC und ICQ Gateways (2003)
- Frühe Smartphones (Nokia Communicator Windows Mobile) stellten IRC und ICQ zur Verfügung
- Privatnutzer häufig nicht in der Lage E-Mail auf Feature- bzw. Smartphones zu konfigurieren und kannten keine „alten“ Chat-Dienste mehr – Digital „Naive“ (SIC!)

Und dann kamen die „neuen“ Smartphones iPhone/Android

WhatsApp

- 2009 WhatsApp Gründung durch Brian Acton und Jan Koum
- Zunächst unverschlüsselt
- Viral, da Kontaktaufnahme über gespeicherte Telefonbucheinträge
- Netzwerkeffekt ← !!!
- Später auch Audio und Video möglich



WhatsApp

Seit drei Jahren Ende-zu-Ende Verschlüsselung (Open Whisper Systems – aus dem TextSecure Messenger)

Staatliche Gegenmaßnahmen

- Anfragen beim Provider
- Quellen TKÜ → Code auf dem Smartphone einschleusen *bevor* verschlüsselt wird

Trotz Verschlüsselung: Metadaten!

Metadaten – *wer* mit *wem*

Auch hier Netzwerkeffekt: Bei bekannten 30 % Adressbüchern sind alle Kontakte innerhalb einer Peergroup bekannt!

Was sind Ihre Kontaktdaten wert?

WhatsApp

2014 Verkauf von WhatsApp an Facebook für 19 Milliarden US-Dollar

Das war weder die Client-Software noch die Server-Software wert! (lässt sich *genau so* mit Open Source Software realisieren)

Facebook ging es um die Nutzerbasis, um die Nutzerdaten!

WhatsApp übermittelt standardmäßig alle Namen und Nummern aus Telefon-Adressbüchern seiner Nutzer an Server in den USA - auch aller den Dienst nicht nutzenden Kontaktpersonen

2015 wurde erstmals offiziell bekannt, dass amerikanische Behörden die Möglichkeit haben, WhatsApp-Nachrichten mitzulesen

Altersbeschränkung: Nutzung erst ab 16 Jahren

Warum machen die das?

WhatsApp

- Seit 2016: Offizielle Weitergabe der Adressdaten an Facebook
- Cambridge Analytica → Facebook/WhatsApp → Trump/Brexit
- Pogrome in Myanmar, Wahl in Brasilien → Bolzonaro
- An der UDE: Dienstliche Nutzung durch die „Cloud-Leitlinie“ untersagt
- Seit September 2017 ist WhatsApp in China dauerhaft gesperrt
- Mai 2017 Datenschutzbeauftragte von Rheinland-Pfalz: WhatsApp zu schulischen Zwecken ist tabu
- Empfehlung: Nicht nutzen! Chat-Partner von Alternativen überzeugen!

Threema - Vorteile

Ende-zu-Ende Verschlüsselung

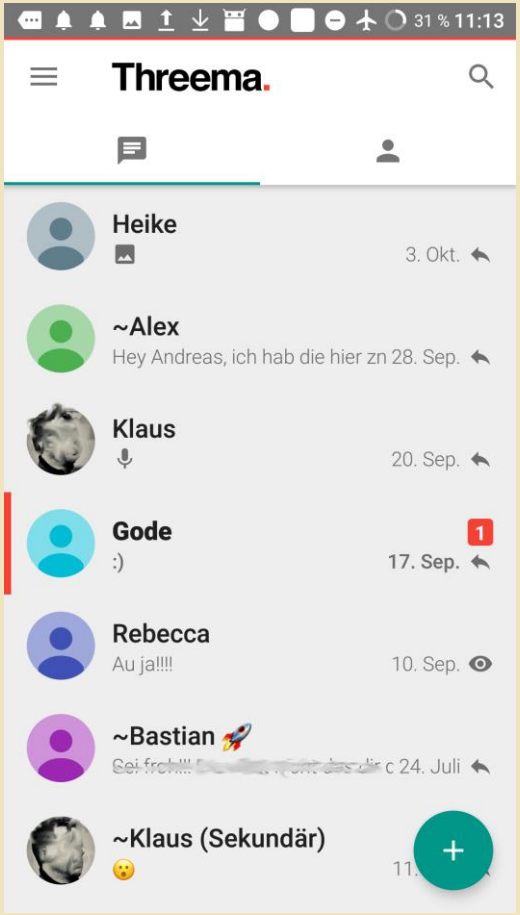
Völlig anonyme Anmeldung möglich (ohne Telefonnummer und E-Mailadresse)

Server in der Schweiz! (Außerhalb der 5 Eyes)

Bezahl-App → Geschäftsmodell sind nicht die Nutzerdaten

Es gibt eine Business Variante (Threema Work)

Klienten für Android, IOS, Web



Threema - Nachteile

Closed Source!

Aber: Wenn nicht alle Kontakte anonym angemeldet sind, kann auf den anonymen Nutzer geschlossen werden

Metadaten liegen *zentral!*

Anbieter kann *mit Metadaten* aufgekauft werden

Signal (ehemals Text Secure) - Vorteile

Clients und Server Open Source (Android/IOS)

Ende-zu-Ende Verschlüsselung

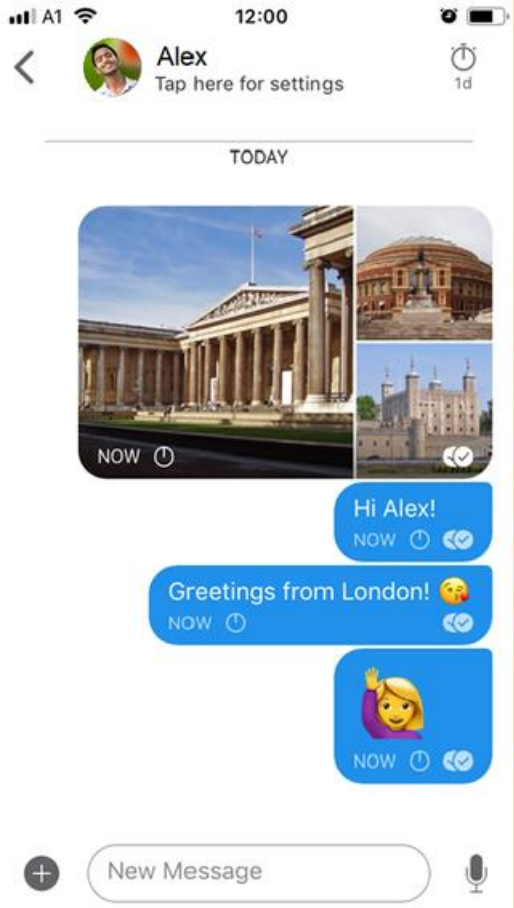
„Zero-Knowledge-Prinzip“

Nummern aus dem Telefonbuch werden gehasht

Nutzerprofile können nicht durch den Provider eingesehen werden.

Wird von der gemeinnützigen Signal-Stiftung entwickelt und betrieben – Finanzierung durch Spenden (Großspende durch WhatsAPP-Gründer)

Zensur-Umgehung mit Domain-Fontling (verstecken hinter Google-Diensten, früher auch Amazon AWS, aber Amazon blockiert das nun)



Quelle: Wikipedia CC BY-SA 4.0

Signal - Nachteile

Server steht in den USA

Metadaten liegen *zentral! Aber Nutzer angeblich nicht identifizierbar*

Ab Version 2.7 keine SMS/MMS-Verschlüsselung mehr

Telegram - Vorteile

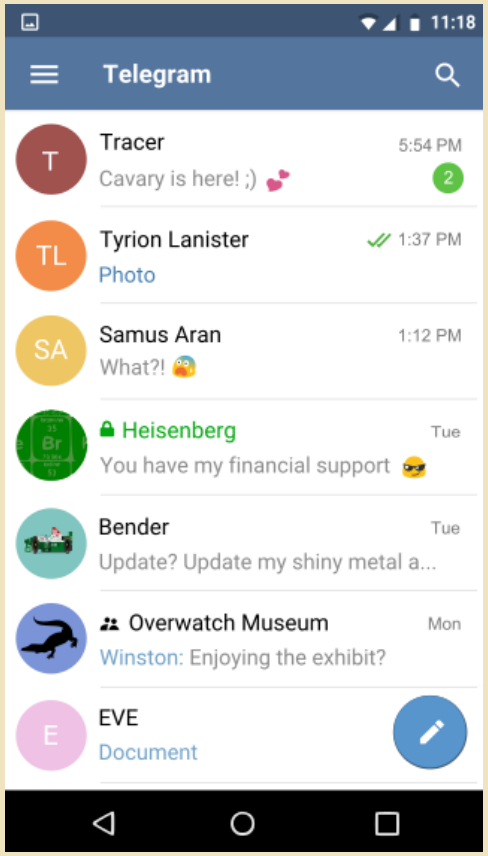
Clients teilweise Open Source

Staatliche Blockadebemühungen durch Russland, Iran (d.h. Krypto funktioniert!)

Ende-zu-Ende Verschlüsselung möglich

Chatverlauf kann automatisch nach einer vorgegebenen Zeitspanne (30 Sekunden) von beiden Endgeräten gelöscht werden (Beschlagname)

Klienten für Android/IOS



Quelle:Wikipedia, GPL

Telegram - Nachteile

Bei Anmeldung Telefonnummer zwingend erforderlich

Server steht in Dubai

Ende-zu-Ende Verschlüsselung nur optional

Metadaten liegen *zentral beim Anbieter!*

Sicherheitsprobleme bei Bots in Gruppen-Chats

Eigene Kryptoentwicklung

Jabber auch XMPP (Protokoll) genannt

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

XMPP – siehe auch https://xmpp.org

Open Source Chat-Protokoll offen und erweiterbar

Zahllose Server und Clients als Open Source verfügbar

Auch Google-Talk und Facebook-Messenger zunächst XMPP → dann absichtlich Interoperabilität unterlaufen um Nutzergruppen (Nutzer sind die Ware) abzuschirmen

Neben Chat auch Audio und Video-Konferenzen möglich

Ursprünglich für den PC gedacht → Anfänglich Probleme mit mobilen Clients → behoben durch Protokollerweiterung

An der UDE:

Jabber-ID: vorname.nachname@jabber.uni-due.de

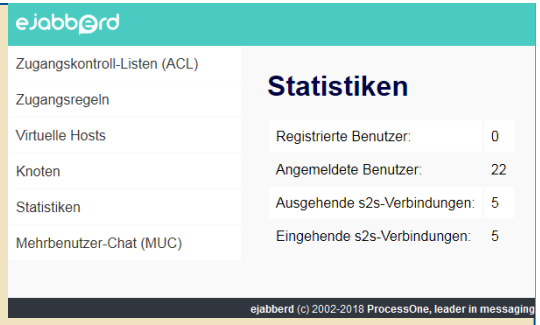
Studierende vorname.nachnameX.stud@jabber.uni-due.de

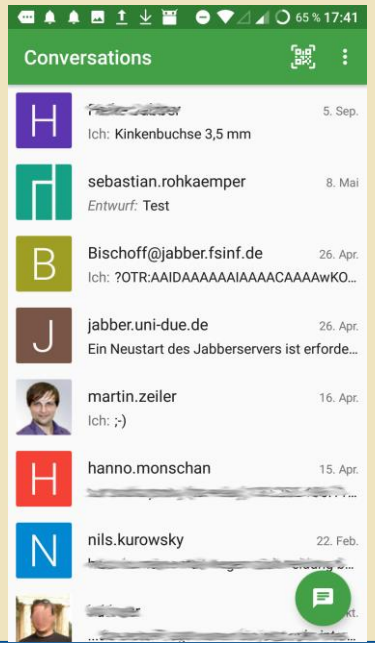
UNIVERSITÄT DUISBURG ESSEN

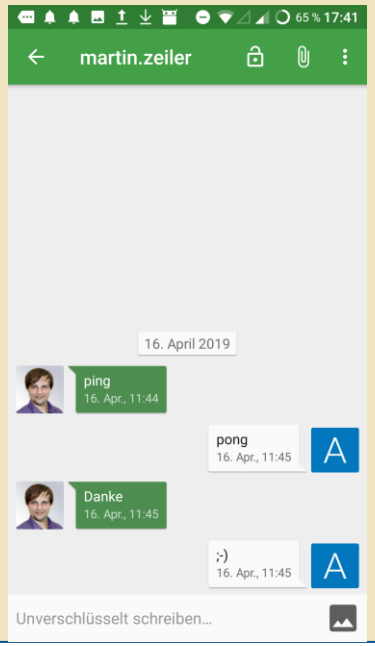
Offen im Denken

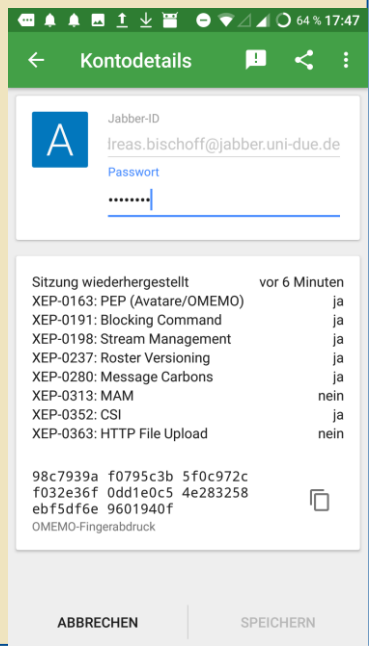
Jabber - Server - Clients

- An der UDE: eJabber als Server – Erlang (wg. LDAP) – viel einfacher Openfire (raspi)
- Großartiger Android-Client „*Conversations*“
- Ende-zu-Ende-Verschlüsselung mit OTR und Nachfolgestandard OMEMO
- Klienten für alle Betriebssysteme!







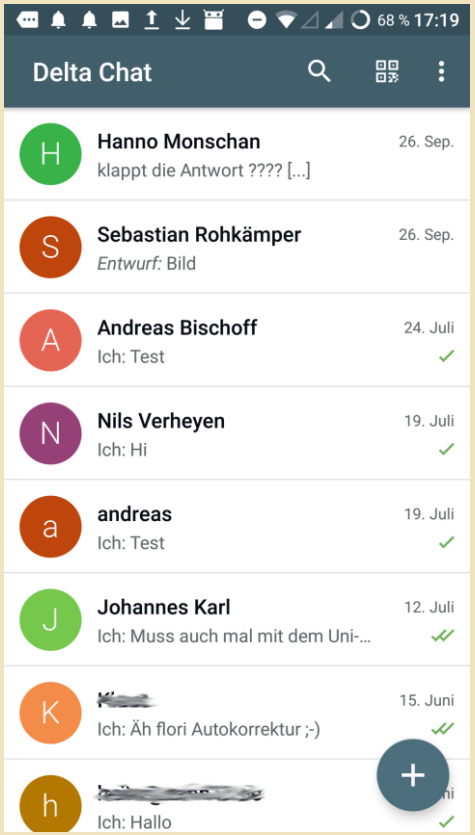


Delta-Chat

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

- Baut auf IMAP-Push auf
- Sieht aus wie ein Chat-Programm (Emoticons, Bilder, Audio Übertragung mit Icon)
- Verschlüsselt mit Autocrypt (GNUPGP – hat Snowden benutzt), transparent in einem IMAP-Verzeichnis
- Separiert Chat und Mail

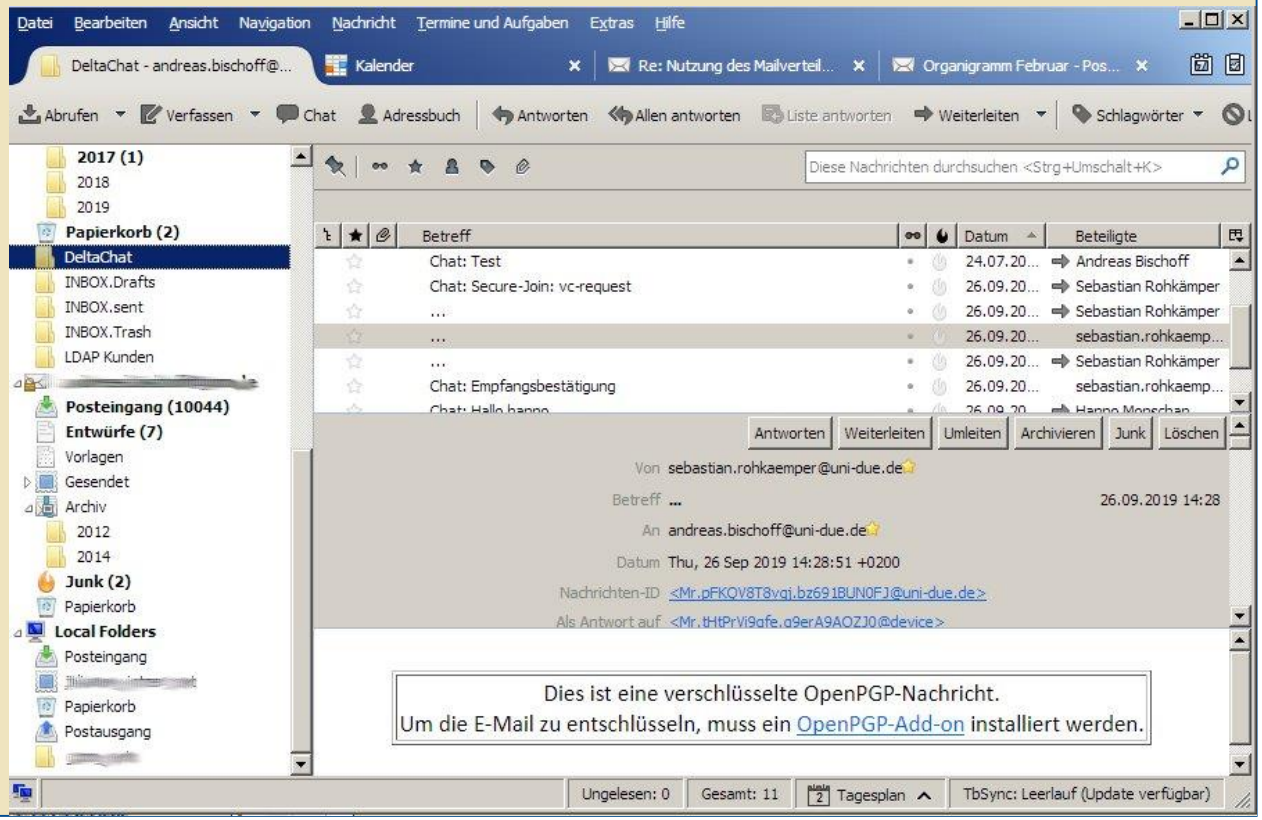


Delta-Chat

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

- „Abwärtskompatibel“ zu Mail – d.h. Nachrichten können auch an jeden versandt werden, der ein gewöhnliches Mailkonto hat
- Gruppenchats



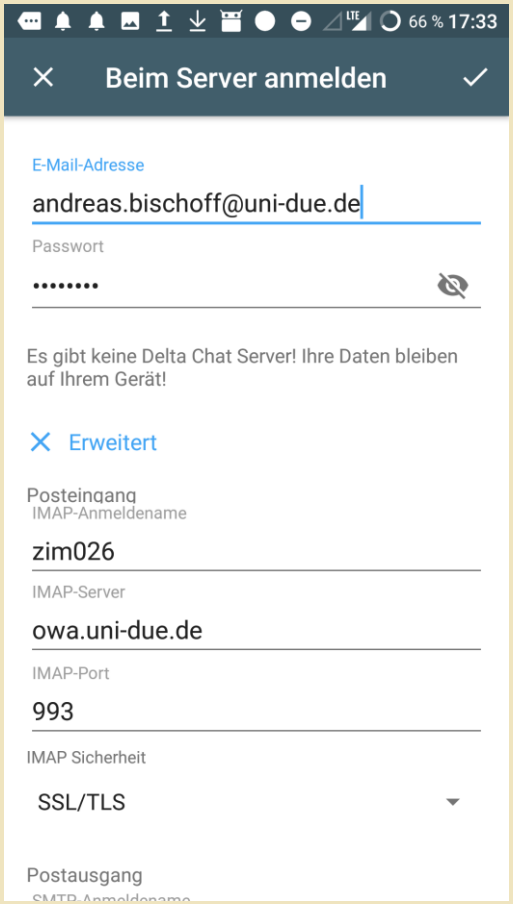
Delta-Chat

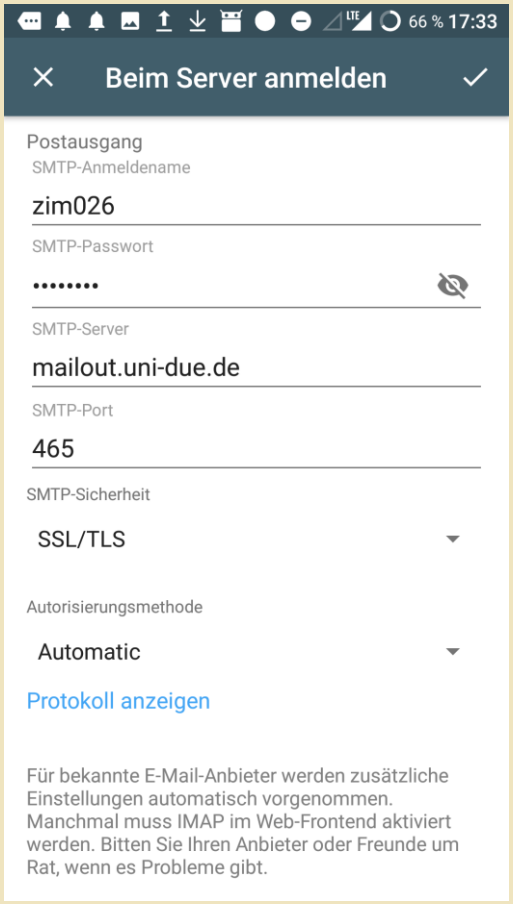
UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

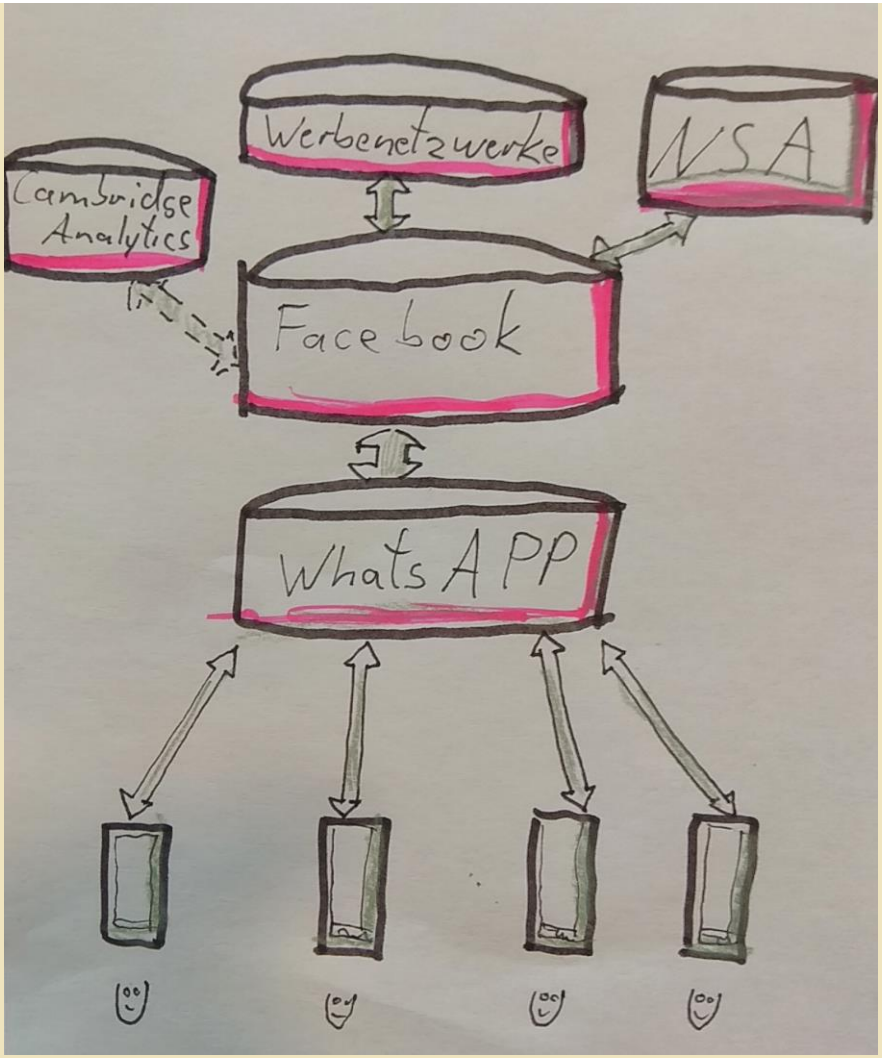
- Konfiguration an der UDE

Studierende geben als IMAP-Server '*mailbox.uni-duisburg-essen.de*', Mitarbeiter '*owa.uni-due.de*' an.



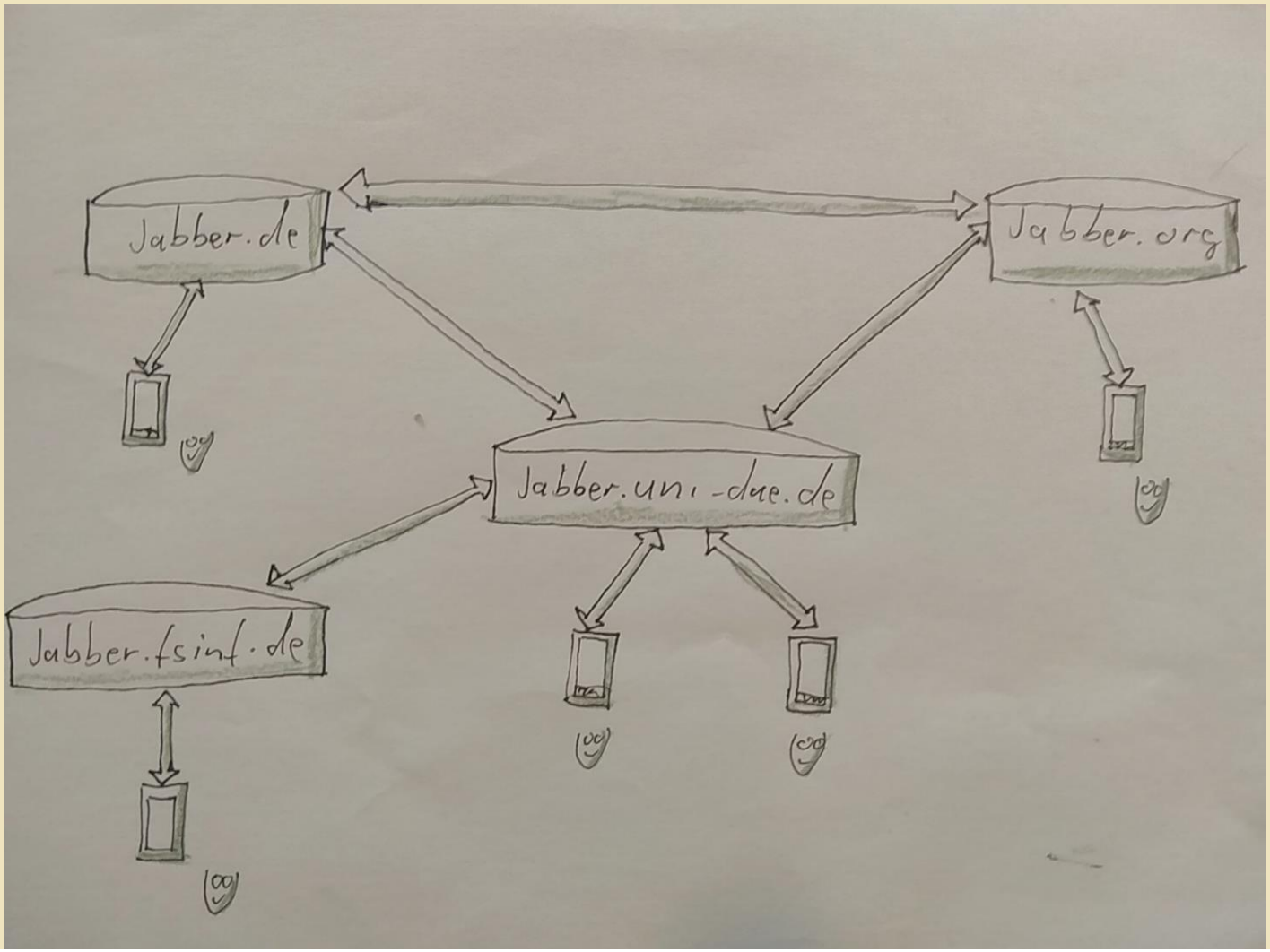


Warum ich so auf Metadaten herumreite



Warum ich so auf Metadaten herumreite

-



Warum ich so auf Ende-zu-Ende Verschlüsselung herumreite

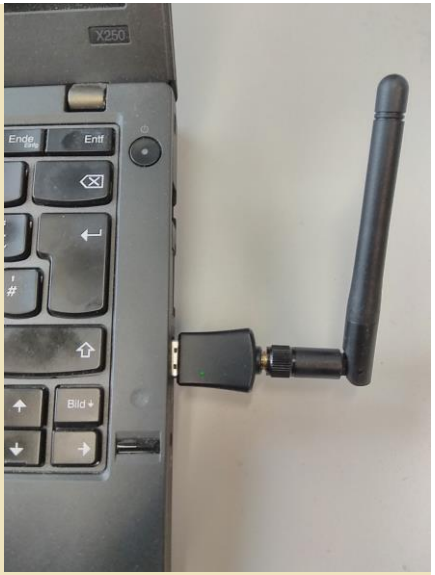
- Public-Private-Key Verfahren zwischen den Endgeräten
- Server sieht nur Metadaten „wer mit wem“
- Wo ist der private Key? Muss *immer geheim* bleiben!
- Kommen da andere Apps dran heran?
- Auf dem Endgerät ist die Kommunikation immer entschlüsselt
- Also sind lokale Angriffe auf das OS/die App möglich!
- Quellen-Telekommunikationsüberwachung (Quellen-TKÜ)
- Die App kann lokal Kommunikationsinhalte lesen und „passende“ Werbung schalten.

UNIVERSITÄT DUISBURG ESSEN

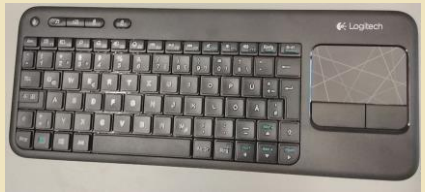
Offen im Denken

Live Hacking

Logitech Presenter, Mäuse und Tastaturen angreifen



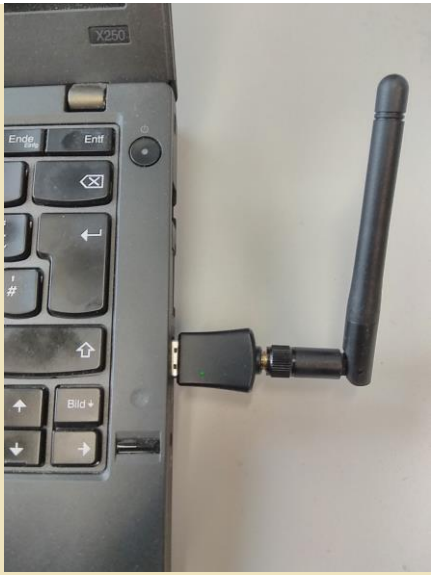
- Angriff auf Logitech Presenter
- Logitech Unifying ist eine *Bluetooth Low Energie* Variante
- Betroffen sind Logitech-Geräte, die mit der Unifying-Funktechnik arbeiten
- LogiTacker-Firmware läuft auf USB-Funk-Sticks mit nRF52840 von Nordic Semiconductor.
- https://github.com/mame82/LOGITacker
- Hardware hier 10€ aus China: April Brother.
- Stellt eine serielle Schnittstelle zur Verfügung für Angriffsbefehle
- Scripting -- Live-Demo



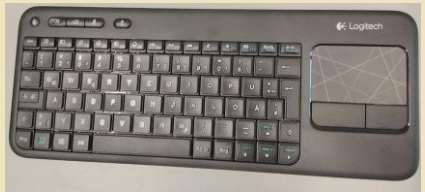
Logitech Presenter, Mäuse und Tastaturen angreifen

- Angriff auf Logitech Presen

Logitech Presenter, Mäuse und Tastaturen angreifen



- Angriff auf Logitech Presenter
- Logitech Unifying ist eine *Bluetooth Low Energie* Variante
- Betroffen sind Logitech-Geräte, die mit der Unifying-Funktechnik arbeiten
- LogiTacker-Firmware läuft auf USB-Funk-Sticks mit nRF52840 von Nordic Semiconductor.
- https://github.com/mame82/LOGITacker
- Hardware hier 10€ aus China: April Brother.
- Stellt eine serielle Schnittstelle zur Verfügung für Angriffsbefehle
- Scripting -- Live-Demo



UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

Sprachassistenten & smarte Lautsprecher (eigentlich *Mikrofone*)

Spracherkennung – ein bisschen Geschichte

- 2005-2007 Pioneer 3 AT Roboter (Spracherkennung erst lokal und dann über das Internet, heute würde man sagen in der Cloud)

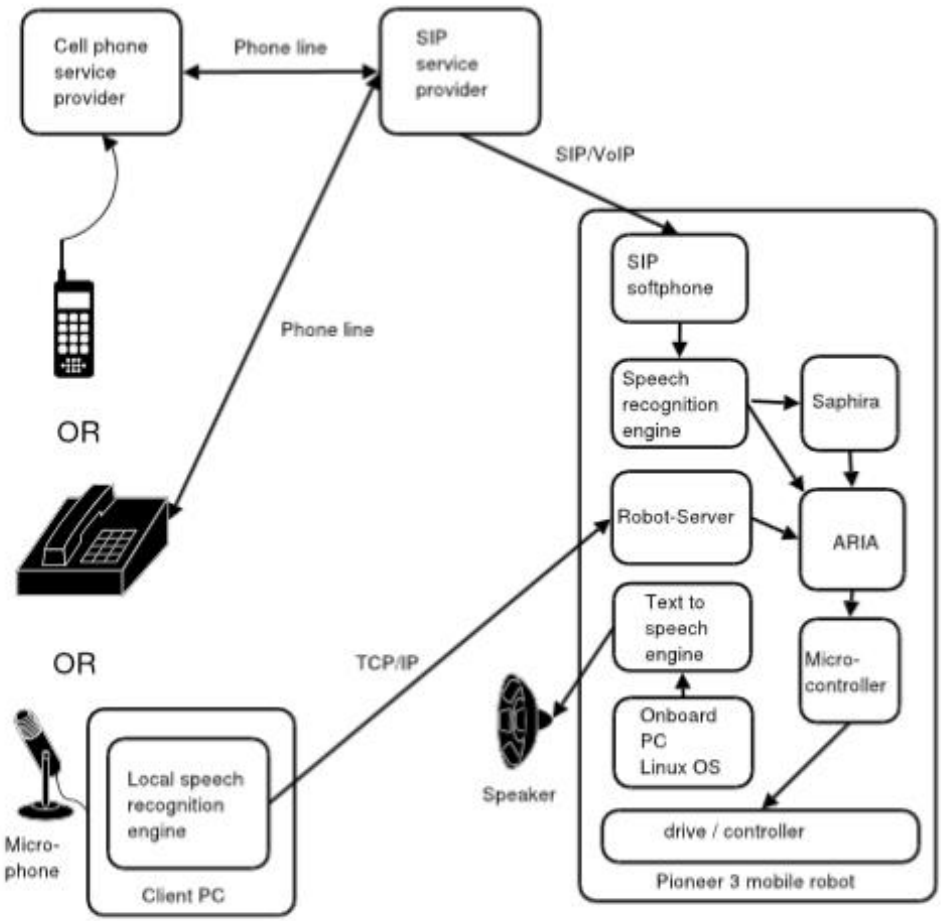
Video Link

Spracherkennung – ein bisschen Geschichte

2005-2007 Pioneer 3 AT Roboter (Spracherkennung erst lokal und dann über das Internet, heute würde man sagen in der Cloud)

So habe ich das 2005 realisiert →

2007 über ein Asterisk-Plugin das einen Spracherkennungs-Server im Netz benutzte



Auf PCs offline schon lange verfügbare Technik

- IBM ViaVoice (1997), Nuance, etc.
- Hype durch Apple-Siri (Apple kauft Siri Inc. 2010) ab 2011 im iPhone 4s
- Google zieht 2012 nach in Android 4.1 „Jelly Bean“ auf dem Galaxy Nexus. Google Now
- 2013 übernimmt Amazon das Startup Ivona und führt mit Amazon Echo mit dem Aktivierungsname „Alexa“ ein

Spracherkennung

Wearables und weitere Anwendungen

- Apple Watch
- Google Watch
- Android Car
- Smart TVs (häufig keine Updates)
- Märkte in der 3.Welt, Barierrefreiheit und funktionelle Analphabeten
- IoT-Devices

- **Android Wear**
  - „OK Google“
  - Bedienkonzept Spracheingabe
  - Nicht abschaltbar!
  - Auch wenn Google Now auf dem Smartphone deaktiviert ist.
  - Deaktivierbar nur durch den Flugmodus der Uhr
  - In diesem Modus ist aber nicht einmal die korrekte Anzeige der Uhrzeit gewährleistet.
  - „OK Google wähle 0900-“ → wählt ohne Nachfrage!

- **Apple Watch (ab 24.4.2015)**
  - „Hey Siri“
  - „Hey Siri wähle 0900-“ → Gespräch maximal 3 Euro pro Minute
  - Schon jetzt:
  - „Hey Siri, wem gehört dieses Telefon?“ http://www.golem.de/news/kontakte-siri-verraet-iphone-besitzer-1501-112006.html

Spracherkennung

- Einzelworterkennung
- Sprecherunabhängige Spracherkennung
- Offline Spracherkennung
- Spracherkennung in der Cloud
- Kommandoverarbeitung in der Cloud
- Die eigentliche KI (Spracherkennung== schwache KI) Google: Semantic Web, Heuristiken, Google-Assistant (einbeziehen weiterer Parameter, Kontext, Ort, Sensoren, weiteres Wissen des Assistenten, Terminkalender, Kontakte, Kommunikations*inhalte*)

Spracherkennung

- Wie lange werden die Sprachsamples dort gespeichert? Beispiel Google: Default ewig → https://myaccount.google.com „Daten & Personalisierung“ – „Sprach- & Audioaktivitäten“ – „Aktivitäten verwalten“ → Liste Ihrer bisherigen Spracheingaben mit Datum, das ist abschaltbar – aber wer weiß das hier?
- Sprachsamples sind *biometrische Daten!*
- *Sie können davon ausgehen, dass die NSA diese Daten für immer speichert! Siehe Edward Snowden „Permanent record“*

https://myaccount.google.com

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

Google Meine Aktivitäten

Gruppierte Ansicht

Einzelansicht

Aktivitäten löschen nach

Andere Google-Aktivitäten

Aktivitätseinstellungen

Google-Konto

Hilfe

Feedback geben

Datenschutzerklärung • Nutzungsbedingungen

YouTube-Verlauf

Im YouTube-Verlauf werden deine angesehenen YouTube-Videos und deine Suchanfragen gespeichert. Mithilfe dieser Daten können wir YouTube für dich optimieren und dich beispielsweise an Inhalte erinnern, die du dir angesehen hast, oder dir bessere Empfehlungen und Hinweise auf YouTuber geben, die dir gefallen könnten.

Sie können sich Ihre Aktivitäten ansehen, sie manuell löschen oder sie mithilfe der Einstellungen auf dieser Seite automatisch löschen lassen. Weitere Informationen

YouTube-Verlauf pausiert

- ✕ Angesehene Videos werden nicht gespeichert
- ✕ Suchanfragen werden nicht gespeichert

Einstellung ändern

Aktivitäten werden so lange gespeichert, bis du sie manuell löschst

Automatisch löschen

Nur Sie können diese Daten sehen. Google schützt Ihre Daten und Ihre Privatsphäre.

https://myaccount.google.com

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

Google Meine Aktivitäten

15. September

Google Assistant

Wie heißt caillous Katze gesagt

19:12 • Details •

Google Assistant

Wie heißt caillous Katze gesagt

Caillou – Wikipedia

Laut Wikipedia:

Rosie heißt im französischsprachigen Original Mousseline.

Wenn du mehr zu diesem Thema erfahren möchtest, folge dem Link in der Google Home App oder der Google Assistant App

19:12 • Details •

Google Assistant

wie schnell ist der schnellste Mensch gesagt

09:49 • Details •

Google Assistant

wie schnell ist der schnellste Mensch gesagt

45 km/h

09:49 • Details •

Google Assistant

Musik aus gesagt

09:26 • Details •

Elementdetails

Google Assistant

guten Morgen gesagt

Im Moment ist es halb sieben.

Im Moment ist es in Essen überwiegend bewölkt bei acht Grad.

Heute wird es überwiegend bewölkt bei Temperaturen zwischen acht und fünfzehn Grad.

Mach's gut!

Details

Heute um 06:30

Google Assistant

Voice und Audio

Google Assistant

Per Hotword gestartet

Google Home

Per Audioeingabe erstellt

Aufnahme ausblenden

0:00 / 0:03

Von meinem Gerät

Ungefähre Region ansehen

Spracherkennung

- Wie lange werden die erkannten Texte gespeichert? *(„Ich bring Dich um – scheiße schon passiert“* – Helge Schneider)
- Werden die Sprachsamples als Trainingsdaten für Neuronale Netze (KI/AI) genutzt?
- Hören Menschen dort zu Korrekturzwecken (möglicherweise als externe Dienstleister) rein? (Aktueller Skandal bei Apple und Amazon Google, etc.)

Menschen als Zuhörer überall - wall of shame:

Apple Siri:

- https://www.heise.de/newsticker/meldung/Verraeterische-Sprachassistentin-Auch-bei-Siri-hoeren-Menschen-zu-4480652.html

Amazon Alexa:

- https://www.heise.de/newsticker/meldung/Amazon-Mitarbeiter-tippen-zum-Teil-Alexa-Sprachbefehle-ab-4374871.html

Google Now:

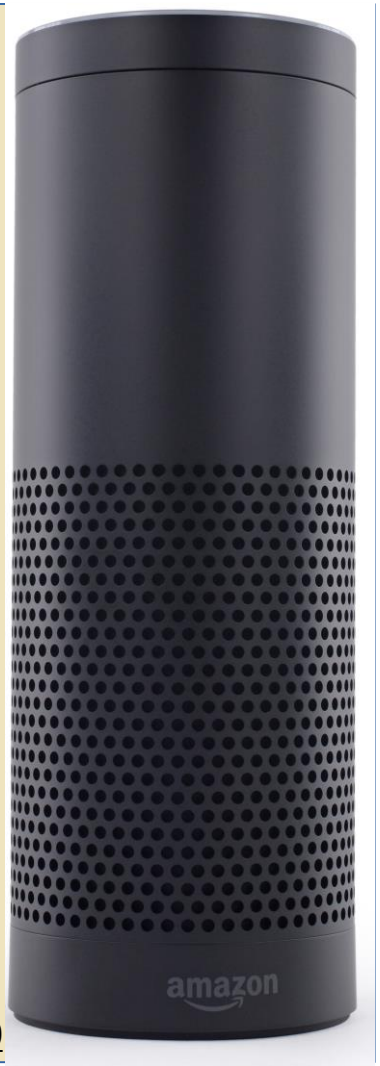
- https://www.heise.de/newsticker/meldung/Googles-Sprachassistent-Mitarbeiter-hoeren-und-bewerten-Audioaufnahmen-4467985.html

Cortana und Skype:

- https://www.heise.de/newsticker/meldung/Microsoft-weist-auf-menschliches-Mithoeren-hin-4497764.html

Spracherkennung

- Wie kann Missbrauch/Stalking/Hacking verhindert werden?
- Hacking-Potential – Sicherheitslücken (Cloud & lokal)
- Bei einem Mikrofon kann nicht sehen, ob es ein- oder ausgeschaltet ist
- Hören die Assistenten immer mit?
  Zwangsläufig ja, sie warten ja auf das Aktivierungswort! (Hoffentlich) erst dann Übertragung an den Cloud-Dienst. Also Vorsicht!
- Versehentliche Aktivierung „Alexander …“
- Was ist mit öffentlichen Räumen oder Sitzungen?
- Sind Sprachassistenten in nichtöffentlichen Sitzungen untersagt?

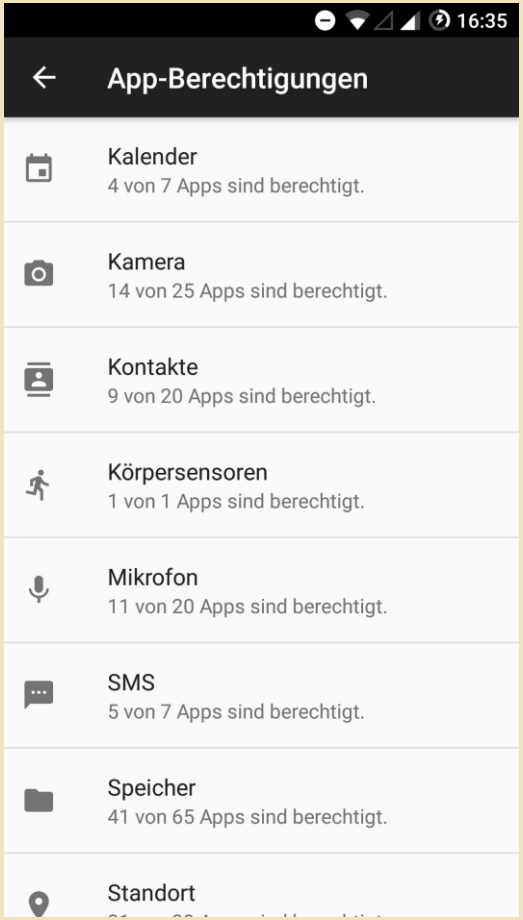


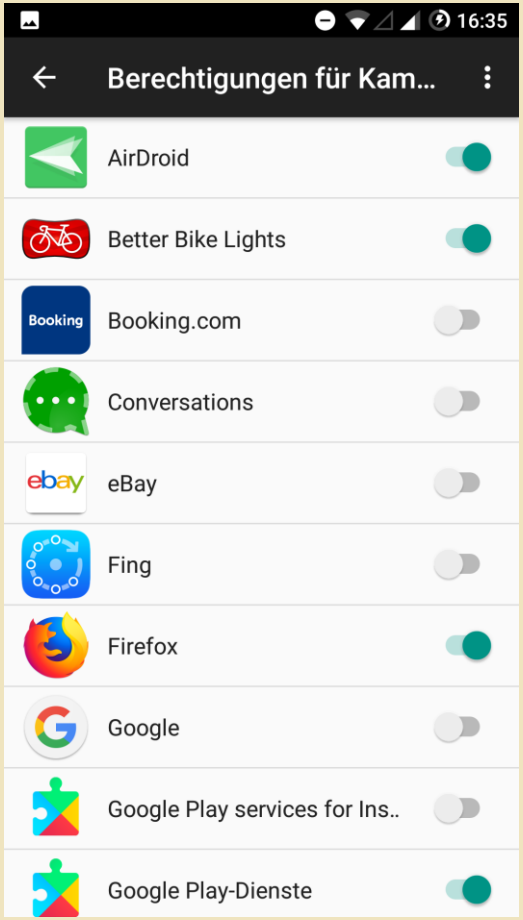
CC BY-SA 3.0

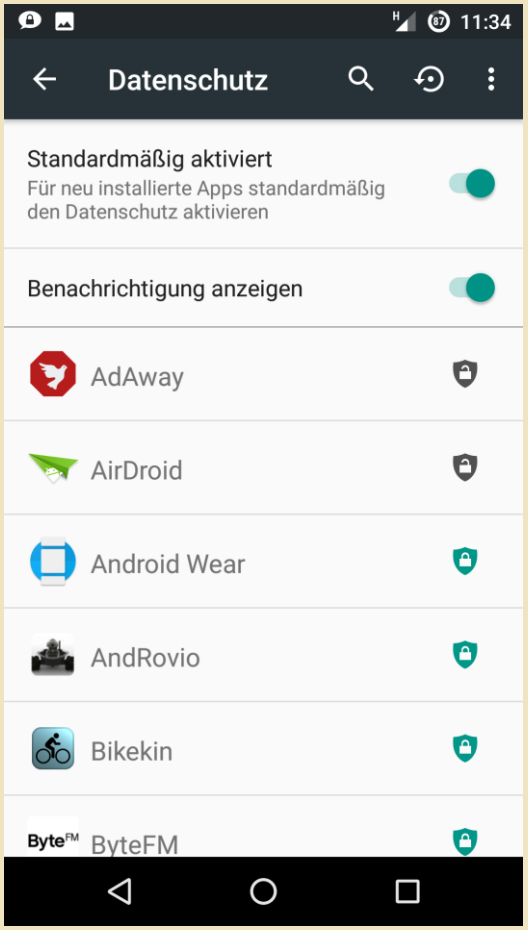
App-Rechte Android

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

APP-Rechte einstellen - Android: Ab Android 6 bzw. ab LineageOS 14 (bzw. einzelne Hersteller Huawei,Gigaset schon früher)







Tipp: „Einstellungen“ „Apps“ – „App-Berechtigungen“

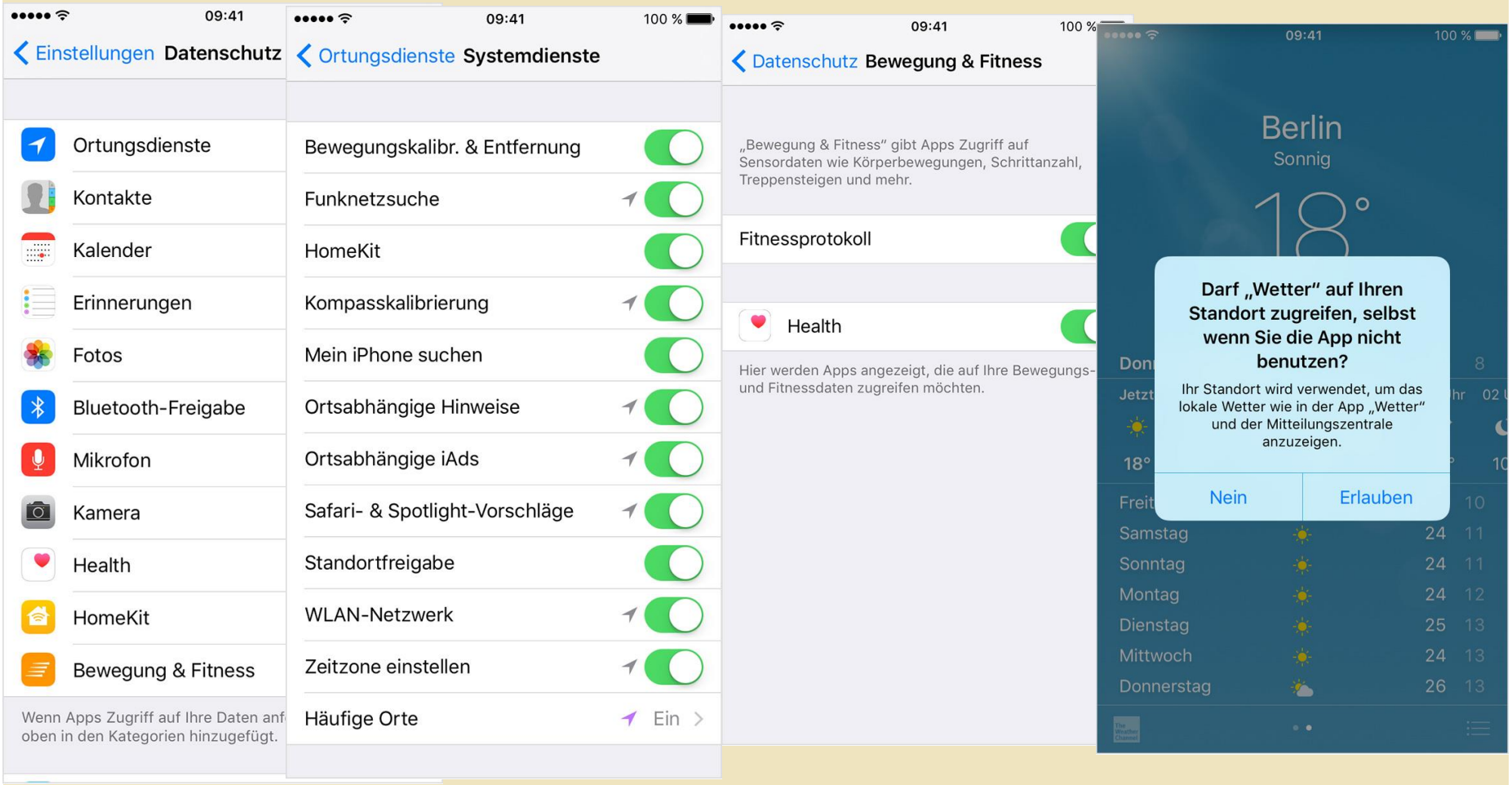
bzw.„ Einstellungen" > „Datenschutz"

App-Rechte IOS

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

APP-Rechte einstellen – iPhone unter Einstellungen Datenschutz:



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

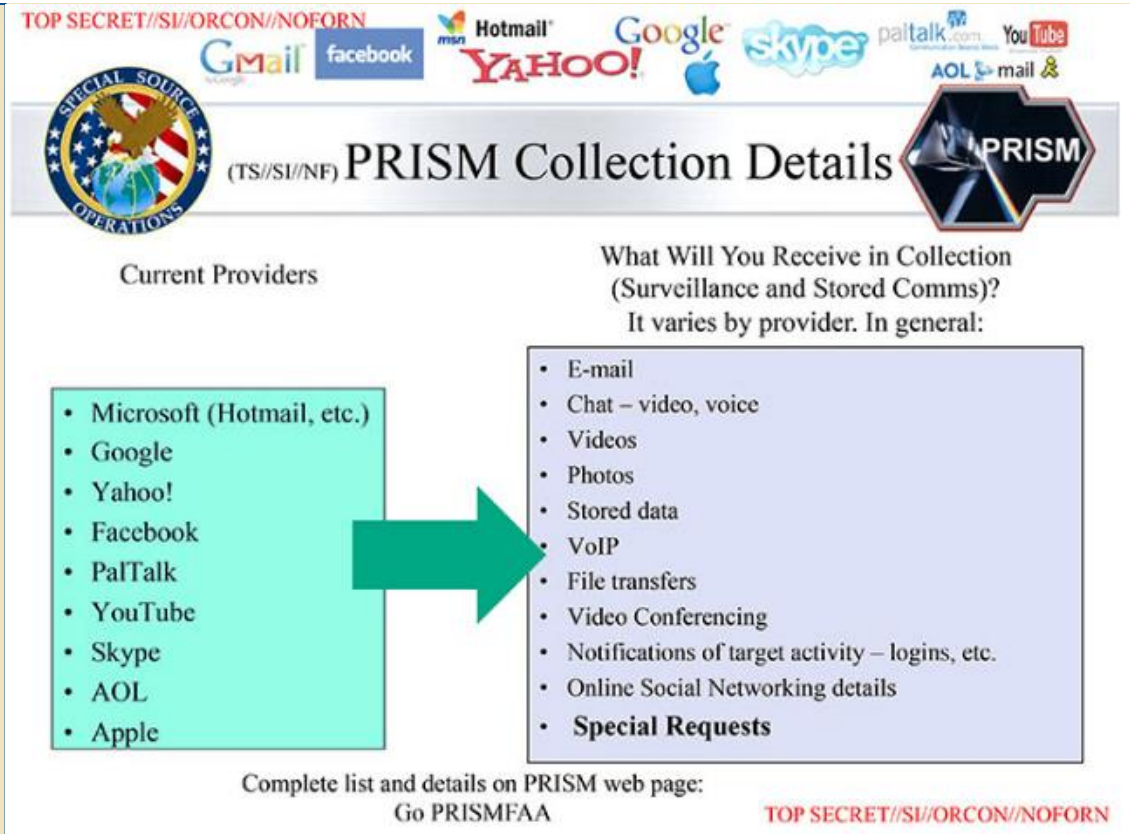
Spracherkennung

- Empfehlung: Cloudbasierte Systeme nicht nutzen!
- Wenn doch, AGBs *sehr genau* prüfen
- Softwareupdates! (lokale Geräte, Plaste-Router, CCC fordert MHD)
- Alle IoT-Geräte können Sicherheitslücken enthalten. Lebenszyklus-Patch-Zyklus siehe https://media.ccc.de/v/35c3-9723-smart_home_-_smart_hack (NODE MCU, ESP32 basierte „smarte Glühlampen“)
- Tipp: Ein abgeschaltetes System kann nicht mithören
- Alternativen: Raspberry PI: Intelligenter Offline Lautsprecher mit Spracherkennung – talking Pi – susi.ai talking speaker
- In der Cloud trainierte Modelle, die dann Offline laufen (aber auch hier Problem mit den Trainingsdaten) diverse Dienstleister
- Oder das Licht/den TV/ selber ein- und ausschalten ;-)

Spracherkennung

Wenn Du meinst Privatsphäre ist Dir egal, weil Du nichts zu verbergen hast, kannst Du genauso behaupten Redefreiheit ist Dir egal, nur weil Du nichts zu sagen hast!

Edward Snowden



This image is a work of a U.S. military or Department of Defense employee, taken or made as part of that person's official duties. As a work of the U.S. federal government, the image is in the public domain.

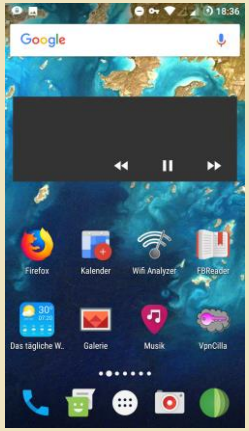
Quelle: Wikipedia

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

Live Hacking

- **Vertrauen schaffen – mit welchem Netz bin ich verbunden? → SSID der Name des WLANs**



mein Handy ←→ mein Router

mein WLAN ←→ mein Passwort

→ mein Internet-Provider

→ DAS I-NET

- Wer ist auf der anderen Seite? Das Internet? Wer ist dazwischen?
- Verschlüsselung!
- WEP (unsicher)/ WPA (seit 2009 geknackt)/ WPA2 (Angriffe seit 2017)

Angriff → Ich behaupte einfach, ich bin die Telekom oder Freifunk oder irgendein Anderer

dein Handy ←→ mein Router

kein Passwort !

www.facebook.de →

→ ICH bestimme

was hier passiert!

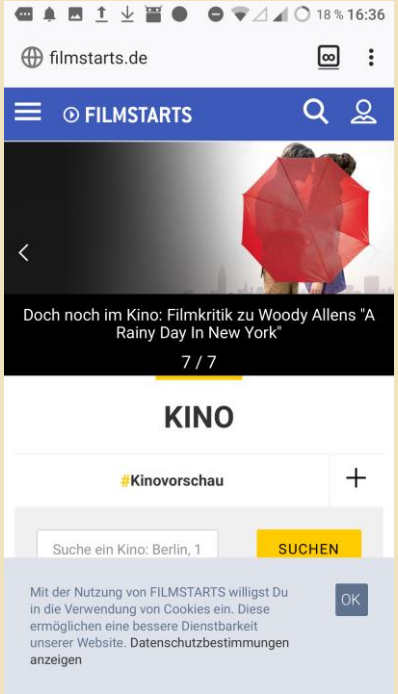
→ mein Webserver

tut so als ob er z.B. facebook wäre!

- Kann man jemals sicher sein mit der richtigen Seite verbunden zu sein?
- Ja – mit https → sicheres Internet
- Wenn Warnungen kommen vorsichtig sein!
- WLAN immer abstellen wenn nicht benötigt!

Im Handy-Browser „filmstarts.de“ eingeben

wer das sieht:



Ist im Internet

Wie ist das passiert?

WLAN an und automatisch verbunden mit Netz telekom/freifunk/WIFIonICE

Abhilfe: WLAN abstellen!

wer das sieht:

ist (von mir) gehackt

WLAN -Sicherheit

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

Wer mutig ist: Auf den Button

„hier niemals klicken“

klicken!

Das passiert – ist aber nur ein Fake ;-)

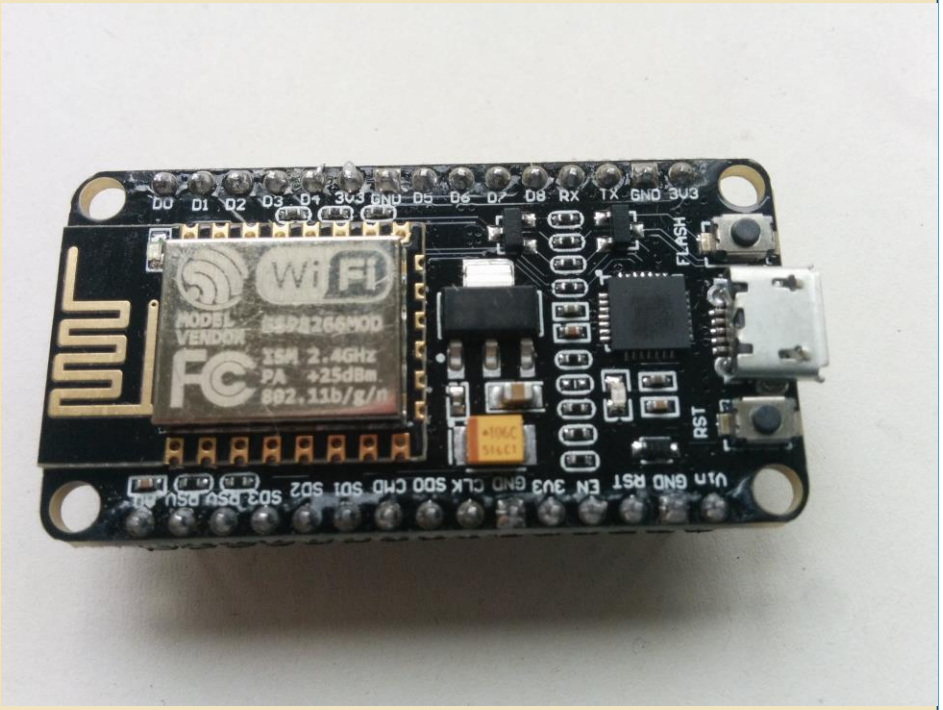
Wie habe ich das realisiert:

- Ich biete die SSIDs freifunk, telekom, WIFIonICE, Stadtwerke-WLAN, RRX, Kamps unverschlüsselt an – das kann jeder AP tun!
- DNSmask auf openWRT so konfiguriert, dass alles außer uni-due.de google.de google.com wikipedia.org auf den lokalen Webserver aufgelöst wird
- Webserver mit modifizierter 404 Seite, die dann immer auf die oberste index.html verweist
- Aber: Damit aktuelle Android und IOS Smartphones denken sie sind im Internet müssen auch: https://connectivitycheck.gstatic.com https://clients3.google.com https://captive.apple.com erreichbar sein! (Captive Portal Detection)
- Durch die Verwendung von https ist dieser Angriff nicht mehr offline möglich! DNSSEC oder https-Anywere hätten den den Angriff auch verhindert!

WLAN - Sicherheit

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

  (nur 2,4GHz)



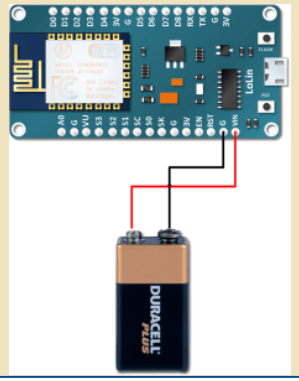
https://github.com/spacehuhn/esp8266_deauther

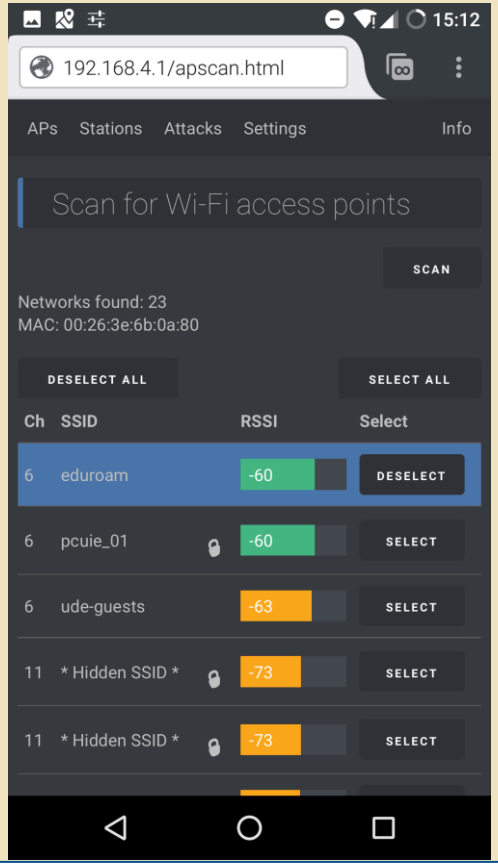
WLAN - Sicherheit

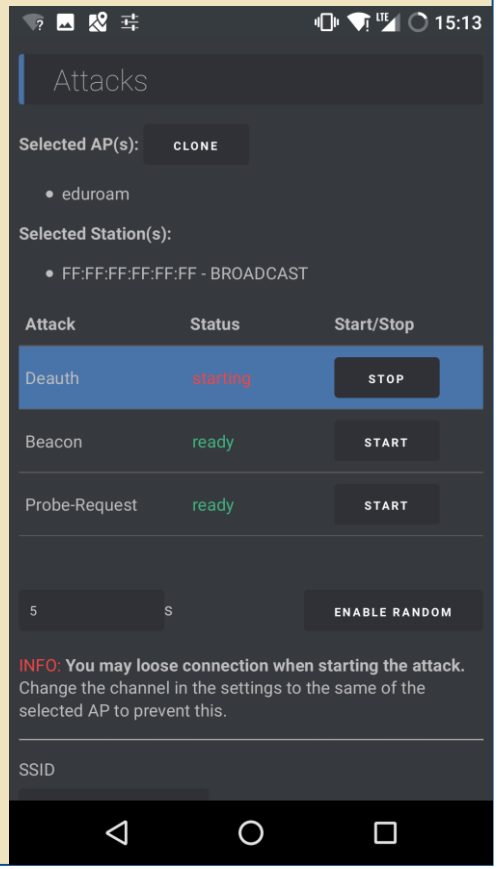
- Jetzt auch als Armbanduhr: NodeMCU ESP8266 mit „Spacehuhn Deauthenticator“
- Sendet für all WLAN-SSIDs in Reichweite Deauth-Pakete an alle WLAN-Klienten in Reichweite
- ALLE fliegen raus! (nur 2,4GHz)
- +Broadcast-Angriff → 60+ freie WLANs mit zufälligen SSIDs tauchen plötzlich auf!

„Spacehuhn Deauthenticator“

- schönes GUI
- HW aus China: 3$ incl. Versand
- mit 9V Batterie < 4€
- 2 Tage fun
- Uhr 30€

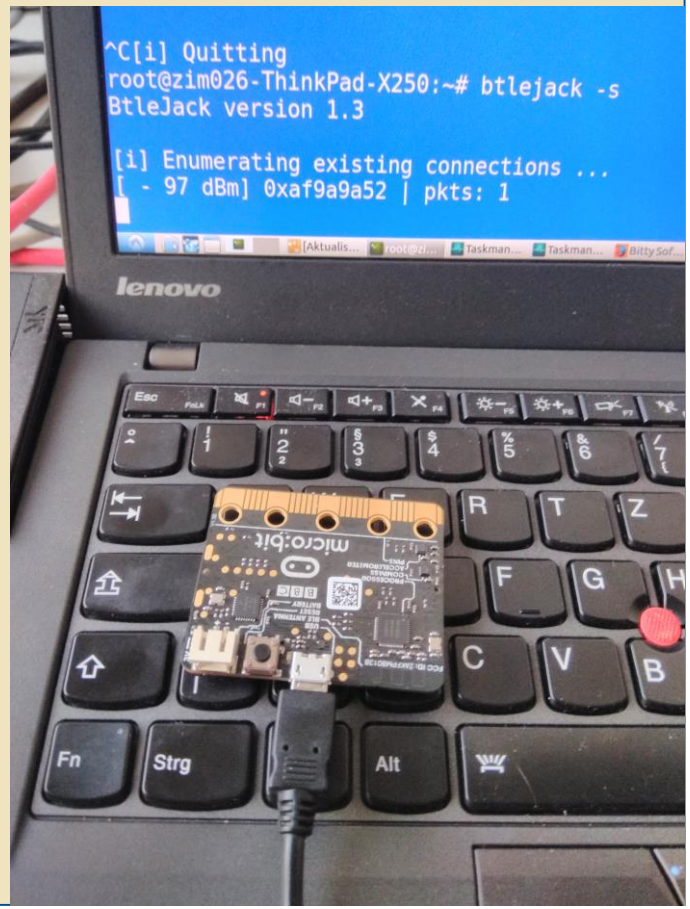






Bluetooth - Sicherheit

- Bluetooth LE (Low Energy) IoT ist angreifbar
- Btlejack
- Mit 3 BBC micro:bit kann jeder Bluetooth LE Verbindungsaufbau belauscht werden!
- Bestehende Verbindungen können ge-jammed und in ein pcap-File (Wireshark) geschrieben werden



Der ECSM – Unsere Vorträge 2019

EUROPÄISCHER MONAT DER CYBER-SICHERHEIT

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

- Warum IT-Sicherheit sinnlos ist

  Mi, 16.10.2019 14:00 Uhr c.t.

  Tim Berghoff (GDATA)

- Phishers Fritze phisht... Neues vom Anglerladen

  22.10.2019 14:00 Uhr c.t.

  Dr. Marius Mertens

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

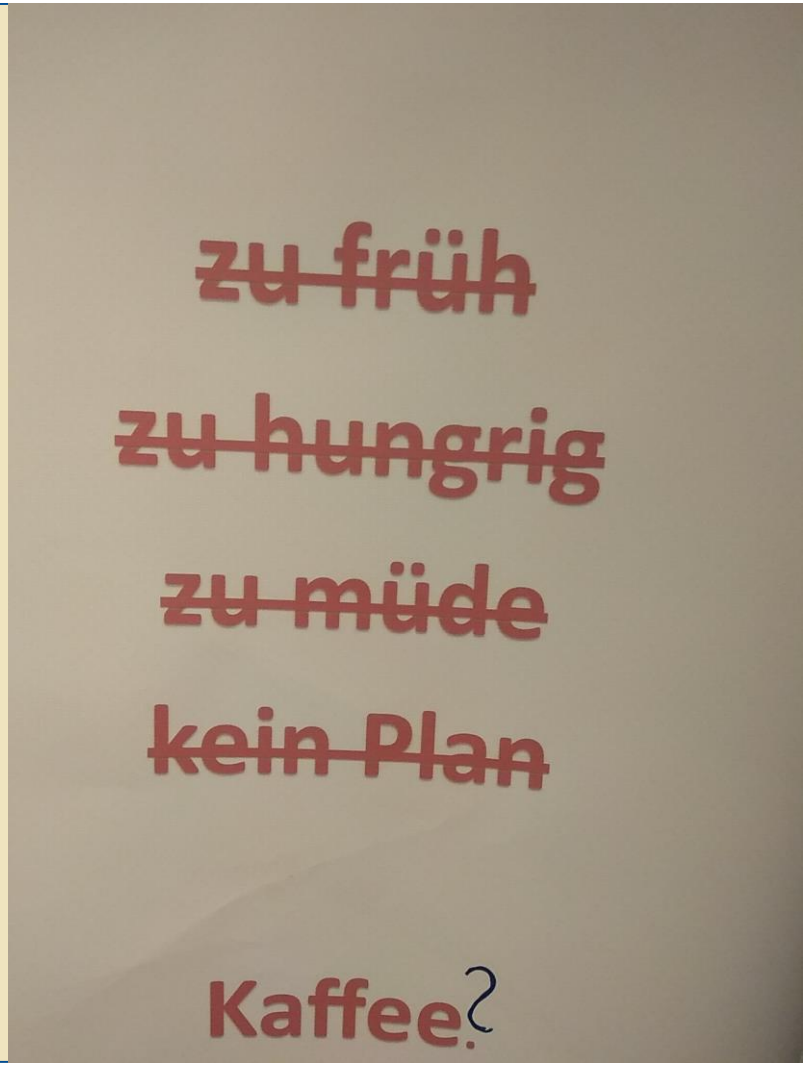
Vielen Dank!

Folien unter:

https://www.uni-due.de/~bischoff/

Kontakt:

Andreas.bischoff@uni-due.de



Der ECSM – Unsere Vorträge 2019

EUROPÄISCHER MONAT DER CYBER-SICHERHEIT

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

- Warum IT-Sicherheit sinnlos ist

  Mi, 16.10.2019 14:00 Uhr c.t.

  Tim Berghoff (GDATA)

- Phishers Fritze phisht... Neues vom Anglerladen

  22.10.2019 14:00 Uhr c.t.

  Dr. Marius Mertens