

Smartphonesicherheit

Marius Melzer (marius@rasumi.net)
Chaos Computer Club Dresden

15.03.2016

Chaos Computer Club



- Verein wurde 1981 gegründet (<https://ccc.de>)

Chaos Computer Club



- Verein wurde 1981 gegründet (<https://ccc.de>)
- Aktuell > 6000 Mitglieder

Chaos Computer Club



- Verein wurde 1981 gegründet (<https://ccc.de>)
- Aktuell > 6000 Mitglieder
- Technologie zum gesellschaftlichen Nutzen (und nicht ihrem Schaden)

Chaos Computer Club



- Verein wurde 1981 gegründet (<https://ccc.de>)
- Aktuell > 6000 Mitglieder
- Technologie zum gesellschaftlichen Nutzen (und nicht ihrem Schaden)
- Betreibt u.a. Öffentlichkeitsarbeit und Politikberatung

Chaos Computer Club



Chaos Computer Club



Chaos Computer Club



- Chaos Computer Club Dresden (<https://c3d2.de>)

Chaos Computer Club



- Chaos Computer Club Dresden (<https://c3d2.de>)
 - Datenspuren: Herbst 2016 (<https://datenspuren.de>)

Chaos Computer Club



- Chaos Computer Club Dresden (<https://c3d2.de>)
 - Datenspuren: Herbst 2016 (<https://datenspuren.de>)
 - Podcasts (<https://c3d2.de/radio.html>)



Chaos Computer Club



- Chaos Computer Club Dresden (<https://c3d2.de>)
 - Datenspuren: Herbst 2016 (<https://datenspuren.de>)
 - Podcasts (<https://c3d2.de/radio.html>)
 - Chaos macht Schule (<https://c3d2.de/schule.html>)



Bundespräsident Gauck zur NSA-Überwachung

“Wir wissen z.B., dass es nicht so ist, wie bei der Stasi und dem KGB, dass es dicke Aktenbände gibt, wo unsere Gesprächsinhalte alle aufgeschrieben und schön abgeheftet sind. Das ist es nicht.” (Gauck, 30.06.2013 im ZDF-Sommerinterview)

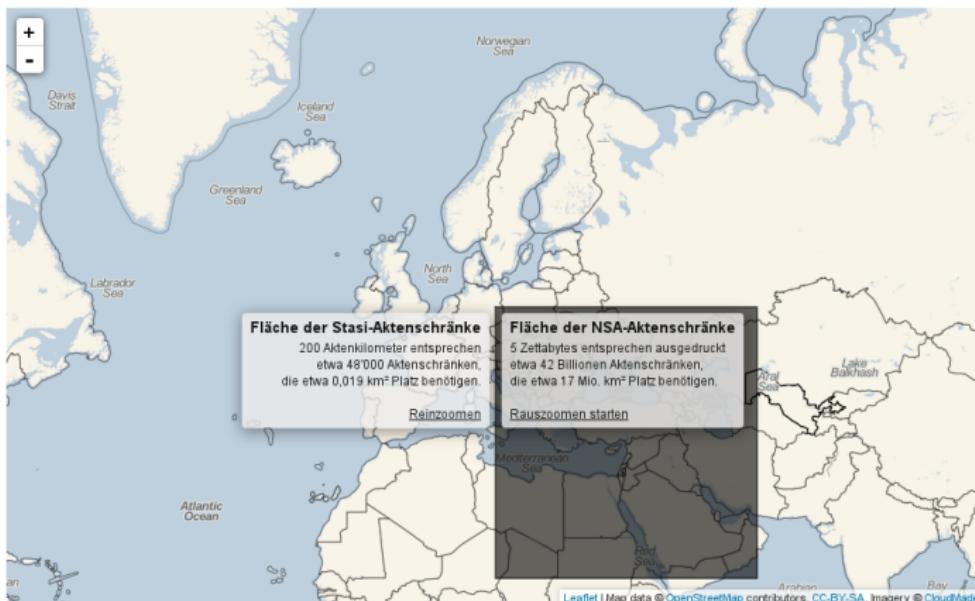
Stasi vs. NSA



Realisiert von [OpenDataCity](#). Anwendung steht unter CC-BY 3.0.



Stasi vs. NSA



“Ich hab ja nichts zu verbergen”

“Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.” (Edward Snowden, 21.05.2015 auf Reddit)

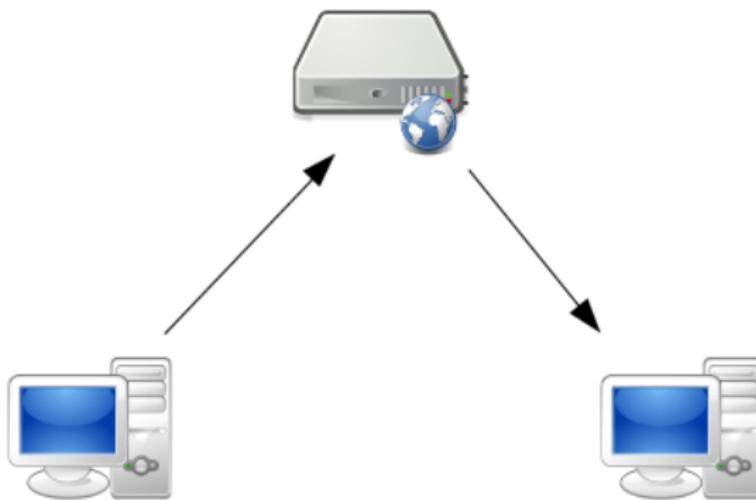
Samsung vs. 1984

Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

If you do not enable Voice Recognition, you will not be able to use interactive voice recognition features, although you may be able to control your TV using certain predefined voice commands. While Samsung will not collect your spoken word, Samsung may still collect associated texts and other usage data so that

Behind Winston's back the voice from the telescreen was still babbling away about pig-iron and the overfulfilment of the Ninth Three-Year Plan. The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live--did live, from habit that became instinct--in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

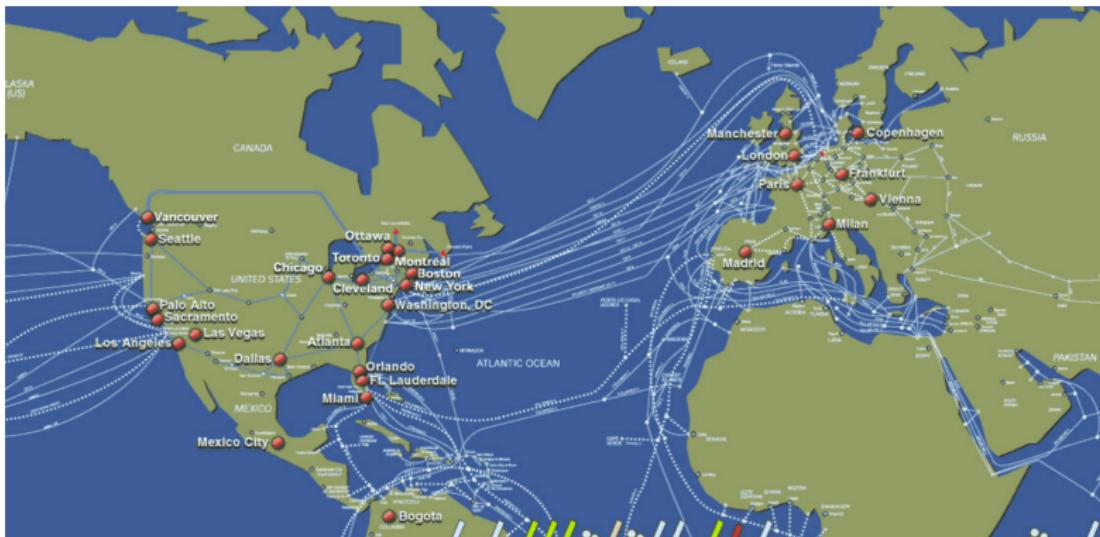
Wie kommunizieren wir im Internet?



Server im Rechenzentrum



Internetknoten (Router)

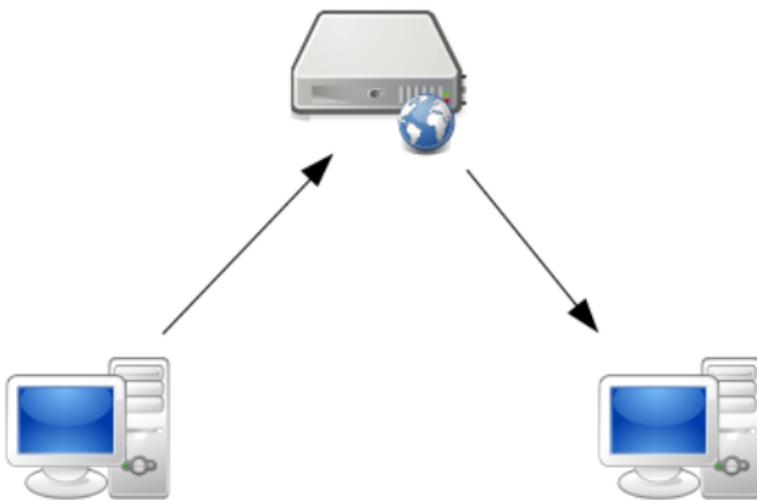


Internetknoten (DE-CIX in Frankfurt)



Grafik:  Stefan Funke

Was ist zu schützen?



Einleitung
oooooooooooo

Einführung
ooooo

Geräte
●oooooooooooooooooooo

Inhalte
oooooooooooo

Metadaten
oooooooooooo

Verhalten
○

Fazit
○

Problematisches Verhalten von Software

Problematisches Verhalten von Software

- Sicherheitslücken

Problematisches Verhalten von Software

- Sicherheitslücken
- Backdoors

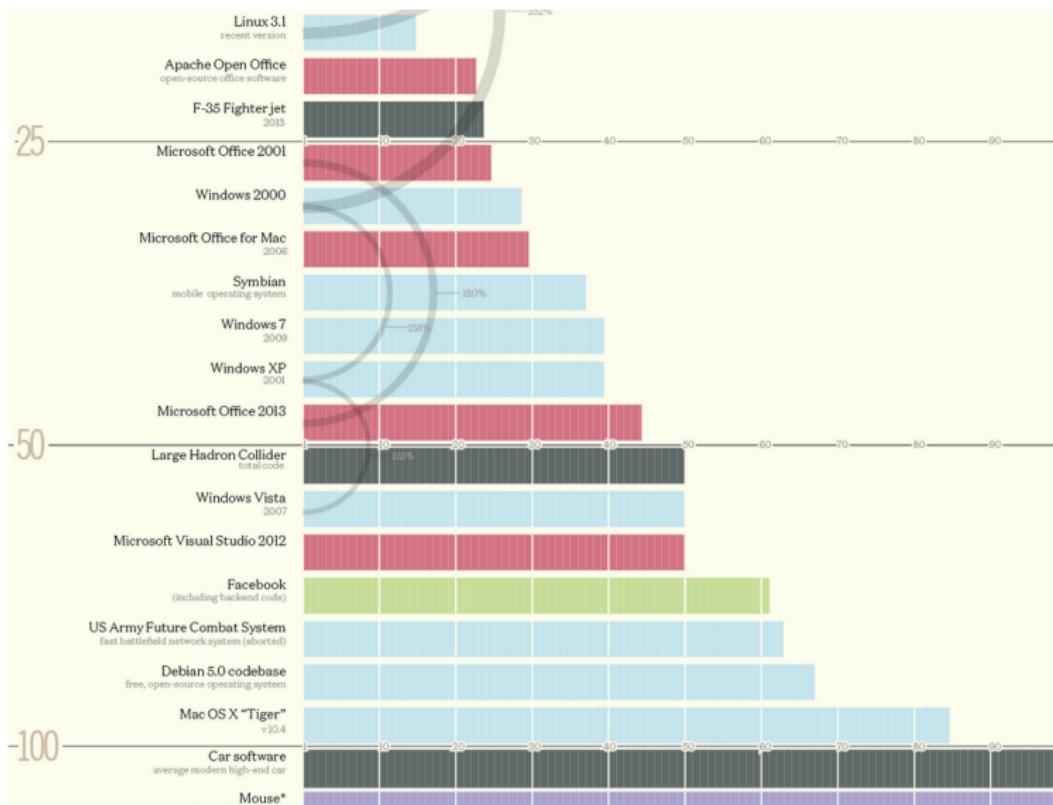
Problematisches Verhalten von Software

- Sicherheitslücken
- Backdoors
- Unerwünschte Funktionalität

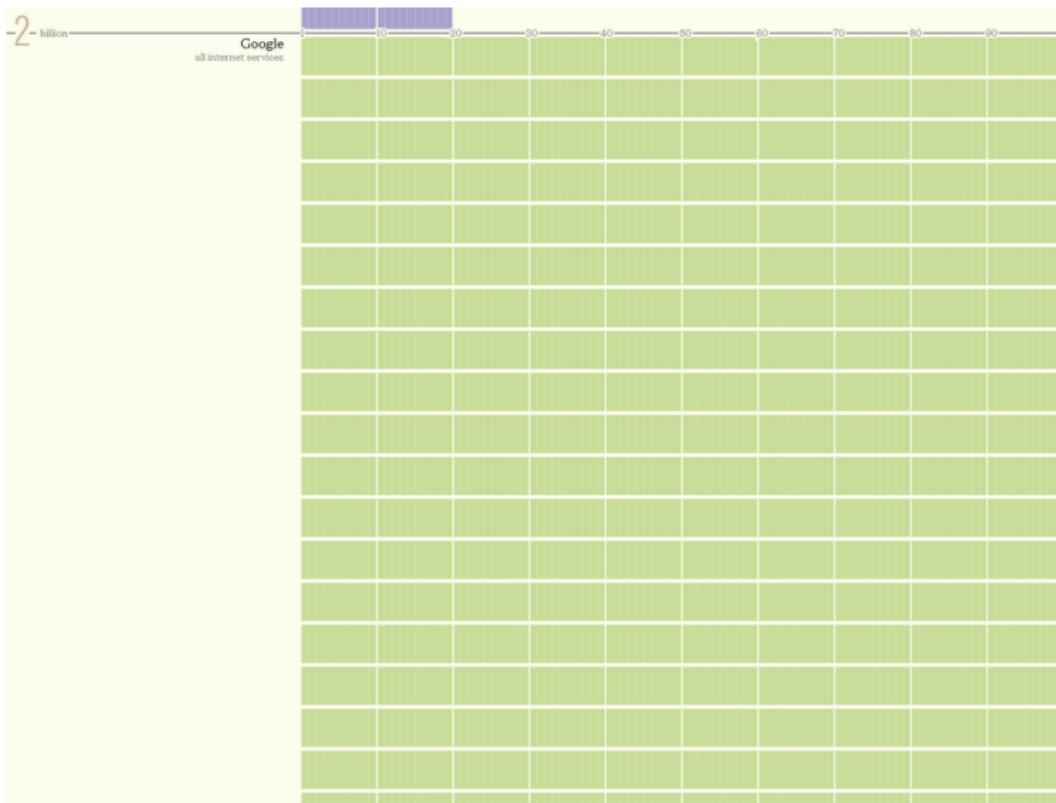
Schwachstellen

```
1 #include "stdio.h"
2
3 int main(int argc, char** argv) {
4     char* secret_number = "Dies ist mein Passwort!\n";
5     printf(argv[1]);
6     return 0;
7 }
```

Größe von Softwareprojekten



Größe von Softwareprojekten



Backdoors

c't magazin Startseite Artikel c't-Projekte Hotline & FAQ

Magazin Internet Software Hardware Know-how Praxis Artikel-Foren

c't > aktuell

Micha Borrmann, Jürgen Schmidt

G't 17/13

Microsofts Hintertür

Zweifelhafte Updates gefährden SSL-Verschlüsselung

Was macht Windows, wenn es auf ein Verschlüsselungszertifikat trifft, dessen Echtheit es nicht überprüfen kann? Es schlägt nicht etwa Alarm, sondern fragt bei Microsoft nach, ob man dort zufällig jemanden kennt, der das Zertifikat für echt erklären möchte.



Backdoors

Android-VirensScanner schnüffeln Surf-Verhalten aus

 vorlesen / MP3-Download

Viele VirensScanner für Android senden mehr Daten an ihren Hersteller, als sie sollten. c't hat sie dabei ertappt, wie sie Privates übertragen und HTTPS unterwandern. Eine der größten Datenpetzen wurde über 100 Millionen Mal installiert.

Millionenfach installierte VirensScanner für Android überwachen das Surf-Verhalten ihrer Nutzer und übermitteln ihre Erkenntnisse an die Hersteller. Dabei untergraben Sie sogar die Sicherheit von verschlüsselten HTTPS-Verbindungen. Dies berichtet c't in der aktuellen Ausgabe 6/14.

Wir analysierten bei sechs verbreiteten Android-Virenscannern die Kommunikation mit dem jeweiligen Hersteller und stießen in vier Fällen auf ernsthafte Datenschutzprobleme. Alle getesteten Apps bieten eine Safe-Browsing-Funktion, bei beim Besuch potenziell bösartiger Web-Seiten Alarm schlagen soll. Ob eine Seite bösartig ist oder nicht, erfragen die Apps bei der Hersteller-Cloud. Dabei gehen oft aber mehr Daten durch die Leitung als nötig.

Backdoors (politische Debatte)

Großbritannien: Cameron will gegen Verschlüsselung vorgehen

 heise online 13.01.2015 10:27 Uhr – Martin Holland

 vorlesen



David Cameron bei der Ankündigung seiner Gesetzespläne (Bild: Screenshot - BBC)

Als Reaktion auf die Anschläge in Paris hat Großbritanniens Premier David Cameron

Unerwünschte Funktionalität

The screenshot shows the Windows Settings interface under 'DATENSCHUTZ' (Data Protection). The left sidebar lists categories: Allgemein, Position, Kamera, Mikrofon, Spracherkennung, Freihand und Eingabe, Kontoinformationen, Kontakte, Kalender, Messaging, Funkempfang, Weitere Geräte, Feedback und Diagnose, and Hintergrund-Apps. The 'Allgemein' tab is selected. On the right, under 'Datenschutzoptionen ändern', several options are listed with toggle switches:

- Apps die Verwendung der Werbungs-ID für App-übergreifende Erfahrungen erlauben (bei Deaktivierung wird Ihre ID zurückgesetzt)
Aus (switched off)
- SmartScreen-Filter einschalten, um von Windows Store-Apps verwendete Webinhalte (URLs) zu überprüfen
Ein (switched on)
- Informationen zu meinem Schreibverhalten an Microsoft senden, um die Eingabe- und Schreibfunktionen in Zukunft zu verbessern.
Aus (switched off)
- Websites den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen
Aus (switched off)
- [Microsoft-Werbung und andere Personalisierungsinfos verwalten](#)
- [Datenschutzbestimmungen](#)

Unerwünschte Funktionalität

App name	iPhone		Android		Does not transmit data		
	Username Password	Contacts	Age, Gender	Location	Phone ID	Phone number	
0.03 Seconds Pro	■	■	■	■	■	■	
Age My Face	■	■	■	■	■	■	
Angry Birds	■	■	■	■	■	■	
Angry Birds Lite	■	■	■	■	■	■	
Aurora Feint II: Lite	■■■	■	■	■	■	■	
Barcode Scanner (BahnTech)	■	■	■	■	■	■	
Bejeweled 2	■	■	■	■	■	■	
Best Alarm Clock Free	■	■	■	■	■	■	
Bible App (LifeChurch.tv)	■	■	■	■	■	■	
Bump	■	■	■	■	■	■	
CBS News	■	■	■	■	■	■	
0.03 Seconds	■	■	■	■	■	■	
Dictionary.com	■	■	■	■	■	■	

Unerwünschte Funktionalität

Google knows nearly every Wi-Fi password in the world

By [Michael Horowitz](#)

September 12, 2013 10:44 PM EDT  194 Comments



If an Android device (phone or tablet) has ever logged on to a particular Wi-Fi network, then Google probably knows the Wi-Fi password. Considering how many Android devices there are, it is likely that Google can access most Wi-Fi passwords worldwide.

Recently [IDC reported](#) that 187 million Android phones were shipped in the second quarter of this year. That multiplies out to [748 million phones](#) in 2013, a figure that *does not* include Android tablets.

Unerwünschte Funktionalität

“Tie all of our products together, so we further lock customers into our ecosystem” (Steve Jobs)

Unerwünschte Funktionalität

WhatsApp to begin sharing your data with Facebook

By Killian Bell



The image shows a screenshot of the WhatsApp Terms and Privacy Policy screen. At the top, there are three tabs: 'Terms and Privacy Policy' (green), 'Account' (blue), and 'Security' (red). The 'Account' tab is active, showing options like 'Privacy', 'Payment info', 'Change number', 'Delete my account', and 'Network usage'. Below these, there's a section titled 'Share my account info' with the sub-instruction 'Share my WhatsApp account information with Facebook to improve my Facebook experiences'. A checked checkbox at the bottom of this section has the same text. At the very bottom, there's a green 'AGREE' button.

Simple. Personal. Real-Time Messaging

Download Now

About

FAQ

Share my WhatsApp account information with Facebook to improve my Facebook experiences

AGREE

← Terms and Privacy Policy ← Account ← Security

WhatsApp Messenger

Privacy

Payment info

Change number

Delete my account

Network usage

Share my account info

Share my WhatsApp account information with Facebook to improve my Facebook experiences

To make WhatsApp secure, your chats and calls are automatically end-to-end encrypted.

This means your content is private, so WhatsApp and third parties can't see it.

Learn more about WhatsApp security.

Show security indicators

If you'd like to verify your chats and calls are end-to-end encrypted, enable this setting and tap "verify security number" in contact info, group info, or when you're in a WhatsApp call. Your chats and calls are encrypted regardless of this setting.

⟨ / ⟩

Share icon

Wie schütze ich mein Smartphone?

- Rechte von Applikationen einschränken (Permissions, Firewall)
- Aktuelle und vertrauenswürdige Software

Permissions

Android

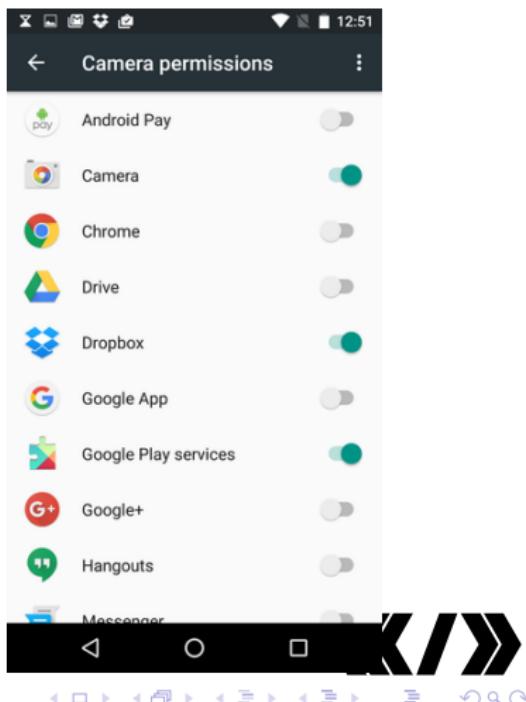
Einstellungen -> Apps -> Appname
-> Berechtigungen ändern

Einstellungen -> Apps -> Zahnrad
-> Appberechtigungen

iOS

Einstellungen -> Privatsphäre ->
Berechtigungsname

In den neuesten Versionen:
Entscheidung bei erster Benutzung



Vertrauenswürdige Software?

Einer Software, die nicht quelloffen ist, kann man nicht vertrauen

Freie Software auf dem Smartphone

F-Droid

Android-Appstore für freie Software



iOS Open Source Apps

[https://github.com/dkhamsing/
open-source-ios-apps](https://github.com/dkhamsing/open-source-ios-apps)

Replicant (Alternativ: Cyanogenmod)

- basiert auf Android
- Ziel, alle proprietären Komponenten durch freie zu ersetzen
- Einbindung von F-Droid
- **Problem:** Verlust der Garantie bei Installation



Ubuntu Phone, Sailfish OS



Geräteverschlüsselung

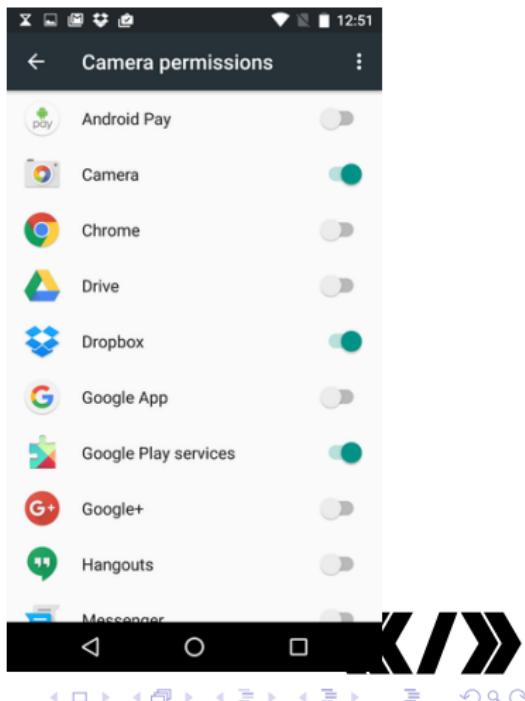
Android

Standard ab 6.0 Einstellungen ->
Sicherheit -> Telefon verschlüsseln

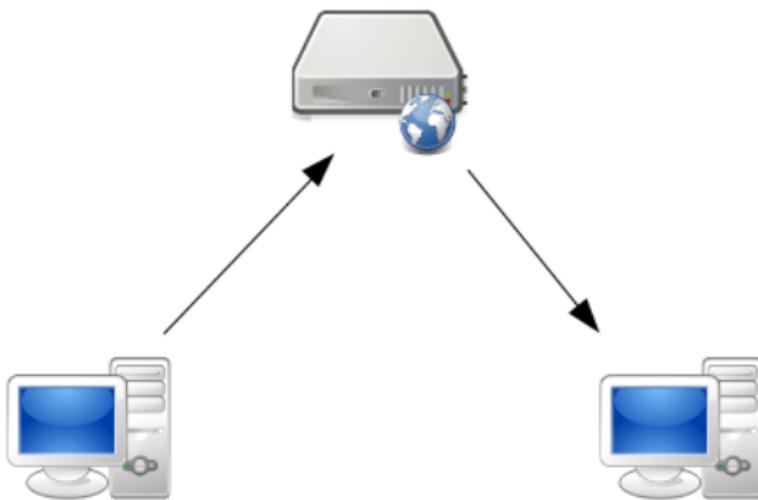
iOS

Standard

wichtig: gute PIN/Muster



Was ist zu schützen?



Tempora

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL-TV | Abo | Shop | Schlagzeilen | Wetter | TV-Programme | mehr ▾

SPIEGEL ONLINE NETZWELT

Login | Registrierung

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwerk | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Schule | Reise | Auto

Nachrichten > Netzwerk > Netzpolitik > Überwachung > Internetüberwachung: Tempora ist schlimmer als Prism

Netz-Spähsystem Tempora: Der ganz große britische Bruder



Hehr als 200 Glasfaserkabel sollen die Briten angezapft haben

DPA/dpa/UKU/ingenitaucher.com

Das umstrittene US-Spähprogramm Prism? Ist harmlos im Vergleich dazu, in welchem Umfang ein britischer Geheimdienst unter dem Codenamen Tempora weltweit das Internet ausspieniert - und damit auch deutsche Nutzer. Doch selbst Datenschutzaktivisten halten das Vergleichen für legal.

Samstag, 22.06.2013 - 20:24 Uhr

Drucken | Versenden | Merken

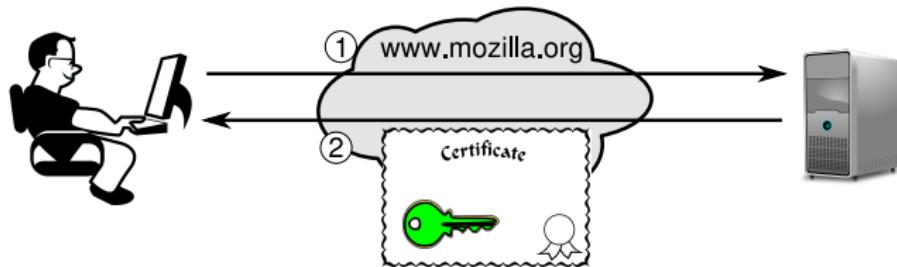
Nutzungsrechte | Feedback

Kommentieren | 389 Kommentare

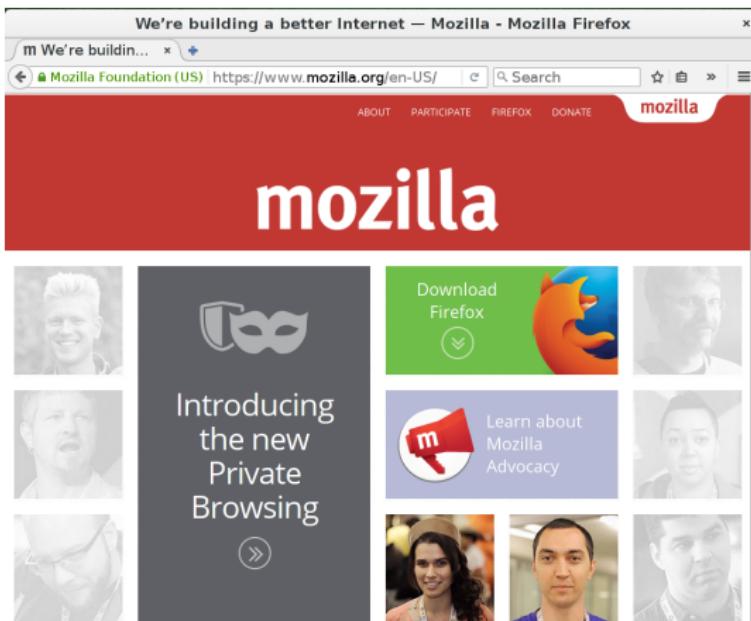
Hamburg/London - Die Aufregung war riesig, als bekannt wurde, dass die National Security Agency (NSA) im Rahmen ihres unter US-Präsident Barack Obama initiierten Spähprogramms Prism die Kunden von Telefon- und Internetfirmen ausleuchtet - Big Barack is watching you. Doch Brit Brother tut genau dies auch. Und in mancher Hinsicht scheint die Überwachung durch die britischen Netzspione viel umfassender zu sein als die der Amerikaner.

Transportwegverschlüsselung

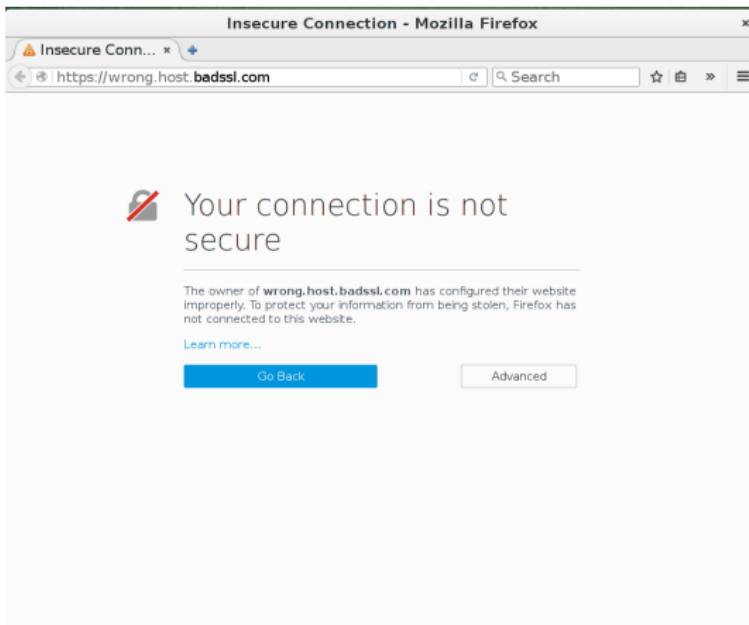
SSL = Secure Socket Layer / TLS = Transport Layer Security



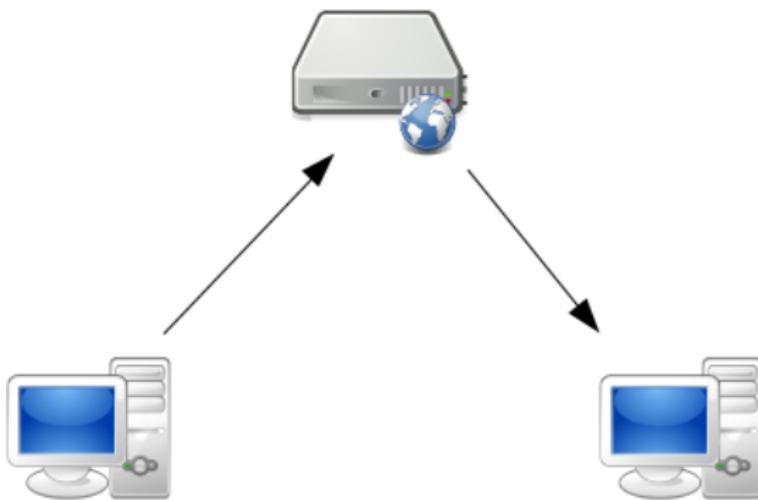
SSL im Browser



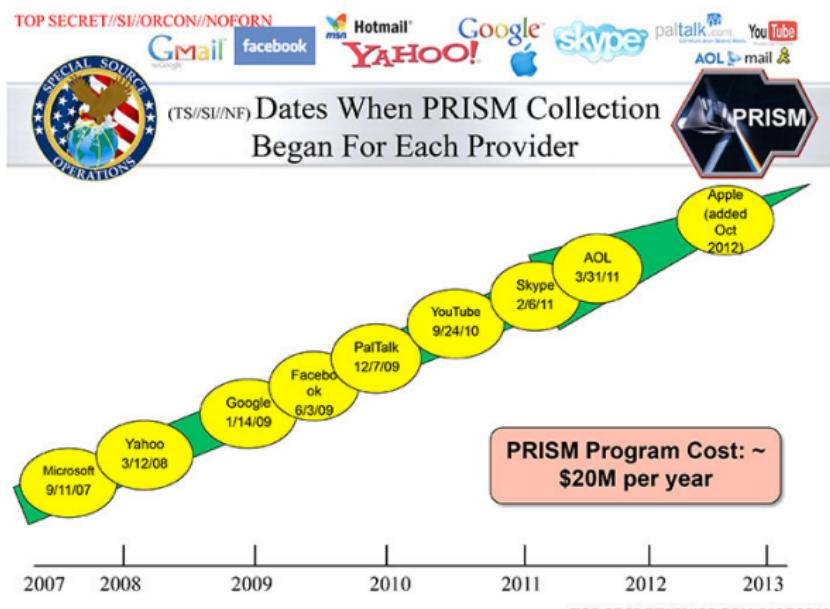
Ungültiges Zertifikat



Was ist zu schützen?



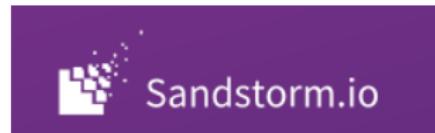
Prism



Dezentrale Dienste

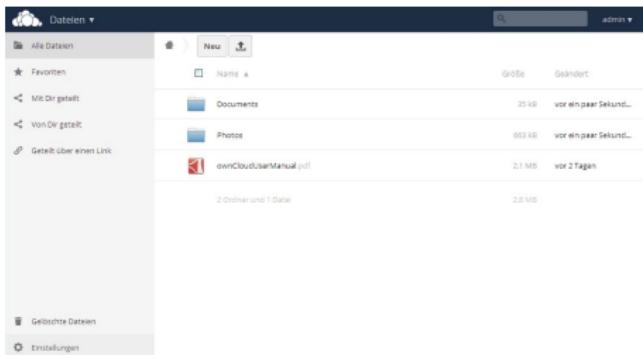


E-Mail



Owncloud

Plattformübergreifende
Synchronisierung von
Dateien, Dokumenten,
Kalendern, Kontakten,
Notizen und News.



Ende-zu-Ende-Verschlüsselung

- GPG für E-Mails

Ende-zu-Ende-Verschlüsselung

- GPG für E-Mails
- OTR/OMEMO für Jabber:
 - Pidgin mit OTR-Plugin für Linux und Windows
 - ChatSecure oder Xabber für Android
 - Adium für Mac, ChatSecure für iOS

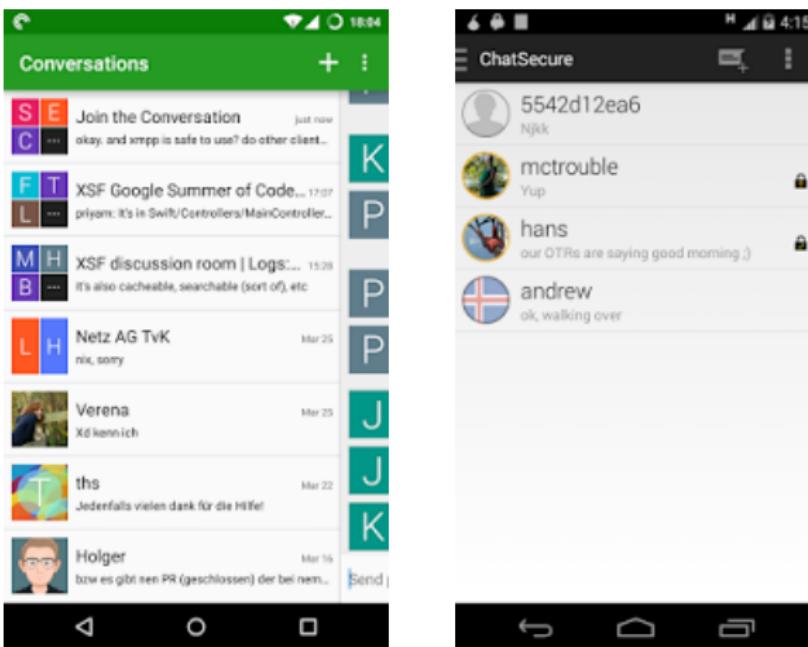
Ende-zu-Ende-Verschlüsselung

- GPG für E-Mails
- OTR/OMEMO für Jabber:
 - Pidgin mit OTR-Plugin für Linux und Windows
 - ChatSecure oder Xabber für Android
 - Adium für Mac, ChatSecure für iOS
- palava.tv, talky.io, Tox, Linphone für Videotelefonie

Ende-zu-Ende-Verschlüsselung

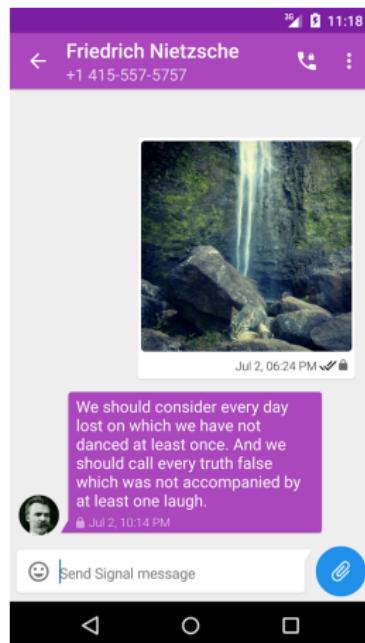
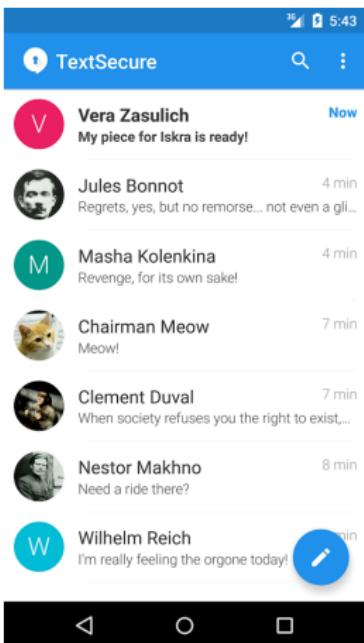
- GPG für E-Mails
- OTR/OMEMO für Jabber:
 - Pidgin mit OTR-Plugin für Linux und Windows
 - ChatSecure oder Xabber für Android
 - Adium für Mac, ChatSecure für iOS
- palava.tv, talky.io, Tox, Linphone für Videotelefonie
- Signal

Jabber: Conversations, ChatSecure



<https://xmpp.net/directory.php>

Signal



Vergleich Messenger

	Whatsapp	Threema	Telegram	Signal	Jabber
Verschlüsselung	orange	yellow	orange	green	green
Vertrauensw.	red	yellow	orange	green	green
Dezentr.	red	red	red	orange	green
Open Source	red	red	yellow	green	green
Mobileignung	green	green	green	green	yellow

Was kümmert es Facebook, Google und co?

Facebook, Google and WhatsApp plan to increase encryption of user data

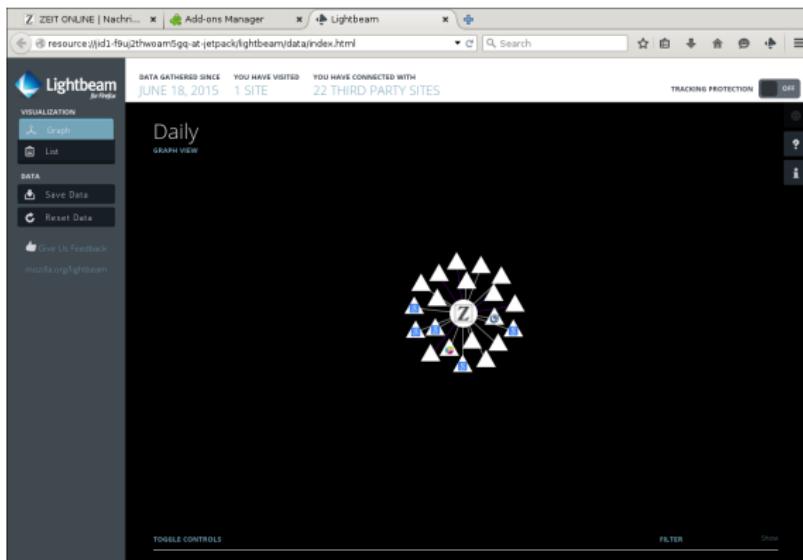
Spurred on by Apple's battles against the FBI, some of tech's biggest names are to expand encryption of user data in their services, the Guardian can reveal



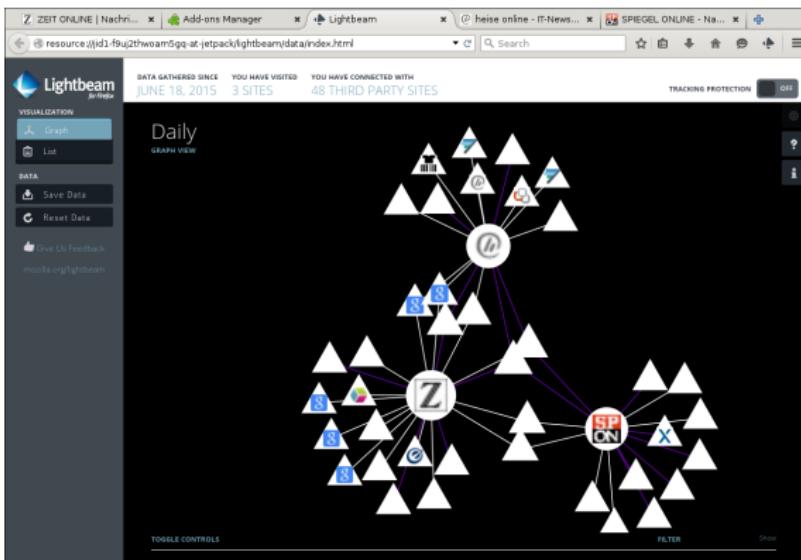
Work on new encryption projects began before Apple entered a court battle with US authorities over the San Bernardino killer's iPhone. Photograph: Philippe Huguen/AFP/Getty Images



Tracking



Tracking



Metadaten - Vorratsdatenspeicherung

- Handynetz
 - Telefonnummern
 - Zeitpunkt und Dauer (Telefonate, SMS)
 - Funkzelle (Ort)
- Internet
 - IP-Adresse (= ungefährer Ort)
 - Alle Verbindungen
 - Email: Adressen von Sender und Empfänger, Zugriff

Metadaten

The screenshot shows the golem.de homepage. At the top, there's a navigation bar with 'golem.de' logo, 'HOME', 'TICKER', a search input field, and a 'Suchen' button. Below the navigation is a 'TOP-THEMEN' section with links to 'Oneplus', 'Wearable', 'Android', 'NSA', 'Apple', 'Google', and 'mehr'.

EX-NSA-CHEF HAYDEN

"Wir töten Menschen auf Basis von Metadaten"

Der frühere NSA-Chef Michael Hayden ist für provokante Äußerungen bekannt. Nun bestätigte er freimütig, zu welchen Zwecken Verbindungsdaten genutzt werden können.

Der frühere US-Geheimdienstchef Michael Hayden hat bestätigt, was durch die Enthüllungen von Edward Snowden schon seit längerem diskutiert wird: "Wir töten Menschen auf der Basis von Metadaten", sagte Hayden vor einigen Wochen auf einer Diskussionsveranstaltung der John-Hopkins-Universität (ab Min. 18:00) in Baltimore. In der Debatte hatte ihm der Juraprofessor David Cole, der das Zitat nun bekanntmachte, vorgehalten, dass es alleine mit Verbindungsdaten möglich sei, über das Leben eines Menschen fast alles zu erfahren. Dies sei "*absolut korrekt*", sagte Hayden. Allerdings würden die Daten, die von US-Amerikanern gesammelt würden, nicht zum Töten von Menschen eingesetzt.



Ex-NSA-Chef Hayden räumt die Tötung von Menschen auf Basis von Metadaten ein. (Bild: Youtube.com/Screenshot: Golem.de)

Datum: 12.5.2014, 13:37

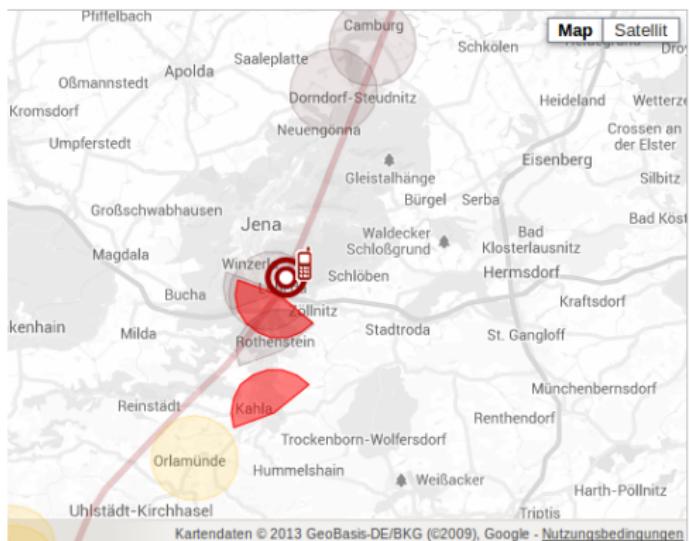
Autor: Friedhelm Greis

Themen: Datenschutz, Edward Snowden, NSA, Prism, Spionage, Verschlüsselung, Whistleblower, Überwachung, Internet, Politik/Recht

Teilen:



Metadaten - VDS



Monday, 31 August 2009

Malte Spitz gives a speech to the Greens in Erfurt against internet censorship.
(source: [Parteiwebsite](#))



6 incoming calls
21 outgoing calls
total time: 1h 16min 8s



34 incoming messages
29 outgoing messages

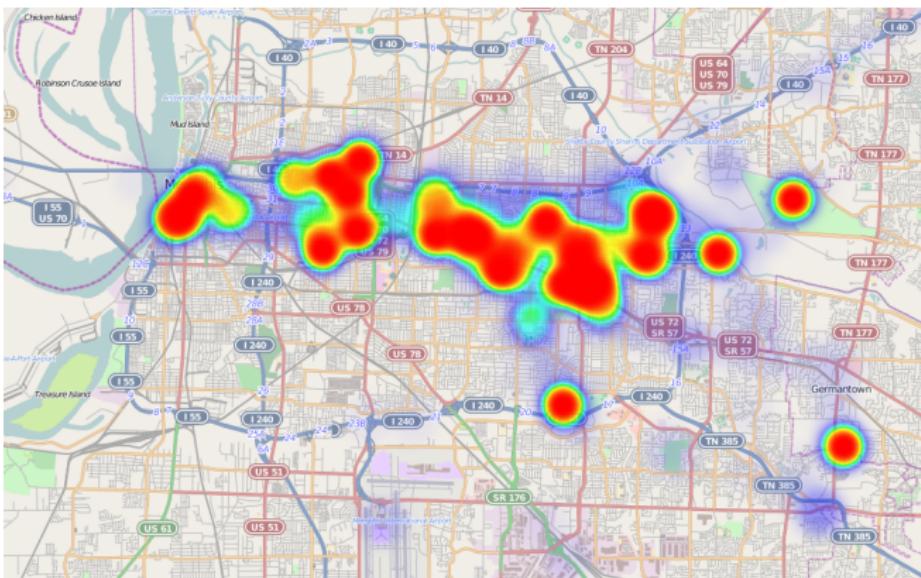


duration of internet connection:
21h 17min 25s

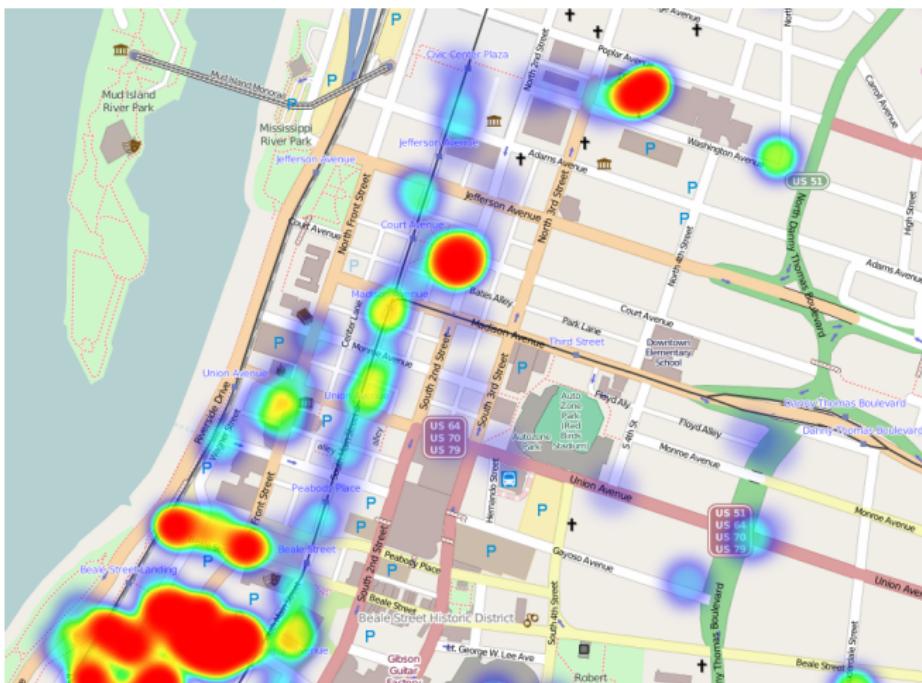
Download Data



Google Takeout



Google Takeout



Zeitstempel

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	.	.							.	●	●	●	●	●	●	●	●	●	●	●	.	.	.	
1	.								.	●	●	●	●	●	●	●	●	●	●	
2	.								.	●	●	●	●	●	●	●	●	●	●	
3									.	●	●	●	●	●	●	●	●	●	●	
4									.	●	●	●	●	●	●	●	●	●	●	
5	
6	

Alan, Microblogging

Zeitstempel

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	●	●	●	●	●	●	.	.	.	●	.	.	●	.	.
1	●	●	●	●	●	●	●
2	●	.	●	●	●	●	●	●	●	.	●	.	.	.
3	●	●	●	●	●	●	●	●	.	.	.
4	●	●	●	●	●	●	●	●	●	.	.	.
5	●	●	●	●	●	●	●	●	●	●	.	.
6	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Bob, Microblogging

Zeitstempel

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	●	•													•	•					•		●	
1		•	•											•	•	•			●		•	•	●	●
2		•			•										•		●					•		
3														•	•	•	•	•	●	●	●	•	•	•
4		●	●												•	•	•	●	●	●	●	●	●	●
5	•	•	●	●	●				•	•				•	•	•	●	●	●	●	●	●		●
6	•	•	•	•	•	●	●	●	•	•	•	•	•	•	•	•	●	●	●	●	●	●	●	•

Charlie, Github

Antitracking für den Browser

Computer

Browser-Plugins: Disconnect, Privacy Badger

Smartphone

Bislang keine Open Source Apps, Privacy Badger in Arbeit

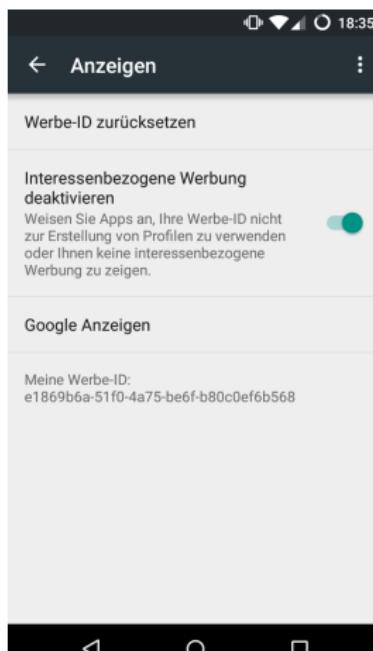
Antitracking für Apps

Android: Google AdID

Google-Einstellungen -> Anzeigen ->
Anzeigen

iOS: Apple IDFA

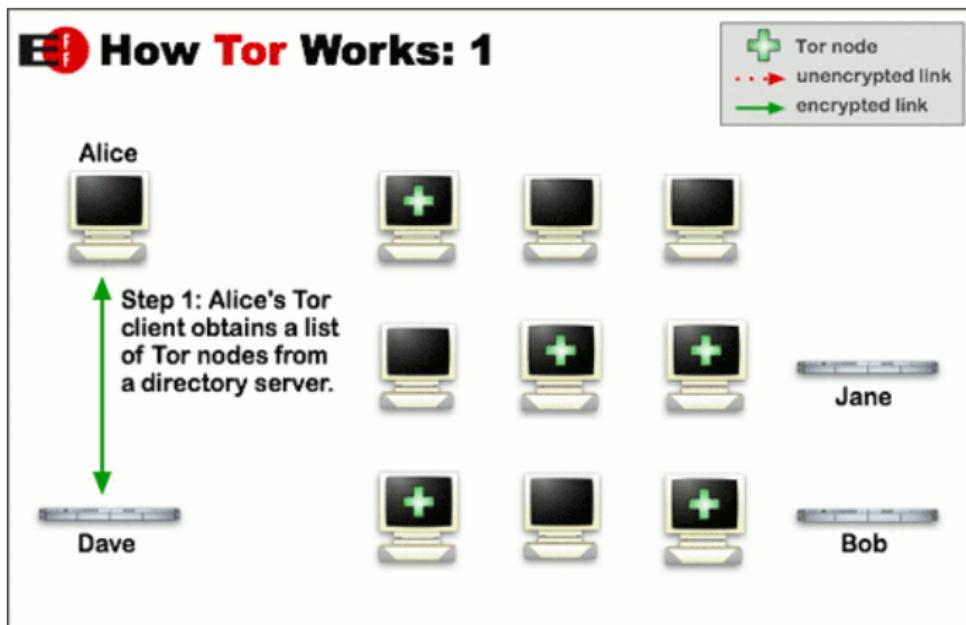
Settings -> General -> About ->
Advertising



Tor (Orbot/Orweb, OnionBrowser)

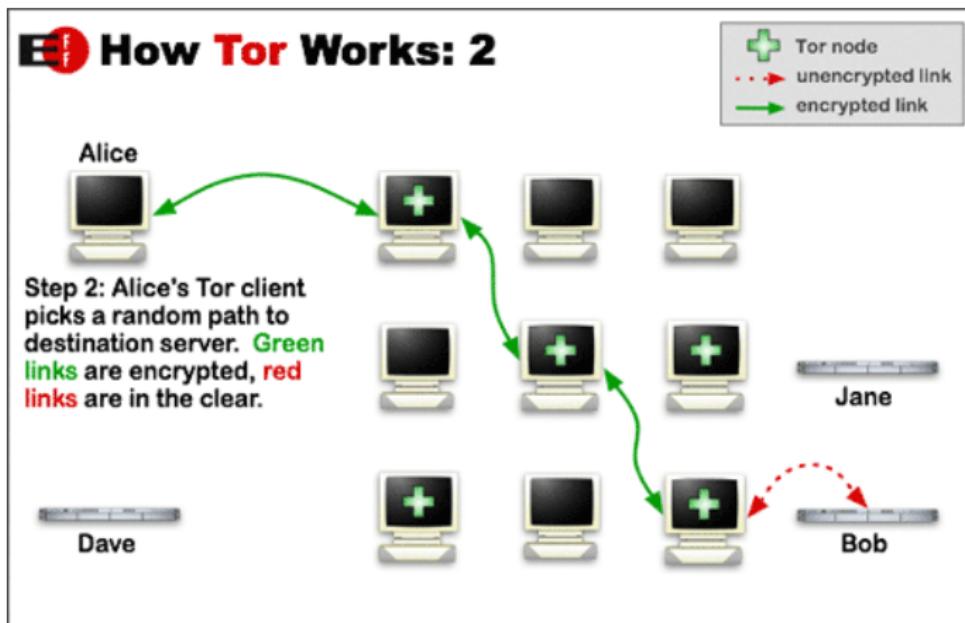


Tor



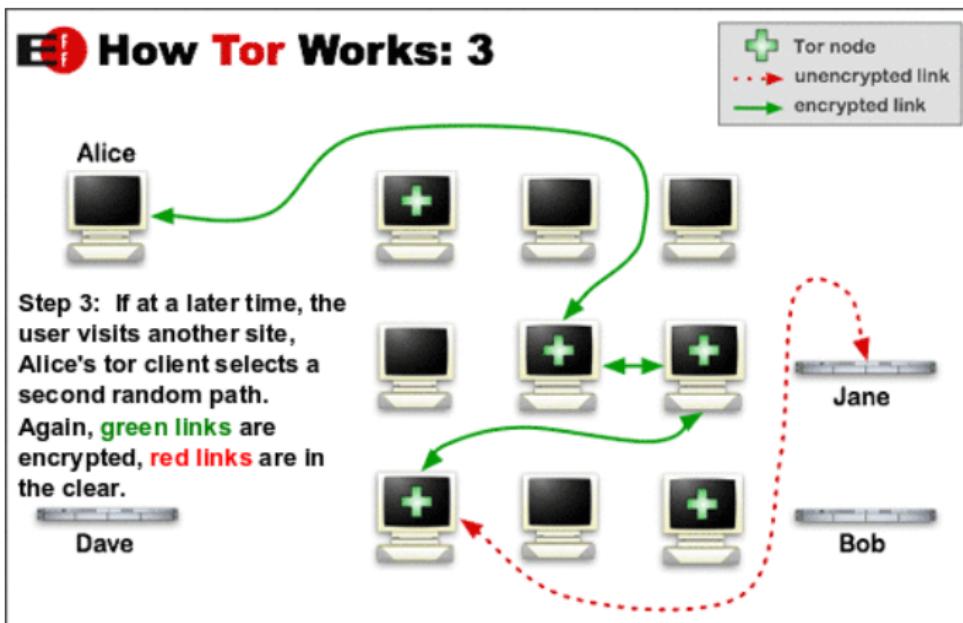
Grafik: The Tor Project

Tor



Grafik: The Tor Project

Tor



Grafik: The Tor Project

Einleitung
oooooooooooo

Einführung
ooooo

Geräte
oooooooooooooooooooo

Inhalte
oooooooooooo

Metadaten
oooooooooooo

Verhalten
●

Fazit
○

Passwörter

Passwörter

- Keine einfachen Wörter

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - .§)=/)='

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - .§)=/)='
 - qwerty

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - .§)=/)='
 - qwerty
 - Mks?o/.u,1Psw!

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - .§)=/)='
 - qwerty
 - Mks?o/.u,1Psw!

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - .§)=/)='
 - qwerty
 - Mks?o/.u,1Psw!
- Verschiedene Passwörter nutzen!

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - .§)=/)='
 - qwerty
 - Mks?o/.u,1Psw!
- Verschiedene Passwörter nutzen!
- Passwort-Manager verwenden
(z.B. Keepass, Password Safe)

Fazit

- Verschlüsselung nutzen (Signal, Conversations, ChatSecure)
- Anonymisieren (Antitracking-Einstellungen, Tor)
- Dezentrale Dienste nutzen (Email, Jabber, Owncloud)
- Endgeräte schützen (Permissions, Freie Software, GerätEVERSCHLÜSSELUNG)

Folien:  Chaos Computer Club Dresden

CMS Dresden: schule@c3d2.de

Vortragender: Marius Melzer (marius@rasumi.net,

PGP-Fingerprint: 6730 E691 36B9 9BB8 FFB1 2662 A97B
F176 52DE FC3E)

