

Wie schütze ich mich vor Überwachung?

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

15.12.2015

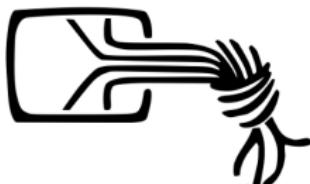
Chaos Computer Club



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



Chaos Computer Club



- Verein wurde 1981 gegründet (<https://ccc.de>)
- Aktuell ca. 4500 Mitglieder

Chaos Computer Club



- Verein wurde 1981 gegründet (<https://ccc.de>)
- Aktuell ca. 4500 Mitglieder
- 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)

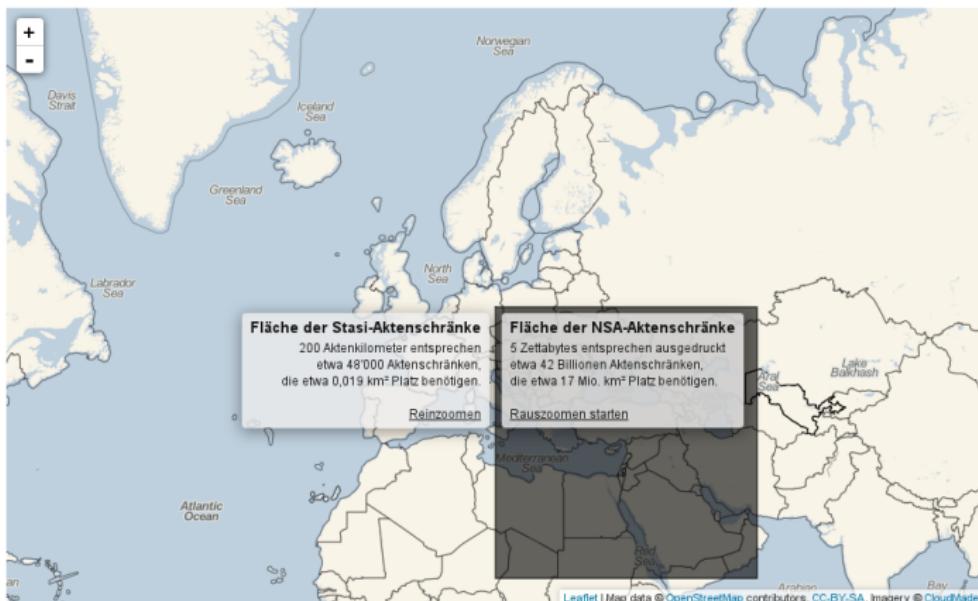
Stasi vs. NSA



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



Stasi vs. NSA



Wer sind potenzielle Angreifer?

- andere Nutzer eines Dienstes

Wer sind potenzielle Angreifer?

- andere Nutzer eines Dienstes
- Fremde (“Hacker”)

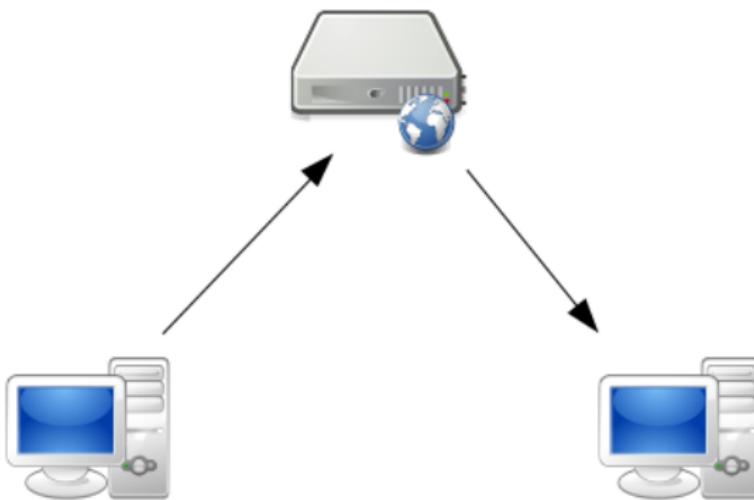
Wer sind potenzielle Angreifer?

- andere Nutzer eines Dienstes
- Fremde (“Hacker”)
- Dienstanbieter (z.B. für Werbung)

Wer sind potenzielle Angreifer?

- andere Nutzer eines Dienstes
- Fremde (“Hacker”)
- Dienstanbieter (z.B. für Werbung)
- staatliche Institutionen, Netzbetreiber

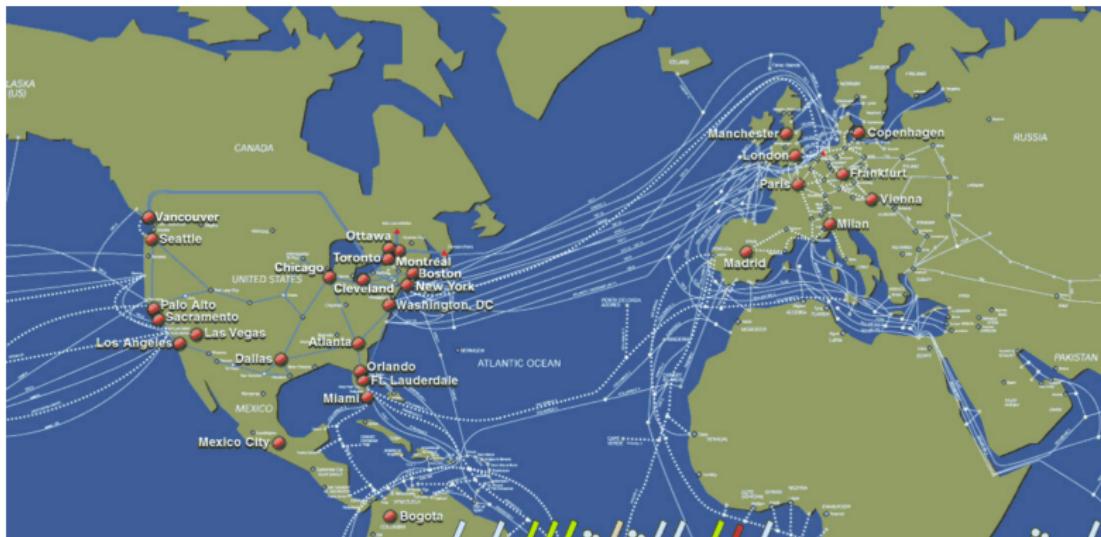
Wie kommunizieren wir im Internet?



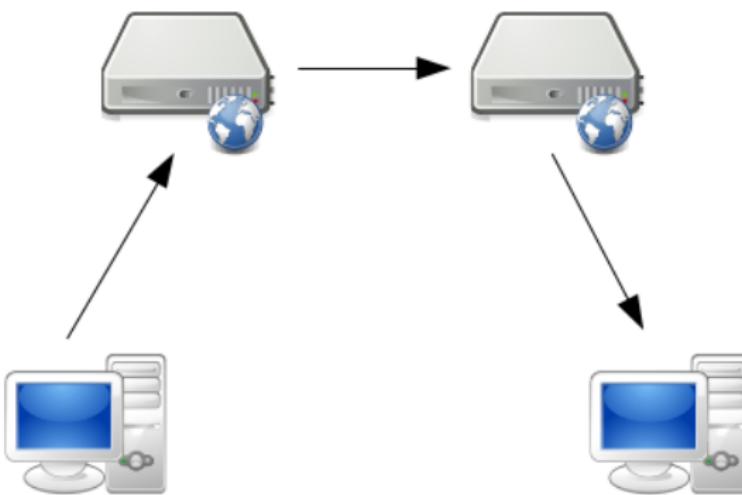
Server im Rechenzentrum



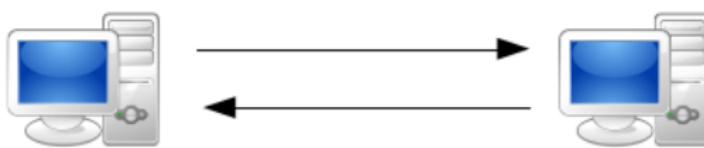
Internet



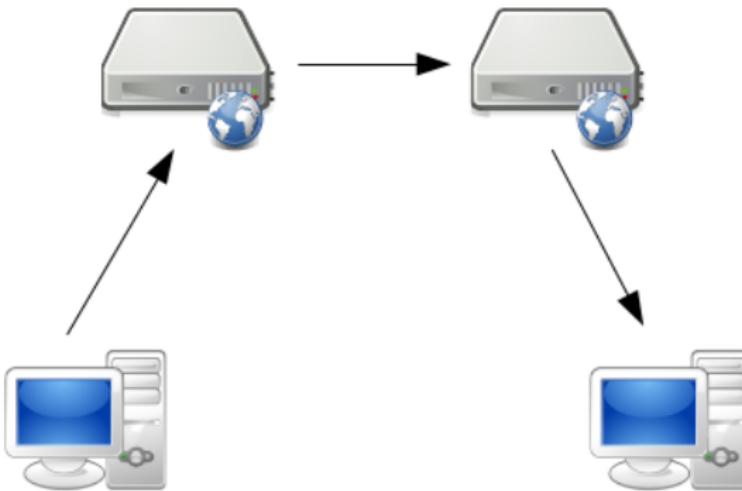
Föderation



P2P



Was ist zu schützen?



Problematisches Verhalten von Software

- Sicherheitslücken

Problematisches Verhalten von Software

- Sicherheitslücken
- Backdoors

Problematisches Verhalten von Software

- Sicherheitslücken
- Backdoors
- Unerwünschte Funktionalität

Backdoors

The screenshot shows the homepage of c't magazin. The logo 'c't magazin' is in the top left. A navigation bar at the top includes 'Startseite', 'Artikel' (which is highlighted), 'c't-Projekte', and 'Hotline & FAQ'. Below the navigation bar is a secondary menu with links to 'Magazin', 'Internet', 'Software', 'Hardware', 'Know-how', 'Praxis', and 'Artikel-Foren'. The main content area features a link 'c't > aktuell' and an article by Micha Borrmann and Jürgen Schmidt. The title of the article is 'Microsofts Hintertür' and the subtitle is 'Zweifelhafte Updates gefährden SSL-Verschlüsselung'. A large block of text discusses how Windows handles untrusted SSL certificates by querying Microsoft. At the bottom right is a navigation bar with icons for search, refresh, and other site functions.

Magazin Internet Software Hardware Know-how Praxis Artikel-Foren

c't > aktuell

Micha Borrmann, Jürgen Schmidt

c'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.

Unerwünschte Funktionalität

DATENSCHUTZ	
Allgemein	Einstellung suchen
Position	Apps die Verwendung der Werbungs-ID für App-übergreifende Erlebnisse erlauben (bei Deaktivierung wird Ihre ID zurückgesetzt) <input checked="" type="checkbox"/> Aus
Kamera	SmartScreen-Filter einschalten, um von Windows Store-Apps verwendete Webinhalte (URLs) zu überprüfen <input checked="" type="checkbox"/> Ein
Mikrofon	Informationen zu meinem Schreibverhalten an Microsoft senden, um die Eingabe- und Schreibfunktionen in Zukunft zu verbessern. <input checked="" type="checkbox"/> Aus
Spracherkennung, Freihand und Eingabe	Websites den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen <input checked="" type="checkbox"/> Aus
Kontoinformationen	Microsoft-Werbung und andere Personalisierungsinfos verwalten
Kontakte	Datenschutzbestimmungen
Kalender	
Messaging	
Funkempfang	
Weitere Geräte	
Feedback und Diagnose	
Hintergrund-Apps	



Unerwünschte Funktionalität

iPhone		Android		Data Transmission		
App name	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.

Wie schütze ich meine Geräte?

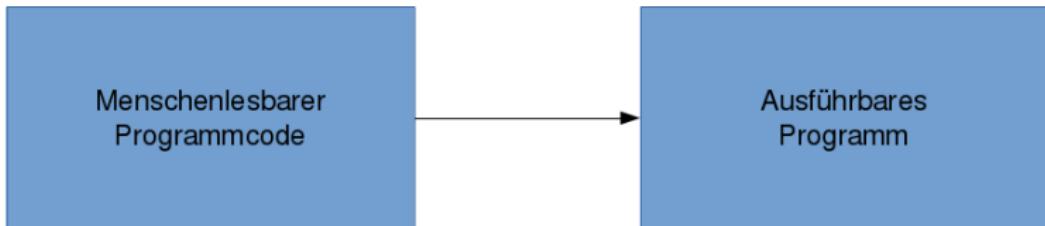
- (VirensScanner)
- Firewall
- Aktuelle und vertrauenswürdige Software

Vertrauenswürdige Software?

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



Kompilierung von Software



Probleme von proprietärer Software

Probleme von proprietärer Software

- Kontrolle unterliegt einer Organisation

Probleme von proprietärer Software

- Kontrolle unterliegt einer Organisation
- Transparenz und Sicherheit

Strategien moderner IT-Unternehmen

Strategien moderner IT-Unternehmen

- Hardware

Strategien moderner IT-Unternehmen

- Hardware
- Software

Strategien moderner IT-Unternehmen

- Hardware
- Software
- Internetdienste

Strategien moderner IT-Unternehmen

- Hardware
- Software
- Internetdienste
- ... aus einer Hand

Strategien moderner IT-Unternehmen

Strategien moderner IT-Unternehmen

- Fehlende Interoperabilität

Strategien moderner IT-Unternehmen

- Fehlende Interoperabilität
- vorgegebene Dienste und Programme

Strategien moderner IT-Unternehmen

- Fehlende Interoperabilität
- vorgegebene Dienste und Programme
- keine ausreichenden Nutzerrechte

Strategien moderner IT-Unternehmen

- Fehlende Interoperabilität
- vorgegebene Dienste und Programme
- keine ausreichenden Nutzerrechte
- Kopierschutz, Online-Zwang, ...

Strategien moderner IT-Unternehmen

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

Das GNU Projekt

- Begonnen von Richard Stallman im Jahr 1984
- Gründung der Free Software Foundation im Jahr 1985



 **FREE SOFTWARE FOUNDATION**



Firefox und Thunderbird

Firefox

- Browser



Thunderbird

- Email-Programm



LibreOffice

- Textverarbeitung
- Tabellenkalkulation
- Präsentationen
- Formeleditor
- nutzt Open Document Format zur Speicherung



Freie Software für Android

F-Droid

- Installationsdienst für freie Android-Software



Signal

- Verschlüsselter Nachrichtenaustausch
- Verschlüsselte Speicherung



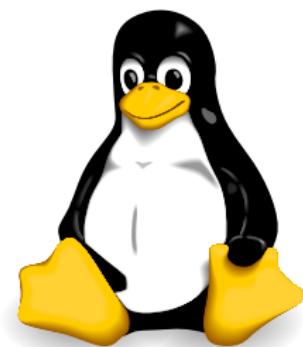
Replicant

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

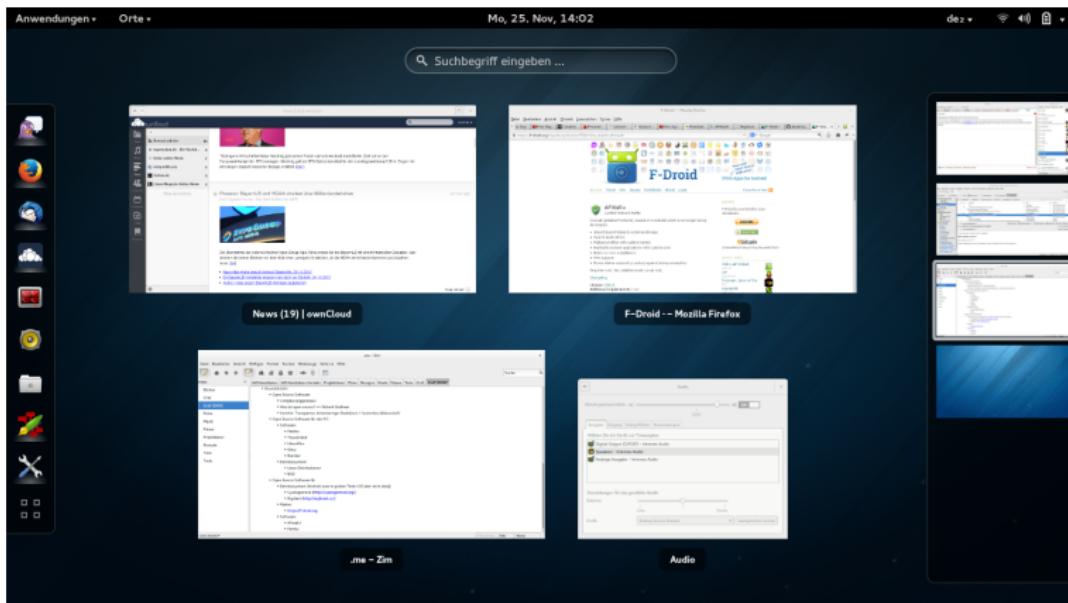


Linux

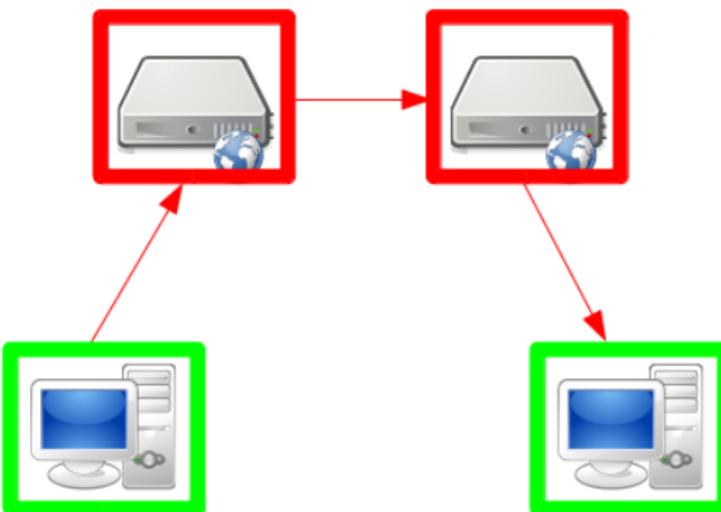
- Weit verbreitet als Server-Betriebssystem
- Bekannte Desktop-Varianten:
 - Ubuntu/Debian Linux
 - Linux Mint
- Können als Live-System ausprobiert werden
- Integrierte Software für Verschlüsselung, Webbrowsing, E-Mail, Textverarbeitung etc.



Linux



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



Mehr 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 ausspielt - und damit auch deutsche Nutzer. Doch selbst Datenschutzaktivisten halten das Vergleichen für legal.

Samstag, 22.06.2013 - 20:24 Uhr

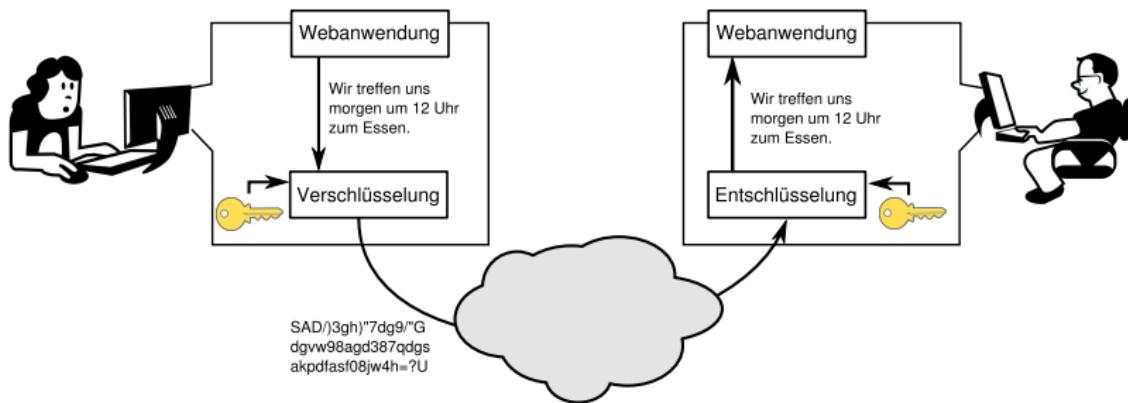
Drucken | Versenden | Merken

Nutzungsrechte | Feedback

Kommentieren | 389 Kommentare

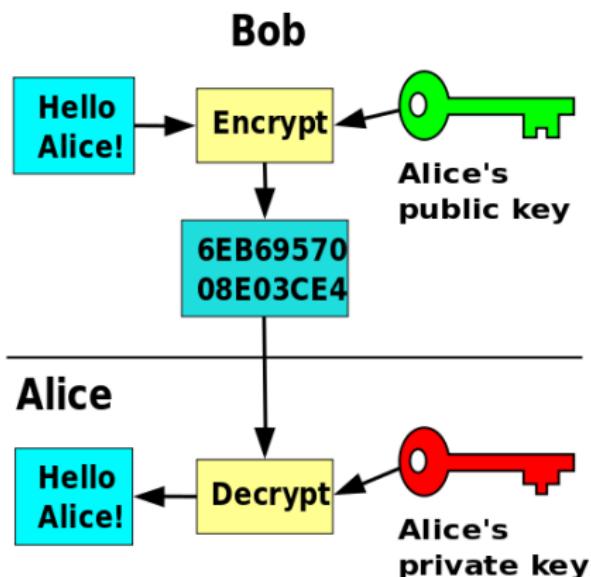
Hamburg/London - Die Aufregung war riesig, als bekannt wurde, dass die National Security Agency (NSA) im Rahmen ihres unter US-Präsident Barack Obama initiierten Spähprogramms Prism die Kunden von Telefon- und Internetfirmen ausleuchtet - Big Barack is watching you. Doch Brit Brother tut genau dies auch.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

Verschlüsselung: symmetrisch



Verschlüsselung: asymmetrisch

Verschlüsselung: asymmetrisch

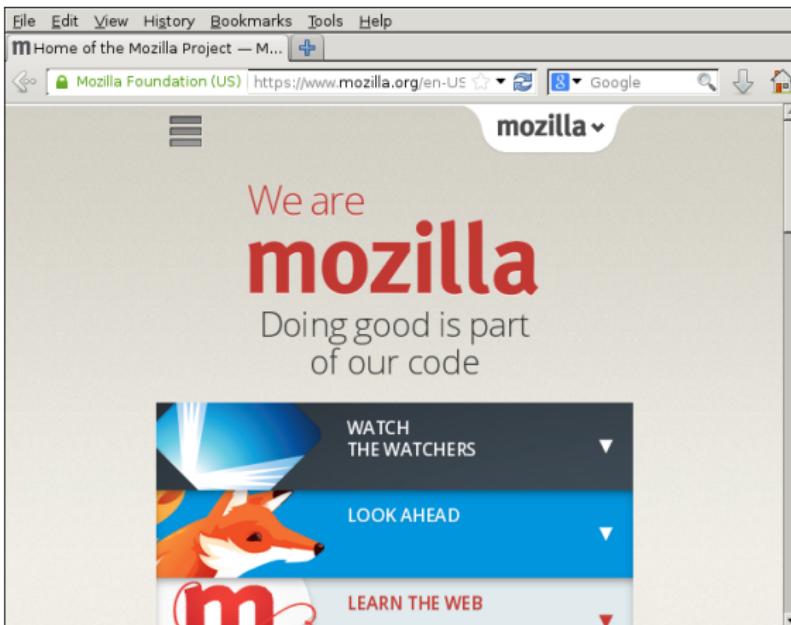


Transportwegverschlüsselung

SSL = Secure Socket Layer / TLS = Transport Layer Security



SSL im Browser



Einleitung
oooooooo

Einführung
ooooooo

Geräte
oooooooooooooooooooo

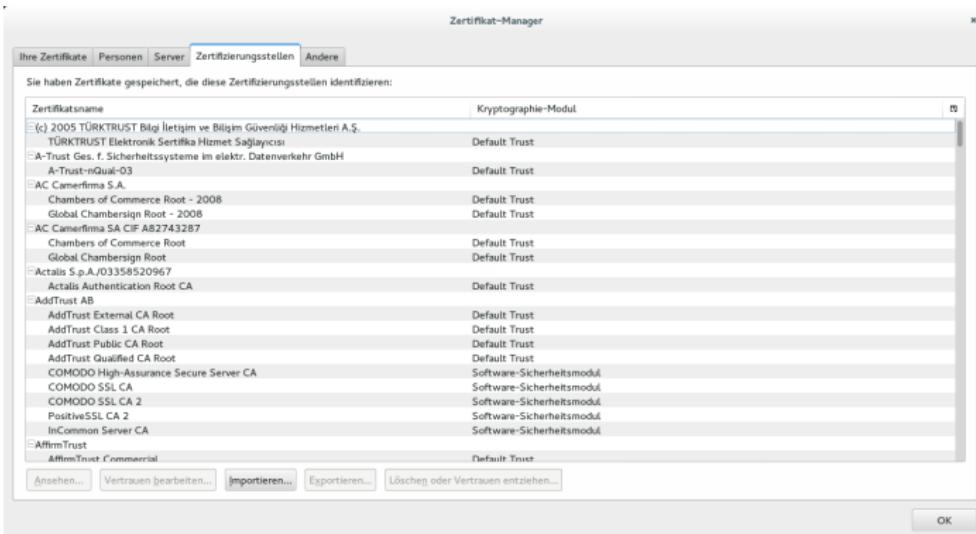
Inhalte
ooooo●oooooooo

Metadaten
oooooooooooo

Fazit
○

Zertifizierungsstellen

Zertifizierungsstellen



HTTPS Everywhere

 ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

SEARCH

[HOME](#) [ABOUT](#) [OUR WORK](#) [DEEPLINKS BLOG](#) [PRESS ROOM](#) [TAKE ACTION](#) [SHOP](#)

 **HTTPS Everywhere**

[HTTPS Everywhere](#) [FAQ](#) [Report Bugs / Hack On The Code](#) [Creating HTTPS Everywhere Rulesets](#) [How to Deploy HTTPS Correctly](#)

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. **Encrypt the web: Install HTTPS Everywhere today.**

[Install in Firefox Version 3 Stable](#) [Install in Chrome Beta Version](#) [Install in Opera Beta Version](#)

Donate to EFF 

Stay in Touch

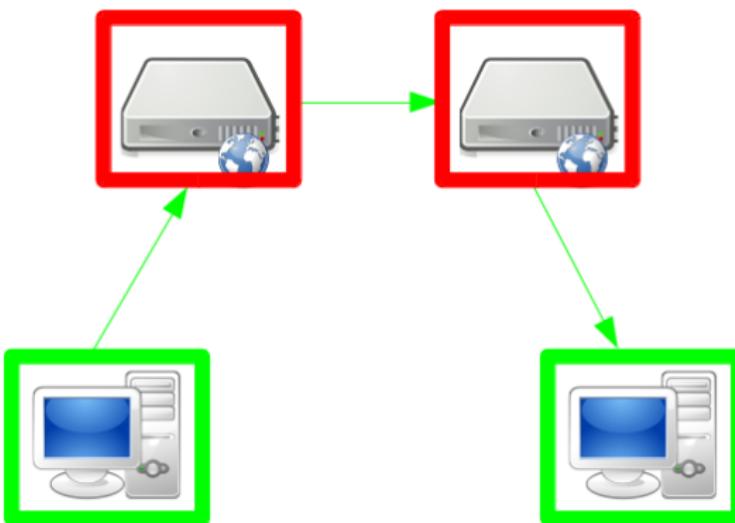
Email Address
Postal Code (optional)
[SIGN UP NOW](#)

NSA Spying

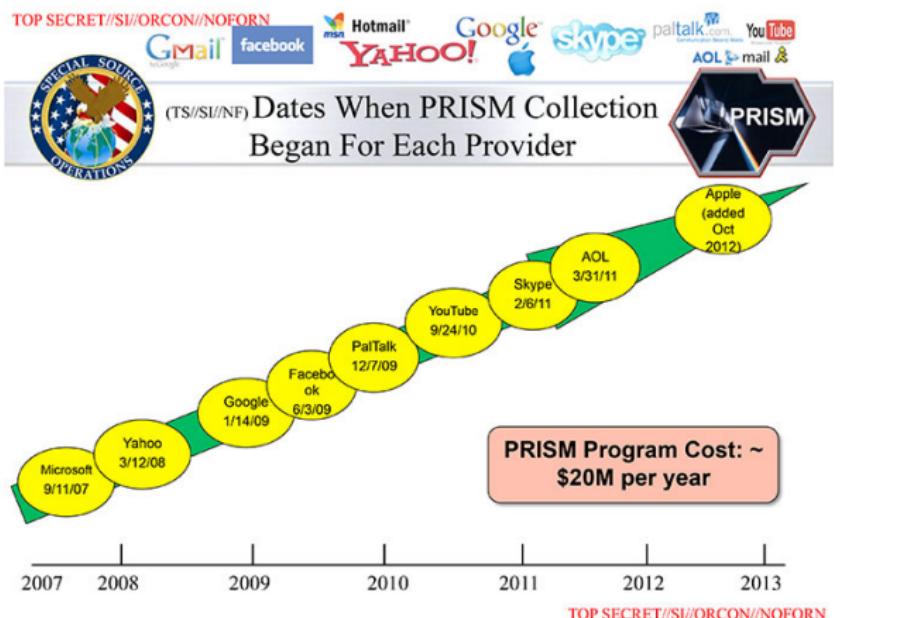
 eff.org/nsa-spying

EFF is leading the fight against the NSA's illegal mass surveillance programs. Learn more about what the program is, how it works, and what you can do.

Was ist zu schützen?



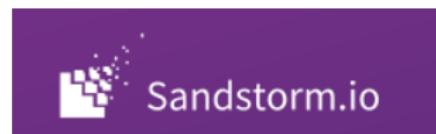
Prism



Dezentrale Dienste



E-Mail



Ende-zu-Ende-Verschlüsselung

- GPG für E-Mails

Ende-zu-Ende-Verschlüsselung

- GPG für E-Mails
- OTR 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 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 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

E-Mail-Selbstverteidigung

E-MAIL-SELBSTVERTEIDIGUNG

LANGUAGE [GNU/LINUX](#) [MACOS](#) [WINDOWS](#) SHARE

SIEH DIR UNSERE INFOGRAFIK AN UND VERBREITE SIE WEITER 

Hassenüberwachung verstößt gegen unsere Grundrechte und bedroht die freie Meinungsäußerung. Diese Anleitung bringt dir eine einfache Selbstverteidigungsstrategie bei E-Mail-Überwachung. Wenn du fertig bist, kannst du E-Mails senden und empfangen, die von Überwachern oder Kriminellen, die deine E-Mails abhören, nicht gelesen werden können. Alles, was du brauchst, ist ein Computer mit einer Internetverbindung, ein E-Mail-Konto und eine halbe Stunde Zeit.

Auch wenn du nichts zu verborgen hast, die Verwendung von Verschlüsselung schützt die Privatsphäre der Menschen, mit denen du kommunizierst, und macht den Systemen der Hassenüberwachung das Leben schwer. Wenn du doch etwas wichtiges verborgen möchten, bist du in guter Gesellschaft. Dies sind die gleichen Werkzeuge, die Edward Snowden benutzt hat, um seine bekannten Geheimnisse über die NSA zu verbreiten.

Sich gegen Überwachung zu wehren, erfordert neben der Verwendung von Verschlüsselung den politischen Kampf dafür, dass wirger Daten über uns gesammelt werden. Aber der erste Schritt ist es, dich selber zu schützen und die Überwachung deiner Kommunikation so schwer wie möglich zu machen. Das geht so:

#1 INSTALLIERE DIE PROGRAMME

Diese Anleitung basiert auf freier Software. Freie Software ist transparent und kann von allen kopiert und angepasst werden. Dadurch ist sie sicher vor Überwachung als nicht-freie Software (wie Windows). Lerne mehr über freie Software auf [fsf.org](#). Auf den meisten GNU/Linux-Systemen ist GnuPG bereits installiert, also musst du es nicht herunterladen. Wenn du GnuPG konfiguriert, brauchst du jedoch ein E-Mail-Programm. Bei den meisten GNU/Linux-Distributionen kann man eine freie Version des Programms Thunderbird installieren. E-Mail-Programme sind eine weitere Art auf E-Mail-Konten zuzugreifen, die ähnlich wie Webmail funktionieren, aber mehr Funktionen bieten.

Wenn du bereits eines dieser Programme hast, kannst du zu [Schritt 1.b](#) springen.

[Spenden](#)

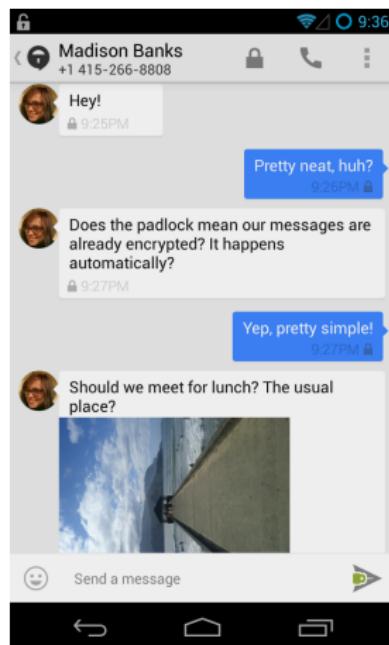
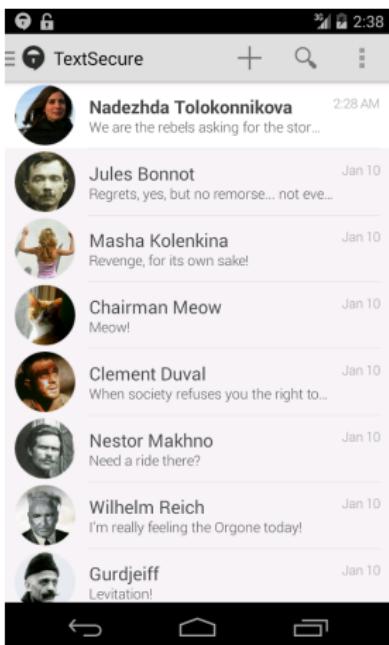


Wir kämpfen für die Rechte von Computerbenutzern und -nutzern und fördern die Entwicklung freier (wie in Freeheld) Software. Widerstand gegen die Hassenüberwachung ist sehr wichtig für uns.

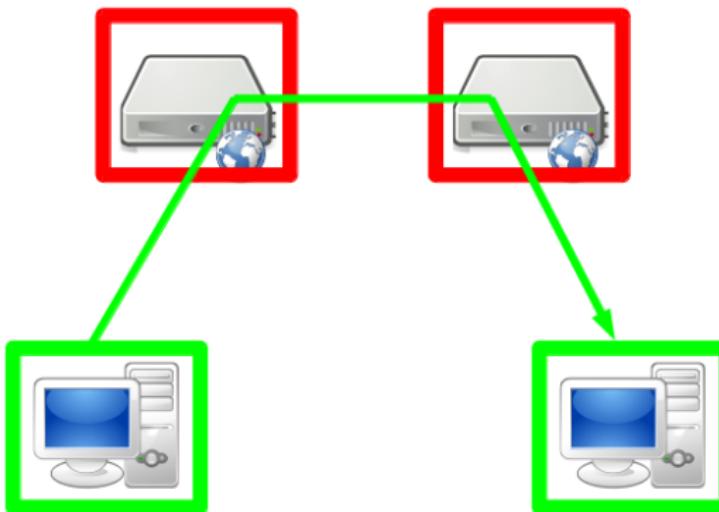
Wir möchten diese Anleitung in weitere Sprachen übersetzen und eine Vision zur Verschlüsselung auf mobilen Geräten erstellen. Bitte spende und helf Menschen auf der ganzen Welt den ersten Schritt zu machen, Ihre Privatsphäre mit Ihrer Software zu schützen.

- <https://emailselfdefense.fsf.org/de/>

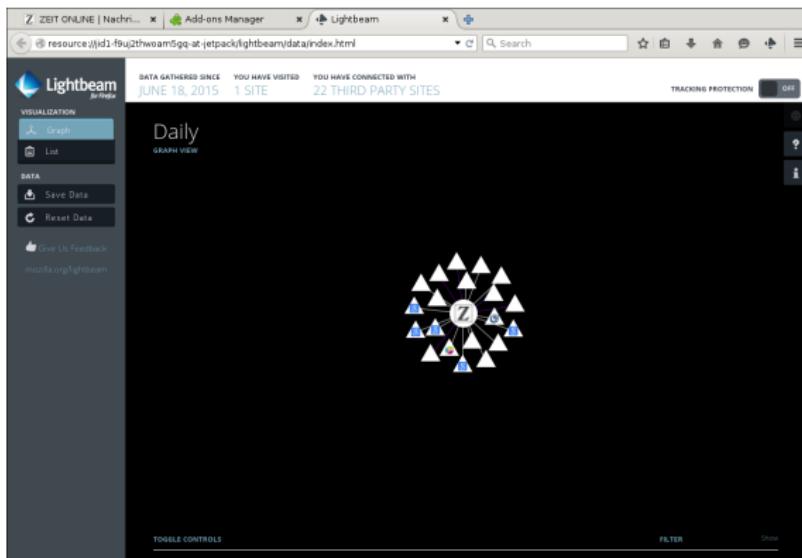
Signal



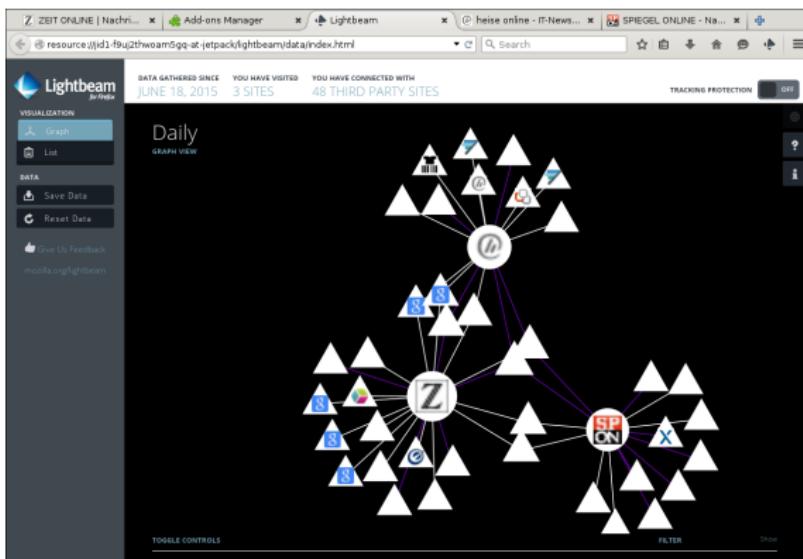
Ich will etwas von einem anderen Nutzer



Metadaten im WWW



Metadaten im WWW



Metadaten - VDS

- 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 links for 'HOME', 'TICKER', and a search bar. Below this, a 'TOP-THEMEN' section lists categories like OnePlus, Wearable, Android, NSA, Apple, Google, and 'mehr'. The main content area features a headline about Michael Hayden.

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

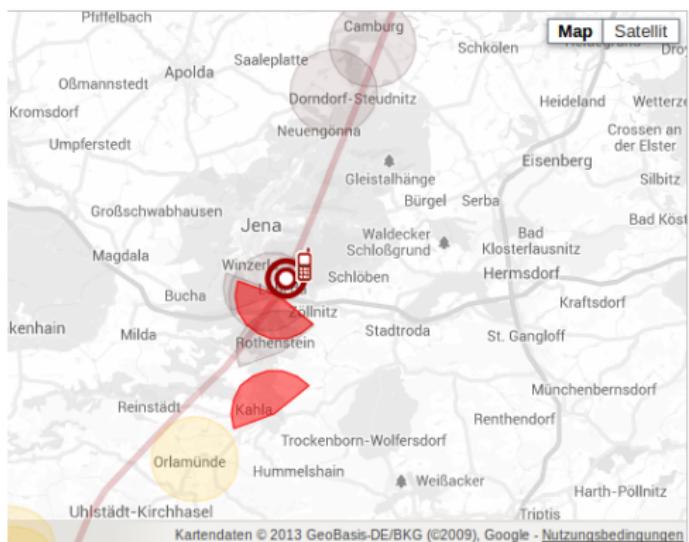
Autor: Friedhelm Greis

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



speed

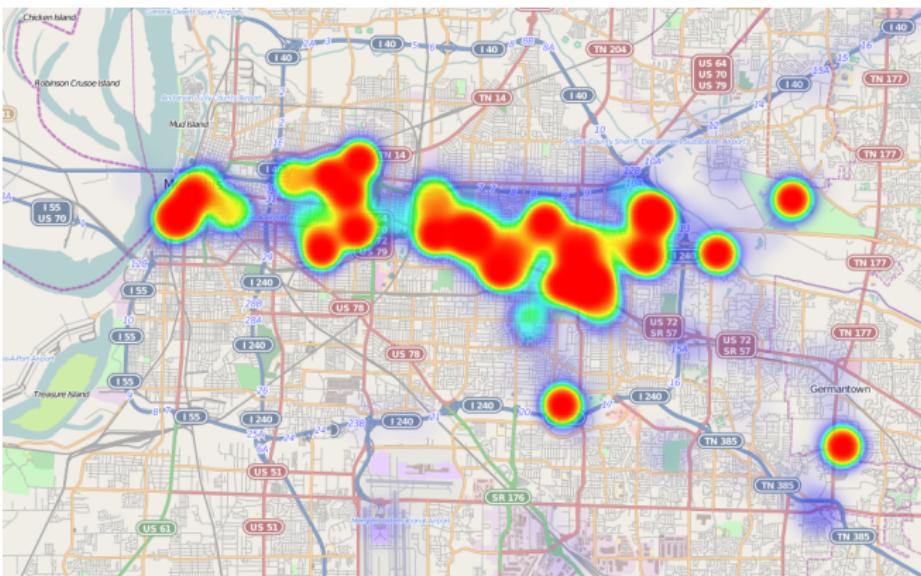
31 Aug 09 15:30

Show the points in time, Malte Spitz was in the selected map segment, too

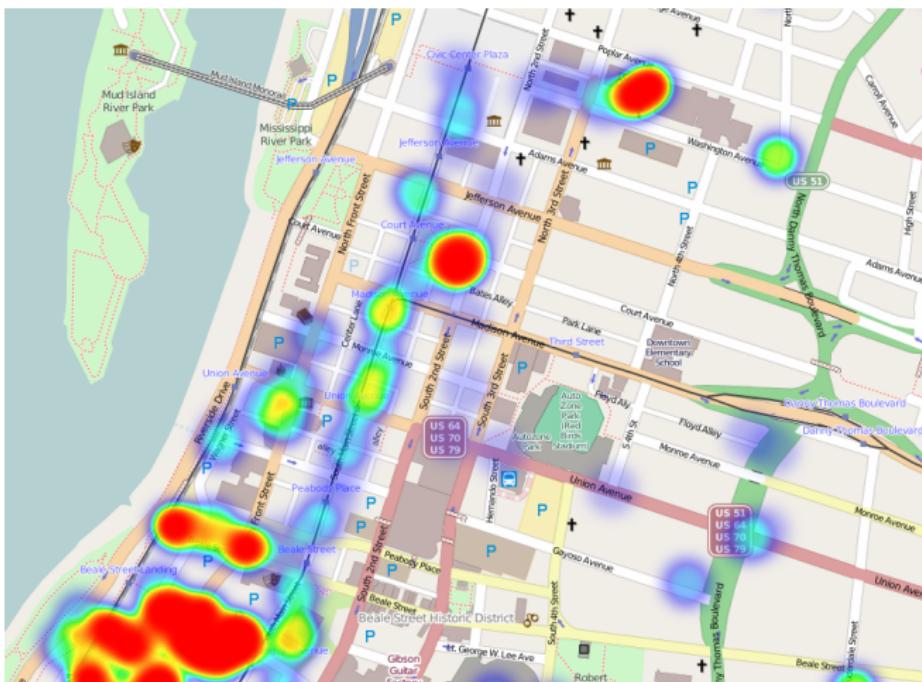
Download Data



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	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

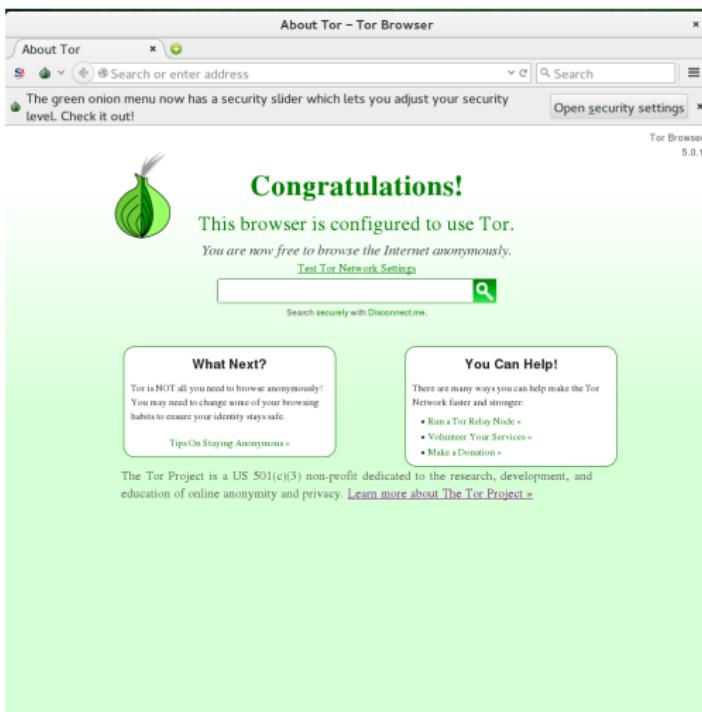
Bob, Microblogging

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	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

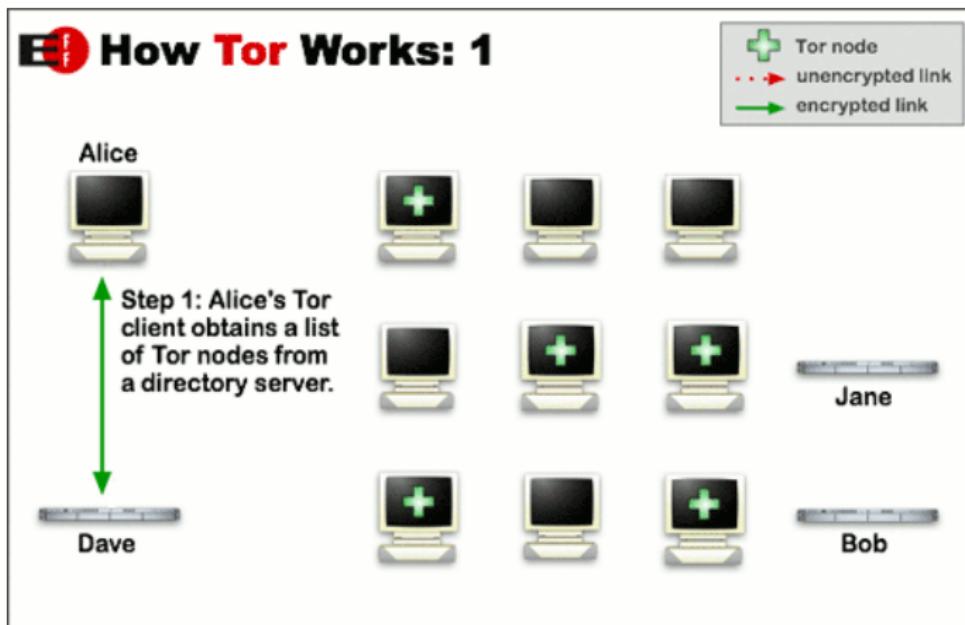
Charlie, Github

Tor



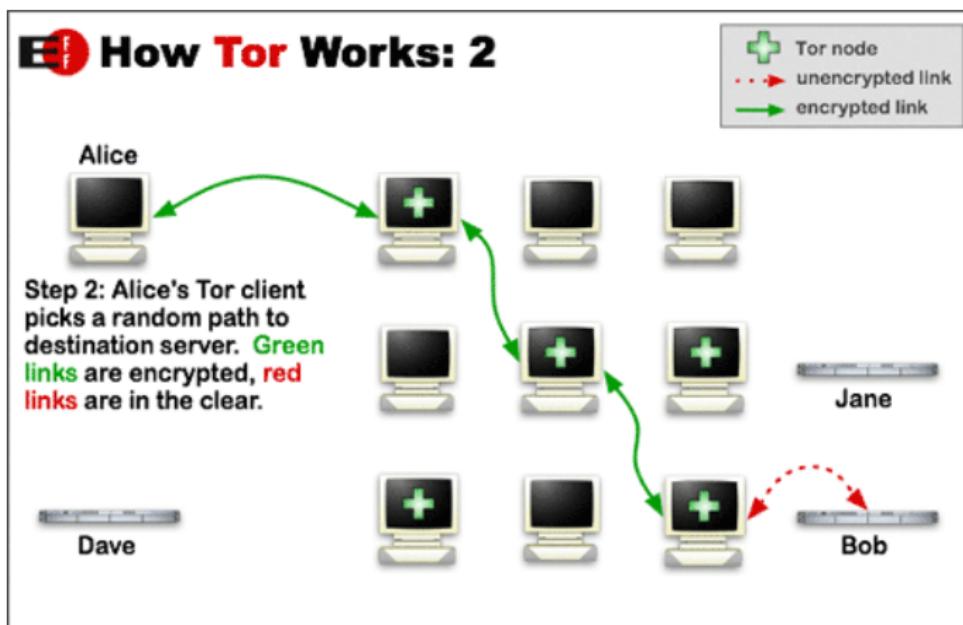
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn more about The Tor Project »](#)

Tor



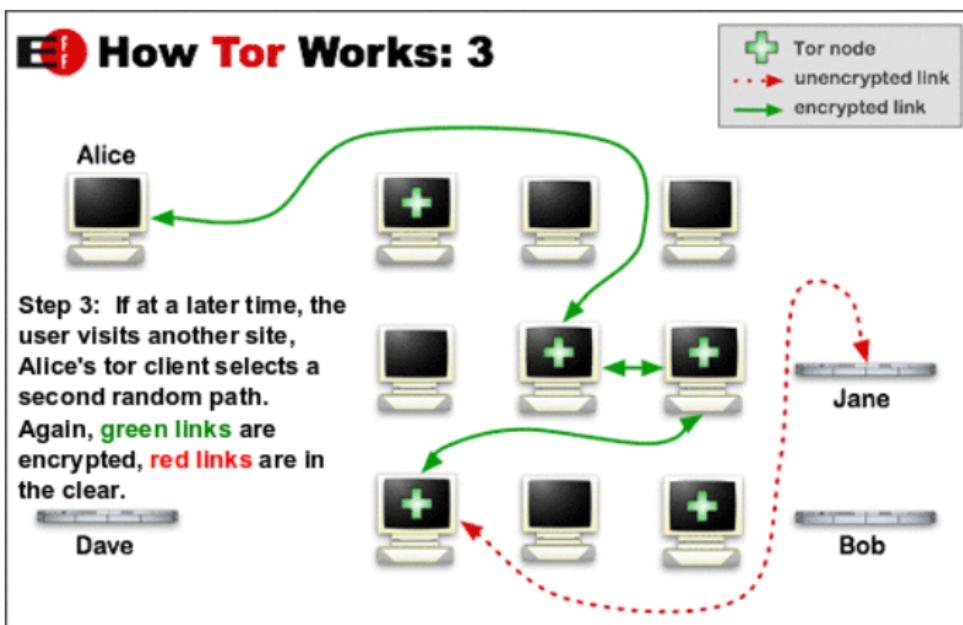
Grafik: The Tor Project

Tor



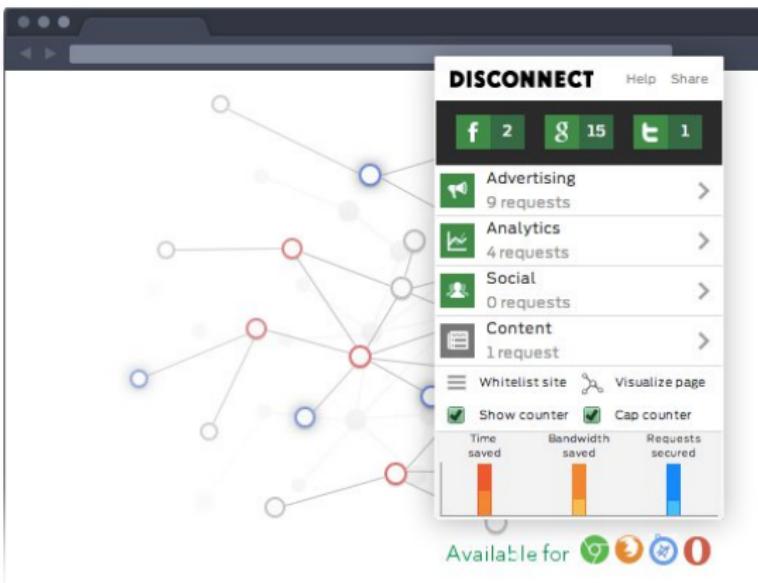
Grafik: The Tor Project

Tor



Grafik: The Tor Project

Disconnect, Privacy Badger, Ghostery



Fazit

- Verschlüsselung nutzen (Inhalte)
- Anonymisieren (Metadaten)
- Dezentrale Dienste nutzen (Inhalte + Metadaten)
- Endgeräte schützen

Folien:  Chaos Computer Club Dresden

CMS Dresden: schule@c3d2.de