

NSA, Prism und co - Wie schützt man sich vor Überwachung?

Marius Melzer & Stephan Thamm
Chaos Computer Club Dresden

19.03.2014

Wer sind wir?



Wer sind wir?



Wer sind wir?

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

Wer sind wir?

- Chaos Computer Club Dresden (<http://c3d2.de>)
 - Datenspuren: 13./14.09. 2014 <http://datenspuren.de>

Wer sind wir?

- Chaos Computer Club Dresden (<http://c3d2.de>)
- Datenspuren: 13./14.09. 2014 <http://datenspuren.de>
- Podcasts (<http://pentamedia.org>)

Wer sind wir?

- Chaos Computer Club Dresden (<http://c3d2.de>)
- Datenspuren: 13./14.09. 2014 <http://datenspuren.de>
- Podcasts (<http://pentamedia.org>)
- Chaos macht Schule

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."

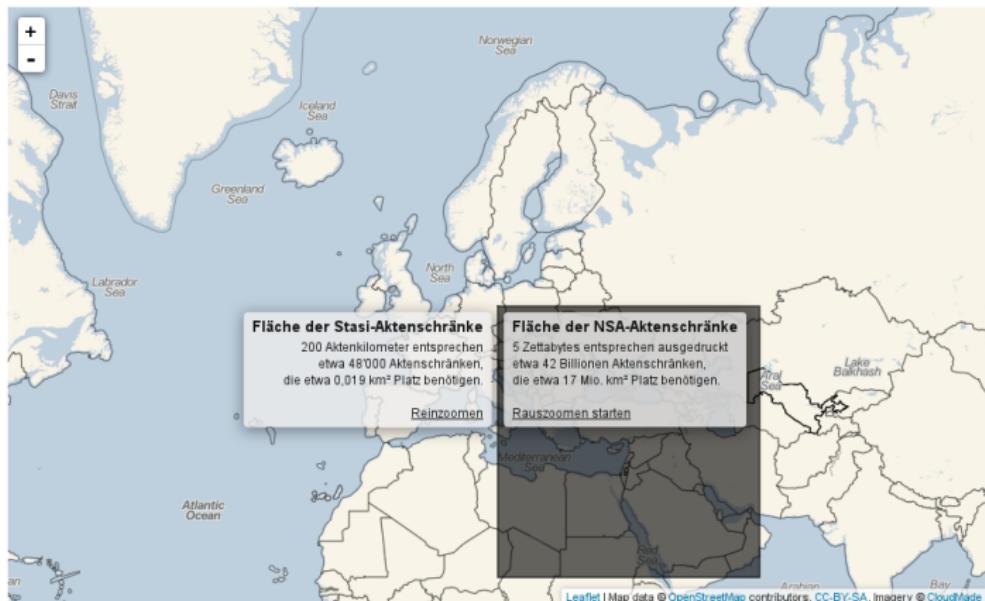
Stasi vs. NSA



Realisiert von OpenDataCity. Anwendung steht unter CC-BY 3.0.



Stasi vs. NSA



Realisiert von OpenDataCity. Anwendung steht unter CC-BY 3.0.



Merkels Handy

News Newsticker 7-Tage-News Archiv Foren



Topthemen: NSA Xbox Playstation 4 Windows 8.1 VDSL iPad iPhone Android Google Nexus

heise online > News > 2013 > KW 48 > NSA-Affäre: Merkel angeblich von fünf Geheimdiensten abgehört

26.11.2013 09:43



« Vorige | Nächste »

NSA-Affäre: Merkel angeblich von fünf Geheimdiensten abgehört

vorlesen / MP3-Download

Angela Merkel wurde in ihrer Amtszeit als Bundeskanzlerin nicht nur von der NSA, sondern auch den Geheimdiensten Russlands, Chinas, Nordkoreas und Großbritanniens abgehört. [Das berichtete](#) der Focus am Sonntag unter Berufung auf eine nicht näher erläuterte Analyse deutscher Sicherheitsbehörden. Hilfreich bei den Angriffen [auf das ungesicherte Handy](#) der Kanzlerin sei das weitläufige Regierungsviertel in Berlin, das sich hervorragend für die Funkspionage eigne, wird ein hochrangiger Sicherheitsbeamter zitiert.

Dem Bericht zufolge arbeiten alleine für Russland 120 Geheimdienstler in Deutschland und spähen die Bundesrepublik aus. Offiziell eingesetzt würden sie von der russischen Botschaft. Weiterhin hätten ausländische Geheimdienste in den vergangenen Jahren versucht, mehr als 100 deutsche Politiker, Beamte, Militärs, Manager und Wissenschaftler als Quellen anzuwerben. Das sei aber nur die Zahl derer, die sich danach bei deutschen Behörden gemeldet hätten, die tatsächliche Dunkelziffer sei unbekannt, aber wohl beträchtlich.

Top-News

Rätselhafte Entführungen im Internet

Ungewisse Zukunft für Windows RT

Satelliten made in Germany

NSA soll 75 Millionen US-Dollar zum Schutz vor Whistleblowing erhalten

Große Koalition setzt auf intelligente Stromzähler

Videos bei heise online

1 2 3 4 5

ct zockt (Episode 23)

Diesmal: Tower-Defense-Spiel "Kingdom", Japan-Gruseler "Run into the Dark" und "Code Combat".



heise open

Zehn Jahre bei Fedora

Bei der Mitarbeit an einer Linux-



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



DPA/dpa/UKU/ingenitaucher.com

Hehr als 200 Glasfaserkabel sollen die Briten angezapft haben

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 Netzsپione viel umfassender zu sein als die der Amerikaner.

Mail

SCHUTZ VOR ÜBERWACHUNG

Telekom plant innerdeutsches E-Mail-Netz

Die Deutsche Telekom will ausländischen Geheimdiensten das Ausspionieren von Daten erschweren. Laut einem Medienbericht plant der Konzern, den E-Mail-Verkehr nur noch über Knotenpunkte in Deutschland laufen zu lassen.

ANZEIGE

Die Deutsche Telekom will ausländische Geheimdienste durch eine kontrollierte Weiterleitung von Daten daran hindern, E-Mails und andere vertrauliche Informationen auszuspionieren. Das berichtet die Rheinische Post unter Berufung auf Telekom-Datenschutzvorstand Thomas Kremer.

Der Konzern wolle mit seinen Geschäftspartnern in Deutschland vereinbaren, bestimmte Daten über ein innerdeutsches Netz auszutauschen. Knotenpunkte im Ausland sollen dabei nicht berücksichtigt werden. "Reim Transport zwischen



(Bild: Deutsche Telekom)

Datum: 12.10.2013, 13:38

Autor: Steve Haak

Themen: E-Mail, GMX, NSA, Spionage, Telekom, United Internet

Teilen:



Einleitung
oooooooo

Tempora
○○●○○○○

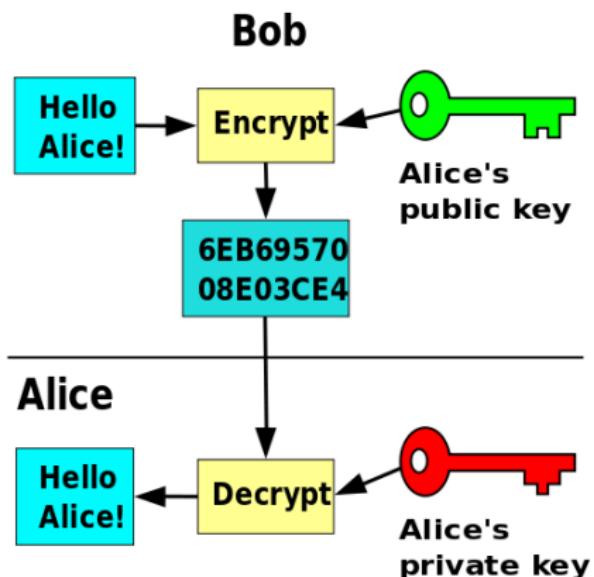
Prism
○○○○○

Vorratsdatenspeicherung
○○○○○○○○○○

Verhalten
○○○○○○○○○○○○

Verschlüsselung

Verschlüsselung



Einleitung
oooooooo

Tempora
oooo●ooo

Prism
ooooooo

Vorratsdatenspeicherung
oooooooooooo

Verhalten
oooooooooooo

SSL / TLS



SSL / TLS

- SSL = Secure Socket Layer

SSL / TLS

- SSL = Secure Socket Layer
 - eingesetzt im Web, Mail, ...

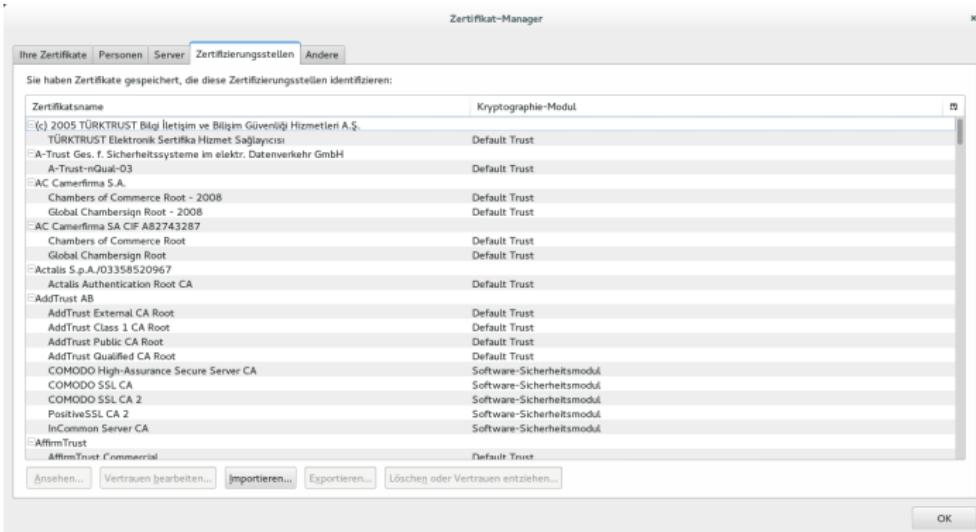
SSL / TLS

- SSL = Secure Socket Layer
- eingesetzt im Web, Mail, ...
- hierarchische Struktur

SSL / TLS

- SSL = Secure Socket Layer
- eingesetzt im Web, Mail, ...
- hierarchische Struktur
- gespeicherte Liste von vertrauenswürdigen Zertifikaten

Von Firefox vertraute Zertifikate



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.



Nichts zu verbergen?

[heise online](#) > [News](#) > [2007](#) > [KW 34](#) > Durch Google-Suche in die Einzelhaft [Update]

22.08.2007 13:31



« Vorige | Nächste »

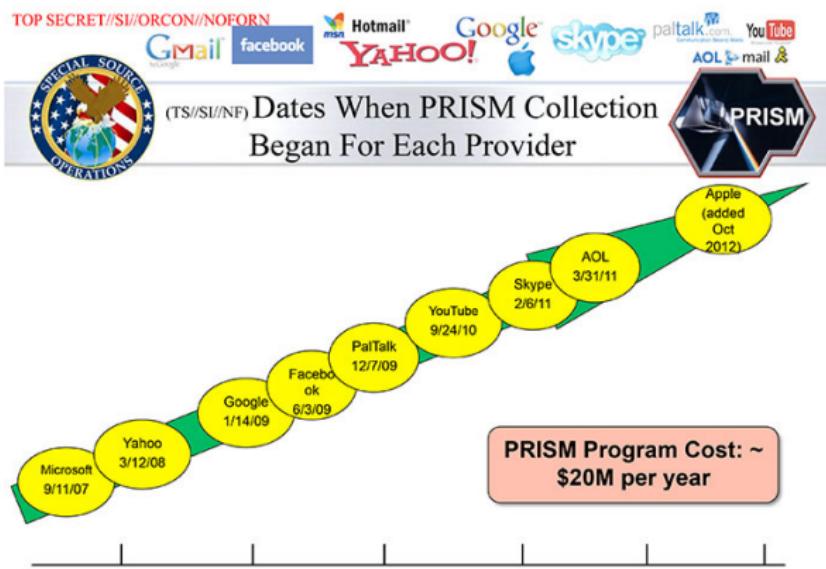
Durch Google-Suche in die Einzelhaft [Update]



vorlesen / MP3-Download

Vor drei Wochen wurde der Berliner Stadtsoziologe Andrej H. unter dem Verdacht der "Mitgliedschaft in einer terroristischen Vereinigung gemäß § 129a" festgenommen. Als Grund für die Festnahme nannte die ermittelnde Generalbundesanwaltschaft in Karlsruhe die Benutzung von Vokabeln, die auch in Schriften der sogenannten "Militanten Gruppe" vorkommen. Außerdem verfügte er nach Angaben der Ermittler "über Zugang zu Bibliotheken, um dort die Recherchen durchzuführen, die notwendig sind, um Texte für eine militante Gruppe zu verfassen."

Prism



TOP SECRET//SI//ORCON//NOFORN

Dezentrale Dienste



E-Mail



Bitmessage



palavatv



Lavabit

heise online > News > 2013 > KW 32 > Lavabit: E-Mail-Anbieter von Edward Snowden schließt und protestiert

09.08.2013 09:12

 « Vorige | Nächste »

Lavabit: E-Mail-Anbieter von Edward Snowden schließt und protestiert

 vorlesen / MP3-Download

Der US-amerikanische E-Mail-Anbieter Lavabit, der bekannt geworden war, weil der NSA-Whistleblower Edward Snowden jhn benutzt hat, wurde dicht gemacht. Ladar Levison, der Chef des Dienstes, der verschlüsselte Kommunikation anbietet, erklärte, er könne sich entweder an Verbrechen gegen US-Amerikaner beteiligen oder das Ergebnis zehn Jahre harter Arbeit aufgeben. Er habe sich für das zweite entschieden. Ihm sei es aber gesetzlich verboten, mitzuteilen, was ihn zu diesem Schritt bewogen hat. Vor der Schließung hatte Lavabit etwa 350.000 Nutzer und es konnten kostenlose aber auch kostenpflichtige Accounts eingerichtet werden, berichtete Ghacks.

Levison erwähnt in dem Statement seine Erfahrungen der "vergangenen sechs Wochen", auf die er nicht eingehen dürfe, obwohl er zwei Anfragen gestellt habe. Es liegt nahe, dass US-Behörden Druck ausübt haben, etwa um einen Zugang zu

Ende-zu-Ende-Verschlüsselung I

- Email: GPG = Gnu Privacy Guard
- Thunderbird: Enigmail
- Outlook: Gpg4win
- Apple Mail: GPGTools
- Web: Mailvelope (Firefox, Chrome)

Einleitung
oooooooo

Tempora
oooooooo

Prism
oooo●○

Vorratsdatenspeicherung
oooooooooooo

Verhalten
oooooooooooo

Ende-zu-Ende-Verschlüsselung II

Ende-zu-Ende-Verschlüsselung II

- OTR für Jabber:

- Pidgin mit OTR-Plugin für Linux und Windows
- GibberBot oder Xabber für Android
- Adium für Mac, ChatSecure für iOS

Ende-zu-Ende-Verschlüsselung II

- OTR für Jabber:
 - Pidgin mit OTR-Plugin für Linux und Windows
 - GibberBot oder Xabber für Android
 - Adium für Mac, ChatSecure für iOS
- palava.tv für Videotelefonie

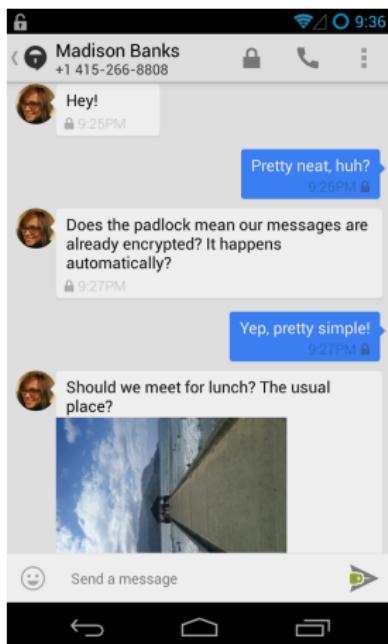
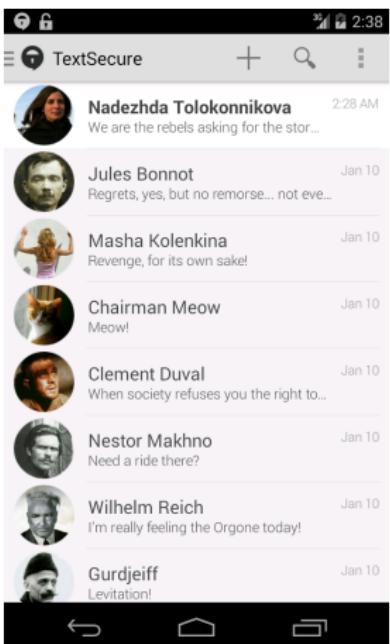
Ende-zu-Ende-Verschlüsselung II

- OTR für Jabber:
 - Pidgin mit OTR-Plugin für Linux und Windows
 - GibberBot oder Xabber für Android
 - Adium für Mac, ChatSecure für iOS
- palava.tv für Videotelefonie
- Redphone für Handytelefone (Android)

Ende-zu-Ende-Verschlüsselung II

- OTR für Jabber:
 - Pidgin mit OTR-Plugin für Linux und Windows
 - GibberBot oder Xabber für Android
 - Adium für Mac, ChatSecure für iOS
- palava.tv für Videotelefonie
- Redphone für Handytelefonate (Android)
- TextSecure für Nachrichten (Android)

TextSecure



Vorratsdatenspeicherung (USA)



US-Geheimdienst NSA der geheimen Vorratsdatenspeicherung überführt

Von Markus Beckedahl | Veröffentlicht: 06-06-2013 um 2:51h | 1 Antwort

Was der US-Geheimdienst National Security Agency (NSA) alles überwacht, ist in der Regel Spekulation. Weil dieser im Geheimen agiert. Es wird vermutet, dass die NSA als eine Art Staubsauger sehr viele öffentlich im Netz fluktuierende Daten sammelt und speichert. Aber da die NSA im geheimen operiert, fällt es in der Regel schwer, etwas zu beweisen.

Der Journalist Glenn Greenwald schreibt im britischen Guardian über eine als geheim klassifizierte Verordnung des Foreign Intelligence Surveillance Court (FISC), die der Guardian auch veröffentlicht hat: **NSA collecting phone records of millions of Americans daily - revealed**. In dieser wird der US-Provider Verizon angewiesen, eine Vorratsdatenspeicherung für drei Monate durchzuführen. Und zwar für lokale, nationale und ausländische Verbindungen mit allem, was dazu gehört. Es wird spekuliert, dass eine solche Verordnung regelmäßig erneuert und zudem nicht nur an Verizon verschickt wird.

Die Electronic Frontier Foundation (EFF) berichtet darüber: [Confirmed: The NSA is Spying on Millions of Americans.](#)

Suchen

Suchtext eingeben

Über uns

netzpolitik.org ist ein Blog und eine politische Plattform für Freiheit und Offenheit im digitalen Zeitalter.

Blog abonnieren

netzpolitik.org Blog Feed

Spenden

netzpolitik.org produziert eine Reihe kostenloser Inhalte. Eine Spende erhält das Projekt am Leben und ermöglicht uns einen Ausbau der Redaktion.

Unser Bank-Konto (ohne Gebühren)

Inhaber: netzpolitik.org e. V.



Vorratsdatenspeicherung (Deutschland)



Einleitung
oooooooo

Tempora
oooooooo

Prism
oooooo

Vorratsdatenspeicherung
oo●oooooooo

Verhalten
oooooooooooo

Metadaten

Metadaten

- Handynetz

Metadaten

- Handynetz
 - Telefonnummern

Metadaten

- Handynetz
 - Telefonnummern
 - Zeitpunkt und Dauer (Telefonate, SMS)

Metadaten

- Handynetz
 - Telefonnummern
 - Zeitpunkt und Dauer (Telefonate, SMS)
 - Funkzelle (Ort)

Metadaten

- Handynetz
 - Telefonnummern
 - Zeitpunkt und Dauer (Telefonate, SMS)
 - Funkzelle (Ort)
- Internet

Metadaten

- Handynetz
 - Telefonnummern
 - Zeitpunkt und Dauer (Telefonate, SMS)
 - Funkzelle (Ort)
- Internet
 - IP-Adresse

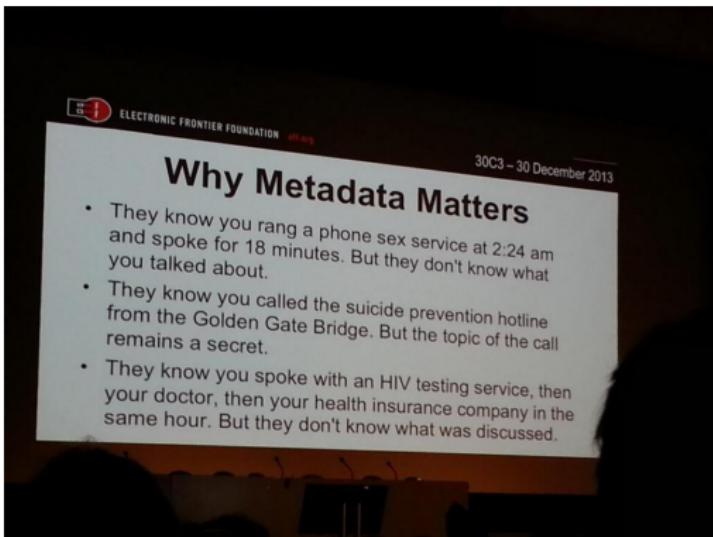
Metadaten

- Handynetz
 - Telefonnummern
 - Zeitpunkt und Dauer (Telefonate, SMS)
 - Funkzelle (Ort)
- Internet
 - IP-Adresse
 - Alle Verbindungen

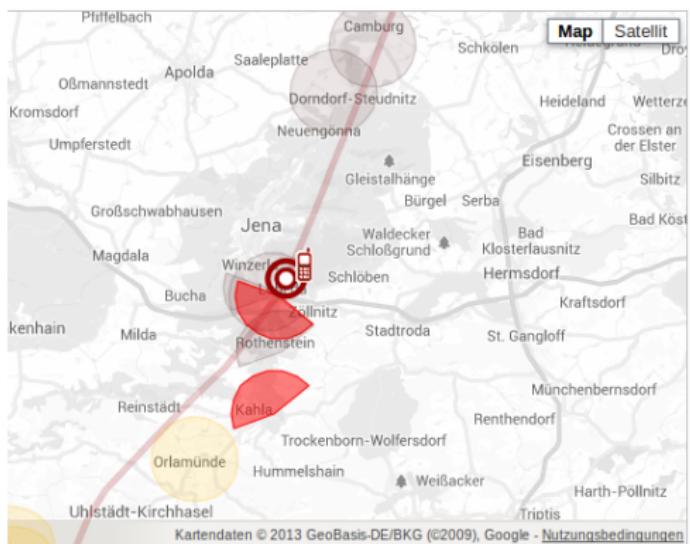
Metadaten

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

Metadaten



Metadaten



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



Einleitung
oooooooo

Tempora
oooooooo

Prism
oooooo

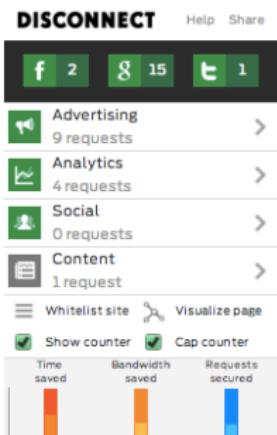
Vorratsdatenspeicherung
ooooo●oooo

Verhalten
oooooooooooo

Lightbeam

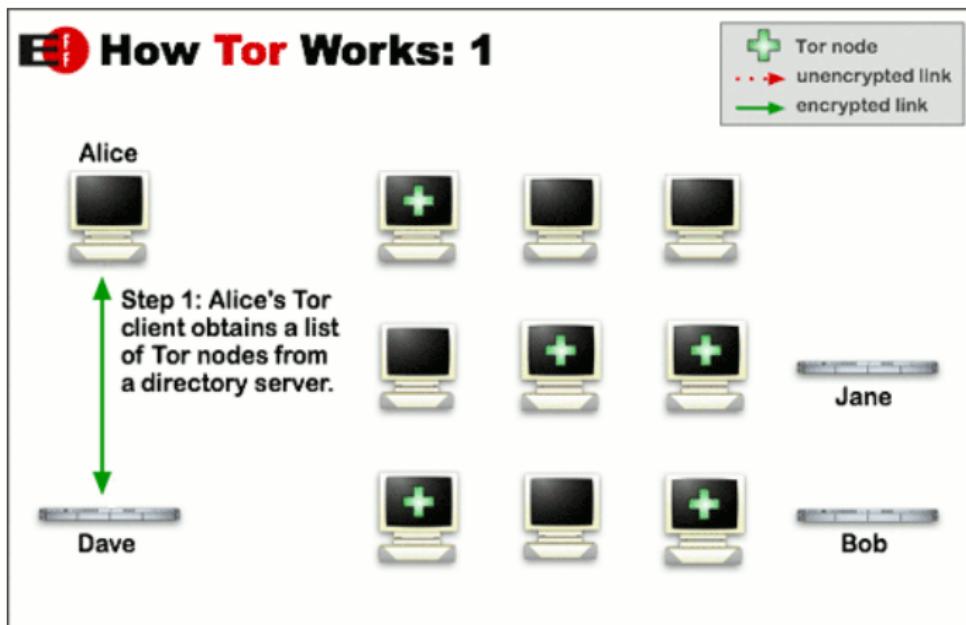


Disconnect.me



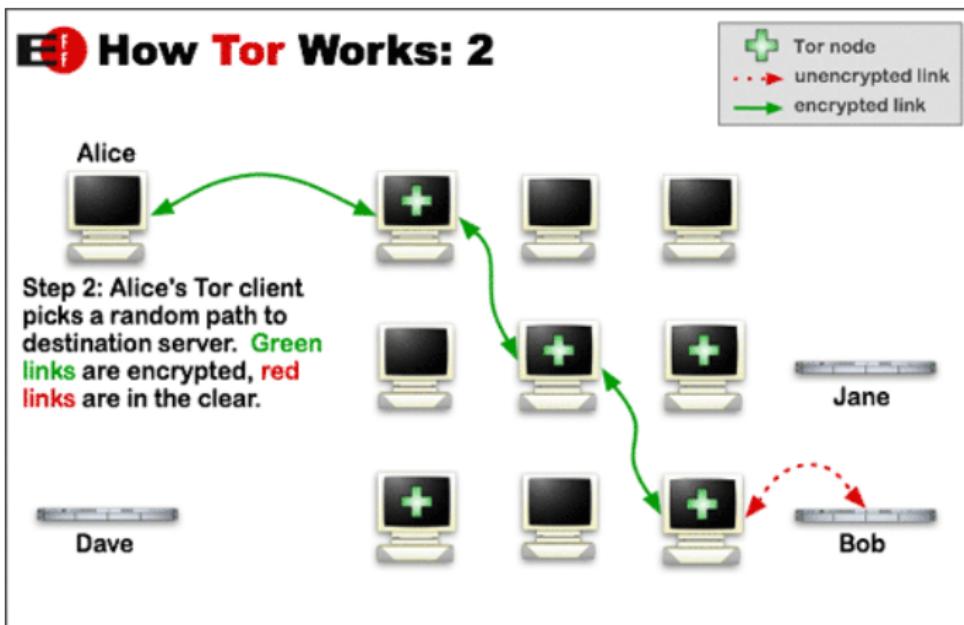
Disconnect.me

Tor



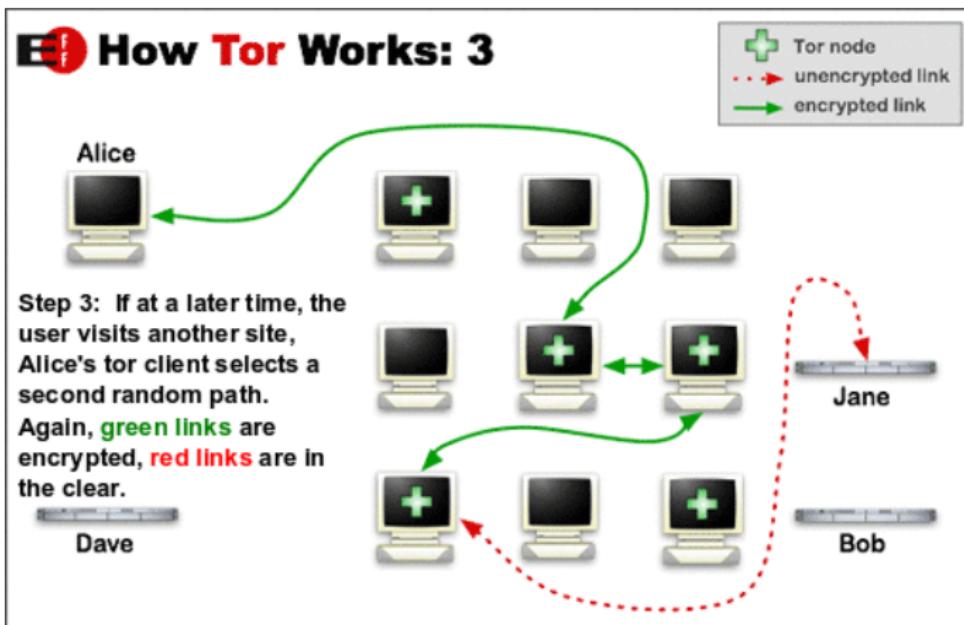
Grafik: The Tor Project

Tor



Grafik: The Tor Project

Tor



Grafik: The Tor Project

Technische Hilfsmittel

- Browser-Plugin "HTTPS Everywhere" (eff.org/https-everywhere)
- Browser-Plugin "Disconnect.me" (disconnect.me)
- GPG (gnupg.org)
- Tor (torproject.org)
- Redphone (whispersystems.org)
- TextSecure (whispersystems.org)

Einleitung
oooooooo

Tempora
oooooooo

Prism
oooooo

Vorratsdatenspeicherung
oooooooooooo

Verhalten
o●oooooooooooo

Datensparsamkeit

Datensparsamkeit

- Viele Daten zusammen ergeben Profile

Datensparsamkeit

- Viele Daten zusammen ergeben Profile
- Werden die Daten gebraucht?

Datensparsamkeit

- Viele Daten zusammen ergeben Profile
- Werden die Daten gebraucht?
- Werden echte Daten gebraucht?

Datensparsamkeit

- Viele Daten zusammen ergeben Profile
- Werden die Daten gebraucht?
- Werden echte Daten gebraucht?
 - Pseudonymität

Datensparsamkeit

- Viele Daten zusammen ergeben Profile
- Werden die Daten gebraucht?
- Werden echte Daten gebraucht?
 - Pseudonymität
 - mailinator.com (Wegwerf-Email-Adresse)

Datensparsamkeit

- Viele Daten zusammen ergeben Profile
- Werden die Daten gebraucht?
- Werden echte Daten gebraucht?
 - Pseudonymität
 - mailinator.com (Wegwerf-Email-Adresse)
 - frank-geht-ran.de (Wegwerf-Telefonnummer)

Einleitung
oooooooo

Tempora
oooooooo

Prism
oooooo

Vorratsdatenspeicherung
oooooooooooo

Verhalten
oo●oooooooo

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
 - .§)=")='

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!
- 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)

Wie schütze ich meinen Computer?

- Firewall
- Aktuelle und vertrauenswürdige Software

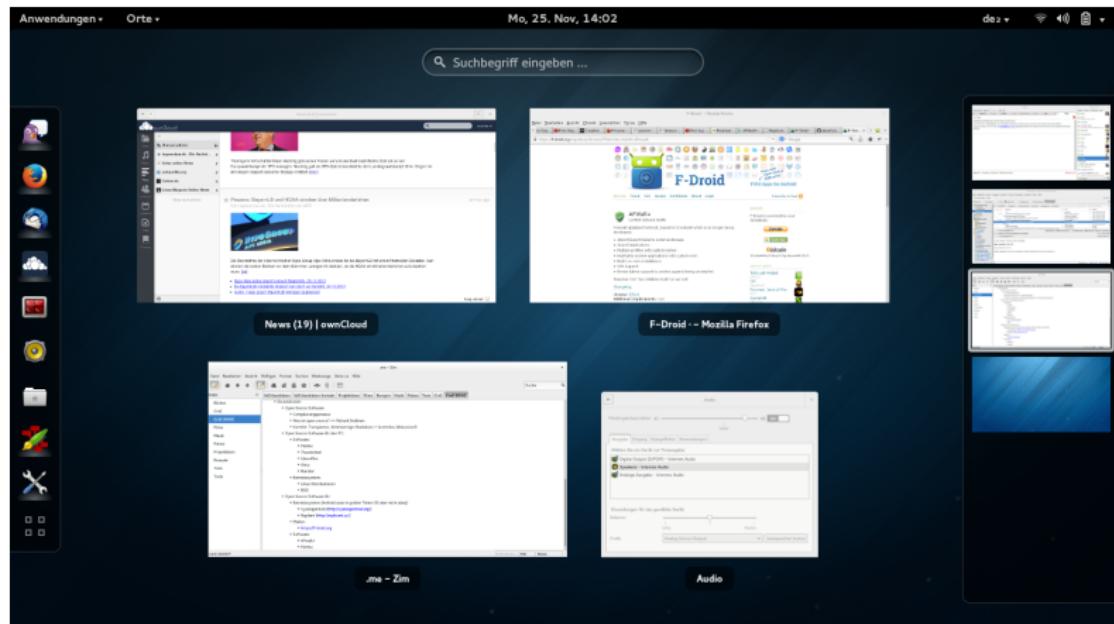
Wie schütze ich mein Smartphone?

- Permissions
- Firewall (z.B. AFWall+)
- Aktuelle und vertrauenswürdige Software
- Alternativer Appstore: f-droid.org

Freie Software

- Firefox
- Thunderbird
- LibreOffice
- Pidgin
- Evince/Okular
- Gimp
- VLC

Freie Software



Freie Software

| PRISM ↵ BREAK | | Platforms | Protocols |
|---------------|---|-----------|-----------|
| Mobile |  Android | > | |
| |  iOS | > | |
| Computer |  BSD | > | |
| |  GNU/Linux | > | |
| |  OS X | > | |
| |  Windows | > | |
| Network |  Routers | > | |
| |  Servers | > | |



Freie Software

https://prism-break.org/en/categories/android/

Operating Systems

| Proprietary | Free Recommendations |
|-------------------------|--|
| BlackBerry | CyanogenMod Aftermarket firmware for Android devices. |
| Google Android | Replicant Fully free Android distribution based o... |
| Microsoft Windows Phone | Firefox OS Open source operating system for And... |

Productivity

| Proprietary | Free Recommendations |
|---------------------------|---|
| Doodle | dudle A free online poll with an optional priva... |
| Evernote | EtherCalc Multi-user spreadsheet server. |
| Microsoft Office Web A... | Etherpad Self-hosted, real-time collaborative doc... |
| Zoho Office Suite | ProtectedText Free online encrypted notepad. |
| | Riseup Secure communication tools for peop... |

Categories

- Anonymizing Networks
- App Store
- DNS
- Email Accounts
- Email Clients
- Email Encryption
- File Storage & Sync
- Finance
- Instant Messaging
- Media Publishing
- Mesh Networks
- Operating Systems
- Productivity
- Social Networks
- Video & Voice
- VPN Accounts
- VPN Clients
- Web Browser Addons
- Web Browsers
- Web Hosting
- Web Search
- World Maps



Diskussion

Diskussion
Marius Melzer und Stephan Thamm
CMS Dresden: schule@c3d2.de

Weiterführende Links

- Überwachungsstaat, was ist das? -
<https://www.youtube.com/watch?v=iHlzsURb0WI>
- Übersicht freier PDF-Betrachter -
<http://pdfreaders.org>
- Freie Alternativen zu kommerzieller Software -
<http://prism-break.org>
- Übersicht öffentlicher Jabber-Server -
<https://xmpp.net/directory.php>