

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

Marius Melzer und Stephan Thamm  
Chaos Computer Club Dresden

23.07.2014

# Chaos Computer Club



# Chaos Computer Club



# Chaos Computer Club

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

# Chaos Computer Club

- Chaos Computer Club Dresden (<http://c3d2.de>)
  - Datenspuren: 13./14.09.2014 <http://datenspuren.de>

# Chaos Computer Club

- Chaos Computer Club Dresden (<http://c3d2.de>)
  - Datenspuren: 13./14.09.2014 <http://datenspuren.de>
  - Podcasts (<http://pentamedia.de>)

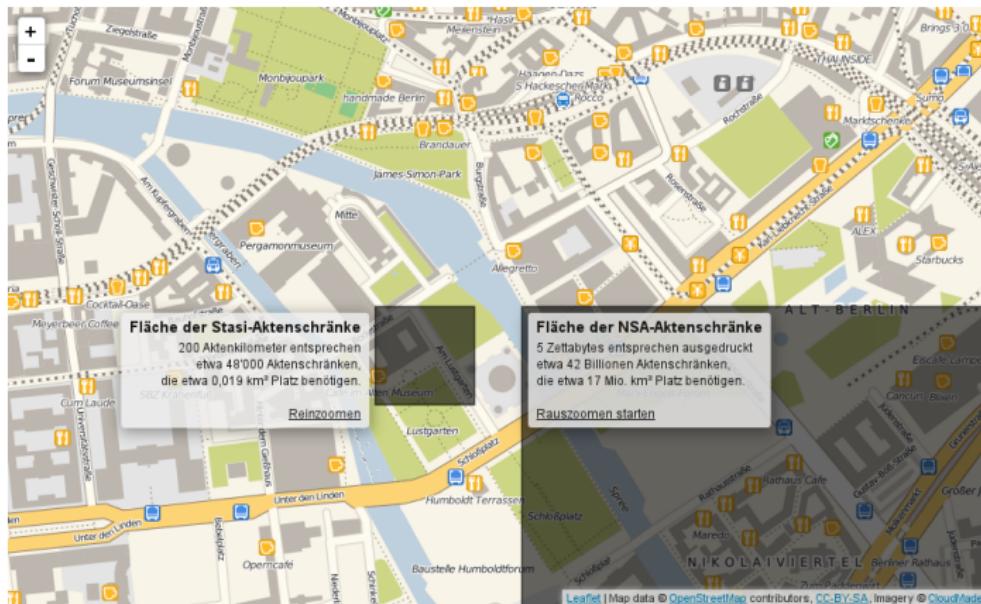
# Chaos Computer Club

- Chaos Computer Club Dresden (<http://c3d2.de>)
  - Datenspuren: 13./14.09.2014 <http://datenspuren.de>
  - Podcasts (<http://pentamedia.de>)
  - 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.”

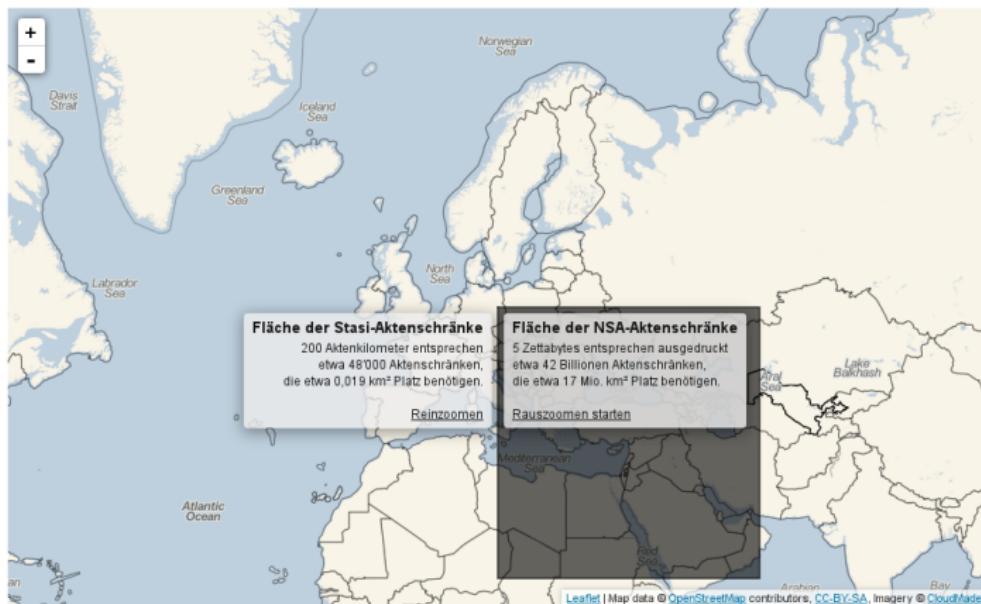
# Stasi vs. NSA



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-



# NSA-Skandal



Grafik: Laura Poitras / Praxis Films



# 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 Netzsperne 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

**HOME TICKER**

TOP-THEMEN: NSA iPhone 5S Haswell Xbox One Playstation 4 Windows 8 mehr

Suchen



(Bild: Deutsche Telekom)

**Datum:** 12.10.2013, 13:38

**Autor:** Steve Haak

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

**Teilen:**

 4    207    62    15

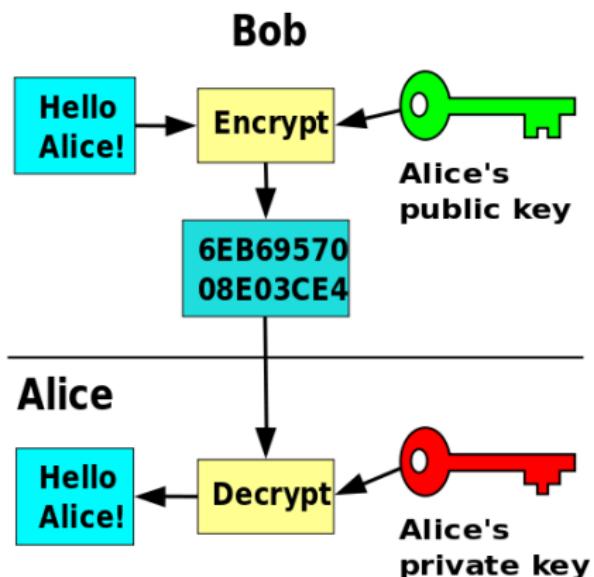
# Verschlüsselung: Analogie



Grafik: Ronald Preuss

## Verschlüsselung: Asymmetrische

# Verschlüsselung: Asymmetrische



Einleitung  
ooooooooo

Kommunikation  
oooo●oooo

Inhalte  
ooooooo

Metadaten  
oooooooooooo

Freie Software  
oooooooooooooooooooo

Verhalten  
ooo

# SSL / TLS

# SSL / TLS

- SSL = Secure Socket Layer

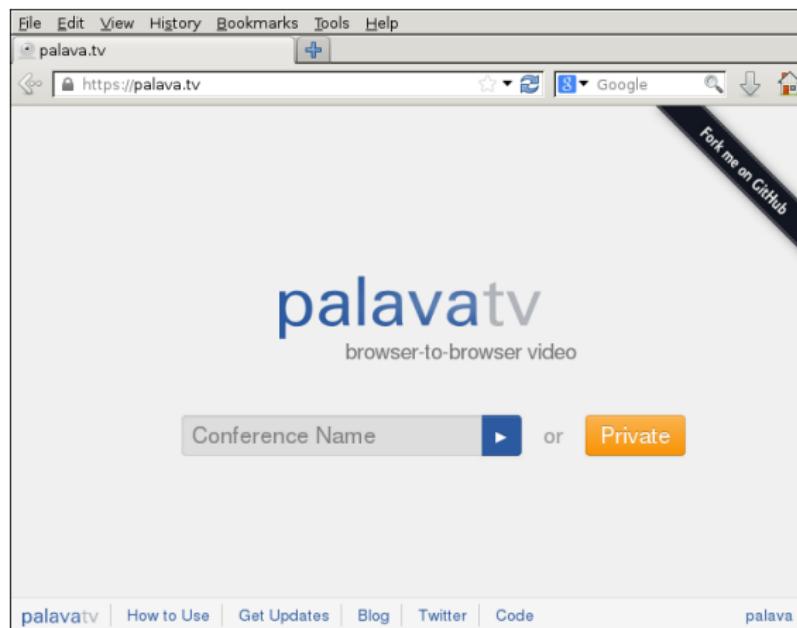
# SSL / TLS

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

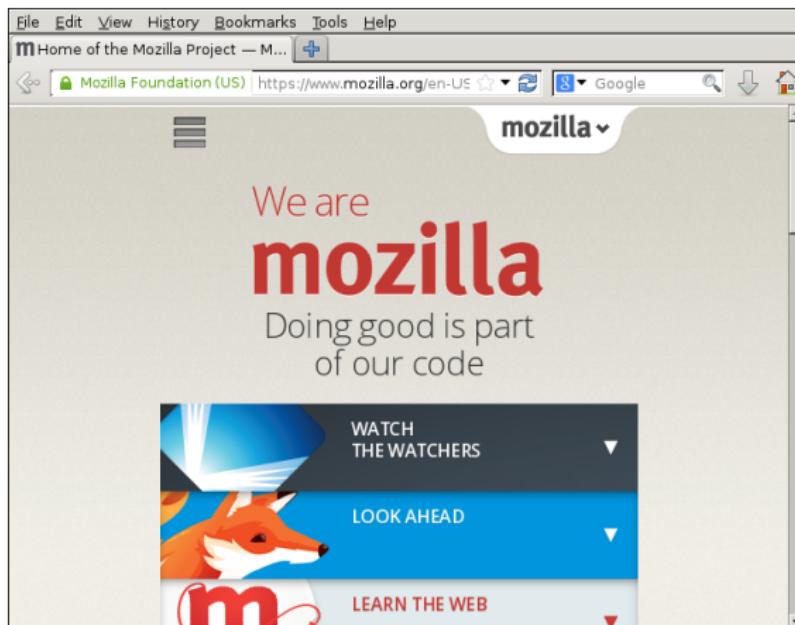
# SSL / TLS

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

# SSL im Browser



# SSL im Browser



# SSL im Browser

The screenshot shows a web browser window with the following details:

- Menu Bar:** File, Edit, View, History, Bookmarks, Tools, Help.
- Title Bar:** Untrusted Connection, https://pentapad.c3d2.de, Google.
- Content Area:**
  - Icon:** A yellow icon of a person with a speech bubble.
  - Title:** This Connection is Untrusted
  - Text:** You have asked iceweasel to connect securely to **pentapad.c3d2.de**, but we can't confirm that your connection is secure.
  - Text:** Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
  - Section:** What Should I Do?
  - Text:** If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
  - Button:** Get me out of here!
  - Section:** ▾ Technical Details
  - Text:** pentapad.c3d2.de uses an invalid security certificate.
  - Text:** The certificate is not trusted because no issuer chain was provided.  
(Error code: sec\_error\_unknown\_issuer)
  - Section:** ▶ I Understand the Risks

Einleitung  
oooooooo

Kommunikation  
oooooooo●○

Inhalte  
ooooooo

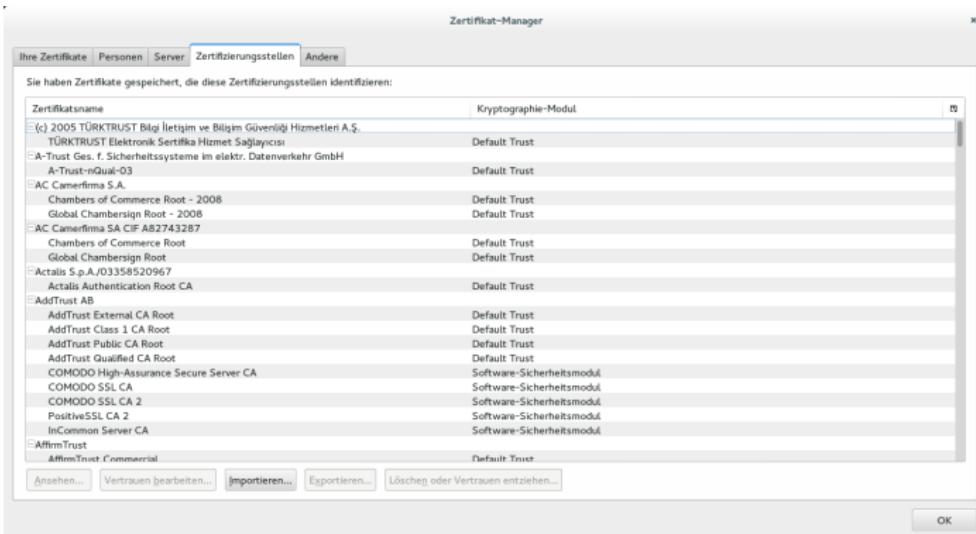
Metadaten  
oooooooooooooooooooo

Freie Software  
oooooooooooooooooooo

Verhalten  
ooo

# 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](#)

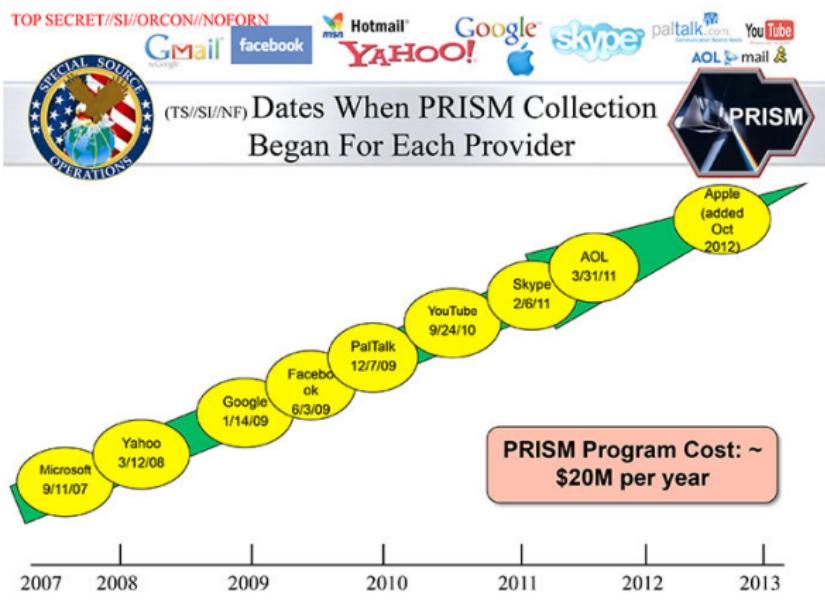
---

**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.

# Prism



# 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)

# 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)

# Authentifizierung

Frage und Antwort

Frage und Antwort

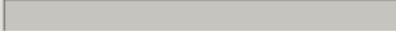
Gemeinsames Geheimnis

Fingerabdruck-Verifizierung

Stellen Sie eine Frage dessen Antwort nur Sie und thammi@debianforum.de kennen.

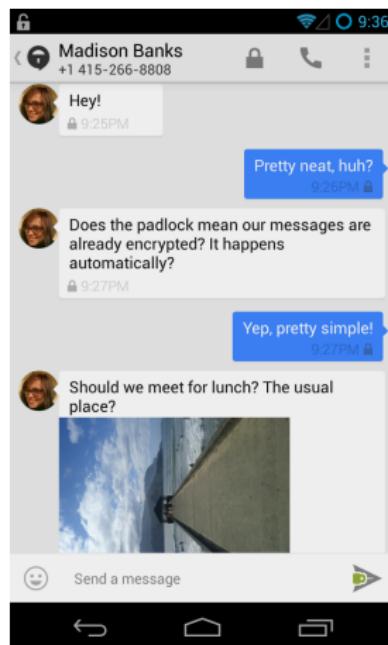
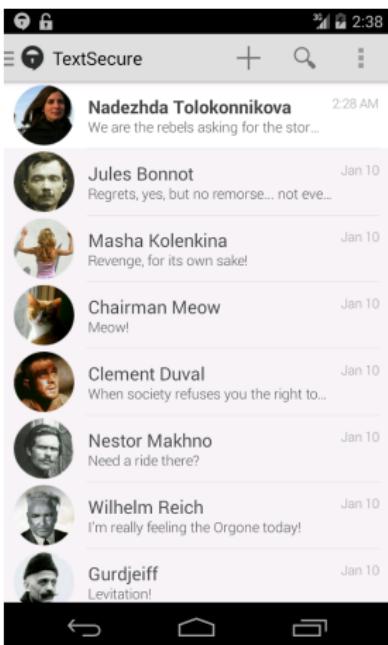
Frage:

Antwort:

 0%

Abbrechen Authentifizieren

# TextSecure



## Vorratsdatenspeicherung (USA)



US-Geheimdienst NSA der geheimen Vorratsdatenspeicherung überführt

Von Markus Beckedahl | Veröffentlicht: 06.06.2013 um 7:51h | 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](#).

Suchow

**Suchtext eingeben**

Шашки

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

Blog abonnieren

[View all reviews](#)

Spender

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)

ARD Home Nachrichten Sport Börse Ratgeber Wissen Kultur Kinder ARD Intern Fernsehen Radio ARD Mediathek **ARD** 

tagesschau.de  

Startseite Videos & Audios Inland Ausland Wirtschaft Wahlarchiv Wetter Ihre Meinung Kontakt & Mehr



Nicht mit EU-Recht vereinbar

## **EuGH kippt Vorratsdatenspeicherung**

Die Speicherung von Kommunikationsdaten ohne Verdacht auf Straftaten ist nicht mit EU-Recht vereinbar. Das hat der Europäische Gerichtshof (EuGH) in Luxemburg entschieden und damit die EU-Richtlinie zur Sicherung von Telefon- und E-Mail-Informationen gekippt. Die Richtlinie muss nun reformiert und die verdachtlose Speicherung von Verbindungsdaten von Telefon, Internet und E-Mails künftig "auf das absolut Notwendige beschränkt" werden.

Die Regelung "beinhaltet einen Eingriff von großem Ausmaß und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz

**VIDEO**



Gigi Deppe, SWR, über das EuGH-Urteil zur Vorratsdatenspeicherung  
tagesschau24 11:15 Uhr, 08.04.2014 | [video](#)

**AUDIO**

[EuGH kippt Vorratsdatenspeicherung - Reaktionen gespalten, Malte Pieper, ARD Berlin, 08.04.14 12:42 Uhr | audio](#)

**LINKS**

[Das EuGH-Urteil zur Vorratsdatenspeicherung \(pdf\)](#)



# Metadaten

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

# Metadaten

heise online > News > 2014 > KW 11 > Studie: Was auf Vorrat gespeicherte Verbindungsdaten verraten

14.03.2014 18:59



=> Vorige | Nächste <

Ausgabe

## Studie: Was auf Vorrat gespeicherte Verbindungsdaten verraten

[MP3] vorlesen / MP3-Download

Stanford-Forscher haben mithilfe eines Crowdsourcing-Verfahrens von "Metadaten" aus der Telekommunikation relativ einfach sehr intime Details über Nutzer wie etwa deren potentielle Krankheiten herausfinden können.

Verbindungsdaten erlauben offenbar ziemlich umfassende Rückschlüsse auf die Personen, die sie verursachen, wie US-Wissenschaftler herausgefunden haben wollen. Sie seien selbst überrascht gewesen, welch tiefe Einblicke ihnen reine Verbindungsdaten gegeben hätten, schreibt ein Mitglied des wissenschaftlichen Teams in einem [Blogbeitrag](#).

Teilnehmer an der Untersuchung hätten Gespräche mit den Anonymen Alkoholikern, Waffengeschäften, Gewerkschaften, Scheidungsnichtern, auf Sexauskrankheiten spezialisierte Kliniken oder etwa Strip-Cubs geführt. Bei den Erkenntnissen habe es sich nicht um eine "hypothetische Horrorparade" gehandelt, sondern um einfache Ableitungen aus dem Verhalten echter Telekommunikationsnutzer, halten die Forscher fest.

Für das [Projekt](#) haben Mitarbeiter des Center for Internet and Society der Stanford-Universität Nutzer von Android-Smartphones gebeten, über die [MetaPhone-App](#) ihre Verbindungsdaten beizusteuern. Über einen Abgleich mit 5000 aus dem so generierten Material zufällig ausgewählten Telefonnummern mit Yelp, Facebook und Google Places war es den Forschern bereits [Ende vergangenen Jahres gelungen](#),



Verbindungsdaten aus Telefongesprächen verraten offenbar mehr über eine Person als gedacht. (G)

Bild: dpa, Marc Müller

## Top-News

Fünfjähriger entdeckt Xbox-One-Backdoor

Metro-Look im Auto: Microsoft verbindet Infotainment und Windows Phone

Android-TV: Googles nächster Angriff auf den Fernseher

Britische Regierung kauft 12 Monate XP-Support

c't zeigt Auswege aus dem Router-Desaster



c't

### Das Router-Desaster

Unbeachtet in einer Ecke oder unter Ihrem Schreibtisch lauert eine Gefahr: der Router für Ihren Internet-Zugang. Ganoven nutzen dessen Sicherheitslücken aus, um Sie zu schädigen.



heise open

### Die Neuerungen von Linux 3.14

Neben einem weiteren Process-Scheduler bringt der neue Kernel eine Reihe von Performance-Optimierungen und Unterstützung für einige kürzlich vorgestellte Grafikkarte.



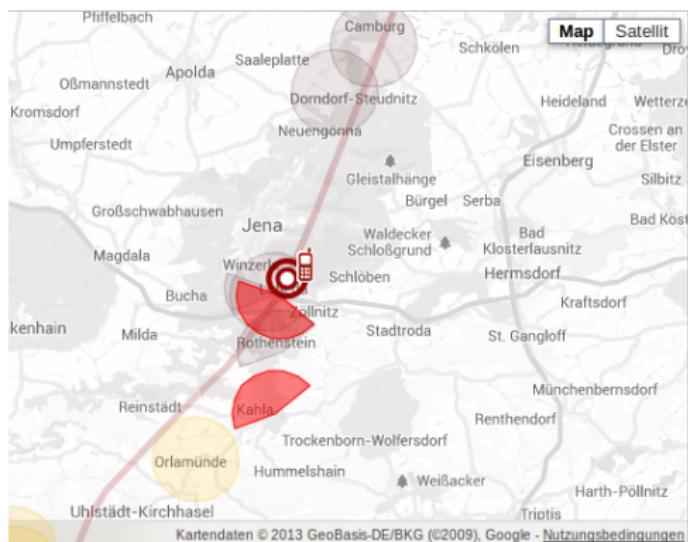
heise security

### Verwurmt, verphishst, verspamt

Echte Firmen-E-Mails sind kaum noch von Phishingmails zu unterscheiden.

Trotzdem sollten Kunden den Durchblick:

# 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



# Metadaten

The screenshot shows the golem.de website's header. It features a logo with a globe icon, the text "golem.de IT-NEWS FÜR PROFIS", and a navigation bar with links for "HOME", "TICKER", and a search bar. Below the header, there's a menu for "TOP-THEMEN" including "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

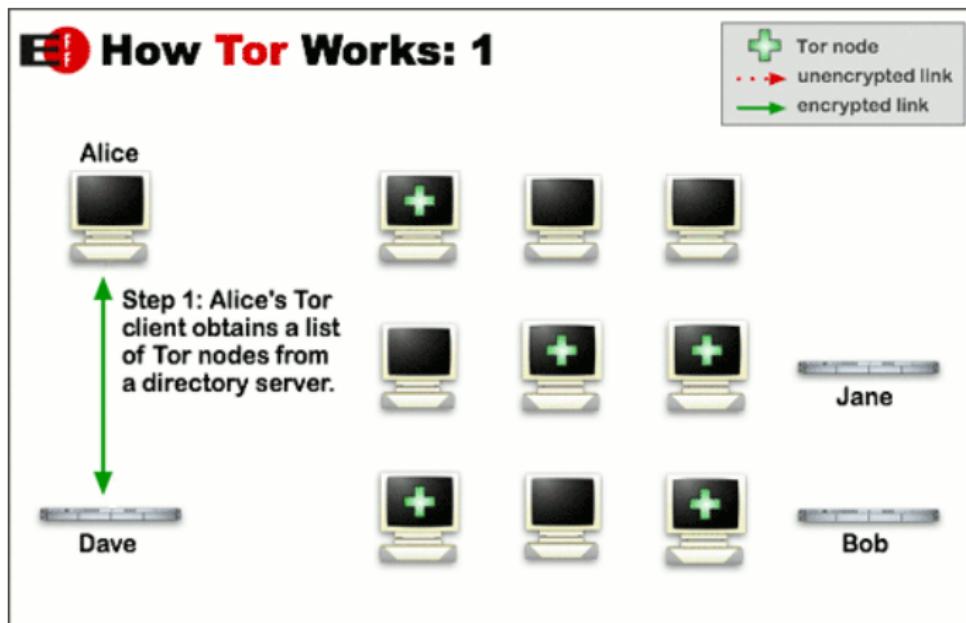
Autor: Friedhelm Greis

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

Teilen:



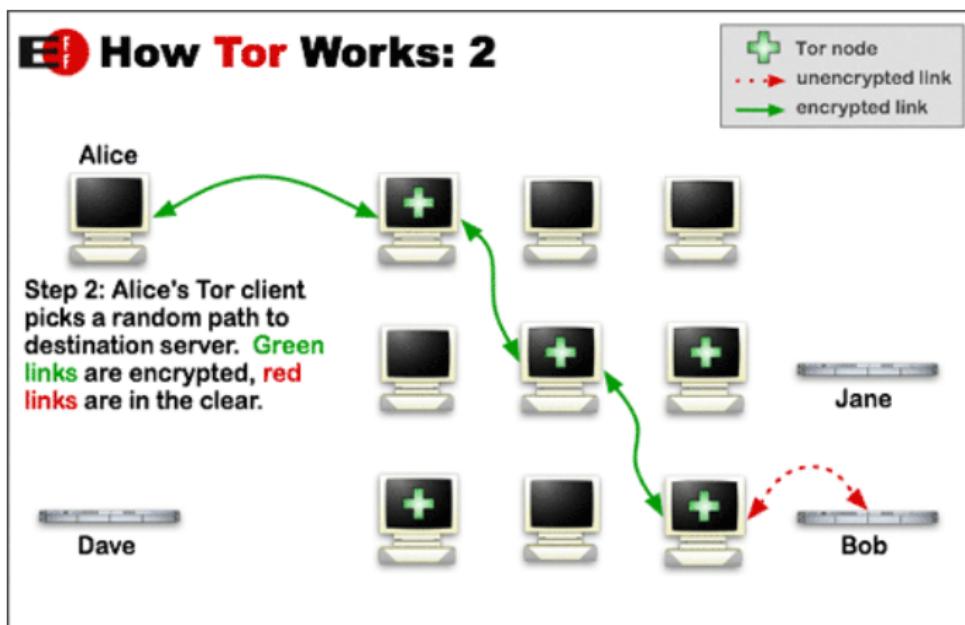
Tor



Grafik:  The Tor Project

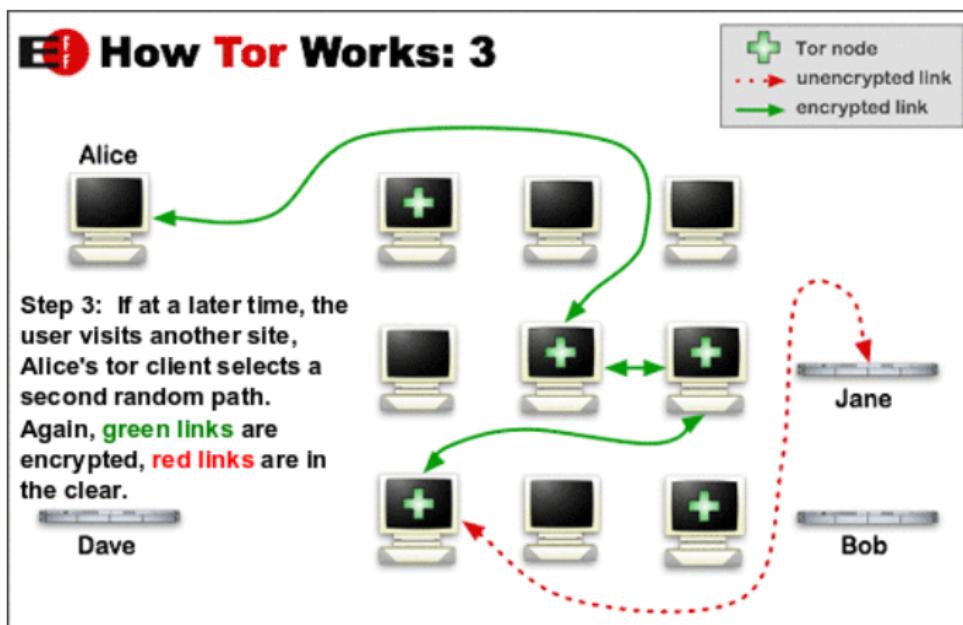


# Tor



Grafik: The Tor Project

# Tor



Grafik: The Tor Project

Tor

# Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.



[Download Tor](#) 

- Tor prevents people from learning your location or browsing habits.
  - Tor is for web browsers, instant messaging clients, and more.
  - Tor is free and open source for Windows, Mac, Linux/Unix, and Android

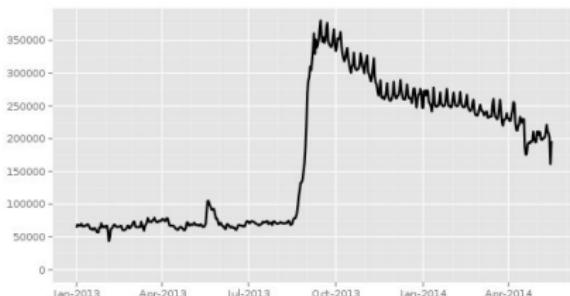
# Tor in Deutschland



## Tor Metrics Portal: Users

### Direct users by country:

Directly connecting users from Germany



The Tor Project - <https://metrics.torproject.org/>

Start date (yyyy-mm-dd):  End date (yyyy-mm-dd):

Source:

# Anonymität unter Vollüberwachung

p. 2

TOP SECRET//COMINT//REL FVEY

## Tor Stinks...<sup>[u]</sup>

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a **very small fraction** of Tor users, however, **no** success de-anonymizing a user in response to a TOPI request/on demand.



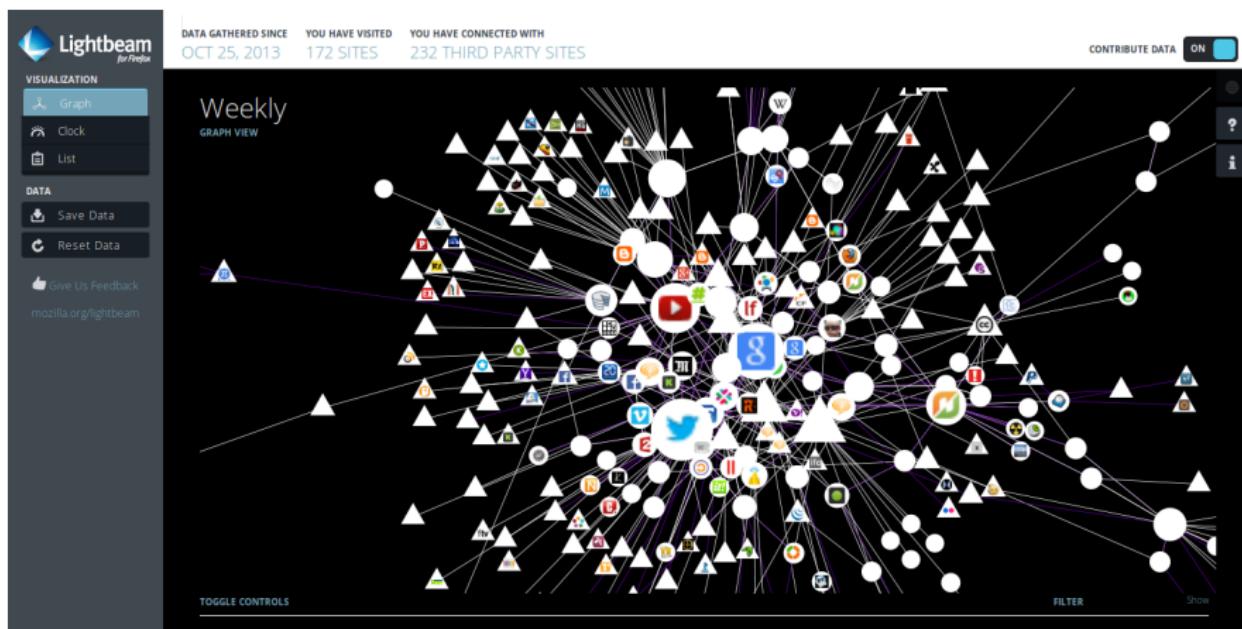
TOP SECRET//COMINT//REL FVEY



## Terroristen

# Torrorist

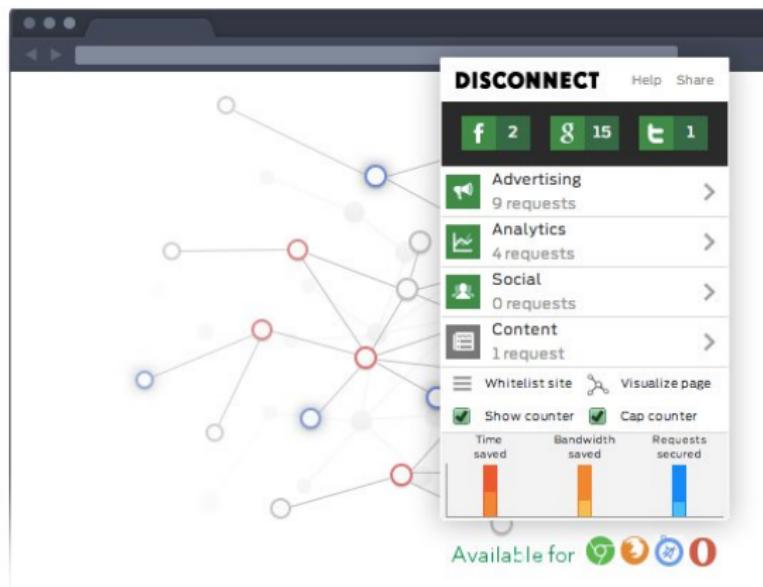
# Metadaten - Lightbeam



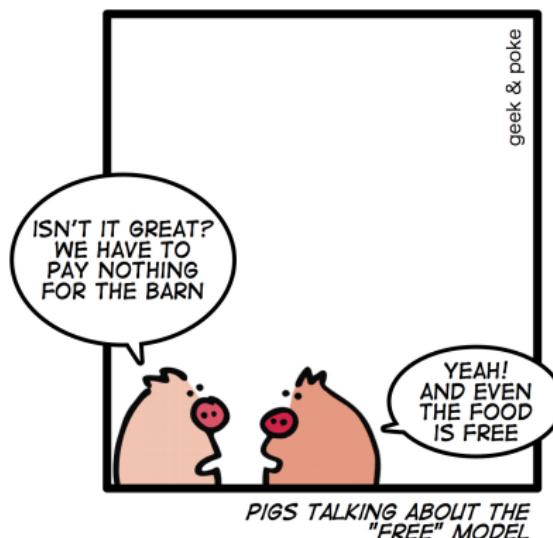
Grafik: Clint Lalonde



# Metadaten - Disconnect



## Geschäftsmodelle



<http://geekandpoke.typepad.com/geekandpoke/2010/12/the-free-model.html>



# Backdoors in Windows

The screenshot shows the homepage of c't magazin. The header features the logo 'ct magazin' on the left and navigation links for 'Startseite', 'Artikel' (which is highlighted), 'c't-Projekte', and 'Hotline & FAQ'. Below the header is a horizontal menu with links for 'Magazin', 'Internet', 'Software', 'Hardware', 'Know-how', 'Praxis', and 'Artikel-Foren'. The main content area displays an article by Micha Borrmann and Jürgen Schmidt, dated 'c't 17/13'. The title of the article is 'Microsofts Hintertür' and the subtitle is 'Zweifelhafte Updates gefährden SSL-Verschlüsselung'. A large block of text describes how Windows handles untrusted SSL certificates.

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 in Windows

Problematische Hintergrunddienste von Windows, die Daten aus dem System heraus [Bearbeiten] an Microsoft senden

## Funktionen:

- "Internetzeit" (sofern time.windows.com als NTP-Server konfiguriert ist)
- Netzwerk Konnektivität (Seit Windows Vista und höher) - siehe  [Windows: Online-Erkennung abschalten](#) 
- [Windows Customer Experience Improvement Program](#) (regelmäßige Übertragung anonymisierter Daten zum Nutzerverhalten an Microsoft)
- Fehlerberichterstattung (WER) (automatische Übertragung von Fehlerberichten an Microsoft nachdem eine Anwendung oder das Betriebssystem Probleme hatte)
- [Windows Smart Search](#) (Integration von Bing Suche in die allgemeine Suche in Windows, alle Suchanfragen werden an [Microsoft Bing](#) weitergeleitet.)
- [Microsoft Security Compliance Manager](#) Die Microsoft-Sprecherin (...) stellt klar, dass sich die Mitarbeit der NSA auf das so genannte **Security Compliance Management Toolkit** beschränke. Dieses enthält eine Reihe von Sicherheitseinstellungen, die verschiedene Gefahrenstufen abdecken sollen, für die Windows 7 ab Werk nicht konfiguriert ist.  
[www.computerworld.com](http://www.computerworld.com) - Microsoft denies it built backdoor in Windows 7  -  Ist das Win7-spezifisch, wie ist es mit Win 8 / 8.1??
- Windows Management Instrumentation: [NSA/WISTFULTOLL](#) (externe Migration von Daten möglich qua WMI):
  -  [LeakDoc "WISTFULTOLL"](#)  [\(DOC\)](#)
- Windows Update: Microsoft kann ohne Erlaubnis Updates einspielen [Heise](#) 

- Windows-WLAN-Fernzugriff: [NSA/SOMBERKNAVE](#)-Wanze: —  [LeakDoc "SOMBERKNAVE"](#)  [\(DOC\)](#)
- externer Zugriff auf Windows-Festplattenformat / - Filesysteme: Befall des MBR durch [NSA/IATEMONK](#)-Wanze:
  -  [LeakDoc "IATEMONK"](#)  [\(DOC\)](#)
- BIOS-Befall vor OS-Start zum Festplatten-Zugriff: [NSA/SWAP](#)-Wanze: (WIN, Linux, FreeBSD, Solaris): —  [LeakDoc "SWAP"](#)  [\(DOC\)](#)
- Hintergrunddienste zum **Komplettzugriff auf den Rechner**: [NSA/OLYMPUSFIRE](#), [NSA/VALIDATOR](#)-Wanzen
  - (wird **automatisiert ferninstalliert**, z.B. wenn eine vorgetäuschte Internetseite geöffnet wurde: [NSA/QUANTUM](#), [NSA/QUANTUMTHEORY](#) - [GCHQ](#))
  - kommerziell erhältlichen Formen: [Malware](#)

# Backdoors in iOS

**Arik Hesseldahl**[ethics statement](#) | [bio](#) | [✉ e-mail](#) | [RSS](#) | [Follow @ahess247](#)

## Apple Denies Working with NSA on iPhone Backdoor

DECEMBER 31, 2013 AT 8:49 AM PT

[Tweet](#) | [Share](#) | [Share](#) | [Print](#)

Apple just responded to newly released documents claiming that the U.S. National Security Agency has a method for gaining backdoor access to its iPhone. It says it has never worked with the agency, and is unaware of the alleged program targeting the iPhone known as DROPOUTJEEP.

The program was disclosed in a [trove of documents](#) leaked yesterday and shared by the security researcher Jacob Appelbaum and the German news magazine Der Spiegel.

Here's Apple's statement in full:



## Backdoors in Apps

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	■■■■■	■■■■■	■■■■■	■■■■■	■■■■■	■■■■■



# Backdoors in Android

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.



# Backdoors in Apps

## 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 in Apps

SPIEGEL ONLINE NETZWELT Login | Registrierung Search icon

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

Nachrichten > Netzwerk > Web > Google > Standortdaten verkauft: Beliebte Android-App spionierte Nutzer aus

## Standortdaten verkauft: Beliebte Android-App spionierte Nutzer aus

The image shows a screenshot of a news article from SPIEGEL ONLINE NETZWELT. The headline reads "Standortdaten verkauft: Beliebte Android-App spionierte Nutzer aus". Below the headline is a large image of the "Brightest Flashlight Free" app's interface, featuring a green Android robot holding a flashlight. The app's name is displayed prominently at the top. A small caption at the bottom left of the image states: "'Brightest Taschenlampe': Diese App verriet den Aufenthaltsort ihrer Nutzer". The SPIEGEL logo is visible in the top right corner of the page.

"Brightest Taschenlampe": Diese App verrät den Aufenthaltsort ihrer Nutzer

# Backdoors in Apps

[Log in](#) [Help!](#) [Members](#)[about](#) [campaigns](#) [licensing](#) [membership](#) [resources](#) [commu](#)[Community](#) >

## Replicant developers find and close Samsung Galaxy backdoor

by [Paul K](#) — Published on Mar 12, 2014 04:50 PM

**While working on Replicant, a fully free/libre version of Android, we discovered that the proprietary program running on the applications processor in charge of handling the communication protocol with the modem actually implements a backdoor that lets the modem perform remote file I/O operations on the file system.**

*This is a guest post by [Replicant](#) developer Paul Kociakowski. The Free Software Foundation supports Replicant through its Working Together for Free Software fund. [Your donations to Replicant](#) support this important work.*

Today's phones come with two separate processors: one is a general-purpose applications processor that runs the main operating system, e.g. Android; the other, known as the modem, baseband, or radio, is in charge of communications with the mobile telephony network. This processor always runs a proprietary

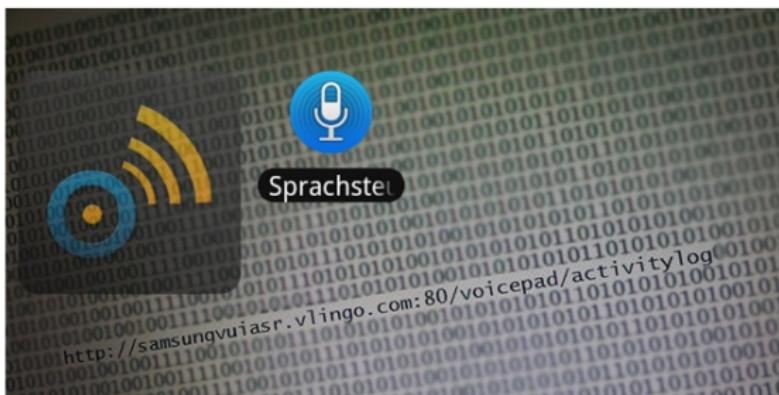


# Backdoors in Apps

## Sprachsteuerung und Vlingo telefonieren nach Hause

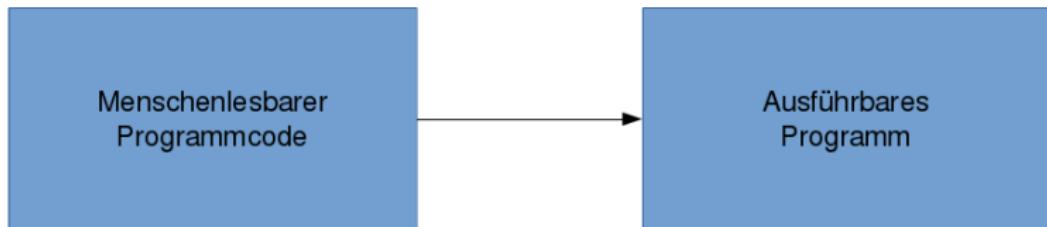
Käpt'n Andreas V. v 22.01.2012

68



(Bildquellen: Jörg Voss)

# 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**



# LibreOffice

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



# Freie Software für Android

## F-Droid

- Installationsdienst für freie Android-Software



## TextSecure

- Verschlüsselter Nachrichtenaustausch
- Verschlüsselte Speicherung



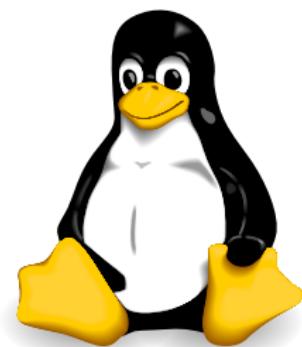
# Replicant

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

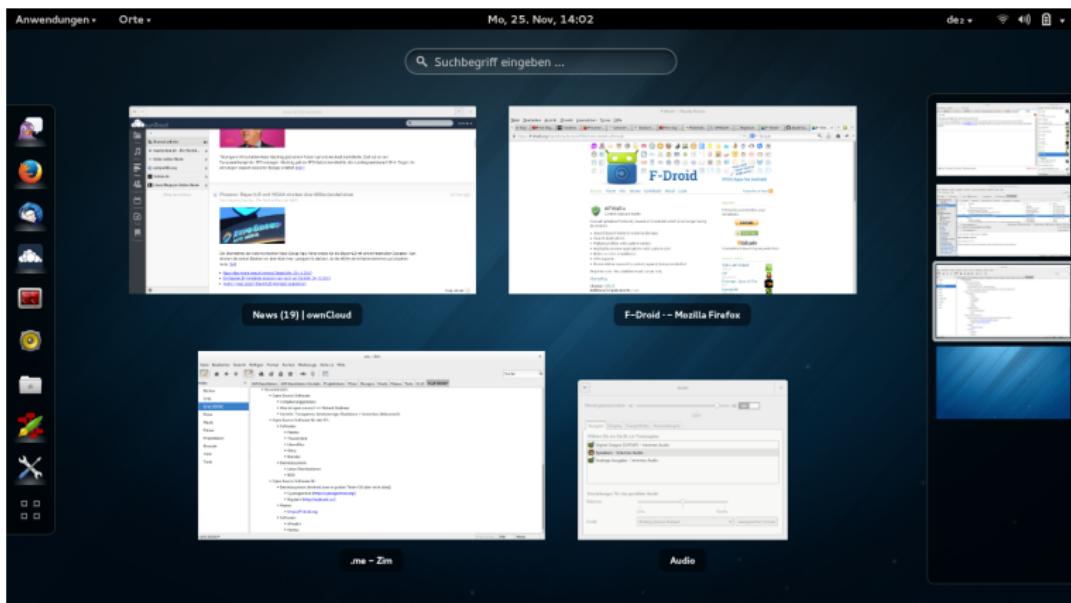


# Linux

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



# Linux



# 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)

# 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)
  - bugmenot.com (Fake Accounts)

## 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)

# Diskussion

## Diskussion

Folien:  Chaos Computer Club Dresden

CMS Dresden: schule@c3d2.de