
CRYPTO
PARTY

„Ich möchte nicht in einer Welt leben, in der alles, was ich sage, alles, was ich tue, jedes Gespräch, jeder Ausdruck von Kreativität, Liebe oder Freundschaft aufgezeichnet wird.

Das ist nichts, was ich bereit bin zu unterstützen.
Das ist nichts, das ich bereit bin mit aufzubauen.
Das ist nichts, unter dem ich zu leben bereit bin.
Ich denke, jeder, der eine solche Welt ablehnt, hat die Verpflichtung, im Rahmen seiner Möglichkeiten zu handeln.“

- Edward Snowden

Was ist eine CryptoParty?

- Workshop zur digitalen Selbstverteidigung
  - "Tupperware-Party zum Lernen von Kryptographie" (Cory Doctorow)
- Einsteigerfreundlich
- Öffentlich & unkommerziell
- Fokus auf Freier Software
- Von Anwendern für Anwender -> Gelerntes weitertragen

Agenda

- Inputvortrag zu:
  - Sichere Passwörter
  - Verschlüsselung von E-Mails (PGP)
  - Tracking beim Browsen vermeiden
  - Dateiverschlüsselung (VeraCrypt)
  - Verschlüsselung von Chats (Pidgin-OTR)
- Praxis

Sichere Passwörter

Wie werden Passwörter geknackt?

- Brute Force
  - Alle möglichen Kombinationen ausprobieren
- Listen / Wörterbuch-Angriffe
  - Alle Wörter einer Liste ausprobieren
- Social Engineering
  - Phishing, Person austricksen um PW zu erfahren

Wie erschwert man das Knacken des Passworts?

- Brute Force

  => Länge (10+ Zeichen)

  => Verschiedene Zeichentypen

  (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)

Wie erschwert man das Knacken des Passworts?

- Brute Force

  => Länge (10+ Zeichen)

  => Verschiedene Zeichentypen

  (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)

- Listen / Wörterbuch-Angriffe

  => Kein einzelnes Wort als PW verwenden

  => Keine Wörter aus dem Umfeld (Namen, Geburtsdaten)

Wie erschwert man das Knacken des Passworts?

- Brute Force

  => Länge (10+ Zeichen)

  => Verschiedene Zeichentypen

  (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)

- Listen / Wörterbuch-Angriffe

  => Kein einzelnes Wort als PW verwenden

  => Keine Wörter aus dem Umfeld (Namen, Geburtsdaten)

- Social Engineering

  => Niemandem das Passwort verraten!

Brute-Force-Angriffe und Passwortlänge

Nutzung von Kleinbuchstaben (26 Zeichen)

Zeichen	Kombinationen	Sekunden	Stunden	Jahre
1	26			
2	676			
3	17576			
4	456976			
5	11881376			
6	308915776	0.14		
7	8031810176	3.83		
8	208827064576	100		
9	5429503678976	2590		
10	141167095653376	67344	18.71	
11	3670344486987776	1750948	486.37	
12	95428956661682180	45524643	12645.73	1.44
13	2481152873203736600	1183640714	328789.09	37.53
14	64509974703297150000	30774658570	8548516.27	975.86
15	$1.67725934228572 6 \times 10^{21}$	800141122825	222261423.01	25372.31

Quelle: http://www.1pw.de/brute-force.html (Rechengeschwindigkeit: 2096204400 Schlüssel pro Sekunde (Keys/sec))

Brute-Force-Angriffe und Passwortlänge

Nutzung von Groß-, Kleinbuchstaben und Zahlen (62 Zeichen)

Zeichen	Kombinationen	Sekunden	Stunden	Jahre
1	62			
2	3844			
3	238328			
4	14776336			
5	916132832			
6	56800235584	27		
7	3521614606208	1680		
8	218340105584896	104160	28.93	
9	13537086546263552	6457904	1793.86	
10	839299365868340200	400390041	111219.46	12.70
11	52036560683837100000	24824182548	6895606.26	787.17
12	$3.2262667623979 \times 10^{21}$	1539099317985	427527588.33	48804.52
13	$2.000285392686698 \times 10^{23}$	95424157715092	26506710476.41	3025880.19
14	$1.2401769434657528 \times 10^{25}$	5916297778335704	1643416049537.70	187604571.87
15	$7.689097049487666 \times 10^{26}$	3668104622568136 30	101891795071337.12	11631483455.63

Quelle: http://www.1pw.de/brute-force.html (Rechengeschwindigkeit: 2096204400 Schlüssel pro Sekunde (Keys/sec))

Wie erstelle ich ein sicheres Passwort?

- DbiR&DSd90M!
  - Merksatz: »**D**er **B**all **i**st **R**und **&** **d**as **S**piel **d**auert **90** **M**inuten**!**«
- HausLocherTasteMelone
  - Wortreihung
- 2UrN47oCfK6jAZ8xuKHiop4upPsI73
  - Passwortgenerator

Passwortverwaltung

Wichtig: Für jeden Dienst ein anderes Passwort verwenden!

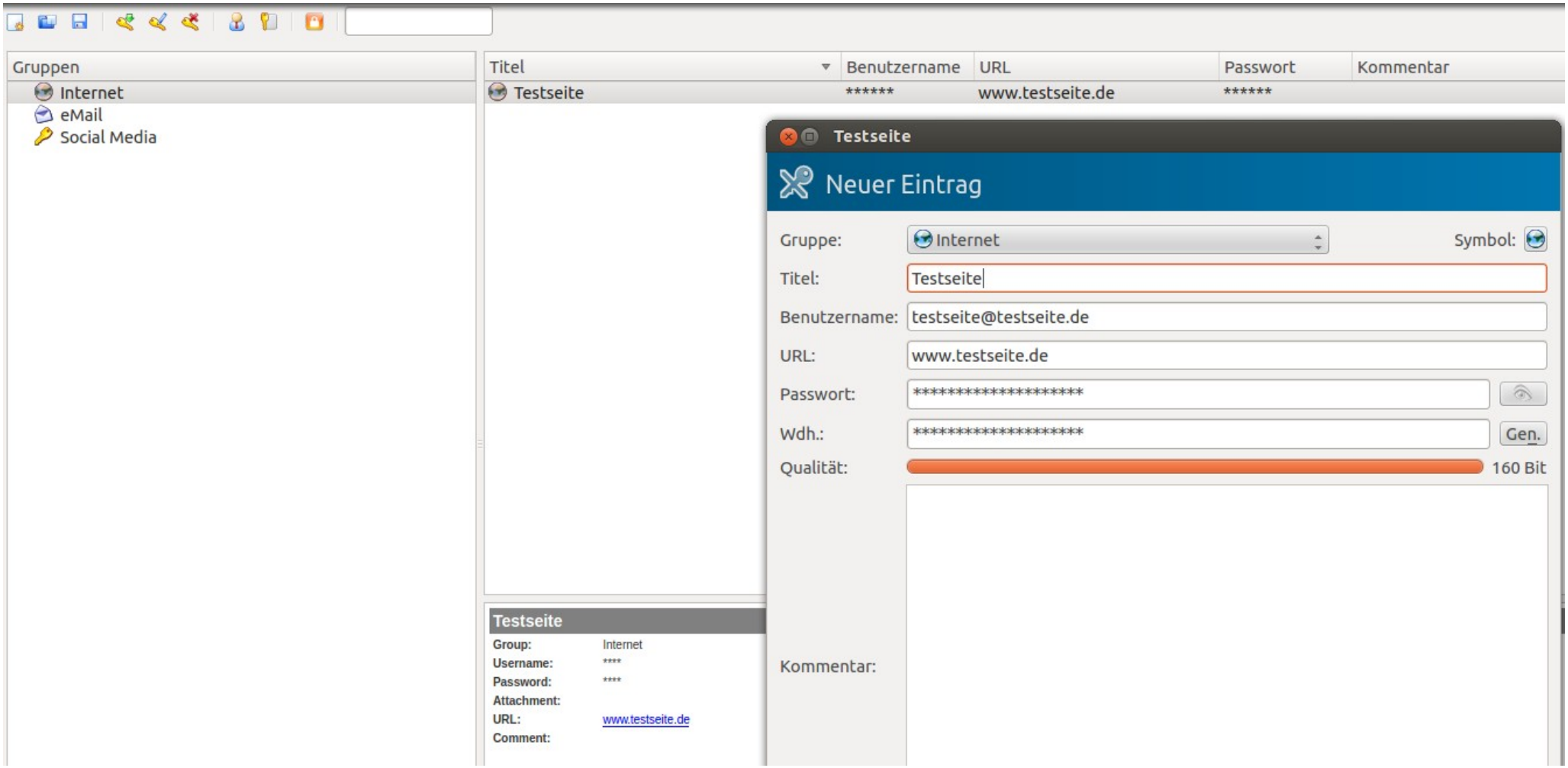
Software: **KeePass / KeePassX**

Vorteile

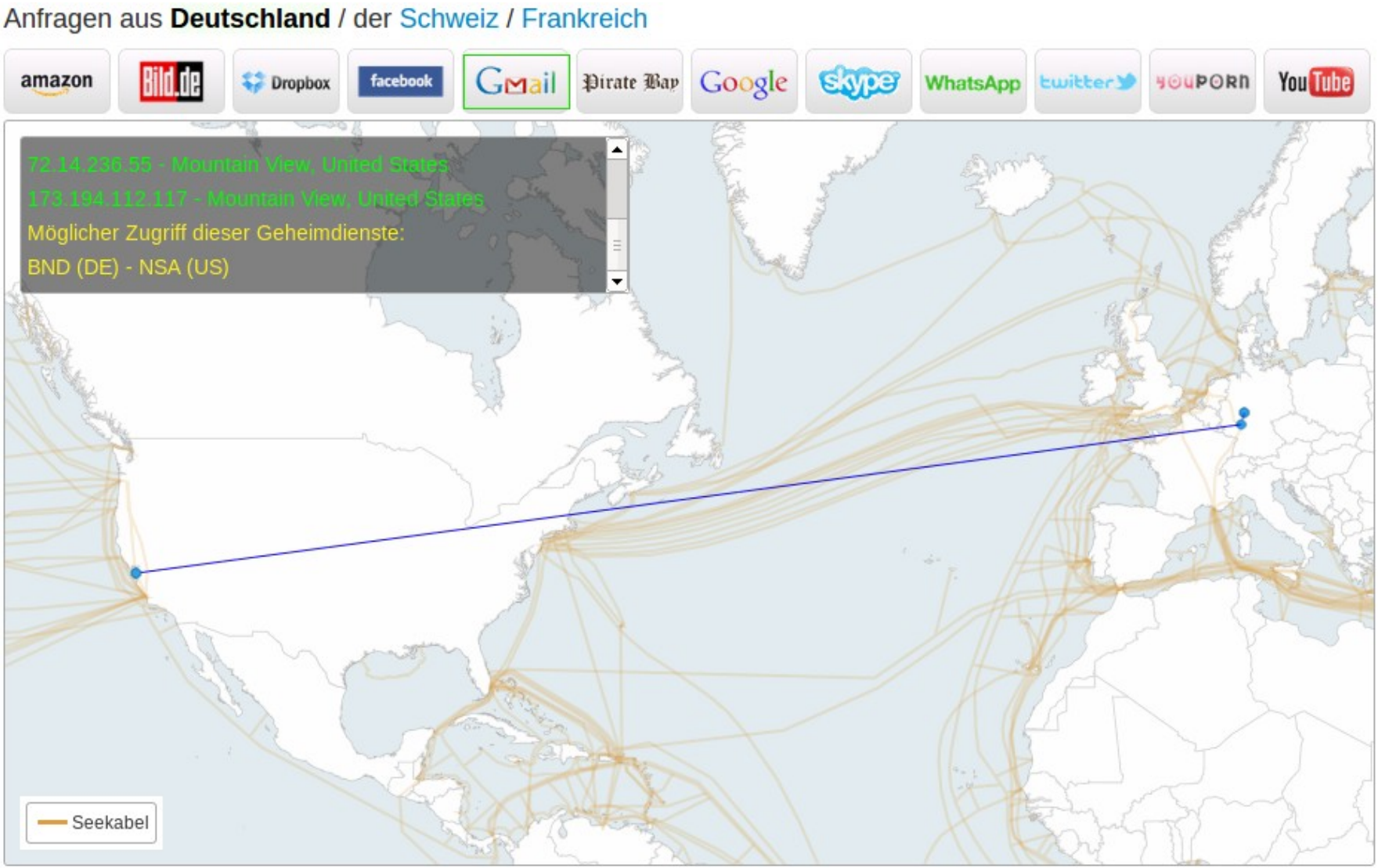
- Open Source
- Viele Plattformen
  - Win, Linux, Mac, Android
- Passwortgenerator
- Verschlüsselt gespeichert

Nachteile

- Masterpasswort
  - Darf nicht vergessen oder geknackt werden!
- Komfort
  - Kein Sync zwischen verschiedenen Geräten


Gruppen
Internet
eMail
Social Media
Titel
Benutzername
URL
Passwort
Kommentar
Testseite
******
www.testseite.de
******
Testseite
Neuer Eintrag
Gruppe:
Internet
Symbol:
Titel:
Testseite
Benutzername:
testseite@testseite.de
URL:
www.testseite.de
Passwort:
Wdh.:
Gen.
Qualität:
160 Bit
Kommentar:
Testseite
Group:
Internet
Username:
****
Password:
****
Attachment:
URL:
www.testseite.de
Comment:

E-Mail Anbieter



Quelle: http://apps.opendatacity.de/prism/de

Alternativen zu "kostenlosen" E-Mail-Anbietern

- **Posteo.de** oder **mailbox.org**
- Gratis 24h-Einmal-E-Mail-Adresse: anonbox.net (CA-Cert)

Vorteile

- Standort in Deutschland
- Datensparsamkeit
- Keine Inhaltsanalyse
- Keine Werbung
- Anonyme Nutzung möglich
- Datenschutz hat Priorität

Nachteile

- Kostet 1,- € pro Monat

E-Mail Verschlüsselung (PGP)

Vorteile

- Inhalt Ende-zu-Ende verschlüsselt
- Sender & Empfänger sind eindeutig

Nachteile

- Metadaten unverschlüsselt
- Sender & Empfänger müssen PGP nutzen

Benötigte Software:

- E-Mail Programm: Thunderbird
- Add-on: Enigmail

Unterschied Symmetrische / Asymmetrische Verschlüsselung

- Symmetrische Verschlüsselung (secret key)
  - Wie analoge Schlüssel
  - Ein Schlüssel zum ver- und entschlüsseln
  - Alle Teilnehmer brauchen den Schlüssel

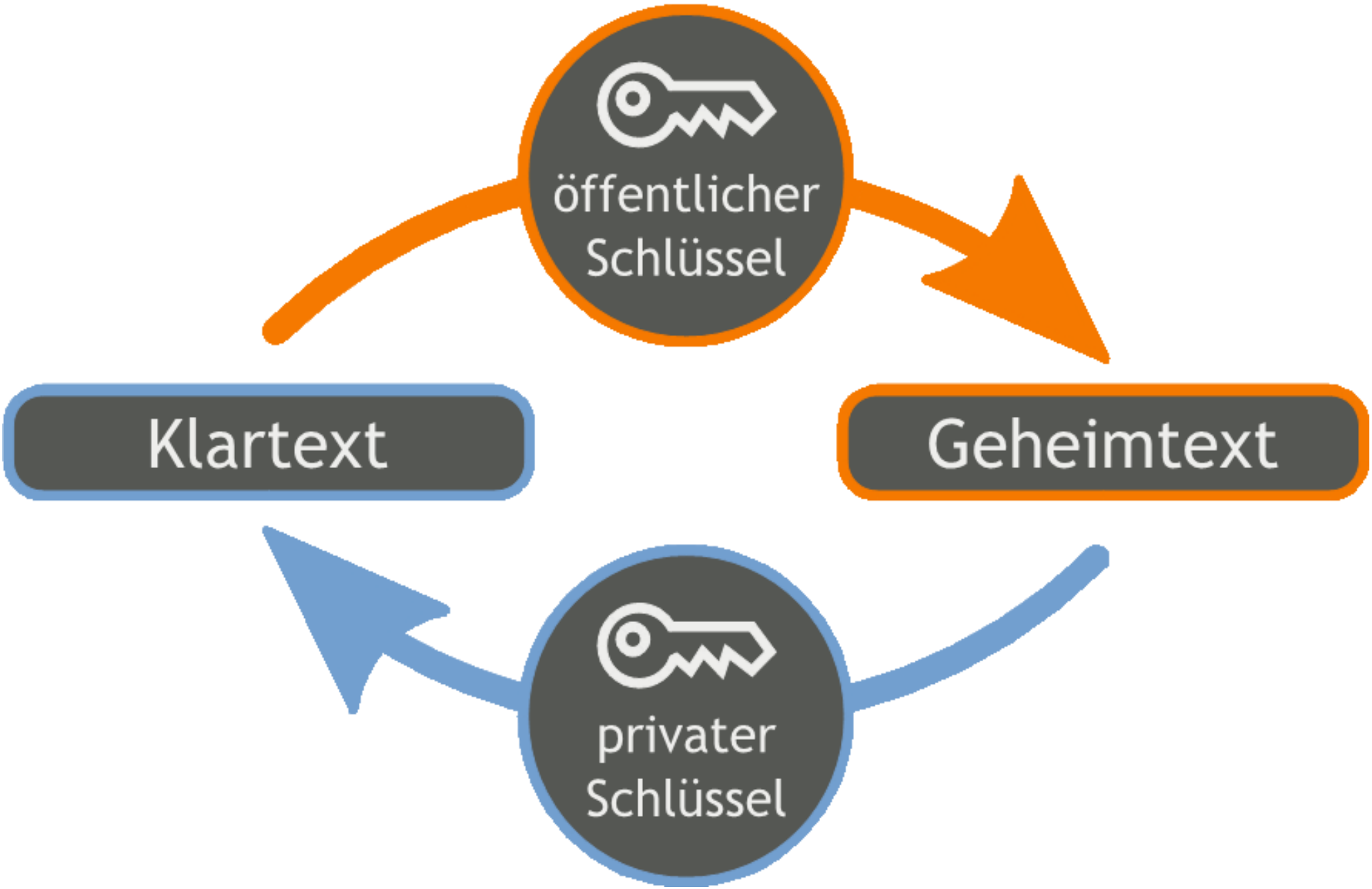
- Asymmetrische Verschlüsselung (public key)
  - Schlüsselpaar

Wie funktioniert PGP (Pretty Good Privacy)?

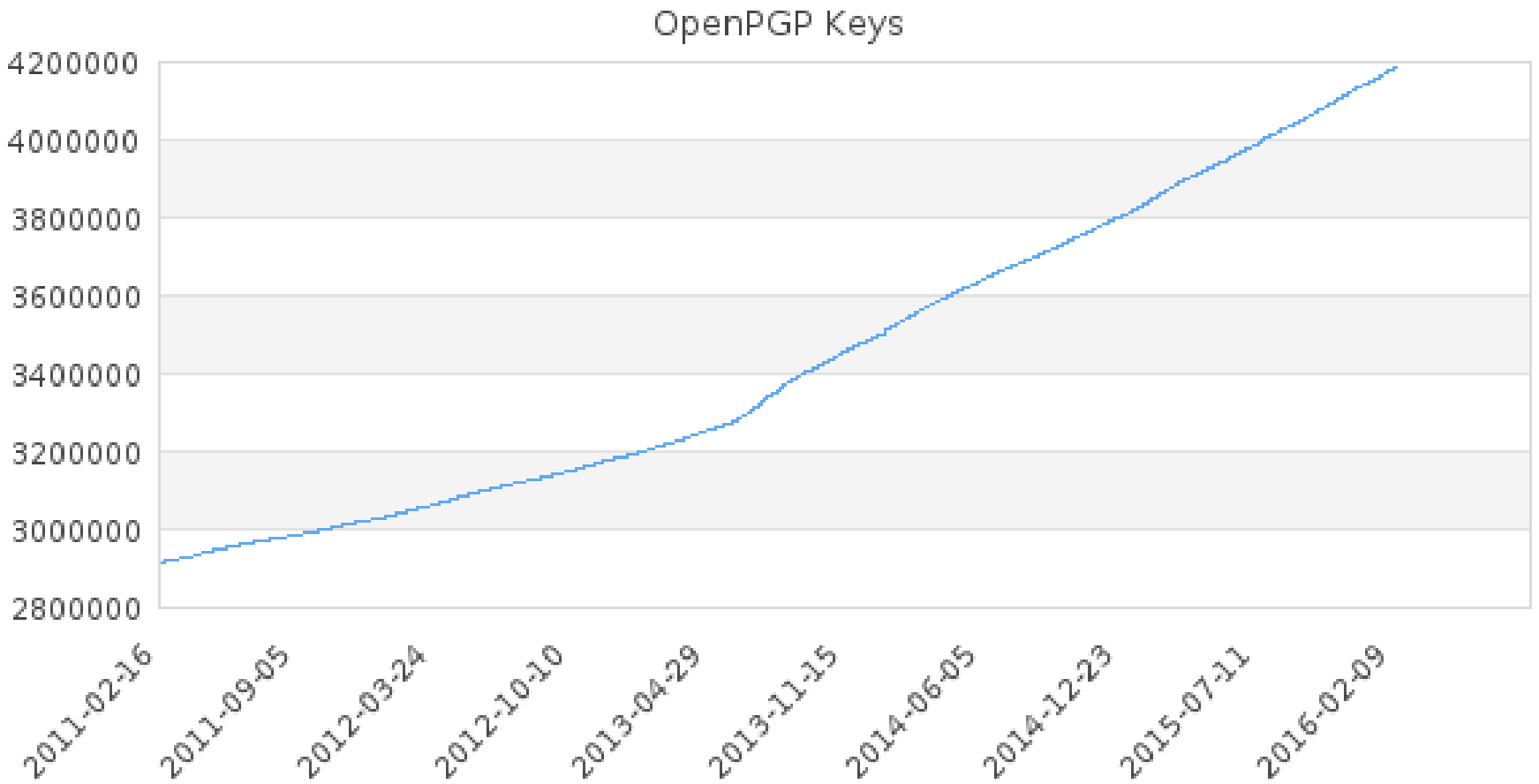
- Asymmetrische Verschlüsselung
- Schlüsselpaar: **privater** und **öffentlicher** Schlüssel.

- Öffentlicher Schlüssel:
  - verschlüsselt die E-Mail
  - gibst du deinen Kommunikationspartnern

- Privater Schlüssel:
  - entschlüsselt die E-Mail
  - bleibt privat, gibst du niemals raus!

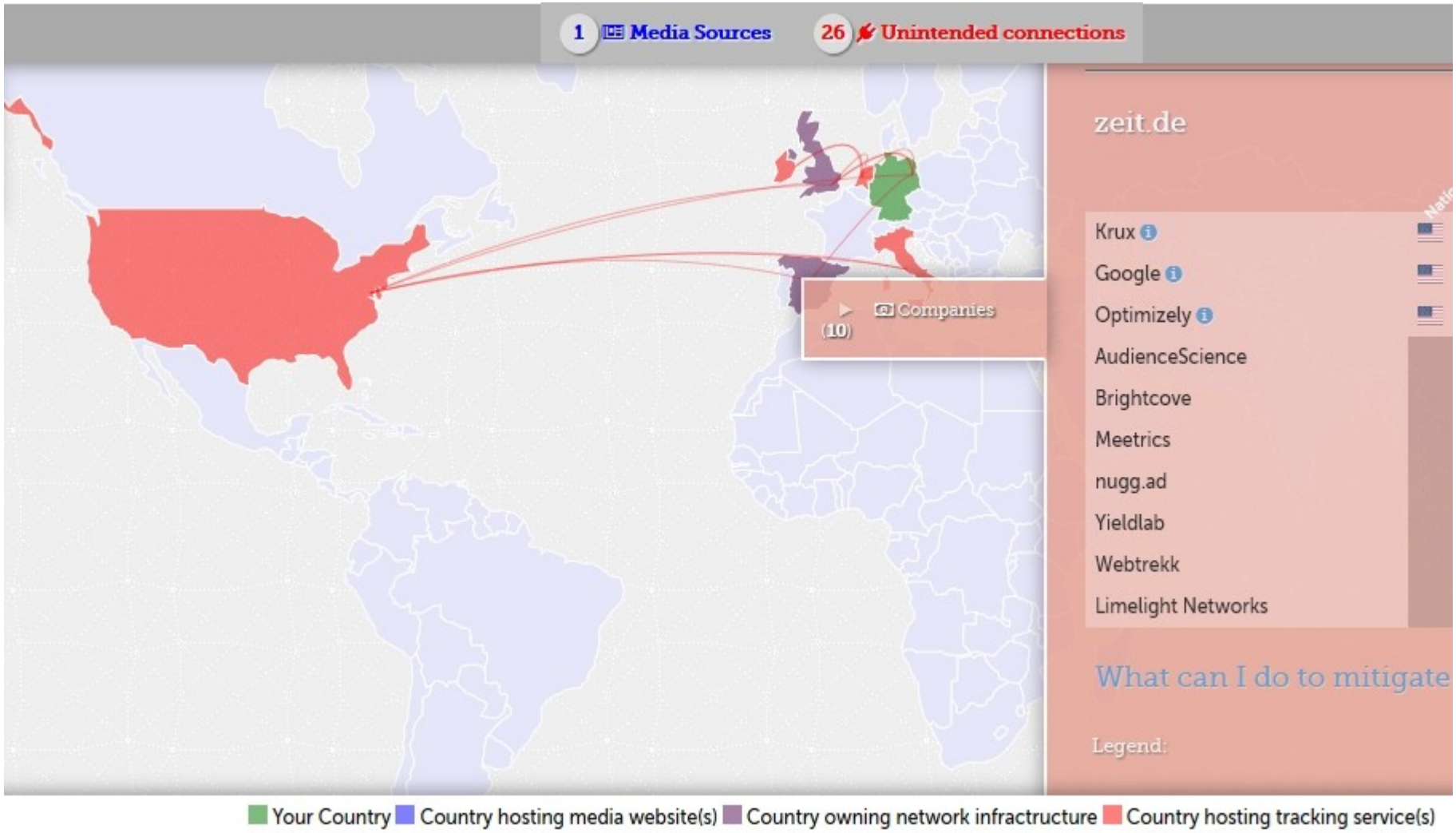

öffentlicher Schlüssel
Klartext
Geheimtext
privater Schlüssel

Verbreitung von PGP



Quelle: https://sks-keyservers.net/status/key_development.php

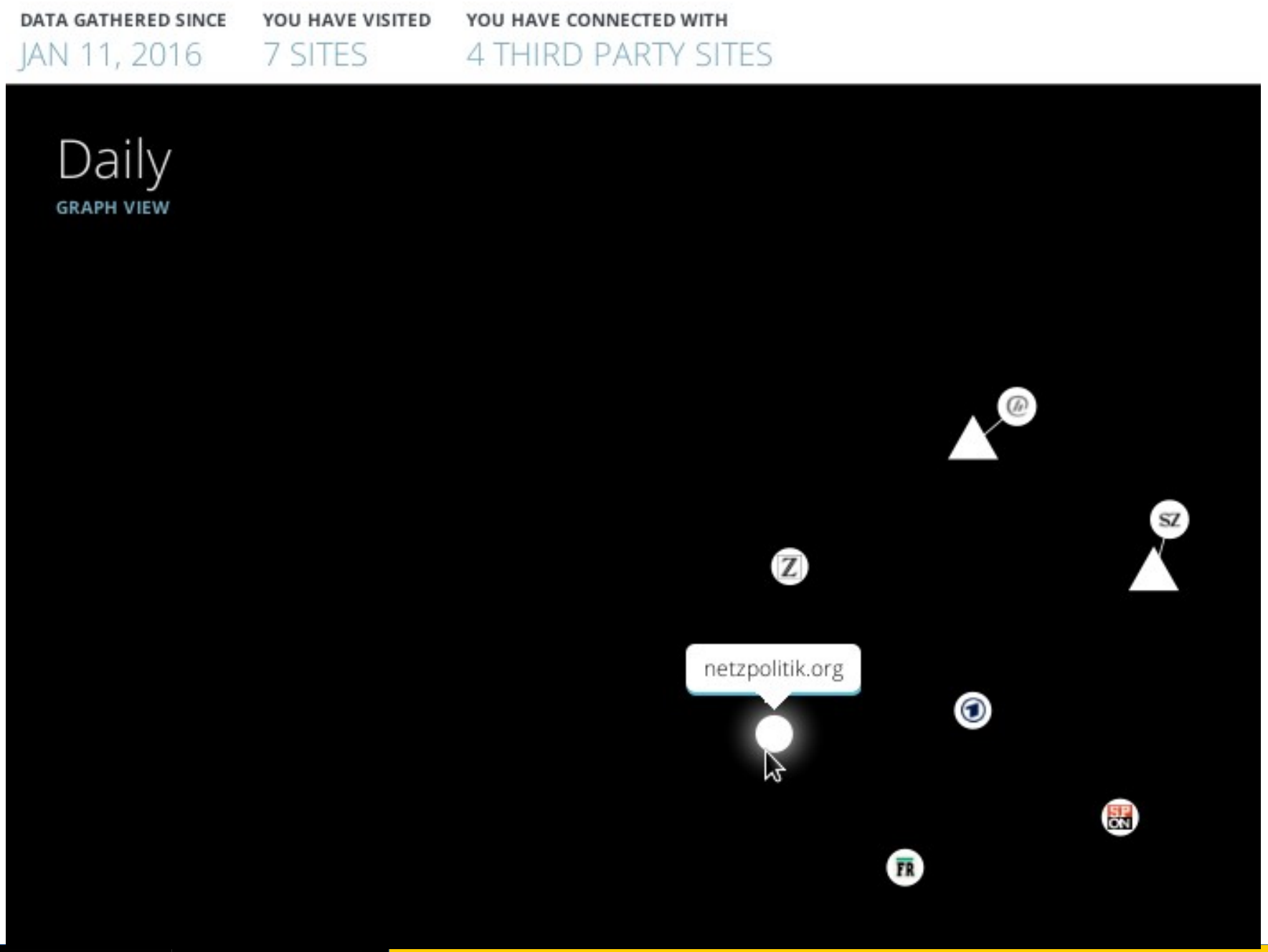
Tracking beim Browsen vermeiden



Quelle: https://trackography.org/

Analyse mit Firefox-Addon Lightbeam

Analyse mit Firefox-Addon Lightbeam



Wie kann ein Webserver mich identifizieren und verfolgen (Tracking)?

- Cookies:
  - kleine Textdateien, die die aufgerufene Webseite im Browser speichern und wieder abrufen kann.
- Passive Merkmale:
  - IP-Adresse, Sprache, Browser, Betriebssystem
- Aktive Merkmale (Javascript, Flash, Java, h264, ...)
  - Schriftarten, Browser-Add-ons, Bildschirmauflösung, uvm.

=> Eindeutiger Browser-Fingerabdruck

- siehe https://panopticlick.eff.org/

Wie kann ich mich vor Tracking schützen?

- Browser-Wahl
  - Firefox, Chromium (https://download-chromium.appspot.com)
- Browser-Einstellungen
  - Do-not-Track Option
  - Benutzerdefinierte Chronik:
    Cookies (für Drittanbieter) deaktivieren
- Suchmaschinen
  - Ixquick.com, Startpage.com, DuckDuckGo.com, MetaGer.de, etc.
    (im Gegensatz zu Google auch keine individuellen Ergebnisse)
- Browser-Add-ons! ...

Schutz durch Firefox-Add-ons

- Tracker und Werbung blocken: **uBlock origin**
- Aktive Inhalte blocken: **NoScript**
  - Skripte allgemein erlauben (nicht empfohlen)
- Webseiten immer verschlüsseln: **HTTPS Everywhere**
- Flash-Cookies löschen: **BetterPrivacy-signed**

Etwas komplizierter und aufwendiger:

- Alle Skripte blocken: **NoScript**
- Anfragen an Drittanbieter blocken: **RequestPolicy**
- Referer blocken: **RefControl** (Vorsicht!)

TOR (The Onion Router)

Was ist TOR?

- Netzwerk zur Anonymisierung von Verbindungsdaten
- IP-Adresse wird verschleiert

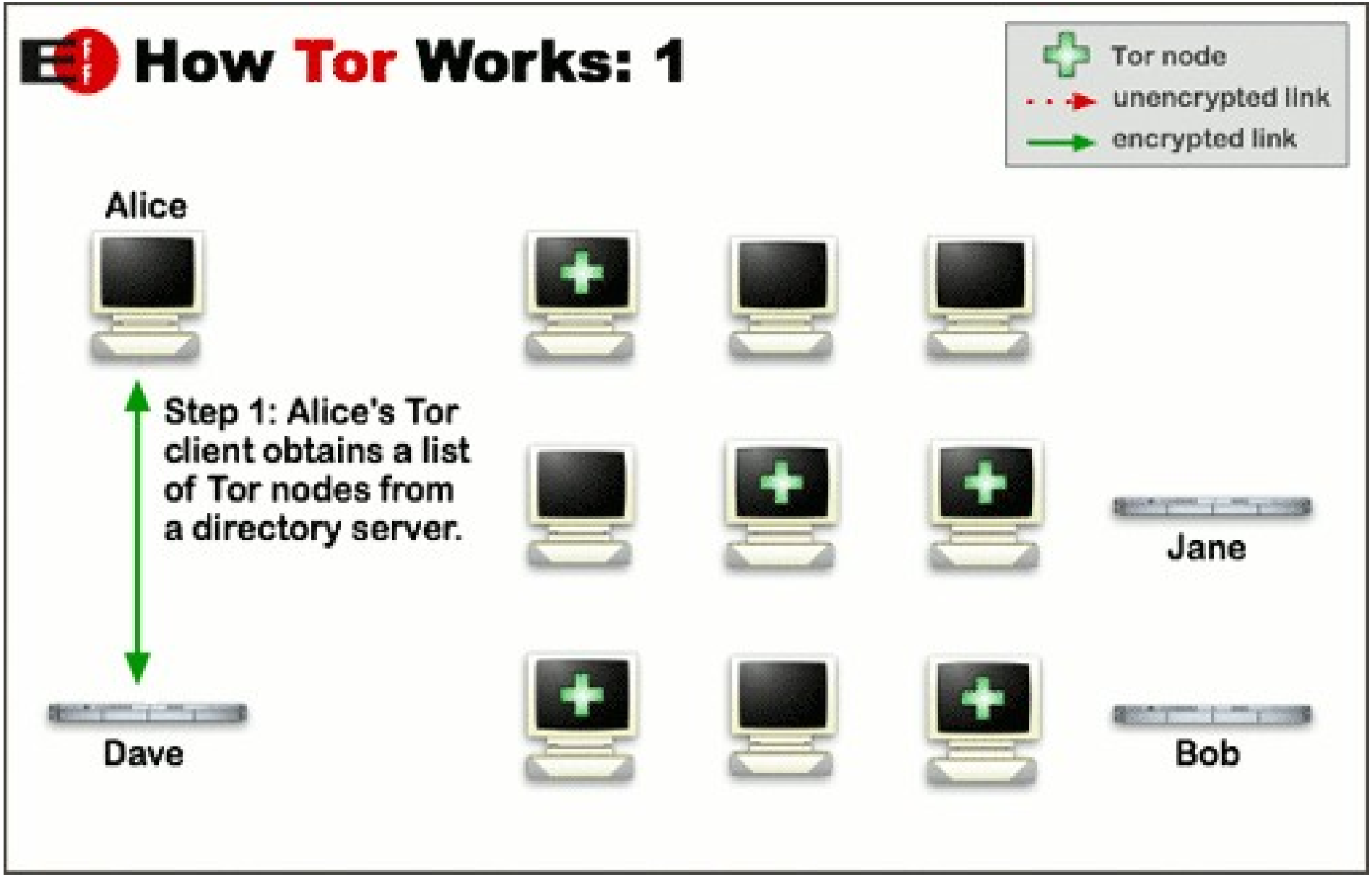
Vorteile

- Anonymes Surfen

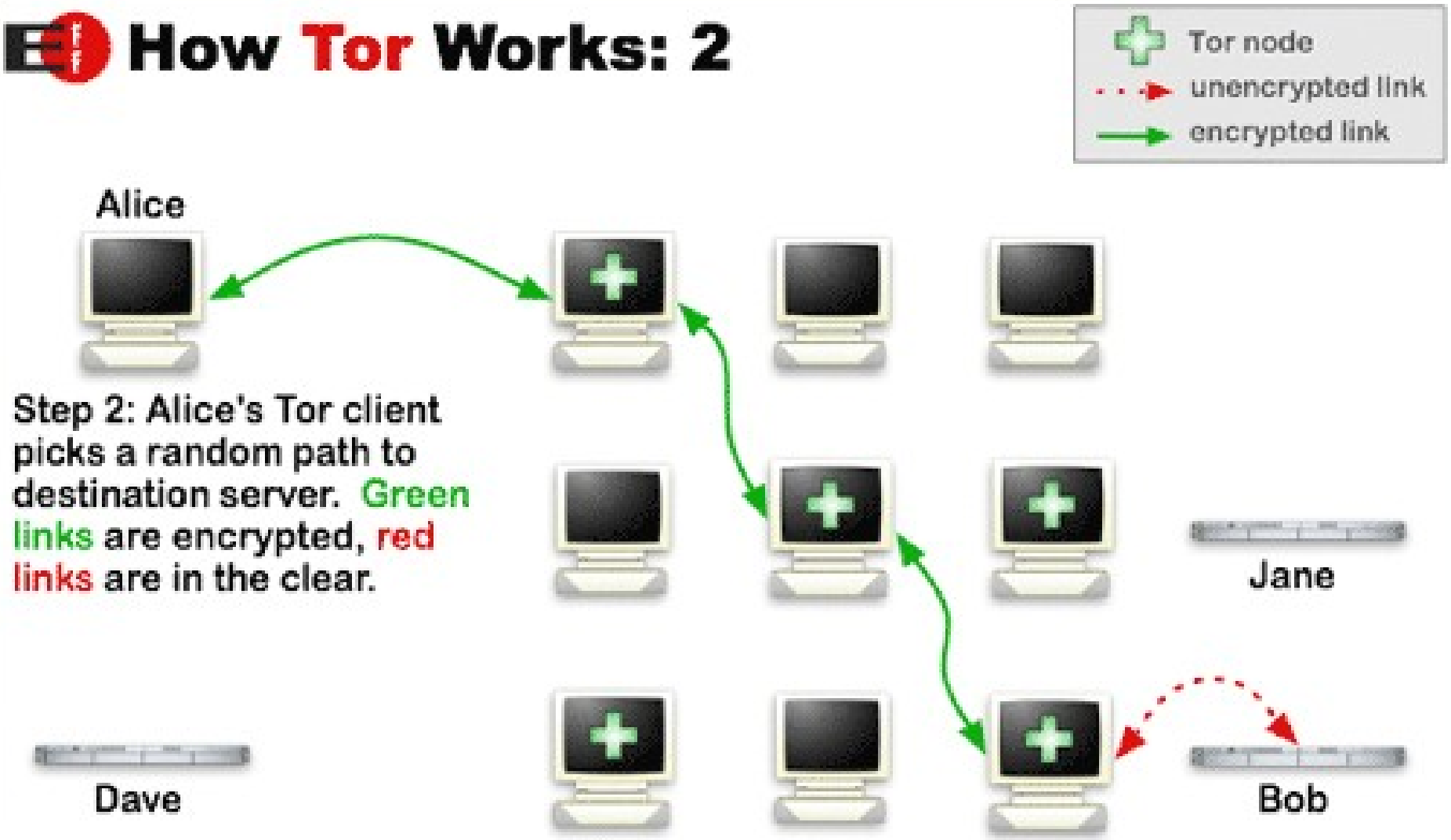
Nachteile

- Langsam
- Login bei personalisierten Seiten nicht sinnvoll

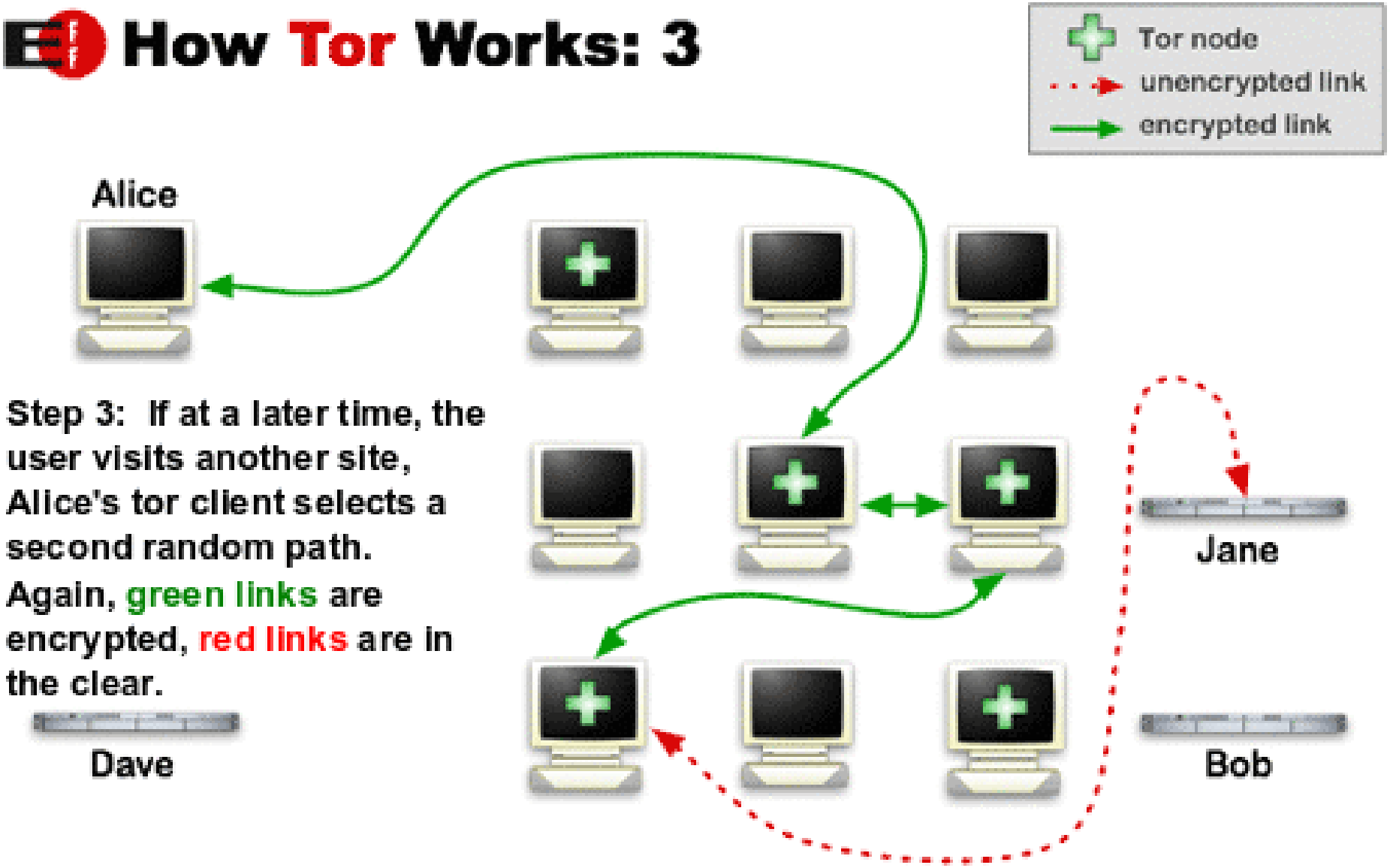
How Tor Works: 1



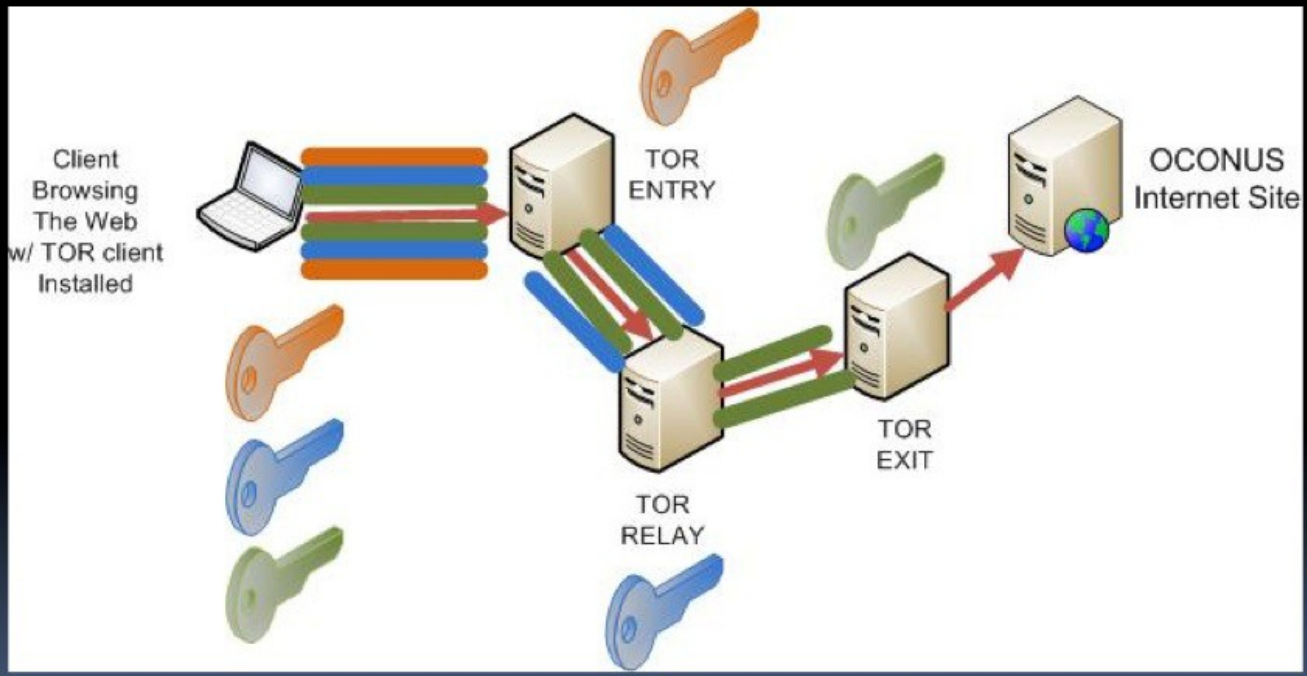
How Tor Works: 2



How Tor Works: 3



(U) What is TOR?


Client
Browsing
The Web
w/ TOR client
Installed
TOR
ENTRY
TOR
RELAY
TOR
EXIT
OCONUS
Internet Site

Dateiverschlüsselung

Software: VeraCrypt

- Weiterentwicklung von TrueCrypt
- Software zur Datenverschlüsselung

Was kann ich mit VeraCrypt machen?

- Verschlüsselte Container (Ordner) erstellen
- Komplette Festplatte verschlüsseln
- USB-Sticks und andere Wechseldatenträger verschlüsseln

VeraCrypt

Vorteile

- Plattformübergreifend
  - Win, Mac, Linux
- Quelloffen, freie Software
- Kompatibel mit alten TrueCrypt-Containern

Nachteile

- Komfort
- Passwort vergessen?
  => Daten weg!

Verschlüsselung von Chats

Software: Pidgin

- Chatprogramm
- Beherrscht alle gängigen Chat-Protokolle
  - ICQ, MSN, Facebook-Chat, Jabber

Plugin: OTR (Off-The-Record)

- Chat wird verschleiert
- Kommunikationspartner sind eindeutig

Chatdienst

Jabber

- Dezentraler Service
  - Jeder kann einen Jabber-Server betreiben
- Quelloffenes XMPP-Protokoll
- Gruppenchats möglich

Neue Alternative

Tor Messenger (Beta)

- Verschlüsselt und anonym

Weitere Projekte I

- **Prism-break.org:** (https://prism-break.org/de/all/)
  Liste datenschutzfreundlicher Software und Anbieter, z.B.:
  - *Startpage* und *DuckDuckGo* statt Google-Suche
  - *OpenStreetMap* statt Google Maps
  - *Dudle* statt doodle
  - *EtherCalc* und *EtherPad* statt Google Docs
  - *Diaspora** statt facebook oder Google+
  - ...
- **DigitalCourage: Digitale Selbstverteidigung**

  (https://digitalcourage.de/digitale-selbstverteidigung)

Weitere Projekte II

- **freifunk**: freie, eigene Internet-Infrastruktur mit offenen WLANs (auch in Braunschweig)
- **Tails** (The amnesic incognito live system): Anonyme Live-DVD

Noch in Entwicklung:

- **p≡p** (Pretty Easy Privacy): Einfach zu bedienende E-Mail- und Chat-Verschlüsselung (PGP kompatibel) für Outlook, Thunderbird, WhatsApp, Facebook und Jabber, auf iOS-, Android-, Windows- und GNU/Linux-Geräten

Kontakt & Termine

E-Mail: digitalcourage.hsg@uni-bielefeld.de
Homepage: https://hsg.digitalcourage.de

Treffen der Hochschulgruppe:
Erster und dritter Montag des Monats im SozCafé (X-C2-116), 18 Uhr.

Linux Install Party:
2. Juni (Do), 18 Uhr in U2-205

Es liegt außerdem eine Liste aus, auf der man sich in unseren Newsletter eintragen kann.