vmann & sid

Inhalt

Anmerkung

Alles ist sehr sehr Basic und vereinfacht dargestellt, zum leichteren Verständnis.
Im Anschluss helfen wir euch beim Installieren und Benutzen.

Was ist Verschlüsselung und warum sollte man verschlüsseln?

Verschlüsselung 101:

- für alle lesbaren Text so umwandeln, dass er nicht mehr lesbar ist, wenn man keine Berechtigung dazu hat

Warum verschlüsseln?

- Allgemein: mensch möchte nicht, dass alle wissen was es tut
- Hier konkret: Repression umgehen, andere Menschen schützen

Beispiele, warum es sinnvoll ist zu verschlüsseln

Beispiel 1: Hausdurchsuchung
Bei euch gibt es eine Hausdurchsuchung. Durch Verschlüsselung eurer Festplatten verhindert ihr, dass ihr Repression durch die Informationen, die auf eurer Festplatte sind, erhaltet.

Beispiel 2: Abhören
Ihr plant eine Aktion. Durch Kommunikation durch verschlüsselte Wege macht ihr es schwerer abgehört zu werden und eure Aktion bleibt so nur unter euch.

Schützt eure Mitmenschen durch Verschlüsselung!

Was macht gute Verschlüsselung aus?

- Offen: Alle können nachlesen, wie die Verschlüsselung funktioniert und die Sicherheit liegt nur im Schlüssel
- Aktuelle Kryptographie: Die mathematische Methode, wie es verschlüsselt wird ist von vielen **unabhängigen** Mathemenschen bewiesen worden

Sinnvoll zu haben:

- Ende-zu-Ende: Es sind nicht nur Teile verschlüsselt, sondern alles
- Glaubhafte Abstreitbarkeit: Mensch kann glaubhaft abstreiten, dass es bei etwas involviert war
- Perfect forward secrecy: Auch in Zukunft kann man nicht mehr die Verschlüsselten Sachen entschlüsseln

Messenger-Vergleich

messanger-vergleich tabelle: open source, crypto e2e/deniability/pfs, open infrastructure, desktop client
messanger: whatsapp, facebook, threema, telegram, signal, wire, conversations/gajim, briar, deltachat/email

Verschlüsselung von Geräten

Problem: Je nach Gerät anders :(

- Aber: Prinzip ist gleich
- Mensch nutzt ein Programm, dass das Gerät verschlüsselt
- Nur welches Programm?

Aktuelle Programme zur Festplattenverschlüsselung

System	Programm	Anmerkung
Windows	Veracrypt*	muss extra installiert werden
Mac	FireVault	nicht offenes Verfahren!
Linux	LUKS	
Android	Device Encryption	
iOS	Device Encryption	
Festplatte (ext)	Veracrypt*	muss extra installiert werden

*`https://www.veracrypt.fr`

Verschlüsselung von E-Mails

Wer benutzt denn noch E-Mails?

Verschlüsselung von E-Mails

Wer benutzt denn noch E-Mails?

Allgemeines zu E-Mails:

- benutzt Alternativen zu "kostenlosen" E-Mail-Anbietern
- gute Beispiele: `riseup.net`, `systemli.org`, ...
- schlechte Beispiele: `gmail.com`, `hotmail.com`, ...

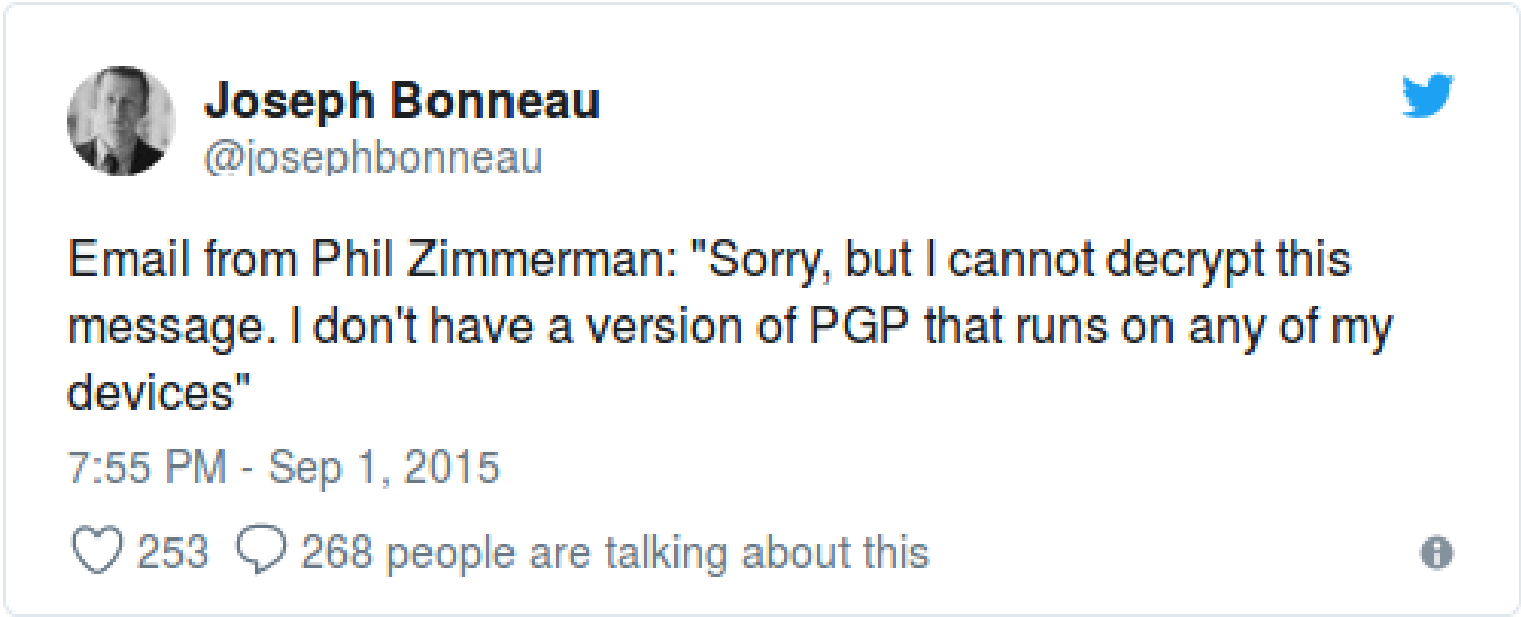
Verschlüsselung von E-Mails

Wer benutzt denn noch E-Mails?

Allgemeines zu E-Mails:

- benutzt Alternativen zu "kostenlosen" E-Mail-Anbietern
- gute Beispiele: `riseup.net`, `systemli.org`, ...
- schlechte Beispiele: `gmail.com`, `hotmail.com`, ...

E-Mail-Verschlüsselung mit PGP kurzgesagt:



Autocrypt

Soll PGP einfach machen.
Wie funktioniert PGP nochmal?

- PGP ist asymmetrische Veschlüsselung
- das heißt es wird ein geheimer und ein öffentlicher Schlüssel von einem Programm generiert (Mathemagic)
- der öffentliche Schlüssel wird weitergegeben an alle
- der private Schlüssel wird bei sich selbst geheim gehalten
- Menschen die an dich verschlüsselt eine E-Mail schicken wollen, verschlüsseln diese mit dem öffentlichen Schlüssel
- du kannst diese verschlüsselte Nachricht dann entschlüsseln mithilfe deines privaten Schlüssels

Klingt kompliziert?

Autocrypt hilft

Autocrypt (`https://autocrypt.org/`) ist ein Standard, der Menschen PGP einfacher macht, indem es die Programme automatisch von Beginn an alles mit PGP verschlüsseln lässt.

Welche E-Mail-Programme unterstützen das gerade?

- Deltachat (App)
- K9-Mail (App)
- Enigmail (Thunderbird Plugin)

Und wie benutze ich das nun?

- Lade das Programm herunter und richte dein E-Mail-Konto darin ein. Fertig. Jetzt werden alle E-Mails von und zu Menschen die auch Autocrypt verwenden mit PGP verschlüsselt.

Anonymität & Sicherheit im Internet

Ist an sich keine Verschlüsselung, sondern wie man sich anonym im Internet verhält.

Was ist Anonymität?

- Mensch ist anonym, wenn es nicht identifiziert werden kann

Warum ist das wichtig?

- Es ist sehr einfach verfolgt zu werden, während man im Internet ist.
- Antirepression

Ich meine es ernst, es ist sehr sehr einfach!

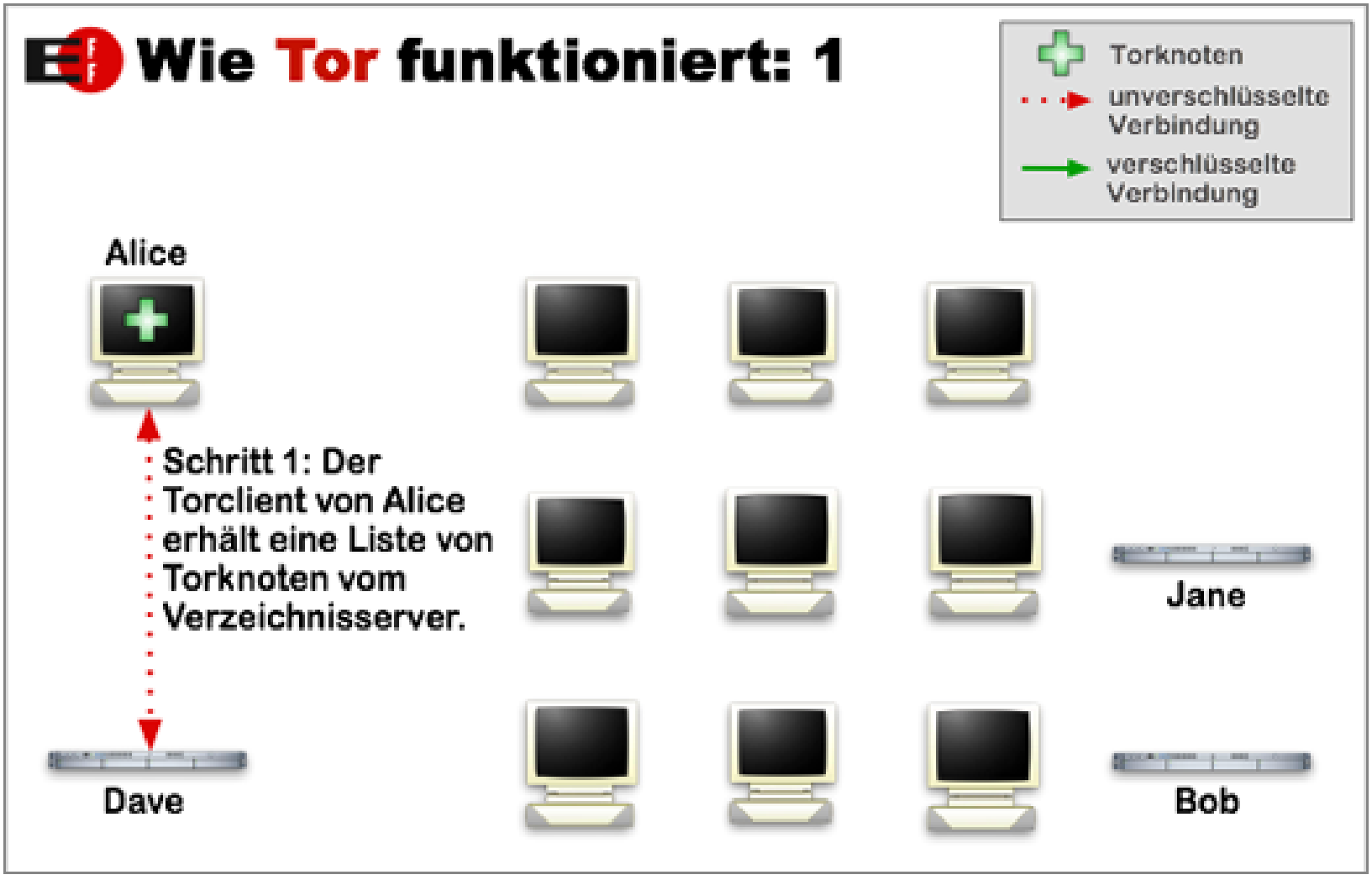
Anonymes Browsen mit TOR

Was ist TOR?

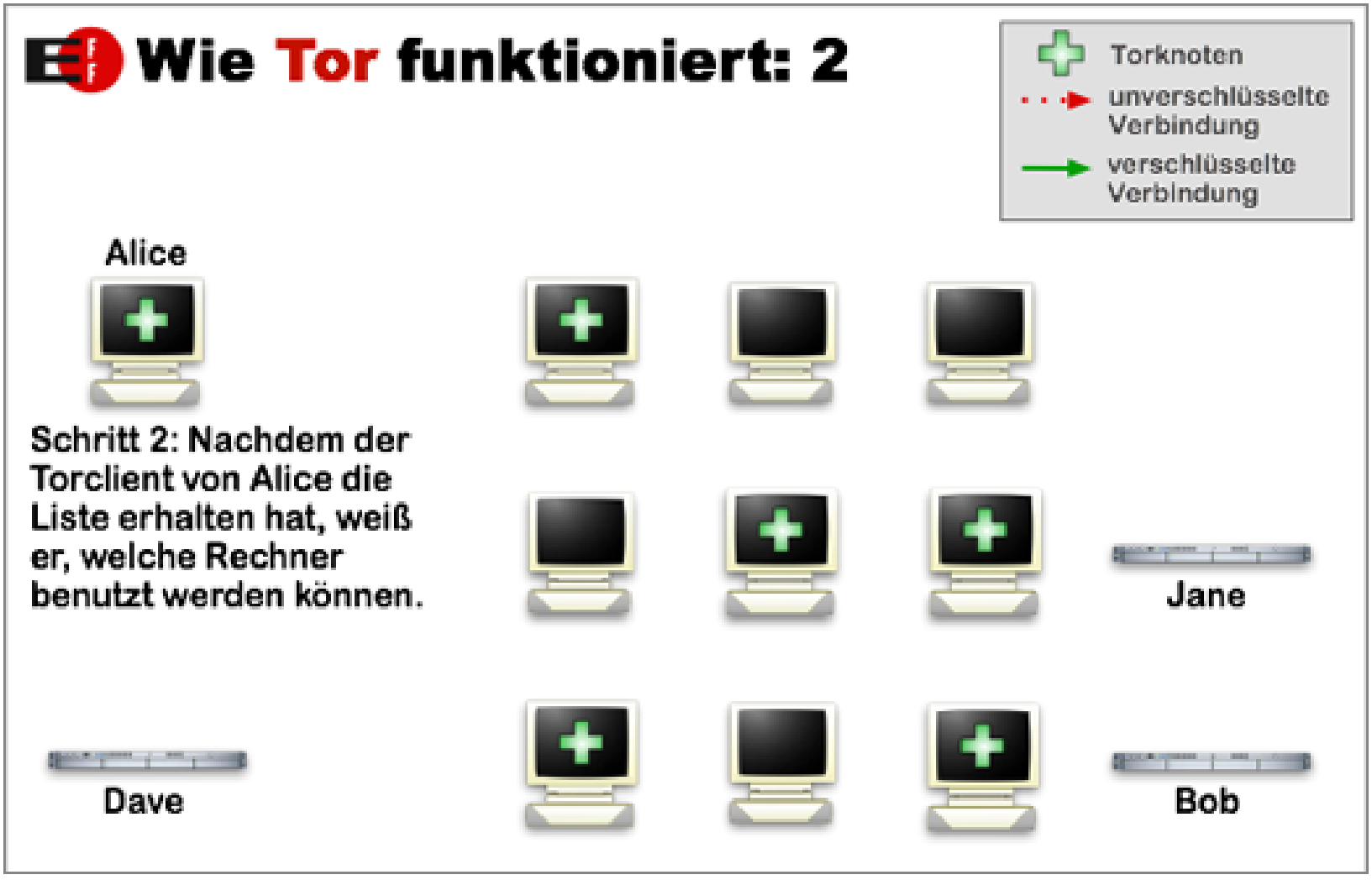
- kurz für The Onion Router
- ein Browser (wie Firefox/Chrome/...) der euch hilft anonym zu sein
- (außerdem gibt es Websiten, die man nur mit diesem Browser erreichen kann)
- kann man herunterladen auf `https://www.torproject.org/` und einfach starten

Wie funktioniert es?

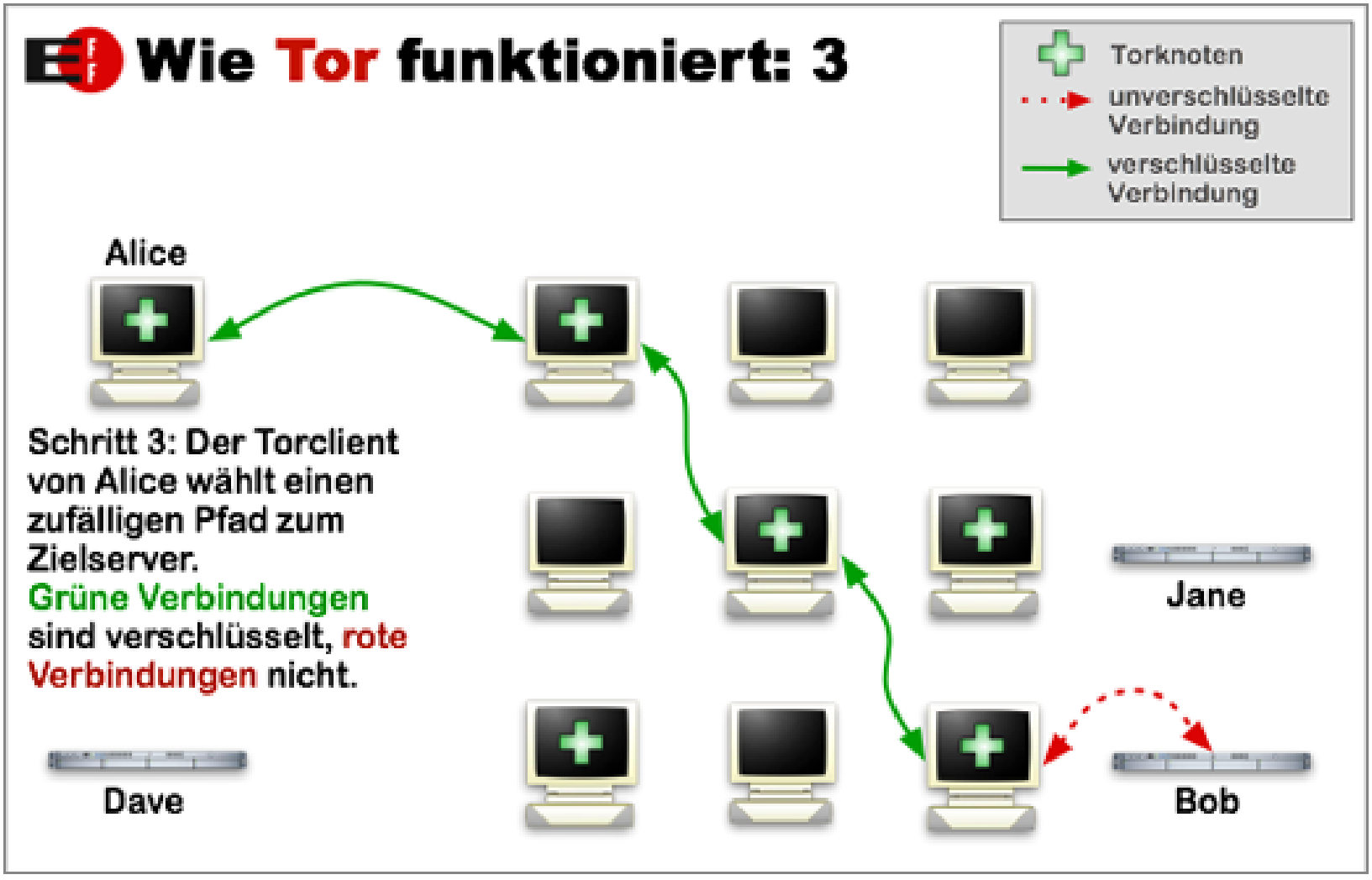
Tor - The Onion Router



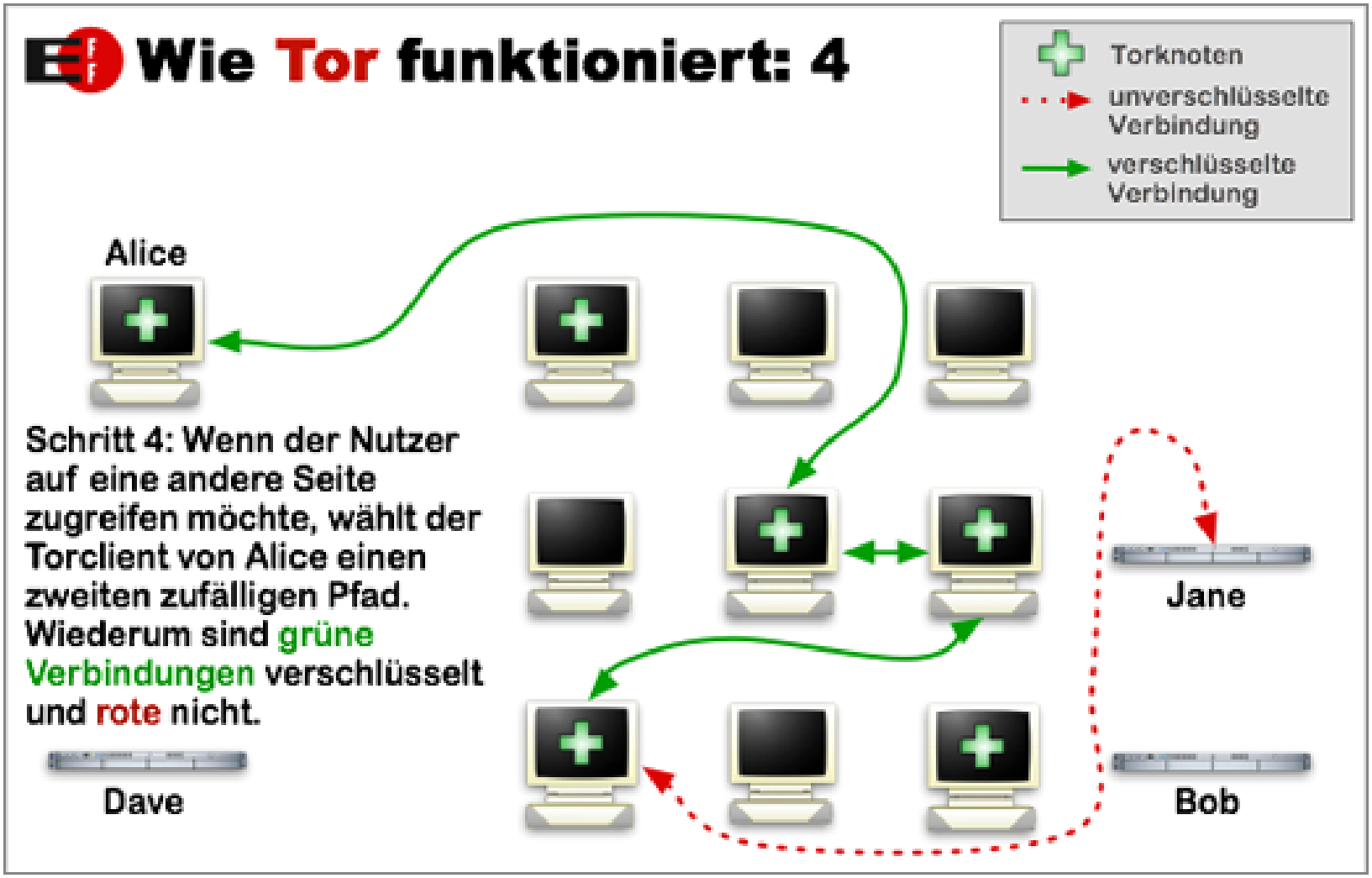
Tor - The Onion Router



Tor - The Onion Router



Tor - The Onion Router



- The Onion Router

demo: panopticlick

Tails
theamnesicincognitolivesystem

tails demo: live?

Allgemeine Umgangsformen mit Technik

Technikdingse sind neue Lebensformen mit denen mensch speziell ungehen muss, damit das Zusammenleben harmonisch stattfindet.

Softwareupdates installieren

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- Muss ich wirklich alle installieren?

Softwareupdates installieren

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- Muss ich wirklich alle installieren?
  Ja.

Softwareupdates installieren

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- Muss ich wirklich alle installieren?
  Ja.
- Wie häufig ist es, dass das System nicht mehr funktioniert nach einem Softwareupdate?

Softwareupdates installieren

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- Muss ich wirklich alle installieren?
  Ja.
- Wie häufig ist es, dass das System nicht mehr funktioniert nach einem Softwareupdate?
  Das ist nicht vorhersagbar, aber selten.

Softwareupdates installieren

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- Muss ich wirklich alle installieren?
  Ja.
- Wie häufig ist es, dass das System nicht mehr funktioniert nach einem Softwareupdate?
  Das ist nicht vorhersagbar, aber selten.
- Soll ich es trotzdem installieren?

Softwareupdates installieren

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- Muss ich wirklich alle installieren?
  Ja.
- Wie häufig ist es, dass das System nicht mehr funktioniert nach einem Softwareupdate?
  Das ist nicht vorhersagbar, aber selten.
- Soll ich es trotzdem installieren?
  Ja.

Softwareupdates installieren

Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- Muss ich wirklich alle installieren?
  Ja.
- Wie häufig ist es, dass das System nicht mehr funktioniert nach einem Softwareupdate?
  Das ist nicht vorhersagbar, aber selten.
- Soll ich es trotzdem installieren?
  Ja.
- Wieso?

Softwareupdates installieren

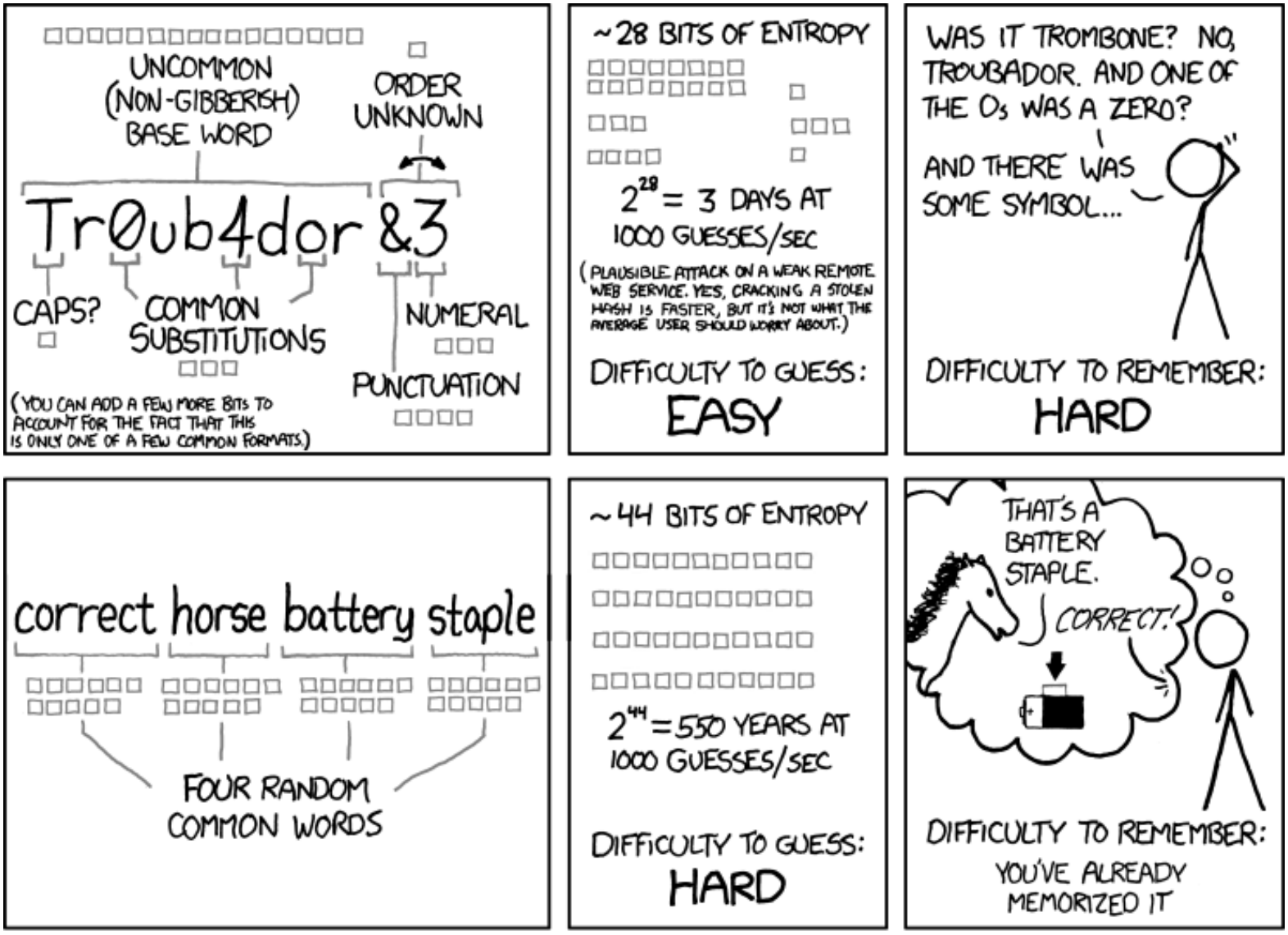
Euer System wird euch (hoffentlich) sagen, wenn es Updates gibt. Und wenn es sie gibt, installiert sie.

FAQ:

- Muss ich wirklich alle installieren?
  Ja.
- Wie häufig ist es, dass das System nicht mehr funktioniert nach einem Softwareupdate?
  Das ist nicht vorhersagbar, aber selten.
- Soll ich es trotzdem installieren?
  Ja.
- Wieso?
  Was nützt dir ein funktionierendes System mit all deinen wichtigen Dingen, wenn sie einfach dir genommen und gegen dich verwendet werden können?

Passwortlänge

- benutzt nie 2x dasselbe Passwort
- benutzt ein Passwort das länger als 20 Zeichen lang ist
- benutzt einen Passwortmanager
- wenn ihr keinen benutzen könnt, dann tut wenigstens das:



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Workshop!

Jetzt seid ihr dran!
Fragen?
Braucht ihr Hilfe bei der Installation oder beim Benutzen?

Wir sind für euch da :)

Danke fürs zuhören!