Freie Universität Berlin

Vorlesung "Anwendungssysteme"

Privatsphäre

Prof. Dr. Lutz Prechelt
Freie Universität Berlin, Institut für Informatik
http://www.inf.fu-berlin.de/inst/ag-se/

- Definition,
- Begründung, Entwicklung
- Niederschlag in Grundrechte

- Bedrohung durch Computerisierung
  - staatliche Spionage
  - Datensammeln durch Firmen
  - elektronisches Bezahlen
  - Gegenmaßnahmen

Definition "Privatsphäre" (privacy)

Freie Universität Berlin

Definitionsversuch:

- Der Bereich, in dem eine Person selbst bestimmt (oder bestimmen können sollte), wem sie wann und warum welche Information über sich selbst zugänglich macht.

- Eine einheitliche Definition gibt es nicht
  - Die Meinungen gehen sogar recht weit auseinander

Philosophische Begründung

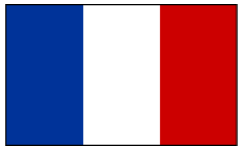
- Die Forderung, Privatsphäre zu schaffen und zu schützen, ist ein Ausfluss der Goldenen Regel

- Goldene Regel (Prinzip der Reziprozität):
  - Als deutsches Sprichwort:
    "Was Du nicht willst, dass man Dir tu,
    das füg auch keinem Andern zu."
  - Als kategorischer Imperativ (Immanuel Kant):
    "Handle so, dass die Maxime deines Willens jederzeit zugleich als Prinzip einer allgemeinen Gesetzgebung gelten könne."
    (aus: Kritik der praktischen Vernunft, 1788)
  - Im Buddhismus (6. Jh. v. Chr.):
    "Verletze nicht andere auf Wegen, die Dir selbst als verletzend erschienen." (Udana-Varga 5, 18)
  - u.s.w.

Historische Entwicklung

- Seit Aufkommen der Rechtsstaatsidee wird auch die Idee von Persönlichkeitsrechten verfolgt
  - z.B. Recht auf Leben, Recht auf körperliche Unversehrtheit

- Mit dem allmählichen Ausbau solcher Rechte ordnen sich diese zunehmend der Idee der Selbstbestimmung unter
  - Meilensteine:
    Unabhängigkeitserklärung der USA 1776,
    französische Revolution 1789



- Mit zunehmender Computerisierung erweitert sich die Idee der Selbstbestimmung auf die Kontrolle über Information über sich selbst
  - Meilenstein: "Volkszählungsurteil" des deutschen Bundesverfassungsgerichts 1983
    ("Recht auf informationelle Selbstbestimmung")

Allgemeine Erklärung der Menschenrechte

Freie Universität Berlin

United Nations (UN), 1948:

- http://de.wikisource.org/wiki/Allgemeine_Erkl%C3%A4rung_der_Menschenrechte

- Artikel 12:
  - "Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden."

- Siehe UN High Commissioner for Human Rights
  - http://www.ohchr.org

Grundrechte, die die Privatsphäre betreffen

Freie Universität Berlin

Grundgesetz der Bundesrepublik Deutschland:

- http://www.gesetze-im-internet.de/gg/

- Artikel 2 (Entfaltung d. Persönlichkeit), Abs 1:
  - Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt u. nicht gegen die verfassungsmäßige Ordnung oder d. Sittengesetz verstößt.

Auch relevant:

- Artikel 3 (Gleichberechtigung)
- Artikel 4 (Glaubens-, Gewissens- und Religionsfreiheit)
- Artikel 8 und 9 (Versammlungs-/Vereinigungsfreiheit)
- Artikel 11 (Freizügigkeit)
- Artikel 14 (Eigentum)

sowie ganz besonders:

Grundrechte, die die Privatsphäre betreffen (2)

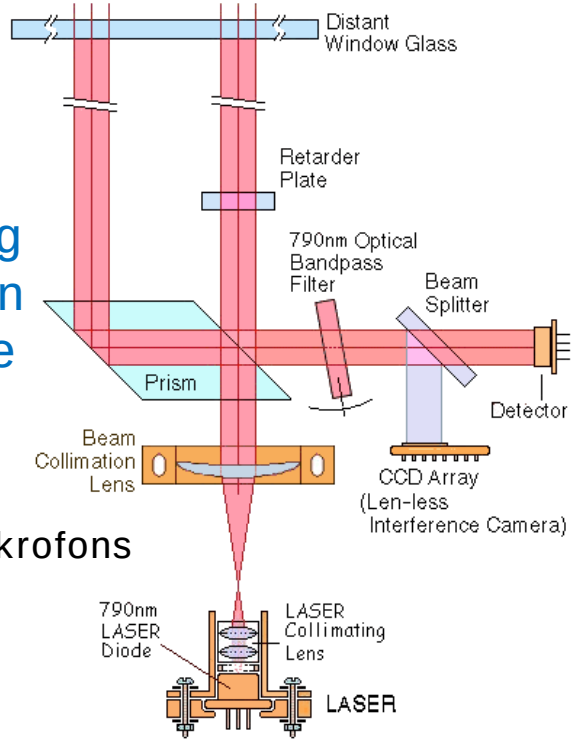
Freie Universität Berlin

- Artikel 10 (Kommunikationsgeheimnis), Absatz 1 und 2:
  - (1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
  - (2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung [...], so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird [...].
    - Beim letzten Satz wird es kompliziert: https://de.wikipedia.org/wiki/G10-Gesetz

Grundrechte, die die Privatsphäre betreffen (3)

Freie Universität Berlin

- Artikel 13 (Unverletzlichkeit der Wohnung), Absatz 3:
  - "Begründen bestimmte Tatsachen den Verdacht, daß jemand eine durch Gesetz einzeln bestimmte besonders schwere Straftat begangen hat,
    so dürfen zur Verfolgung der Tat auf Grund richterlicher Anordnung technische Mittel zur akustischen Überwachung von Wohnungen, in denen der Beschuldigte sich vermutlich aufhält, eingesetzt werden,
    wenn die Erforschung des Sachverhalts auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre.
  - Die Maßnahme ist zu befristen. Die Anordnung erfolgt durch einen mit drei Richtern besetzten Spruchkörper. Bei Gefahr im Verzuge kann sie auch durch einen einzelnen Richter getroffen werden."



Funktionsprinzip eines Doppelstrahl-Lasermikrofons
www.williamson-labs.com/laser-mic.htm

Grundrechte, die die Privatsphäre betreffen (USA)

Freie Universität Berlin

- Artikel 4 der Bill of Rights der US-Verfassung
  - "Fourth Amendment"
  - http://de.wikipedia.org/wiki/4._Zusatzartikel_zur_Verfassung_der_Vereinigten_Staaten

- "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
  - Durchsuchungen/Beschlagnahmen müssen verhältnismäßig sein,
  - benötigen hinreichenden Verdacht (amtlich bestätigt),
  - und müssen spezifisch sein

  - *"The people"* sind US-Bürger und legale Ausländer auf US-Boden
    - *http://en.wikipedia.org/wiki/Second_Amendment_to_the_United_States_Constitution#Meaning_of_.22the_right_of_the_People.22*

Maßnahmen zum Schutz der Privatsphäre

Freie Universität Berlin

Sehr verschiedene Arten und Bereiche (Beispiele):

- Physische Blockaden: z.B.
  - Türen, Schlösser, Behälter, Jalousien
  - Kleidung u.a.

- Höflichkeitsregeln: z.B.
  - Anklopfen
  - "So was fragt man nicht" u.a.

- Anonymität:
  - Geheime Abstimmungen
  - Bezahlen mit Bargeld
  - Vermummung u.a.

Maßnahmen zum Schutz der Privatsphäre (2)

Freie Universität Berlin

- Geheimhaltungsgebote:
  - Bankgeheimnis http://de.wikipedia.org/wiki/Bankgeheimnis
    - A, CH: Recht und Pflicht der Bank gemäß Bankgesetz
    - D: Gewohnheitsrecht, Vertragspflicht
  - Schweigepflicht
    - §203 StGB: Ärzte, Rechtsanwälte, Sozialarbeiter u.a.

- Informationelle Selbstbestimmung (Beispiele):
  - Datenschutzrecht (z.B. bei Datenweitergabe)
  - Verschlüsselung von Daten(verkehr)
  - Anonymer Datenverkehr
  - Weglassen von einigen Ziffern der gewählten Nummern auf Telefonrechnungen etc.

- etc.

Privatsphäre und Computerisierung

- Im Vor-Computer-Zeitalter kannte man seine Privatsphäre recht gut
- und konnte Sie auch überwiegend genügend schützen
  - Einschränkungen betrafen hauptsächlich Kenntnisse von Personen in der nahen Umgebung
    - die nämlich schwierig zu beschränken sind
- Computerisierung bringt zahllose neue Bedrohungen der Privatsphäre hervor
  - Hauptsächlich im Umgang mit Informationen
  - Aber fast alle Aspekte der Privatsphäre schlagen sich in Informationen nieder…

Die Spannungsfelder

- Freiheit ←→ Sicherheit
  1. staatliche Stellen reduzieren unsere Privatsphäre (Freiheit), um für Sicherheit zu sorgen

- Freiheit ←→ Effizienz/Bequemlichkeit
  2. viele Bürger/innen sind zu bequem, um persönliche Maßnahmen gegen (1.) zu ergreifen.
  3. viele Konsument/inn/en geben aus Bequemlichkeit viel Privatsphäre gegenüber Unternehmen auf

Freiheit ↔ Sicherheit

- 2001-09-11 Terroranschlag auf das World Trade Center
- 2001-10-26 PATRIOT Act in Kraft (342 Seiten!)
  - http://en.wikipedia.org/wiki/Patriot_Act
    http://de.wikipedia.org/wiki/USA_PATRIOT_Act
  - Befristungen (bis 2005) z.T. verlängert
    z.T. aufgehoben (2005, 2006, 2010, 2011)
  - weite Überwachungsbefugnisse für Telefon-/Internet-/Bibliotheks-/Bank-/Gesundheitsdaten
    - National Security Letters: Datenbeschlagnahme ohne Richtervorbehalt, mit Schweigepflicht (bis 10 Jahre Haft)
  - Viele Formulierungen sehr weit und vage
    - z.B. 5 Jahre Haft für "expert assistance to a terrorist"
- 2002-2003 Total Information Awareness

Auswirkungen (nicht *nur* von 9/11)

Freie Universität Berlin

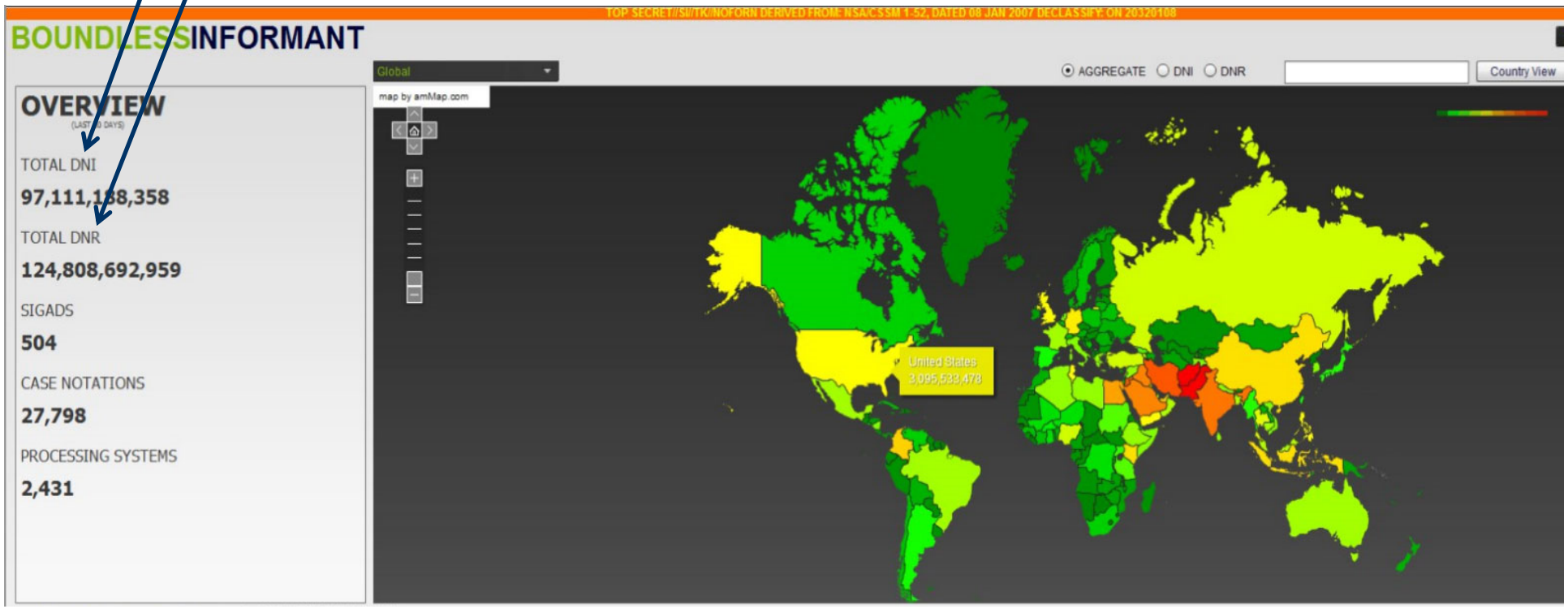
- (ohne Edward Snowden würden wir davon kaum etwas wissen)
  - http://en.wikipedia.org/wiki/2013_mass_surveillance_disclosures

1. Massive Sammlung von Verbindungsdaten ("Metadaten")
   - Nach NSA-Definition ist das keine Überwachung, deshalb auch fast flächendeckend für Amerikaner
2. Weitreichende Fähigkeit zur bedarfsweisen Sammlung von Inhaltsdaten (Telefongespräche, SMS, Emails)
   - Für deren Analyse ist Verdacht nötig oder Aufenthalt im Ausland
3. XKeyscore: Komfortabler Zugriff auf all diese Daten
   - hat Funktion zur automatischen Komplettverfolgung einer Person
     - https://en.wikipedia.org/wiki/XKeyscore

- u.a.m.

Auswirkungen: Verbindungsdaten

- Massive Sammlung von Kommunikations-Verbindungsdaten
  - DNI: Netzverbindungen (z.B. Emails, http-Abrufe)
    DNR: Telefonverbindungen (Festnetz, Mobilfunk)
    - z.B. 2006-12: ca. 30 Datensätze pro Kopf der Weltbevölkerung:



Überwachungsintensität Dezember 2006
https://en.wikipedia.org/wiki/Boundless_Informant

Sind Verbindungsdaten heikel?

- Verbindungsdaten beschreiben
  - wer
  - wann, wie oft, in welchem Umfang (Dauer oder Datenmenge)
  - mit wem kommuniziert
- und ergeben in Summe ein erstaunlich reichhaltiges Bild des Lebens einer Person:
  - Telefonate
  - SMS
  - Emails und Instant Messages
    - hier sieht man auch Gruppen von Kontakten
  - Webseitenabrufe

Auswirkungen: Inhaltsdaten

- Abfangen riesiger Datenmengen auf Glasfaserkabeln
- PRISM: Zugriff auf Datenbestände großer Internetanbieter
  - GMail, Hotmail, Facebook, Yahoo, Skype, Apple u.a.

Resultat

- Formulierungen von Edward Snowden im Interview:
  - http://www.ndr.de/ratgeber/netzwelt/snowden277_page-3.html
  - "You could read anyone's email in the world.
    Anybody you've got email address for,
    any website you can watch traffic to and from it,
    any computer that an individual sits at you can watch it,
    any laptop that you're tracking you can follow it as it moves from place to place throughout the world.
    It's a one stop shop for access to the NSA's information.
    And what's more you can tag individuals using XKeyscore."
  - Diese Aussagen sind vereinfachend übertrieben,
    treffen aber die Tendenz.

Wie kommt sowas zustande?

Freie Universität Berlin

Problem 1: Technische Lösung skaliert gut

- Überwachung mit menschlichen Agenten (HUMINT) ist teuer, aber doppelt so viel technische Überwachung (SIGINT) kostet nur wenig Mehraufwand
  - https://de.wikipedia.org/wiki/MfS#Organisation 1 MA/180 Einw.
  - https://en.wikipedia.org/wiki/NSA#Employees 1 MA/8000 Einw.~

Problem 2: Geheimdienste sind geheim

- Geheimdienste unterliegen einer stark verringerten Kontrolle
  - z.B.: D: Geheimdienstausschuss, USA: FISC (u.a.)
  - Die Aufseher sind mit der Komplexität völlig überfordert
    - z.B: NSA Jahresbudget ~10 Mrd USD ←→ FISC 11 Nebenjob-Richter
- "Five Eyes": Geheimdienste von USA, UK, CAN, NZ, AUS kooperieren (seit ~1946); umgehen damit Einschränkungen
  - https://en.wikipedia.org/wiki/Five_Eyes#List_of_FVEY_surveillance_targets
  - BND macht auch mit (Spiegel Online 30.06.2013)

Wie kommt sowas zustande? (2)

- Problem 3: Technische Überwachung ist für die Betroffenen abstrakt
  - Thomas Drake: "Put your entire life in a box, your documents, bank accounts, your passwords, everything, and give it to a complete stranger, a fellow American, for safekeeping. Would you do it?"
    - https://en.wikipedia.org/wiki/Thomas_Andrews_Drake
  - ACLU: "The NSA is coming to town"
    - http://youtu.be/8pcWlyUu8U4

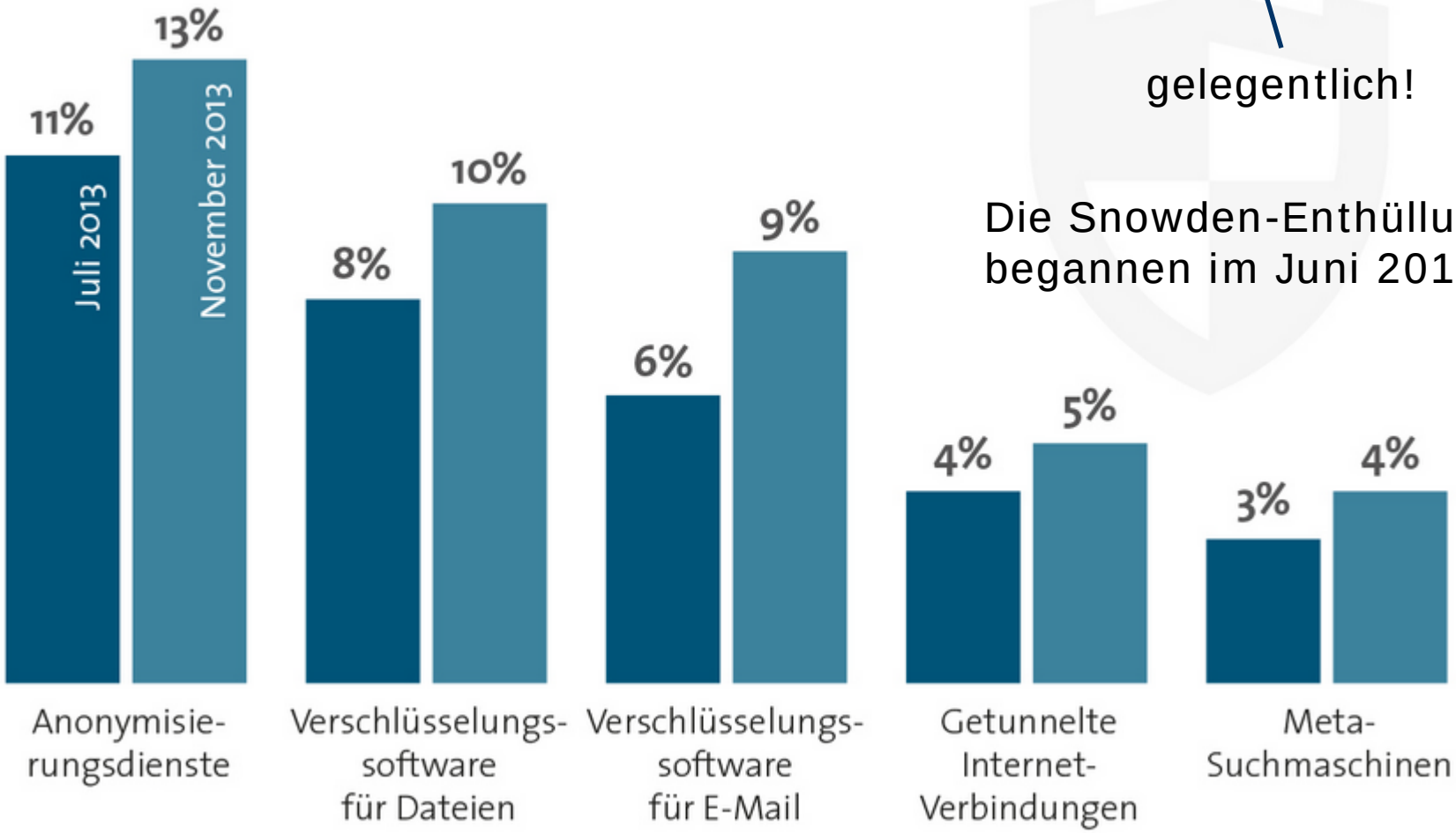
Privatsphäre ←→ Bequemlichkeit

Welche Sicherheitslösungen auf dem eigenen Computer genutzt werden[1]

http://www.bitkom.org/de/markt_statistik/64026_78217.aspx

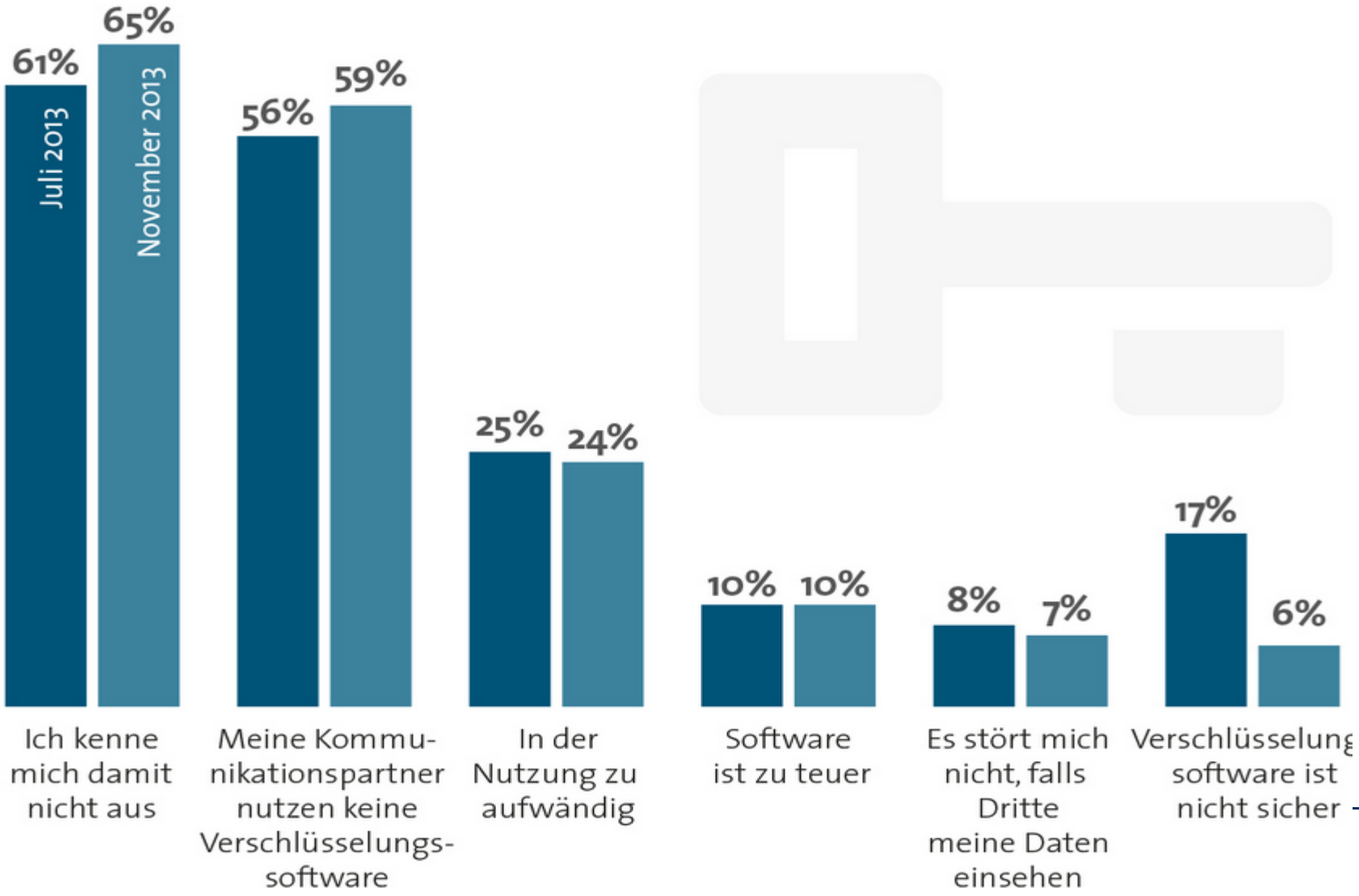
gelegentlich!

Die Snowden-Enthüllungen begannen im Juni 2013

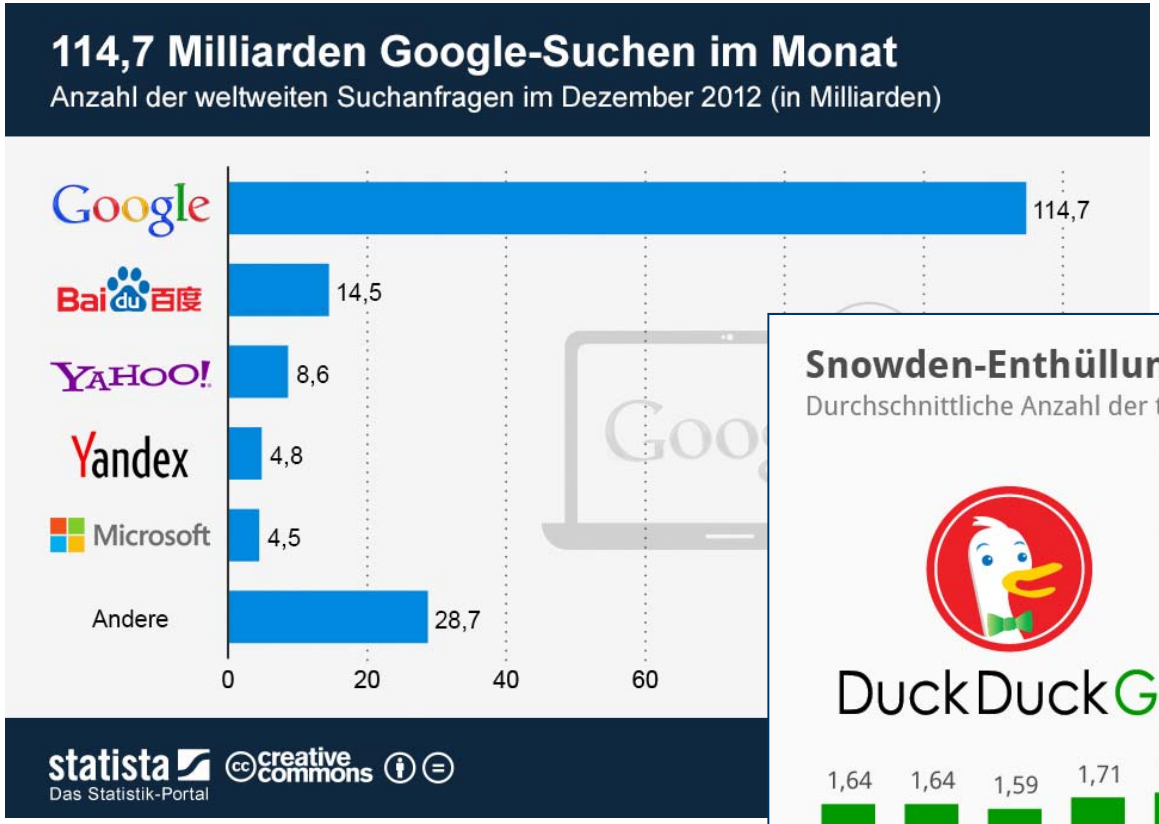


Angeführte Gründe

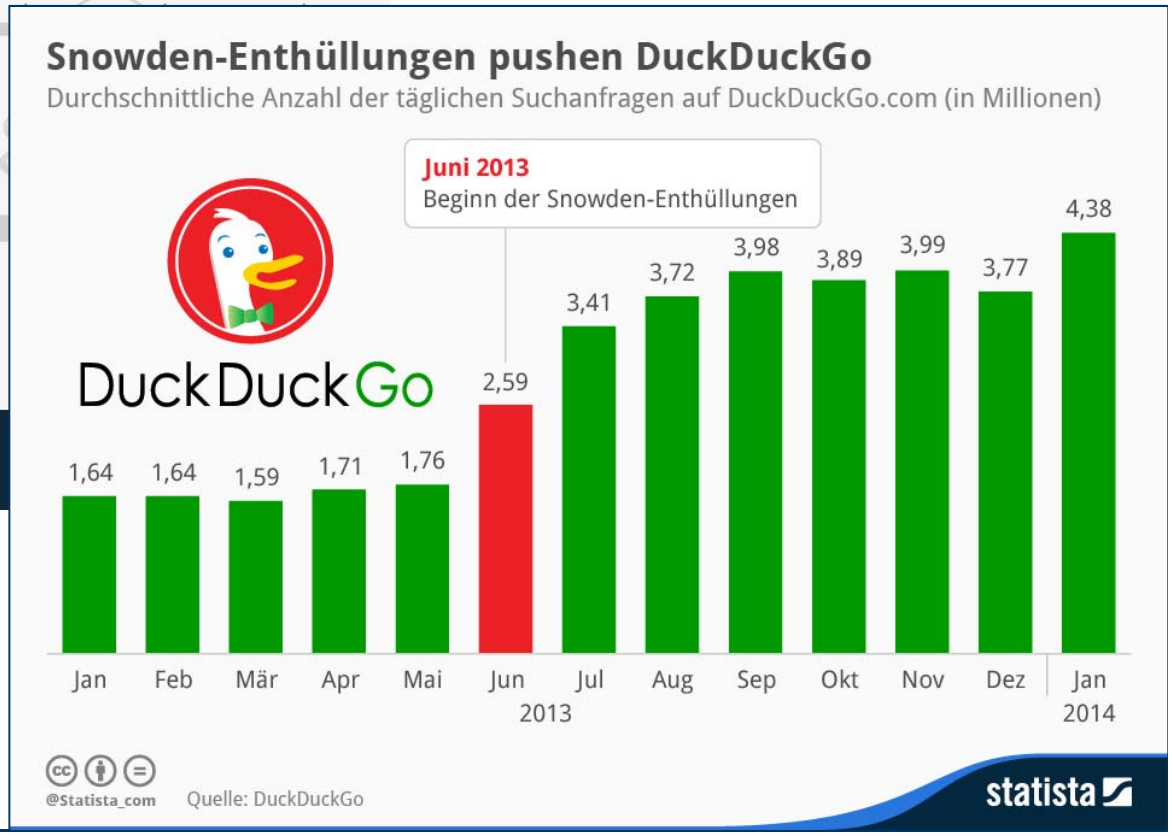
Gründe für den Verzicht auf Verschlüsselungssoftware für Dateien & E-Mails
http://www.bitkom.org/de/markt_statistik/64026_78217.aspx



Wen stört es, wenn die Suchmaschine seine Anfragen zum Profil verdichtet?



DuckDuckGo, ixquick und wenige andere Suchmaschinen speichern ausdrücklich <u>keine</u> Benutzerdaten.



Der Welt-Marktanteil von DuckDuckGo ist ca. 0,1%

Sind Suchanfragenprofile heikel?

Freie Universität Berlin

Ja.

- Thomas Drake: "Put your entire life in a box, your documents, bank accounts, your passwords, everything, and give it to a complete stranger, a fellow American, for safekeeping. Would you do it?"
  - https://en.wikipedia.org/wiki/Thomas_Andrews_Drake

- Aus der Summe alle Suchanfragen lassen sich z.B. oft ablesen:
  - persönliche Wünsche und Sehnsüchte, inkl. sexuelle
  - Gesundheitsprobleme
  - Streitigkeiten
  - Konsumwünsche und –gewohnheiten
  - Hobbies und Interessen
  - Freizeitpläne und -aktivitäten
  - Karrierepläne und -aktivitäten

Noch erstaunlicher: Facebook

- Facebook sammelt sowohl Verkehrsdaten
  - Seitenabrufe (sogar von Fremdseiten!), Likes
- als auch Inhaltsdaten
  - Kontakte (sogar von Nichtmitgliedern!), Nachrichten, Bilder
- und räumt sich selbst dafür volle Nutzungsrechte ein.

- Die konkrete Nutzungsart ändert sich evtl. nachträglich:
  - 20?? Meldung "verdächtiger Aktivitäten" an die Polizei
  - 2008 Anmeldung an Fremdseiten mit Facebook-Passwort
  - 2009 Aufweitung der Sichtbarkeits-Standardeinstellungen
  - 2011 Gesichtserkennung
  - 2011 Chronik (Timeline)
  - 2013 Graphensuche ("Freunde, die diesen Monat in Rom waren")

Besonders relevant: Geldverkehr

- Barzahlungen sind anonym
  - Jedenfalls, wenn niemand die Scheine mit ihren Seriennummern verfolgt…
- Bargeldlose Zahlungen sind es fast nie: Kreditkarten, Lastschrift, Überweisungen, Paypal, Mobiltelefon-Systeme, etc.
  - Buchgeld
- Das heißt
  - der Händler kennt (je nach System) meine Identität
  - der Zahlungsdienstleister kennt meine Zahlungsgeschichte: Wie viel wann wie oft an wen?
    - Auch das ist häufig wieder sehr aussagekräftig
- Viele Leute zahlen aber weit überwiegend bargeldlos

Wie kommt sowas zustande?

Problem 1: Technische Lösung skaliert gut

- Google sucht super gut
- Facebook ist sehr praktisch
- Bargeldloses Zahlen ist sehr praktisch

Problem 2: Firmen sind nur mäßig transparent

- Komplizierte Regeln in Gesetzen und Nutzungsvereinbarungen
- Geschäftsgeheimnisse

Problem 3: Der Verlust an Privatsphäre ist anfangs sehr abstrakt

Wahrung der Privatsphäre: Was könnte man tun?

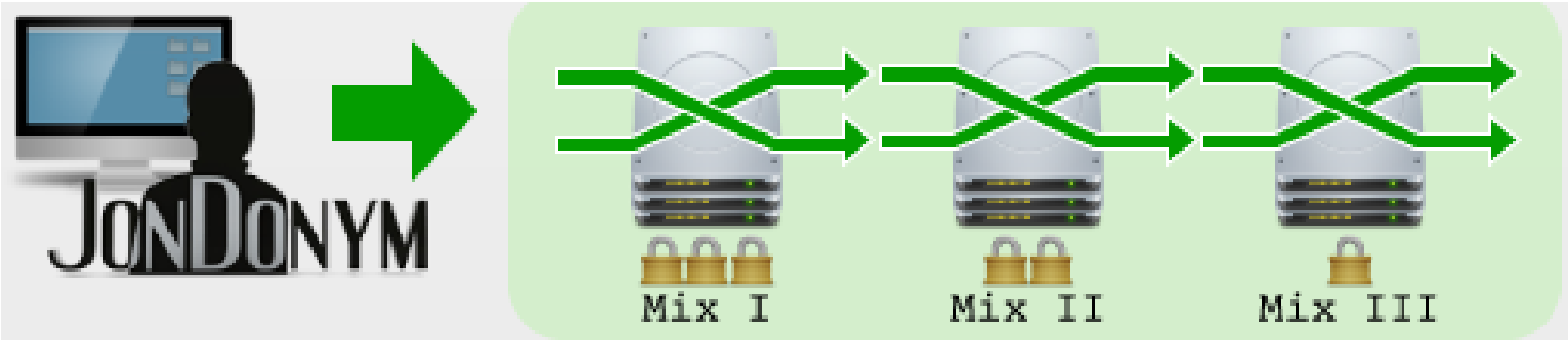
Freie Universität Berlin

- Inhaltsdaten: Verschlüsselung
  - siehe Einheit über Informationssicherheit (Security)
- Verkehrsdaten: Vermischung // Flutung
  - TOR, JAP // Bitmessage ➔
- Suchmaschine: Ausweichen
  - startpage, DuckDuckGo, ixquick
- Facebook: Ausweichen
  - diaspora* (diasporafoundation.org) oder Kombination von Einzeldiensten
- Geldverkehr: elektronisches Bargeld (anonym)
  - Bitcoin ➔

Schutz von Web-Verkehrsdaten: JAP/JonDonym

- http://anon.inf.tu-dresden.de/ JAP/AN.ON gratis, langsam
- https://www.anonym-surfen.de JonDonym kommerziell, schnell

- Man schaltet absichtlich zusätzliche Zwischenstationen ein
  - z.B. 3, genannt "Mixe"; jeder Mix hat viele Benutzer
- Mixe leiten die Daten nicht nur weiter, sondern geben sich dabei selbst als Absender aus
- Mehrschichtige Verschlüsselung verbirgt sogar Teile der Route



- Um den wahren Absender aufzudecken, müssen Empfänger, Internet-Versorger und alle diese Mixe mitarbeiten
  - und die wollen das gar nicht! Evtl. Mixe in mehreren Ländern

Elektronisches Bargeld (pseudonym): Bitcoin

- Kernproblem: Verhindern von Doppelt-Ausgeben
  - Alles wird abgesichert durch kryptografische Methoden

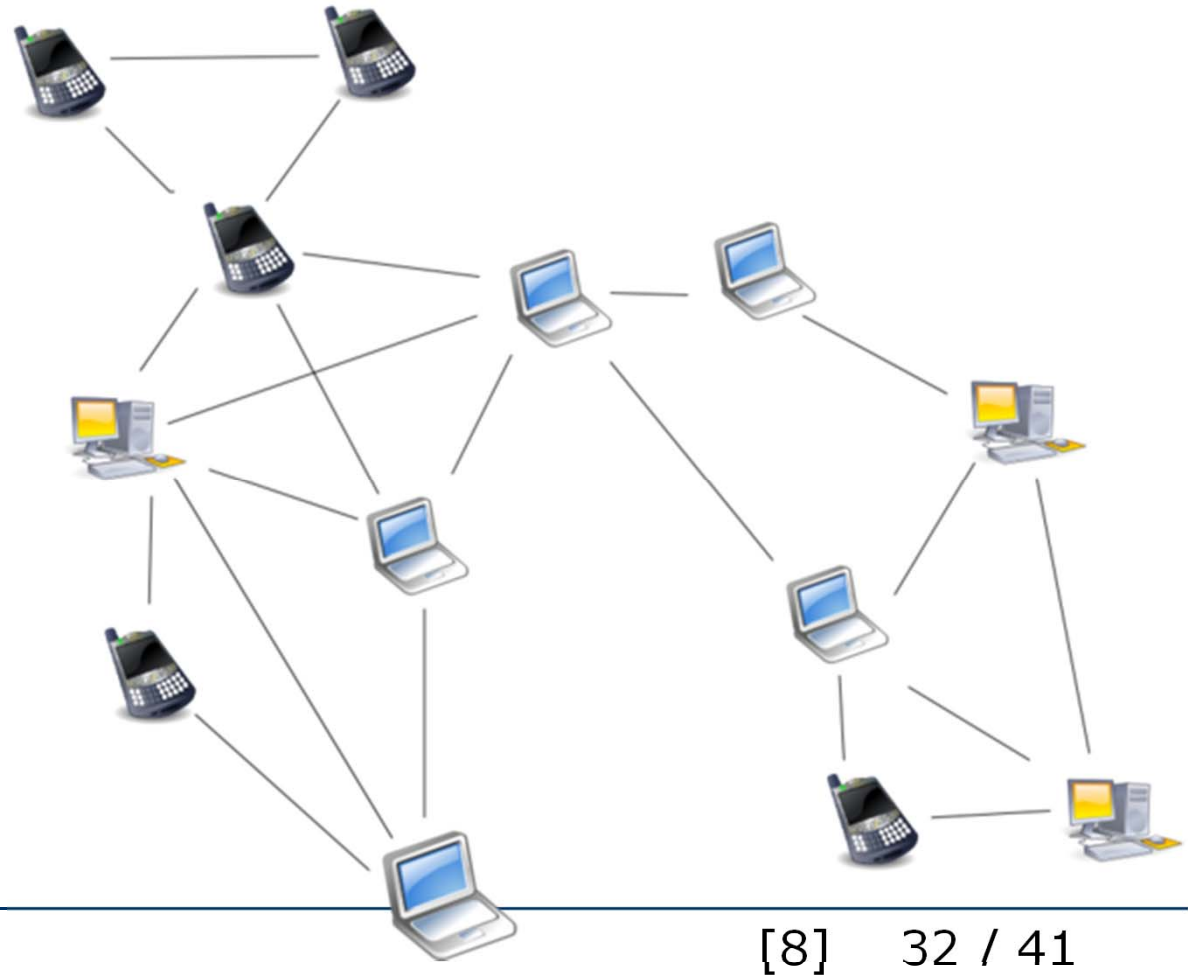
Grundideen:

1. Erschaffung von Bitcoins verlangt viel Rechenarbeit (Vorbild: Gold schürfen)
   - und zwar um die Wette
2. Transfer von Bitcoins verlangt Protokollierung durch sehr viele Bitcoin-Teilnehmer (per Peer-to-Peer-Netz)
   - Eine Bitcoin ist eine Sequenz von Bitcoin-Konto-Transfers
   - Die Kontonummer bildet ein Pseudonym des Kontoinhabers. Wenn der anonym bleibt, ist es die Bitcoin-Verwendung auch.
3. Jeder kann nach Belieben Bitcoin-Konten erzeugen
   - z.B. für jede einzelne Zahlung ein neues

- http://bitcoin.org/bitcoin.pdf Beschreibung des Konzepts
- http://spectrum.ieee.org/img/06Bitcoin-1338412974774.jpg

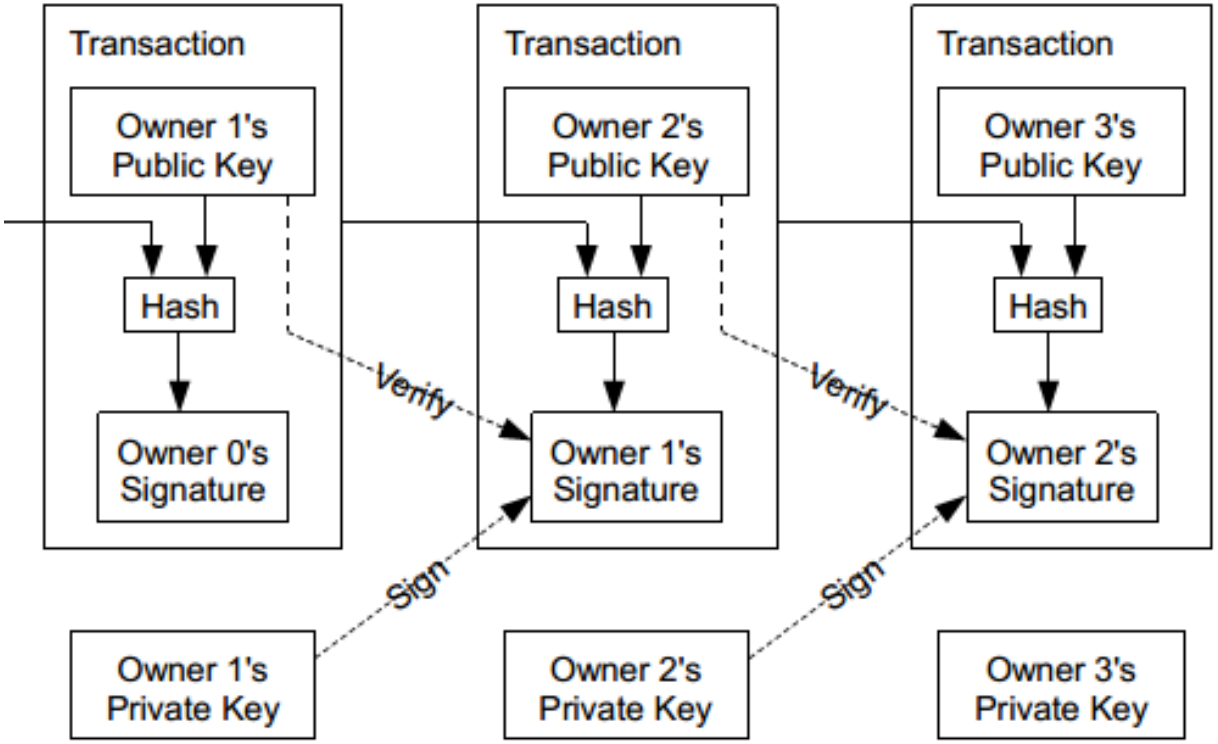
Funktionsweise von Bitcoin: Protokollierung durch Fluten

- Jede Transaktion wird von jedem Teilnehmer an alle seine Nachbarn weitergereicht
  - Jeder protokolliert sie
- Jede Transaktion ist nach kurzer Zeit global bekannt



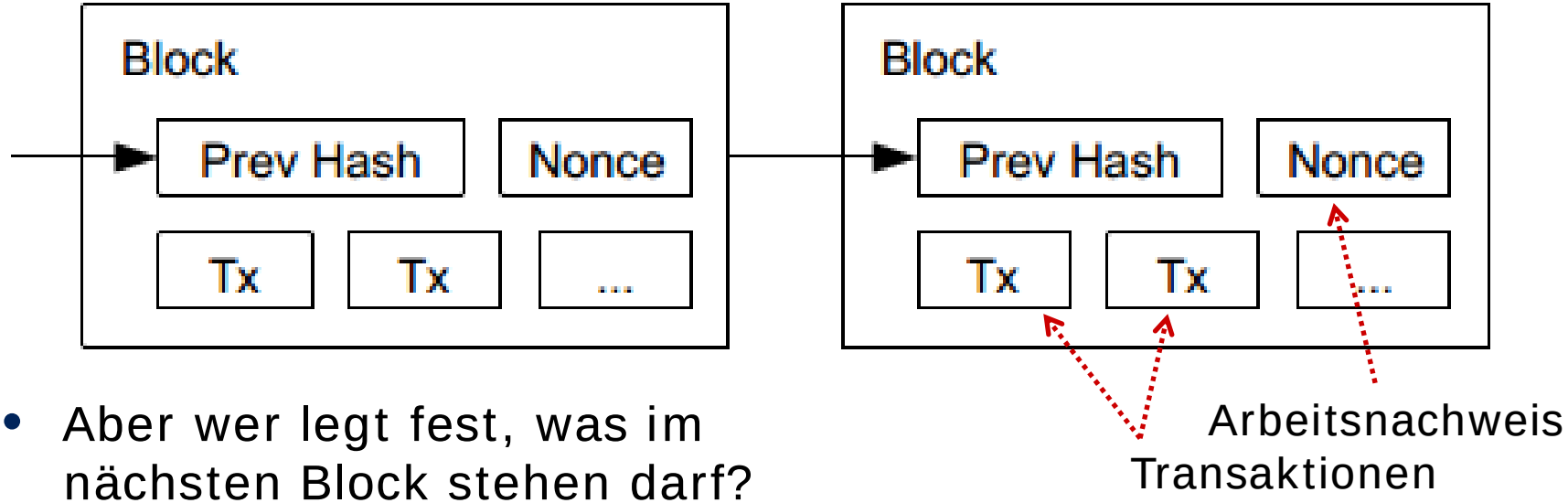
Funktionsweise von Bitcoin: Konto, Signatur

- Ein Bitcoin-Konto ist ein Schlüsselpaar für asymmetrische Kryptographie
  - Der öffentliche Schlüssel dient als Kontonummer, z.B.: 1BTCorgHwCg6u2YSAWKgS17qUad6kHmtQW ("Bitcoin-Adresse")
- Die Weitergabe einer Bitcoin wird vom Voreigentümer signiert:



Funktionsweise von Bitcoin: Transaktionsblockfolge

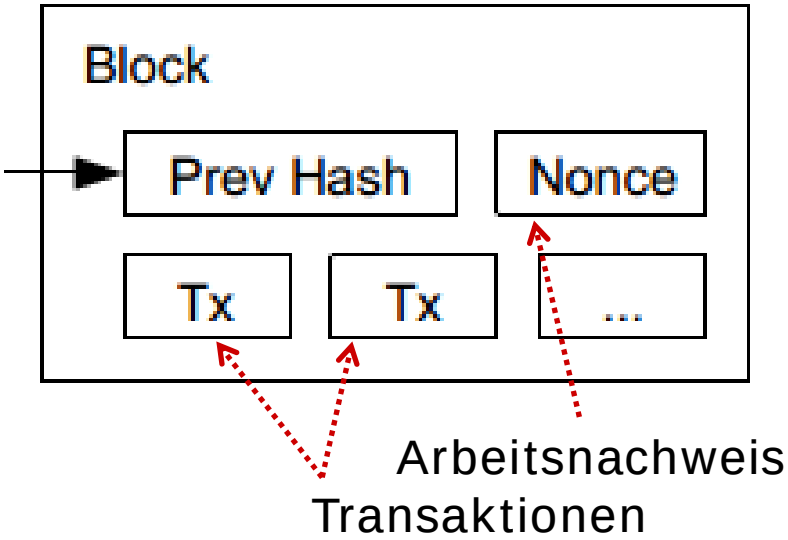
- Bitcoin-Transaktionen werden blockweise zusammengefasst
  - Darin ist kein Doppelt-Ausgeben zugelassen
- Die Blöcke werden in eine einzige globale Sequenz geordnet
  - Darin ist vom ggf. Doppelt-Ausgeben eines gültig, eines ungültig

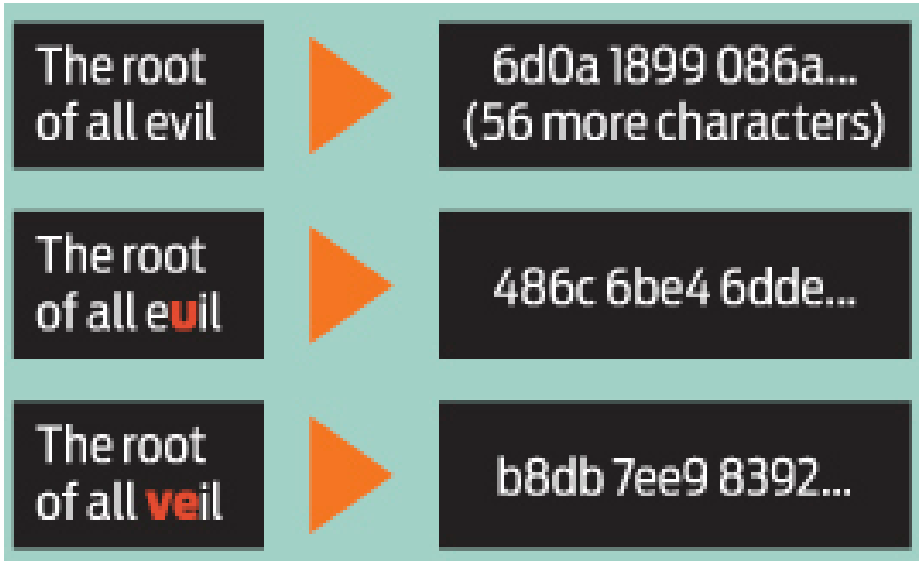


- Aber wer legt fest, was im nächsten Block stehen darf?
  - Jeder Teilnehmer sammelt alle Transaktionswünsche
  - Arbeitsnachweis (Proof-of-work) komplettiert einen Block
  - Es wird immer die aktuell längste Blockkette fortgesetzt

Funktionsweise von Bitcoin: Arbeitsnachweis

- Kryptographische Hashfunktionen liefern wild verschiedene Resultate bei kleinsten Datenunterschieden
  - Es ist unpraktikabel, einen "gewünschten" Hashwert zu erzeugen
- Arbeitsnachweis (proof of work):
  Finde eine Zahl ("nonce"), die den Hashwert des Blocks genügend klein macht





Details siehe https://en.bitcoin.it/wiki/Category:Technical

Funktionsweise von Bitcoin: Erzeugung von Bitcoins ("mining")

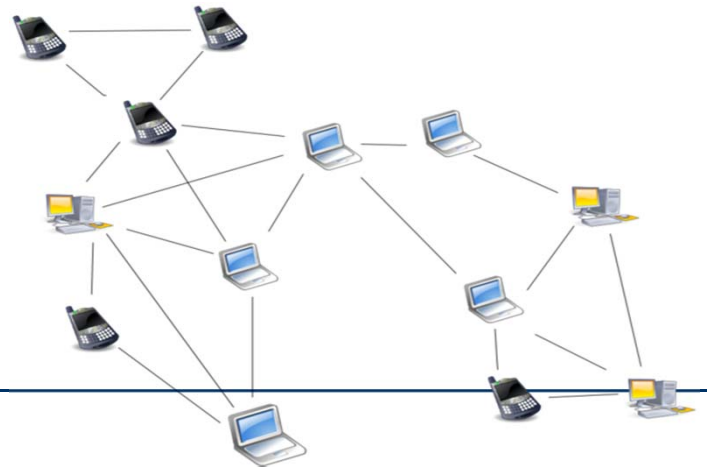
Freie Universität Berlin

- Ein Block enthält eine zusätzliche Transaktion, die Bitcoins aus dem Nichts an den Finder des Nonce ausschüttet
- Deshalb arbeiten viele Knoten am proof-of-work mit
  - Der Erfolg repräsentiert die eingesetzte HW und elektr. Energie
  - Der Prozess wird "Bitcoin mining" genannt, nach dem Vorbild der Goldsuche
- Wie bei der Goldsuche, wird die Belohnung im Laufe der Zeit immer geringer
- Dann leben die Miner statt dessen von Transaktionsgebühren
  - Diese setzen sind Absender der Transaktion selbst fest

(Viele Einzelheiten fehlen in dieser Darstellung)

Schutz von Email-Verkehrsdaten: Bitmessage

- https://bitmessage.org
  - Inspiriert von Bitcoin
- Öffentlicher Schlüssel dient als Email-Adresse
- Jede Nachricht wird durch Fluten an jeden weitergegeben
  - Das erzeugt allerdings viel Verkehr…
- Nur der Empfänger kann sie lesen
  - …gibt sie aber trotzdem auch weiter!
- Niemand kann wissen, wer der Empfänger ist
  - Und nur sehr dichte Überwachung kann entscheiden, wer der Sender war

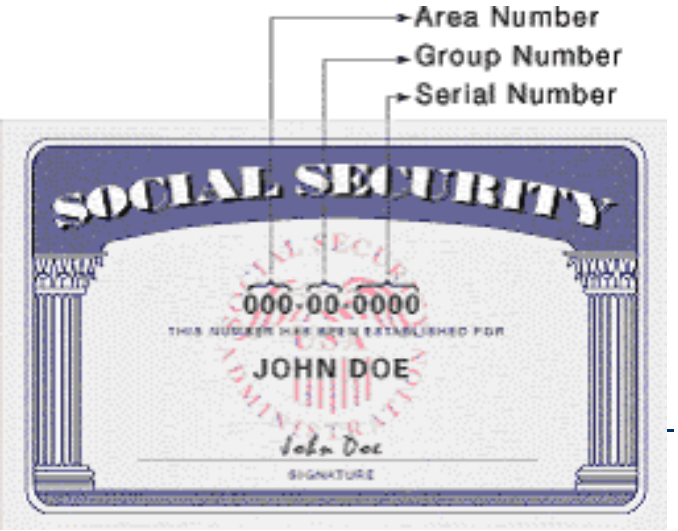


Authentisierung zum Schutz der Privatsphäre

Freie Universität Berlin

- Oft kann oder soll die Identität nicht verborgen werden
- Dann muss Sie zum Schutz der Privatsphäre <u>verlässlich</u> und <u>nachprüfbar</u> offen gelegt werden: Authentisierung
  - z.B. Anmeldung mit Name und Passwort

- Warnendes Gegenbeispiel: Email-Spamming
  - Viele Spam-Emails haben als (vermeintlichen) Absender die Adressen von realen, aber völlig unbeteiligten Personen
  - Das ist für diese gefährlich, denn es kann ihren Ruf schädigen
    - z.B. sind manche der so beworbenen Aktiviäten in vielen Empfängerländern illegal
- Warnendes Gegenbeispiel: US Social Security Number (SSN)
  - Die wird mal als Identitätsmerkmal und mal als Passwort verwendet – chaotisch!



Zusammenfassung

- Die Wahrung der Privatsphäre ist ein wichtiges Persönlichkeitsrecht
- Computerisierung verursacht eine große Zahl neuer Bedrohungen für die Privatsphäre
- Es gibt im Prinzip technische Wege, diesen Bedrohungen zu begegnen
  - Wenn auch teilweise recht aufwendig

Weitere Quellen

- Facebook-Freunde einer Person kennen ermöglicht Bestimmung ihrer sexuellen Orientierung
  - Jernigan, Mistree. First Monday 14(10), Oktober 2009 http://firstmonday.org/ojs/index.php/fm/article/view/2611/2302
- Beispiele für die Aussagekraft von Verbindungsdaten:
  - http://www.heise.de/newsticker/meldung/Studie-Was-auf-Vorrat-gespeicherte-Verbindungsdaten-verraten-2146213.html
- Umfangreiche Bewegungsprofile *kann* man nicht anonymisieren
  - de Montjoye et al.. Nature, Scientific Reports, März 2013 http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html , Zeitungsmeldung darüber: http://www.zeit.de/digital/datenschutz/2013-04/bewegungsprofil-forscher-zuordnung

Danke!

(mehr Information über die SSN folgt im Anhang)

Warnendes Beispiel: US-Sozialversicherungsnummer

- Die Sozialversicherungsnummer (Social Security Number, SSN) ist eine neunstellige Zahl, die einer Person zugeordnet wird
- Eingeführt 1935
  - zunächst ausschließlich zur Nutzung im Wohlfahrtsprogramm
- 1943: Roosevelt ordnet an, dass die SSN in allen neuen staatlichen Aktensystemen zu verwenden sei
- 1961: Die Finanzbehörden (IRS) verwenden die SSN als Identifikationsnummer für jede/n Steuerzahler/in
- 1976: Zahlreiche staatliche Stellen dürfen die SSN zur Identitätsprüfung verwenden
- seit den 1980er Jahren: Zahllose private Einrichtungen aller Art verlangen ebenfalls die SSN

Falsche Annahmen über die SSN

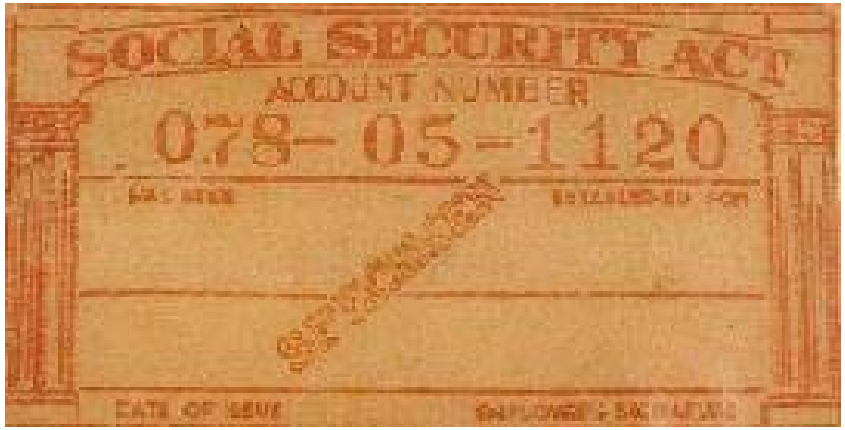
Freie Universität Berlin

Die meisten Verwendungen unterstellen
die folgenden Eigenschaften für die SSN:

- Eindeutigkeit
  - "Es gibt keine zwei Personen mit derselben SSN"
  - Faktisch wurden gleiche Nummern an verschiedene Personen ausgegeben – weil sie Name und Geburtsdatum gemein hatten!
- Universalität
  - "Jeder hat eine SSN" (Kinder und Organisationen aber nicht)
- Identifikation
  - "Die SSN identifiziert eine Person eindeutig und zuverlässig"
  - Faktisch: Wird oft nicht überprüft, Ausweise waren lange nicht fälschungssicher, nicht tippfehlerfest (keine Prüfziffer, recht voller Nummernbereich)

SSN: Es kommt noch schlimmer…

- Einige tausend Amerikaner haben jahrelang die selbe SSN 078-05-1120 benutzt
  - Diese war auf SSN-Ausweis-Dummies in Portemonaies abgedruckt, die in den 1940er und 1950er Jahren verkauft wurden
  - www.ssa.gov/history/ssn/misused.html



- Viele computerisierte Systeme verwenden die SSN als "Passwort"
  - z.B. die Kontoauskunftsterminals vieler Banken

SSN: Folgen

- Aufgrund der weiten Verwendung der SSN kann man bei ihrer Kenntnis in USA sehr viele Information über einen Menschen bekommen:
  - Geburtsurkunde
  - Aktuelle Adresse
  - Telefonnummern (z.T. auch geheime)
  - Kreditwürdigkeit
  - Vorstrafen und Ordnungswidrigkeiten
  - Alimentzahlungen an Ex-Ehepartner und Kinder
  - etc.

- z.B. http://www.net-vestigator.com/?hop=strange
  - *"Find out anything about anybody – without anyone knowing!"*

SSN: Folgen (2)

- Durch die Allgegenwart der SSN kommt es leicht zu Missbrauch:
  - absichtlich oder
  - versehentlich
- Zugleich kann dieser sehr schwerwiegende Folgen haben
  - z.B. Verlust der Kreditwürdigkeit
  - z.B. Verfälschung der Polizeiakten

Was ist das Problem?

- Eine SSN ermöglicht einerseits den Zugang zu sehr vielen Informationen über eine Person
- Zugleich ist es schwierig, seine SSN geheim zu halten
- Das Problem kommt daher, dass die Aufgabe der SSN ohne Nachdenken über Privatheitsüberlegungen immer mehr erweitert wurde
  - Inzwischen haben aber Stellen,
    die unnötigerweise die SSN verlangen,
    erhebliche Akzeptanzprobleme bei *einigen* ihrer Kunden

...und in Deutschland?

- Das deutsche Gegenstück zur SSN ist die *Versicherungsnummer* (Rentenversicherungsnummer)
  - Sie kodiert das Geburtsdatum, das Geschlecht und den Anfangsbuchstaben des Geburtsnamens
  - z.B. 170493 P 528

- Die erlaubte Verwendung der Versicherungsnummer als Personenkennzeichen ist in Deutschland gesetzlich stark beschränkt
  - nicht einmal die Krankenversicherung darf sie benutzen
  - siehe http://de.wikipedia.org/wiki/Versicherungsnummer