Chapter 9

Privacy

Security vs. Privacy

Privacy is the user ability to control what happens to personal information

- The "right to be left alone"
- Security is a necessary building block for privacy, but is not sufficient
- Privacy needs **organizational**, **legal**, and **social** measures!

> „When making public policy decisions about new technologies for the Government, I think one should ask oneself which technologies would best strengthen the hand of a police state. Then, do not allow the Government to deploy those technologies. This is simply a matter of good civic hygiene."

(Phil Zimmerman, author of PGP, to the congress of the US, Oct. 1993
https://fas.org/irp/congress/1993_hr/931012_zimmerman.htm)

What is „Privacy“?

- „The right to be left alone.“

  Louis Brandeis, 1890 (Harvard Law Review)
- “Numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the housetops’”

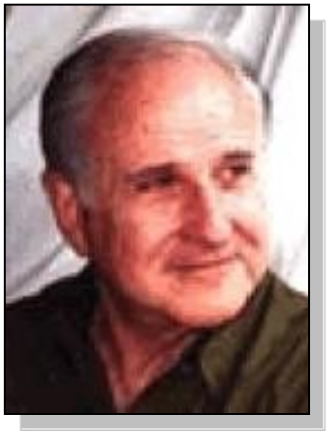
Louis D. Brandeis, 1856 - 1941

Acknowledgments: The following material in this lesson is based largely on slides by Marc Langheinrich, ETH Zurich (translated from German to English with slight modifications).

What is „Privacy“?

„The desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others.“

Alan Westin, 1967 („Privacy And Freedom“)



Aspects of Privacy

- Informational privacy
  - personal information
- Privacy of communication
  - phone calls, letters, email, ...
- Territorial privacy
  - protection of the home, office, ...
- Bodily privacy
  - body search, drug test, ...

History of Privacy

- Justices Of The Peace Act (England, 1361)
  - Punishment for eavesdroppers and voyeurs
- „The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter – but the king of England cannot enter; all his forces dare not cross the threshold of the ruined tenement“
  (Context: Limitation of state powers and binding the king to laws)

William Pitt the Elder (1708-1778)
English parliamentarian,
addressing the House of Commons in 1763

History of Privacy

- 1948 United Nations, Universal Declaration of Human Rights: article 12
  - “No one shall be subjected to arbitrary interference with his **privacy**, **family**, **home** or **correspondence**, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.“
- 1970 The European Convention on Human Rights: article 8
  - “Everyone has the right to respect for his **private and family life**, his **home** and his **correspondence**. ...“

Volkszählungsurteil (BVG, 12/1983)

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, **aus eigener Selbstbestimmung zu planen oder zu entscheiden**. Mit dem Recht auf **informationelle Selbstbestimmung** wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger **nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß**.“

Volkszählungsurteil (BVG, 12/1983)

„Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, **nicht** durch solche Verhaltensweisen **aufzufallen**. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung … behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern **auch das Gemeinwohl**, weil Selbstbestimmung eine **elementare Funktionsbedingung** eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten **freiheitlichen demokratischen Gemeinwesens** ist.”

Example:
House searches

- 4. Amendment of the US constitution

  “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.”

- **Preventing interference? Protecting dignity?**

Mobile and Ubiquitous Computing – Implications on Privacy

- Data collection
  - amount (everywhere, anytime)
  - manner (unobtrusive, invisible)
  - reason (“for future use”)
- Types of data
  - observations instead of facts
- Data access
  - “Internet of Things”

Amount of Data Collection

- Past: public appearance
  - temporarily and spatially distributed
- Now (?): online appearance
  - preferences & problems (online shopping)
  - interests & hobbies (chat, news)
  - place & address (online tracking)
- Tomorrow (– or Now?): everything else
  - at home, at school, in the office, in public, ...
  - no off-button?
  - “worthiness” of the person (→ China)?

Manner of Data Collection

- Past: reasonable heuristics
  - “If you can see me, I can see you”
- Now (?): observable borders
  - online and for electronic transactions
- Tomorrow (– or Now?): „Implicit HCI“
  - interacting with a digital service?
    - life recorders, room computers, smart coffee cups
  - no “recording in progress” LED?

Reasons for Data Collection

- Past: exceptions
- Yesterday: common (group classification)
- Now: „smartness“ by pattern recognition
  - more data = more patterns = more smartness
  - context is everything! everything is context!
- Worthless data? Data-mining!
  - typing speed (enthusiasm?), showering habits (affair?), chocolate consumption (depressed?)
  - location, activities, emotional state, purchases, …
  - often a credit score will have many different influences (pages you like on Facebook, types of adjectives used in posts and emails, etc.)
    → single factors can contribute in counter-intuitive manner

Types of Data

- Past: eyes and ears
- Yesterday: digital and mechanical surveillance
- Now: better sensors
  - more detailed and more accurate data
  - cheaper, smaller, battery-less, ubiquitous!
- Do I know myself best?
  - on-body sensors detect stress, anger, teariness, ...
  - medical sensors alert doctor
  - nervous? floor / seat sensors, eye tracker, ...

Data Access

- Past: natural borders
  - direct communication, gossiping
- Now: online access
  - cheap search
  - database federations
- Tomorrow: cooperating things?
  - standard semantics
  - What does my **<thing>** tell yours?
  - How well can I search your “brain”?

Privacy Methods / Tools

- Legal aspects
  - worldwide privacy laws
  - European (and US) privacy laws
- **Privacy Enhancing Technologies (PETs)**
  - anonymity tools
  - transparency tools
  - confidentiality tools
  - access control tools
- Data protection guidelines

World-wide privacy laws

- Two basic concepts
  - specific (“Don’t Fix if it Ain’t Broken”)
  - general (precautionary principle)
- US: laws specific to some sectors, minimal protection
  - strong federal laws for governmental institutions
  - self regulation and case based for industry
  - International Safe Harbor Privacy Principles declared invalid by the European Court of Justice in October 2015
  - EU-US Privacy Shield currently under review
- Europe: extensive, strong privacy laws
  - laws for industry and government
  - privacy officer in each country
  - current: EU General Data Protection Regulation (GDPR)
    - replaces the Data Protection Directive 95/46/EC (1995)
    - finalized 27.4.2016, effective 25.5.2018, immediately applicable to all member countries without local laws (regulation, not directive)

EU General Data Protection Regulation (GDPR)

Key changes to 1995 Data Protection Directive 95/46/EC

- Increased Territorial Scope (extra-territorial applicability)
  - applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location
- Penalties
  - up to 4% of annual global turnover or €20 Million (whichever is greater)
- Consent
  - **free, informed, specific**
  - request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent

- Details see http://www.eugdpr.org/

EU General Data Protection Regulation (GDPR)

Data Subject Rights

- Breach Notification
  - within 72 hours of first having become aware of the breach
- Right to Access
  - right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose
- Right to be Forgotten / Data Erasure
- Data Portability
- Privacy by Design
  - hold and process only the data absolutely necessary for the completion of its duties (data minimization)
- Data Protection Officers

Basis: Fair Information Practices (FIP)

- Established by OECD, 1980
  - “Organisation for Economic Co-operation and Development”
  - voluntary directives for members
  - easing international data transfer
- Five principles (simplified)
  - openness
  - use limitation and accountability
  - security safeguards
  - sollection limitation (Datensparsamkeit)
  - individual participation and purpose specification
- Basis for many world-wide data privacy laws
  - implication: technical solutions must support FIPs!

How to realise FIPs in practice with smart appliances?

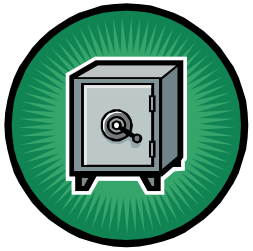
1. Principle: Openness

- No secret data collection
  - legal basis in many countries
- Common solution: privacy policies, AGBs, …
  - who, what, why, for what purpose, for how long, etc.
- Invisible services and privacy policies?
  - invisible privacy service?
  - how to communicate with the data subject?
- Too many smart things?
  - continuous notifications are obtrusive

2. Principle: Accountability

- Identifiable data must be observable / accessible / accountable
  - verification, correction, and deletion by subject
- Data collector is responsible for errors
  - implies coupling privacy policy with use in practice
- Smart things want to know everything (context)
  - increased effort for accountability and access
- Data management: less is more...
  - How much data does a smart appliance need?

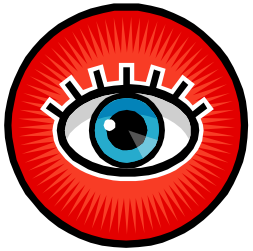
3. Principle: Security Safeguards



- Classical security concepts
  - central database with high security
- Context dependent security for smart things?
  - depending on battery lifetime
  - depending on type of data and communication
  - depending on place and situation
- Complex security requirements in the real world!
  - Accessing medical data in case of an emergency?

4. Principle: Collection Limitation (Anonymity)

- If possible, collect anonymous data
  - no explicit user acceptance, security, data access required
- Pseudonyms for personalization
  - can be changed any time
  - **but: re-identification is often possible!**
- Hiding impossible?!
  - Anonymity in front of cameras and microphones?
- Sensor data hard to anonymize
  - correlation!



5. Principle: User Consent

- User involvement by explicit consent
  - e.g. signature or button press
- Need choice!
  - if possible, support anonymous version
- Consent in implicit HCI?
  - delegating to “agents” (legal?)
- Smart services with freedom of choice?
  - different levels of identification?
    - today often binary choice: “If you want to use this (free) service, here are the privacy policies you need to consent to. It’s completely voluntary of course...”

Technical Tools

- Privacy Enhancing Technologies (PETs)
  - encryption & authentication
  - anonymization & pseudonymization
  - access controls
  - transparency & trust
- „Ubiquitous computing – ubiquitous privacy“
  - everywhere, anytime, infrastructure based, automatic, in the background, unobtrusive

Security helps privacy

- Confidentiality
  - at least the content of some interaction is confidential
  - but: the fact that interaction happens is relevant → "**meta-data**"
- Integrity
  - no "bugs" injected in-transit
- Authenticity
  - no MITM, relaying, transparent proxies, etc.

Example of secure (instant) messenger: all of the above, and more

- Many systems without protection against MITM at the (implicitly trusted) server infrastructure
- Also want to deal with key compromise and mitigate the damage
  - (perfect) forward secrecy
  - backward secrecy, future secrecy → **post-compromise security**

Security hurts privacy

- Authenticity vs. Anonymity (or Pseudonymity)
- Non-repudiability
  - often one aspect why authentication is applied in the first place
  - but: bad for privacy
- Plausible deniability
  - “I didn't do it, my device had a virus/worm/...” is unbelievable when systems are secure

⇒ Privacy **must** be considered from the start when designing a system.
Retrofitting does not work (even less so than with security)!
(good example: [J.-E. Ekberg: “Implementing Wibree Address Privacy”, IWSSI 2007])

Example of secure (instant) messenger:

- “Off the record” (OTR) protocol sends plain text keys after conversation to make messages fakeable after the fact → repudiability by conversation partners afterwards, but authentication during ongoing conversation

Non-identity based authentication

- Authentication is one big threat to privacy
- But only if authentication is based on unique identity (of a person or device)
- Context-/sensor-based authentication does not require identity
- Potential to provide both security and privacy

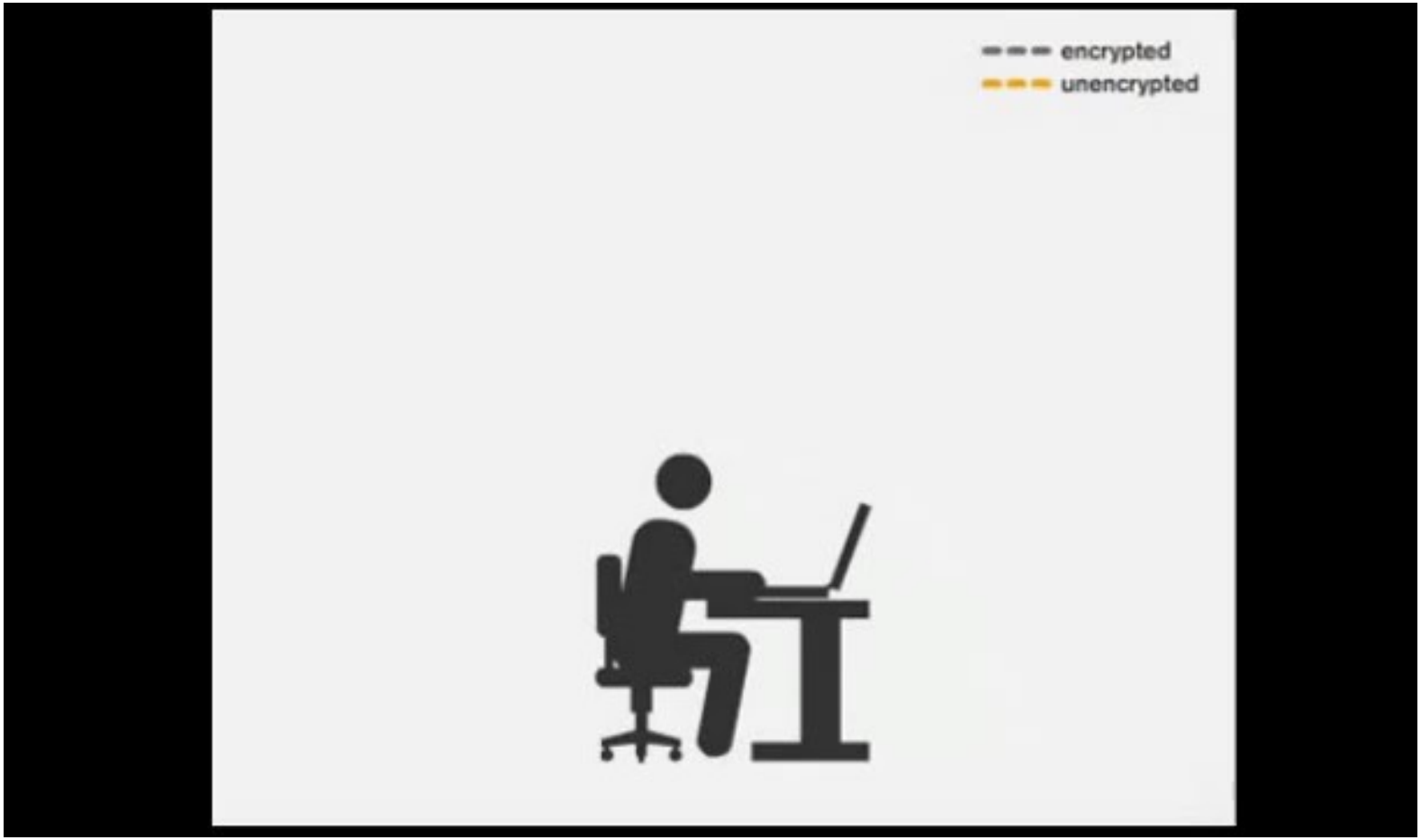
Example:
Secure (Instant) Messenger

- Some messengers already exist that do end-to-end encryption
  - *Signal* best known and analyzed at the moment
    - *WhatsApp* uses Signal protocol in newest versions, but with obfuscated library in closed source app (so who knows) and **meta data stored on Facebook servers**
  - *Wire*, *Threema* (w/ recent fixes) also assumed to be secure at this time
  - some based on XMPP with OMEMO or OTR (e.g. *Conversations*)
- Main problem: **meta data** that is not encrypted
  - who communicates with whom, how long, how often, when, message sizes, distribution, etc.
  - General Michael Hayden, former director of the NSA and the CIA: "**We kill people based on metadata**"
- Only few messengers try to address meta data security/privacy
  - *Briar* and *Ricochet* (seems abandoned, newer *Cwtch.im* builds upon it) based on Tor hidden services
  - *Matrix* focuses on federation

Tor:
The Onion Router

- Open Source project for anonymization of Internet communication
- Based on principle of **Onion Routing**
  - initially developed by US Naval Research Laboratory
  - relays communication over (at least) three hops
    - entry Node
    - middle Node(s)
    - exit Node
  - first version published in 2014
- Under active development
  - „The Tor Project“ as organization driving the development
  - supported by Electronic Frontier Foundation (EFF) since 2006
- https://www.torproject.org/

Tor:
The Onion Router



Source: http://video.mit.edu/watch/how-tor-works-502/, copy at https://www.youtube.com/watch?v=jXFOeXcfcfg

Tor Onion (Hidden) Services

- In addition to “tunneling” of conventional TCP connections from clients (behind Tor network) to servers (in “clear net”)
- Servers can create new identity (= public/private key pair) and register it with (randomly selected) node in Tor network
- Instead of typical hostnames (`www.abc.com`), use pseudo-domain with identity based encryption → domain name derived from public key of server identity
  - e.g. SecureDrop for
    The Intercept: `y6xjgkgwj47us5ca.onion`
    New York Times: `nyttips4bmquxfzw.onion`
  - INS webserver:
    `insjku7fnahueqcohvb7z3bpankhfdg6wub4pojw3jgfzo4praocwtid.onion`
- IP address of **server** remains hidden for clients and most relays
  - contrast to “normal” use of Tor: client addresses are anonymized, but server addresses in clear

What the NSA thinks of Tor

TOP SECRET//COMINT// REL FVEY

Tor Stinks... (U)

- 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.

[redacted]

TOP SECRET//COMINT// REL FVEY

Source: http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document

What the JKU thinks of Tor

Home » Services » Relay Search » Details for ins0

Relay Search

193.171

Details for: ins0

Configuration

Nickname
ins0

OR Addresses

```
193.171.202.146:9001
[2001:628:200a:f001:20::146]:9001
```

Contact
Institute of Networks and Security <office@ins.jku.at>

Dir Address
193.171.202.146:9030

Exit Addresses
193.171.202.150

Advertised Bandwidth
21.14 MiB/s

IPv4 Exit Policy Summary

```
accept
  20-23
  43
  53
  79-81
  88
  110
  143
  194
  220
  389
  443
  464
  531
  543-544
  554
  563
  636
```

IPv6 Exit Policy Summary

Properties

Fingerprint

```
01A9258A46E97FF8B2CAC7910577862C14F2C524
```

Uptime
34 days 24 minute and 40 seconds

Flags
Exit Fast Guard HSDir Running Stable V2Dir Valid

Additional Flags
ReachableIPv6 IPv6 Exit

Host Name

```
tor2e.ins.tor.net.eu.org
```

Country
Austria ( )

AS Number
AS1853

AS Name
ACONET

First Seen
2015-10-16 12:00:00 (2 years 315 days 21 hours 38 minutes and 33 seconds)

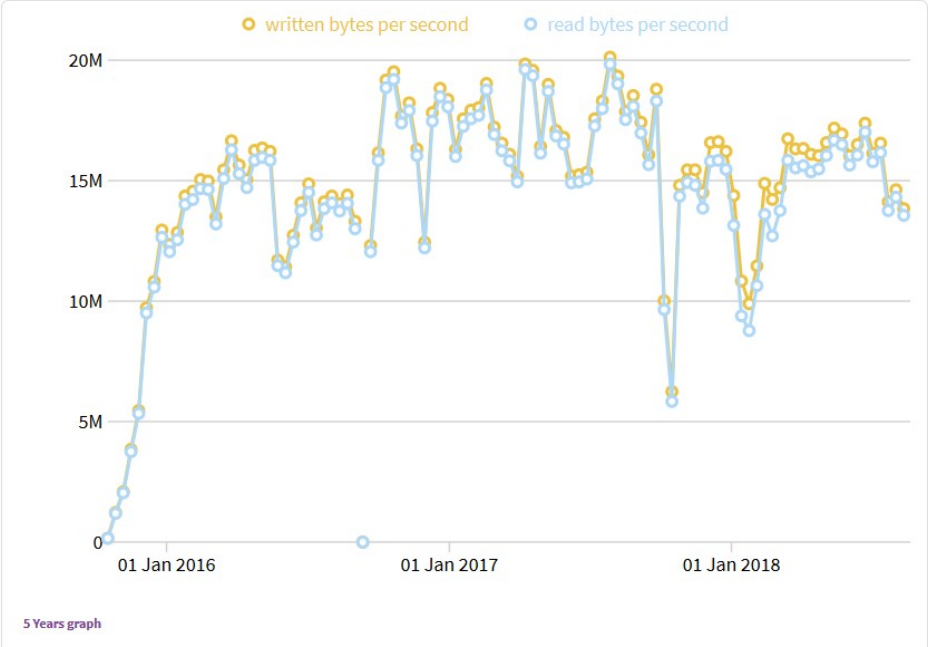
Last Restarted
2018-07-24 09:13:53

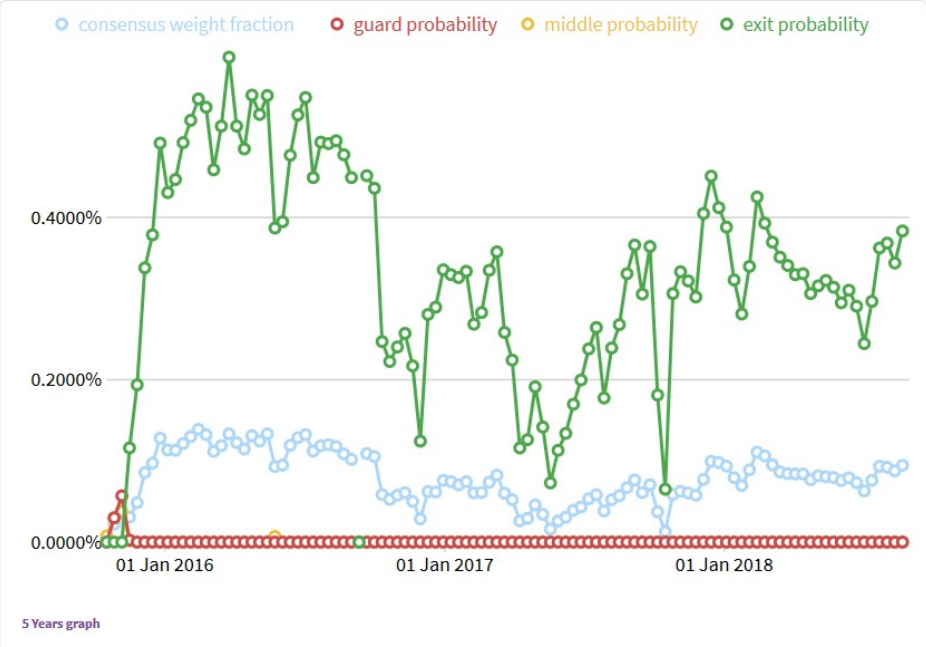
Consensus Weight
44000

Platform
Tor 0.3.3.6 on Linux

https://metrics.torproject.org/rs.html#details/01A9258A46E97FF8B2CAC7910577862C14F2C524

What the JKU thinks of Tor





Example:
Privacy in mobile apps

- Apps usually have access to many data sources on the device
- Permissions are one tool to restrict leaks, but often hard to understand for users (and developers)
  - over-requesting of permissions
  - over-granting of permissions
  - dark patterns to get users to grant permissions unnecessarily
- Access to sensitive data increasingly restricted on major platforms (Android, iOS)
  - interesting/hard problem is closing side channels
    - e.g. EXIF data in pictures abused to get location
    - e.g. MAC address of WiFi routers for location, of device for fingerprinting
    - e.g. accelerometer calibration matrix for device fingerprinting
  - trade-offs are hard
    - BLE scanning requires `location` permission?
    - extremely powerful/abuse-able APIs for accessibility

Responsibility

- „Code is Law“ (Lawrence Lessig)
  - soft- and hardware design defines possibilities
  - legal and social norms often need (a lot of) time for development
- New challenges due to “smart” things
  - challenge of implicit interaction
  - challenge of sensor data
  - challenge of “privacy affordances”
- Who is responsible for these developments?

Optional Reading List

- Edward Snowden: “Permanent Record”
- David Chaum: “Security without Identification - Card Computers to make Big Brother Obsolete”, Communications of the ACM, vol. 28 no. 10, October 1985 pp. 1030-1044
  https://www.chaum.com/publications/Security_Wthout_Identification.html
- “P3P”
  [M. Langheinrich: “A Privacy Awareness System for Ubiquitous Computing Environments”, Ubicomp 2002]
- John Krumm (Microsoft Research, US): Inference Attacks on Location Tracks, Pervasive 2007
- Glenn Greenwald: **Why privacy matters** -
  http://www.ted.com/talks/glenn_greenwald_why_privacy_matters