Free Software for Privacy

Christian Grothoff
christian@grothoff.org

The GNUnet Project

Overview

What is privacy?

Why do we need it?

How can we get it?

Challenges

Free Software

Definition:

Free Software gives individuals control over their computing.

Free Software

Definition:

Free Software gives individuals
control over their computing.

Axiom:

Society must control its essential functions,
not private interests.

Privacy

Definition:

Free Software gives individuals
control over their computing.

Definition:

Privacy means individuals are in control
of how their personal data is used.

Privacy and Free Software

Corrolary:

Privacy-enhancing software must be free.

Controlling Information

- Confidentiality
- Integrity
- Availability

Confidentiality

- Data (storage, transmission)

  $\Rightarrow$ Encryption (OpenSSL, gnuTLS, GnuPG, ...)

- Actors (identity)

  $\Rightarrow$ Anonymization

Overview

What is privacy?

Why do we need it?

How do we get it?

Challenges

Good People Need Anonymity[1]

Private Citizens: Privacy

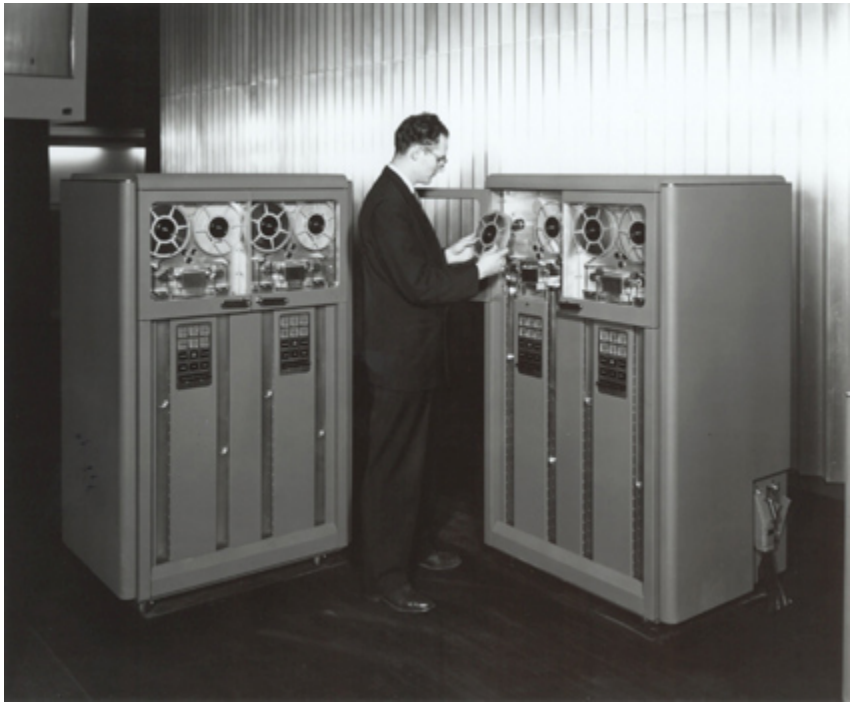
Blocked Users: Reachability

Businesses: Network Security

Governments: Traffic-Analysis Resistance

[1] Thanks to Roger Dingledine.

IBM 726 (1952)



6.1kB/s, 2.3 MB, $850/month ($ 6,775/month inflation adjusted)

IBM TS1130 (2008)

160,000 kB/s, 1,000,000 MB, $11,700 (eBay)

Data Today

- Data does not go away, lives “forever”, instantly accessable to many people
- More expensive to delete data then to retain it

Never Forgetting is a Curse

- Data incorrectly captured
- Data no longer relevant
- Data taken out of context
- Expectations in society change

  $\Rightarrow$ Acceptable today, unaccepatable tomorrow!

Examples

- "Nationwide fined £980,000 over stolen laptop — Details on 11 million customers went awol" (The Register, 14.2.2007)
- "Stolen identities going cheap — access to a bank account was going for $10 (US)" (The Age, 8.4.2008)

Examples

- "1.7 Million Canadians Are Victims of Identity Fraud — Victims spend more than 20 million hours and more than $150 million of their own money to resolve the fraud" (Newswise, 17.11.2008)
- "The Cost of ID Theft — business losses per victim increase (...) to $49,254" (Technology News, 6.2.2008)
- "Security Breaches Cost $90 To $305 Per Lost Record" (InformationWeek, 11.4.2007)

Examples

- "How To (Legally) Spy On Employees" (Forbes, 25.10.2006)
- "UBS claims naming tax evaders would break law" (Times Online, 1.5.2009)

Examples

- "Surveillance warrants? Nah, far too tricky, we don't bother with them — A (Republican) in charge of US Attorney General's Office" (Telecom TV, 30.4.2009)
- "In 2008, two instances were reported of encryptions encountered during state wiretaps; neither prevented officials from obtaining the plain text of the communications." (US 2008 Wiretap Report)

Overview

What is privacy?

Why do we need it?

How do we get it?

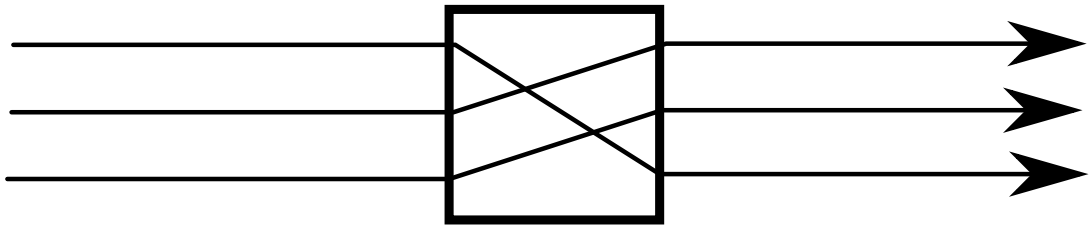
Challenges

Anonymization Techniques

- Mix Cascades
- Onion Routing

Mixing

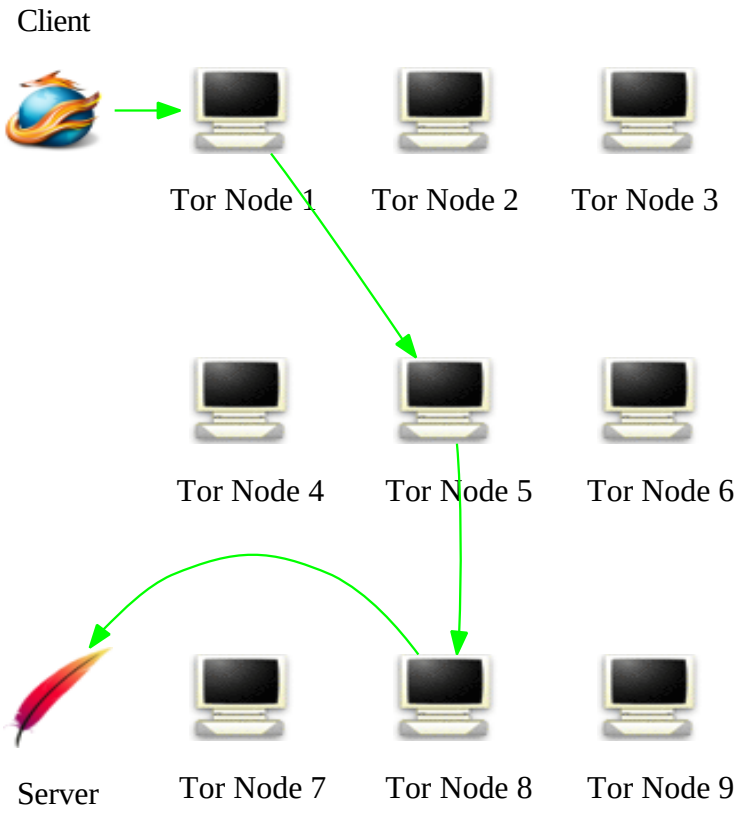
David Chaum's mix (1981) and cascades of mixes are the traditional basis for destroying linkability:



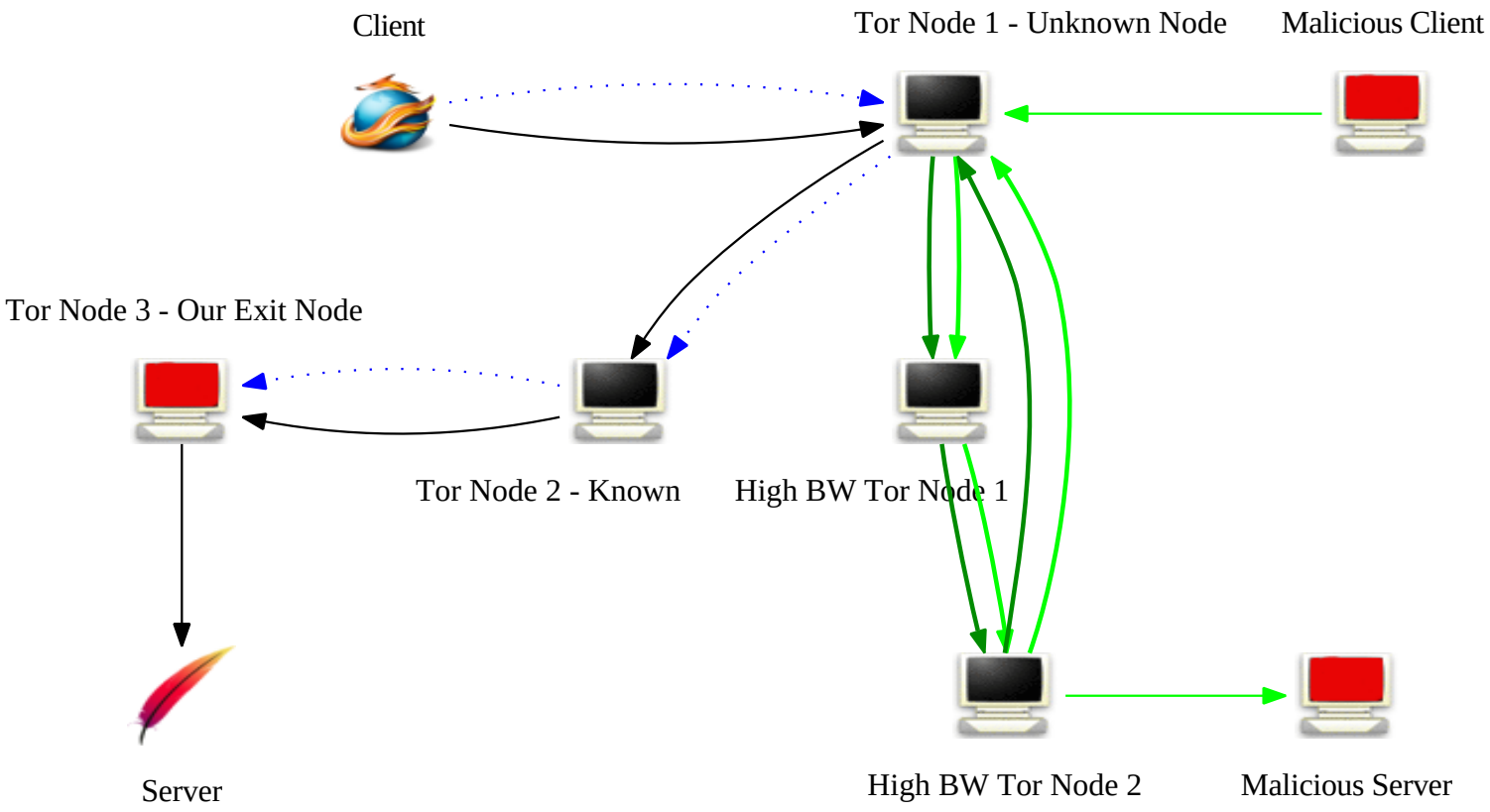
Mixing

David Chaum's mix (1981) and cascades of mixes are the traditional basis for destroying linkability:

Onion Routing (in Tor)



Problems with Onion Routing[2]



[2]Will be presented at USENIX Security 2009.

Privacy-enhancing Free Software

- Tor
- Mixminion
- I2P
- GNUnet

GNUnet Technical Philosophy

- Completely decentralized, open network with malicious participants
- Use “secure” defaults, allow individuals to trade performance for security
- Privacy requires company; enable many applications
- Overall, we are not building a prototype for research

Consequences for GNUnet

- Difficult technical problems
  $\Rightarrow$ slow progress
- Relatively steep learning curve for end-users
  $\Rightarrow$ small userbase
- Need more than file-sharing for a "framework"
- Backwards-compatibility is a goal, not a dogma
  $\Rightarrow$ 0.9.x peers will not work with 0.8.x

Overview

What is privacy?

Why do we need it?

How do we get it?

Challenges

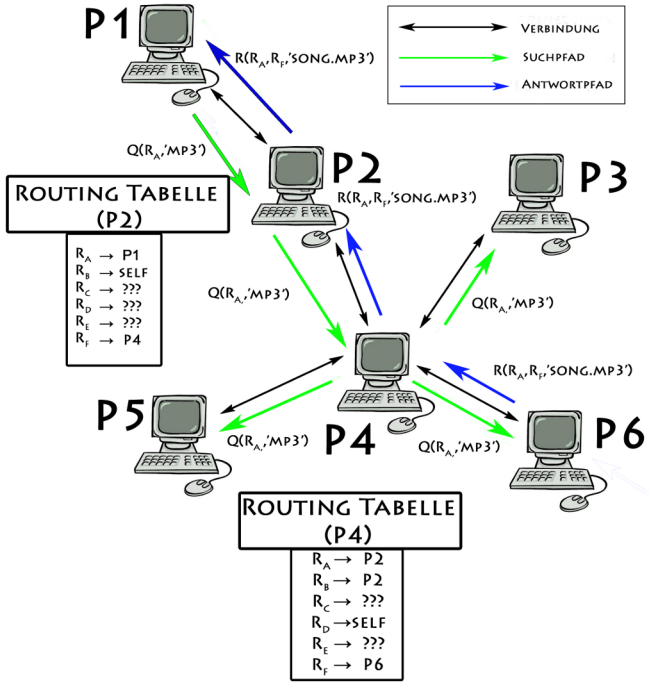
Challenges

- Technical challenges
- Political / Legal challenges
- Social challenges

Technical challenges: Free Software ⇒ Good Software?

- Stealthnet is free software
- CRISP spent ≈ 1 month to analyze

  ⇒ Deanonymized users
- Anonymization is tricky!
- PETs need academic review



Political challenges: Hot Button Issues

Polititical challenges: Data Retention Laws

Directive 2006/24/EC requires providers to retain:

- the source of a communication
- the destination of a communication
- the date, time and duration of a communication
- the type of communication
- the communication device
- the location of mobile communication equipment

$\Rightarrow$ Make sure this information is plentiful and useless.

Polititical challenges: Key Escrow

Political fight for privacy is not just about anonymity anymore:

- Bad Idea in the 90's
- US: back for suitcases!
- UK: encryption key disclosure

Social challenges: Security (1/2)

Lemma:

Good security is more costly and harder to understand and deploy than bad security.

Theorem:

Insecure solutions will continue to be used in capitalistic or democratic societies.

Social challenges: Security (2/2)

Lemma:

If privacy seems to burdensome, temptation to minimize or ignore privacy issues arises.

Social challenges: Volunteers & Abuse

Helping others to remain anonymous can be hazardous:

- Tor exit relays are seen (and prosecuted) as attackers

  $\Rightarrow$ Ideally, we do not have exit relays

- Wiretapping is illegal for non-Republicans (in US), logging is required (in EU)

  $\Rightarrow$ Impossible to abide by all laws

Social challenges: Availability

In France, users caught downloading "illegal" content will:

1. Receive an e-mail warning
2. Receive a written warning
3. Be cut off for a year

A Few Words on Copyright

Popular Culture and Copyright (1/3)

	Art	Software
Before Copyright	Folklore	Hacker culture

Popular Culture and Copyright (2/3)

	Art	Software
Before Copyright	Folklore	Hacker culture
With Copyright	Mass communication Media culture	Helpless users

Popular Culture and Copyright (3/3)

	Art	Software
Before Copyright	Folklore	Hacker culture
With Copyright	Mass communication Media culture	Helpless users
After Copyright	Mass collaboration	Free software

Privacy and Copyright (1/3)[3]

To a computer, facts about me (such as health data with privacy concerns) and copyrighted material are both just data.

Both copyright enforcers and privacy advocates share the same technical problem:

data is out of control

[3]Thanks to Johnathan Zittrain.

Privacy and Copyright (2/3)

The protection methods are fundamentally different:

Concern	Method	Controlled by	Licensing
Copyright	DRM	Data's distributor	Proprietary
Privacy	PET	Who the data is about	free software

Privacy and Copyright (3/3)

Why should we care about free software and PETs?

- Regain control over *our* private data
- Transcend the `ro`-culture and enable creativity (`rw`)

Activities

Human Consider implications of disclosing personal data

Internet-User Learn to use PETs, start with Tor

Developer Contribute to free software projects for privacy

Philosopher Develop guidelines for using data

Conclusion

Privacy is a hard problem

- Critical to modern society

  $\Rightarrow$ Solutions need to be free

- Affects everyone

  $\Rightarrow$ Should you really be using social network sites?

RTFL

Copyright (C) 2009 Christian Grothoff

Verbatim copying and distribution of this entire article is permitted in any medium, provided this notice is preserved.