Tor Research and Development

Andrew Lewman
andrew@torproject.org

November 4, 2009

TorProject.org

The Tor Project, Inc.

501(c)(3) non-profit organization dedicated to the research and development of technologies for online anonymity and privacy

What is Tor?

- online anonymity software and network

What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)

What is Tor?

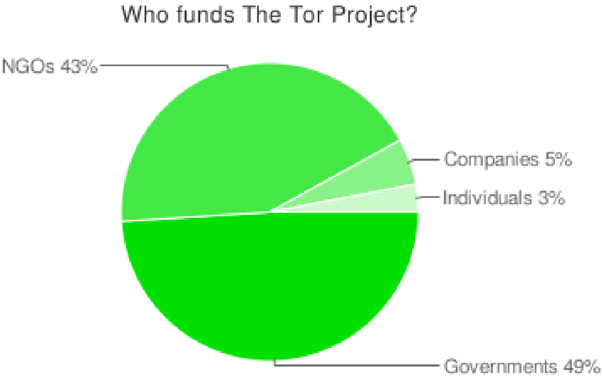
- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston U, Harvard, MIT, RPI, GaTech

What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston U, Harvard, MIT, RPI, GaTech
- increasingly diverse toolset:
  Tor, Torbutton, Tor Browser Bundle, TorVM, Incognito LiveCD, Tor Weather, Tor auto-responder, Secure Updater, Orbot, TorFox, Torora, Portable Tor, Tor Check, Arm, Nymble, Tor Control, Tor Wall

estimated 300,000 daily users

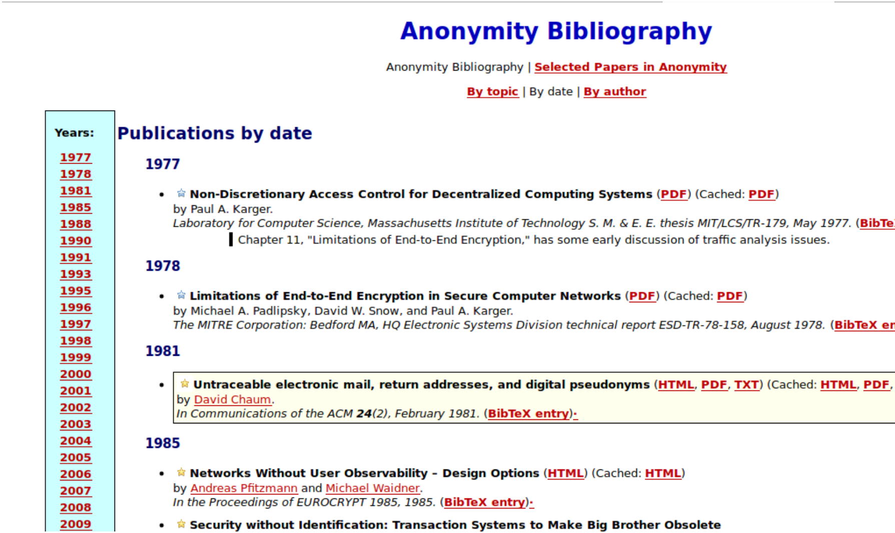
Who funds Tor?



Who uses Tor?

- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims

http://freehaven.net/anonbib/



Anonymity Bibliography

Anonymity Bibliography | **Selected Papers in Anonymity**

By topic | By date | **By author**

Years:

1977
1978
1981
1985
1988
1990
1991
1993
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009

Publications by date

1977

- ☆ **Non-Discretionary Access Control for Decentralized Computing Systems** (**PDF**) (Cached: **PDF**)
  by Paul A. Karger.
  Laboratory for Computer Science, Massachusetts Institute of Technology S. M. & E. E. thesis MIT/LCS/TR-179, May 1977. (**BibTe**

  Chapter 11, "Limitations of End-to-End Encryption," has some early discussion of traffic analysis issues.

1978

- ☆ **Limitations of End-to-End Encryption in Secure Computer Networks** (**PDF**) (Cached: **PDF**)
  by Michael A. Padlipsky, David W. Snow, and Paul A. Karger.
  The MITRE Corporation: Bedford MA, HQ Electronic Systems Division technical report ESD-TR-78-158, August 1978. (**BibTeX er**

1981

- ☆ **Untraceable electronic mail, return addresses, and digital pseudonyms** (**HTML**, **PDF**, **TXT**) (Cached: **HTML**, **PDF**,
  by David Chaum.
  In Communications of the ACM ***24****(2), February 1981.* (**BibTeX entry**)·

1985

- ☆ **Networks Without User Observability – Design Options** (**HTML**) (Cached: **HTML**)
  by Andreas Pfitzmann and Michael Waidner.
  In the Proceedings of EUROCRYPT 1985, 1985. (**BibTeX entry**)·
- ☆ **Security without Identification: Transaction Systems to Make Big Brother Obsolete**

Performance

- Circuit Latency
- Relay capacity estimation
- bandwidth authorities
- cell sizing

Metrics

- Measuring metrics anonymously

Metrics

- Measuring metrics anonymously
- NSF grant to find out

Metrics

- Measuring metrics anonymously
- NSF grant to find out
- Metrics portal: `https://www.torproject.org/projects/metrics`

Bridge Distribution Strategies

- Websites, email, social media tools are working well.

Bridge Distribution Strategies

- Websites, email, social media tools are working well.
  - bridges@torproject.org
  - https://bridges.torproject.org
  - Twitter, QQ, Wordpress Plugin

Bridge Distribution Strategies

- Websites, email, social media tools are working well.
    - bridges@torproject.org
    - https://bridges.torproject.org
    - Twitter, QQ, Wordpress Plugin
- Bootstrapping problem.

Censorship Resistance

- Theoretical blocking strategies from the censors?

Censorship Resistance

- Theoretical blocking strategies from the censors?
  (Cryptographers can dream up some pretty fancy strategies)

Censorship Resistance

- Theoretical blocking strategies from the censors?
  (Cryptographers can dream up some pretty fancy strategies)
- Applied blocking to date

Censorship Resistance

- Theoretical blocking strategies from the censors? (Cryptographers can dream up some pretty fancy strategies)
- Applied blocking to date
  - dns blocking
  - ip address blocking
  - blocking or throttling all SSL

Censorship Resistance

- Theoretical blocking strategies from the censors?
  (Cryptographers can dream up some pretty fancy strategies)
- Applied blocking to date
  - dns blocking
  - ip address blocking
  - blocking or throttling all SSL
- Blocking resistant strategies

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my....

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my.... some call this "sharing"

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my.... some call this "sharing"
- Did you know Microsoft Word and OpenOffice Writer are browsers?

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my.... some call this "sharing"
- Did you know Microsoft Word and OpenOffice Writer are browsers?
- `http://www.decloak.net/` is a fine test

Mobile Operating Systems

- Entirely new set of challenges for something designed to know where you are

Mobile Operating Systems

- Entirely new set of challenges for something designed to know where you are
- Orbot: Tor on Android. `http://openideals.com/2009/10/22/orbot-proxy/`

Mobile Operating Systems

- Entirely new set of challenges for something designed to know where you are
- Orbot: Tor on Android. `http://openideals.com/2009/10/22/orbot-proxy/`
- iphone, maemo, symbian, etc

Mobile Operating Systems

- Entirely new set of challenges for something designed to know where you are
- Orbot: Tor on Android. `http://openideals.com/2009/10/22/orbot-proxy/`
- iphone, maemo, symbian, etc
- Tor on Windows CE, `http://www.gsmk.de` as an example.

Anonymity Online Research

or attacks galore

- Website fingerprinting attacks

Anonymity Online Research

or attacks galore

- Website fingerprinting attacks
- Traffic confirmation attacks

Anonymity Online Research

or attacks galore

- Website fingerprinting attacks
- Traffic confirmation attacks
- Timing attacks

Anonymity Online Research

or attacks galore

- Website fingerprinting attacks
- Traffic confirmation attacks
- Timing attacks
- Routing zones/Autonomous System attacks

Anonymity Online Research

or attacks galore

- Website fingerprinting attacks
- Traffic confirmation attacks
- Timing attacks
- Routing zones/Autonomous System attacks
- Denial of Service resistance

Anonymity Online Research

or attacks galore

- Website fingerprinting attacks
- Traffic confirmation attacks
- Timing attacks
- Routing zones/Autonomous System attacks
- Denial of Service resistance
- Parititioning/DHT/Shared Consensus Attacks

Next steps

Visit `https://www.torproject.org/volunteer#Research` for more information, links, and ideas.

Credits & Thanks

- who uses tor? `http://www.flickr.com/photos/mattw/2336507468/siz`, Matt Westervelt, CC-BY-SA.
- danger!, `http://flickr.com/photos/hmvh/58185411/sizes/o/`, hmvh, CC-BY-SA.
- 300k, `http://www.flickr.com/photos/lukaskracic/334850378/sizes/l/`, Luka Skracic, used with permission.