The Onion Router

A brief introduction and legal aspects

by Alexander „Yalla“ Janßen <alexander.janssen@gmail.com> for the Linuxbierwanderung 2007

Rules, Disclaimer and mini-NDA

- IANAL
- Talk might be biased
- No mobile phones please
- There‘re some aspects in the talk related to ongoing investigations – keep that to yourself, e.g. no blogging, gossip or whatsoever
- Questions are always welcome, however, I‘ll give lots of time for questions after the presentation
- Time needed for presentation: ~20 minutes
- Time available for questions: ~40 minutes

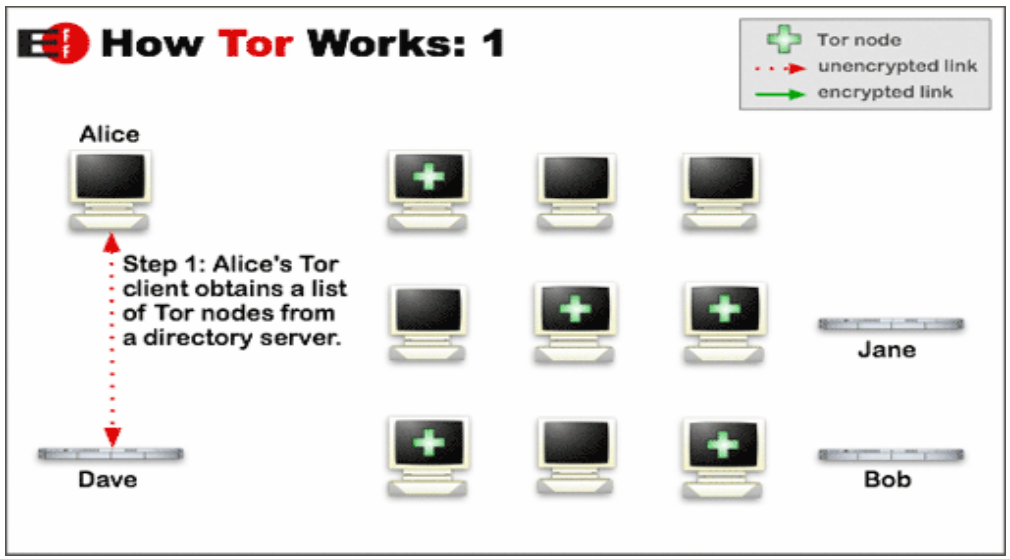
Agenda

1. Brief technical introduction to Tor
2. Discussion of Tor‘s limitations
3. Why should we use anonymising networks
4. What are the legal implications for users and Tor-operators
5. Questions and answers

Section 1: What is Tor?

- Tor is a low-latency anonymizing network run by volunteers
- There‘s a single software available for all major platforms which does client- and server function – just the configuration is different
- Tor obfuscates the client‘s IP-address by shuffling the payload through three different Tor-nodes
- Tor encrypts all data in between the nodes, just the last connection to the destination is unencrypted
- The Tor-client function offers a generic SOCKS-proxy (v4, v4a, v5) so that Tor can be used on generic TCP-/UDP-traffic

Tor in brief – 1/3



Step 1: Alice‘s Tor client obtains a list of Tor nodes from a directory server

Fig. 1: How Tor Works 1 – Picture courtesy of the EFF

Tor in brief – 2/3

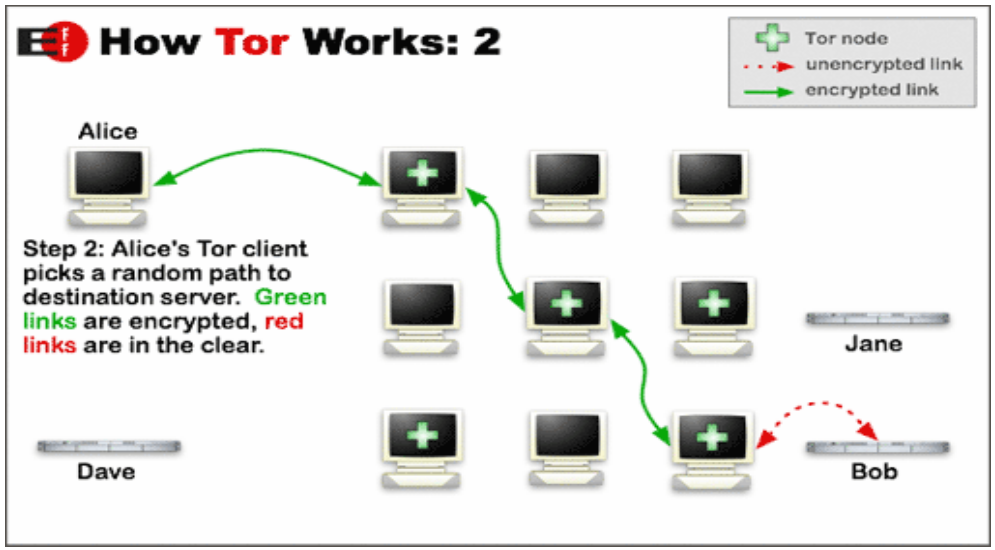


Fig. 2: How Tor Works 2 – Picture courtesy of the EFF

Step 2: Alice‘s Tor client picks a random path to destination Server. Green links are encrypted, red links are in the clear.

Tor in brief – 3/3

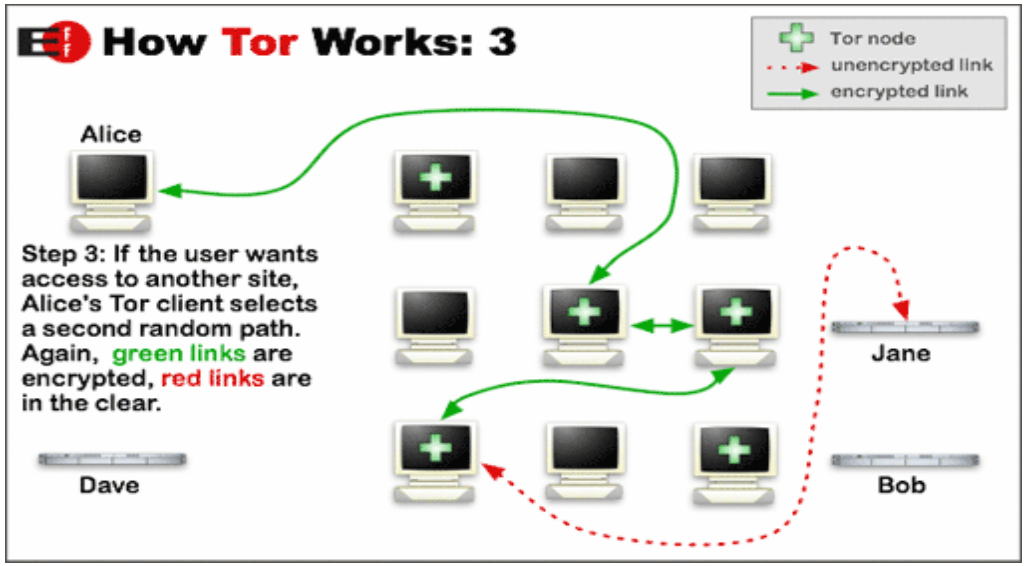


Fig. 3: How Tor Works 3 – Picture courtesy of the EFF

Step 3: If the user wants access to another site, Alice‘s Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

List of Tor-functions

- **Dirserver** – contains a list of all accessible Tor-router on the interweb and their functions: Only a few, run by the EFF, accepted as being „trustworthy“, fingerprint of public key hardcoded in the Tor distribution -> *the most vulnerable nodes in the network in general*.
- **Entry-node** – any Tor-node on the interweb which accepts initial requests from clients: Can be any node which accepts inbound requests (== has an appropriate set of access control lists)
- **Middleman-node** – any Tor-node which takes data from an entry node, forwarding it to an Exit-node
- **Exit-node** – a Tor-node which is the last node in the chain: The encryption is broken here, the request is sent out in the clear to the real destination. It‘s IP-address shows up in logfiles -> *the most dangerous function from an operator‘s point of view*
- **Local client** – not a Tor-node, but the Tor-software running in client-mode only, forwarding requests to an Entry-node: The user‘s access-point to the Tor-network
- Other more bizarre functions exist, but are not covered here

Section 2: Tor‘s limitations

Short reminder what Tor does:

- Obfuscate the IP-address
- Offers a SOCKS-interface to the user
- Connects the different Tor-nodes
- Does not write logfiles

What Tor doesn‘t do for you

- Deal with trojans, virii, malware or whatever you download from the internet
- Protect you from Flash, Java, Javascript which ignore the proxy-settings, resulting in information leakage
- DNS-lookups are done by the libc‘s resolver library, which doesn‘t use Tor -> DNS information leakage
- Protect you from MITM-attacks – in fact, Tor is quite heavily misued for ssh MITM-attacks, advertisement-injection into HTML
- It can‘t protect you from rogue Tor-nodes which have compromised/modified nodes which wiretap or write logfiles
- Prevent PEBKAC/user-errors
- Protect your identity if you sign up with your real-name or regular accounts if you use Tor -> very stupid idea!

Solutions to the problems

- Trojans, virii, malware: Use appropriate third-party software like virus-scanners, rootkit-checkers and use your common sense (checking md5sums of downloaded packages, verify signature)
- Information-leakage from Flash, Java, Javascript: Use flashblock, tell Java in general to use a proxy, use Privoxy (a http-proxy with lot‘s of privacy-options)
- DNS-leakage: Use SOCKS v4a or v5 – for applications which aren‘t SOCKS-enabled use „socksify“ or „torify“ wrappers
- MITM-attacks: For ssh check for stranges warnings about „the hosts‘s key has changed“. For http: Nothing you could do there, except using https and check the certificate. For generic programs: YMMV
- Rogue Tor-nodes: Check the mailing-list regulary for warnings about certain Tor-nodes and put them on your local shitlist – not much what you can do there except waiting for a new concept made up by the developers and researchers. Suffers from the usual „only run trusted code“-problem
- PEBKAC/user-errors: Educate your users. RTFM. Think before you do something. Spread the word. Write documentation suitable for (l)users
- Identity protection: Only you can make sure that you don‘t sign up or login to webpages with your real identity.

Section 3: Anonymity? Why that? (1/2)

- „I have nothing to hide, so I have nothing to fear“

  >> so you really want your employer, wife, government, competitors to know what websites you visit, what sexual orientation you have, with whom you‘re communicating, which Wikipedia-entrys you‘re reading and what colour the cockring had you recently bought in a webshop?

- „Anonymity is bad because if supports terrorists, pedophiles, criminals, Linux-commie-faggots, <insert evildoer du jour>“

  >> Terrorists and criminals have other ways to gain anonymity, and if it‘s identity theft. Pedophiles also have other means of getting their pornography and cracking down on anonymization only really hurts ordinary people who have a million valid reasons to remain anonymous and not criminals. And it wouldn‘t help the children either, cause the real abuse continues.
  You wouldn‘t shut down American Airlines cause they gave terrorists the opportunity to hijack a plane and crash it into a building? You wouldn‘t shut down UPS or TNT for transporting letter-bombs?
  Unless you‘re a crackpot and would.

Anonymity? Why that? (2/2)

- „No one needs anonymity, I feel safe“
  >> Did you ever read the news and heard about information-leackage after compromised servers? The whole point about your privacy on the internet is self-discipline: Keep a low profile and don‘t leave a trail. Think about it. Everything might be used against you.

- „Who wants to know about my personal data anyway? I‘m not an interesting person“
  >> Complete customer profiles of people are worth hard money. Companies, market-research organisations, the government, Scientology and also criminals are interested in every piece of information about you which is accessible by all means. Legal or illegal.

- „It‘s not worth the hassle“
  >> You should reread this presentation.

- „Your arguments suck.“
  >> I don‘t care at all.

Section 4: Legal implications for Tor-operators and users (1/2)

The general situation:

- In most western countries anonymity is not illegal, but also not explicitely mandatory a/o written down in the privacy-laws (if there‘re any)
- The Tor-software basically does routing and the Tor-operator might count as a „carrier“ in the future which would force him to disclose his user-base if the police or secret service asks for logfiles or assistance.
- If that‘s the case you might be forced to install an ETSI-compatible wiretapping interface („Lawful Interception Point“) and do extensive logging – however, this totally contradicts with the nature and purpose of Tor
- Germany has a so called „Störerparagraph“ – if you run a webforum for instance and one of the users publishes a posting in that forum and makes illegal statements – like lies about a product, spreading untrue rumours to damage someone‘s reputation and such – you as the Administrator have to remove the posting immediately.
  In the future this law might be abused to shut down Tor-nodes a/o putting pressure on a certain person although this might not be related to Tor.

Legal implications for Tor-operators and users (2/2)

- People just looking at the IP-address might sue you for actions which went over your Exit-node. This might lead to very bizarre and dangerous situations which will be discussed later.
- Running a Tor-node might be suspicious, especially if you‘re politically „incorrect“ or otherwise involved in „infamous“ organisations – there‘s one known case of a german Tor-operator who‘s under surveillance of some secret service, but the Bundesrepublik Deutschland refuses to hand over details because it might „endanger Germany‘s national security“
- The builtin encryption-functions might be illegal in some countries to import, export, posses, use.
- Offering anonymisation to people in certain countries might be illegal as well

Possible threats per function (1/2)

- Tor-client:
  Outgoing Tor-reqests might be suspicious. There‘s not much you could do except tunneling Tor-traffic through ssh to a Tor-client software running elsewhere. However, if you‘re really under observation that probably won‘t help.
- Tor Entry-node:
  Since you enable users to access the Tor-network some countries with „flexible legislation“ might accuse you of supporting <insert criminal action here>
- Tor Middleman-node:
  Not sure, I never really investigated about that. Suggestions?

Possible threats per function (2/2)

Tor Exit-node:

Possibly the most dangerous thing you can do if you get involved in Tor.
Possible threats (checked if already happened):

- Nastygrams from LEAs – ☑
- Visit from the LEAs – ☑
- Total observation of your house, car, spouse, communication – ☑
- Confiscation of your hardware – ☑
- Arrest – TBD
- Conviction for supporting `$something` - TBD
- Ultimately: „Killed while resisting arrest“ – Hopefully that‘ll never happen!

Hints for Tor-operators

- With the words of Udo Vetter: „You have the right to remain silent. Use it.“
- If a nastygram doesn‘t tell you if you‘re a witness or a suspect, consult a lawyer
- If they raid your house, be sure that they have the correct order from a court/lawyer of the state. Get a witness who‘ll overlook the search. Get a protocol what was searched by whom, for what reason, by whom it was ordered and what was confiscated.
- CALL YOUR LAWYER.
- If you get arrested, think hard if you really don‘t want to remain silent.
- CALL YOUR LAWYER.
- If they arrest you, be sure to take some money with you to pay a Taxi back to your home. They usually don‘t drive you home.
- CALL YOUR LAWYER.

When erverything went wrong:

- CALL YOUR LAWYER.
- Keep a low profile until you know if the state will file suit or not.
- Let your lawyer inform the press. Avoid blog-whoring until you‘re not absolutely sure you‘re safe.
- Sue for compensation if applicable.
- Contact the EFF, FÖBUD, your local civil-rights group
- Protect your family by all means.
  („OMG! There‘s a pedophile living in my neighborhood says the ‚Sun‘!!!“)
- If you got arrested, think about consulting a therapist/psychatrist. Getting arrested can cause a hidden trauma which could show up later.
- Cross your fingers, good luck, you need it.
- If you‘re at the end of your civil courage: Ultimately shut down your Tor-server to protect your family and yourself.

EOF

Thanks for listening.
Thanks to my wife for all the patience, support and understanding.
Thanks to my lawyer Dr. Michael Stehmann.
Thanks to the EFF for this wonderful piece of software.
To all you data-whores out there: Screw you.

Questions?

References:
The Onion Router – http://tor.eff.org
Various poastings about Tor by myself: http://itnomad.wordpress.com/tag/tor/

Figures 1 – 3 courtesy by the EFF.