Deanonymizing Tor – Aktuelle Angriffe auf das Tor-Netzwerk

Markus Zeilinger

OCG Jahrestagung 2015, Workshop Security & Privacy
Why Tor?

How Tor works, Tor Hidden Services

Tor Stats

Is Tor secure (to use)?

More details ...

What to do?
Privacy matters!
- Encryption (confidentiality) is not guarding against all kinds of passive attacks!

Tor is a low latency anonymization tool using onion routing.
- First of all developed by the U.S. Naval Research Laboratory!

Tor offers protection against traffic analysis (TA)
- Who is talking to whom, when, how long, how often, ...
- TA allows tracking of user behavior, interests, activities, ...

Tor hidden services allow users to provide a service without revealing its location/IP address (responder anonymity).

Tor allows censorship circumvention.
1. Alice gets a list of available Tor nodes.

2. Alice selects 3 nodes and builds a Tor circuit (establishing unique shared keys $E_{\text{entry}}$, $E_{\text{middle}}$ and $E_{\text{exit}}$).

3. Alice relays messages $M$ through the circuit in several encrypted layers built on the unique shared keys $E_{\text{entry}}$, $E_{\text{middle}}$ and $E_{\text{exit}}$.

Source: Dingledine et al., Tor: The 2nd-Generation Onion Router, USENIX 2004
1. Bob selects relays as introduction points and builds Tor circuits there.

2. Bob publishes IPos, .onion-URL, ... to the lookup DB.

3. Alice learns about the service and gets more information (IPos, public key, ...) from the lookup DB.

4. Alice selects relay as rendezvous point and builds Tor circuit there. She places a random rendezvous cookie for Bob.

5. Alice builds a Tor circuit to one of Bob's IPos and tells Bob about herself, her RP and the cookie.

6. Bob builds a Tor circuit to Alice's RP and sends the cookie. Alice and Bob now communicate anonymously through Alice's RP.

Source: Dingledine et al., Tor: The 2nd-Generation Onion Router, USENIX 2004
Tor Stats

Number of relays

Aktuell ~ 6500 ORs

August 2014?

Number of relays with relay flags assigned

Source: https://metrics.torproject.org/
Is Tor secure (to use)?

- 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.

Tor Stinks... (H)

- (S/REL) Open Source Multi-Hop Networks
  - (S/REL) Tor
  - (S/REL) Very widely used worldwide
  - (S/REL) Open Source
    - (S/REL) Active Development
    - (S/REL) Mitigates Threats
  - (S/REL) Very Secure
  - (S/REL) Still the King of high secure, low latency Internet Anonymity
    - (S/REL) There are no contenders for the throne in waiting

Why was the Black Hat talk on Tor de-anonymization mysteriously canceled?

The Washington Post

By Richard A?$
Aug 1, 2014 4:21 PM PT

Forbes

Global law enforcement conducted a massive raid of the Dark Web this week. It started with the FBI takedown of Silk Road 2.0 and the arrest of its alleged operator Blake Renthall in San Francisco on Wednesday. But it quickly exploded from there, as European counterparts seized over 400 black market "hidden sites" and arrested 19 other people alleged to be involved in their operation.

Wired called it "a scorched-earth purge of the Internet underground." But how exactly did law enforcement take their digital blow torches to the Dark Web sites that were using Tor anonymity software to protect themselves? Law enforcement has been mysterious on that count, saying it won't reveal its methods because they are "sensitive."

Tor Has Been Breached - What Now?

An attack on Tor, a network designed to cloak users in anonymity, resulted in a breach that caused the project team to scramble for a solution. The Carnegie Mellon researchers who figured out how to de-anonymize users of the network have been suspected of working hand-in-hand with the NSA, but that's unlikely. If the government had learned how to identify Tor users, why wouldn't they announce the fact?
Tor is abused for (cyber) crime (hiding the bad guys)
  - E. g. Silk Road, Botnets (Sefnit), child pornography, ...

Tor’s security heavily depends on the number of relays and users.

Tor relays/directory servers can be blocked for censorship reasons.

Tor is by concept vulnerable to several attacks like end-to-end correlation, malicious (entry/exit) relays, Sibyl attacks, and more.

You can get in trouble with the law when running a Tor exit node!

Tor is not a cure-all solution!
Winter, P., et al., Spoiled Onions: Exposing Malicious Tor Exit Relays, PETS 2014

- Tor exit relays forward user traffic to the destination (end-to-end encryption is strongly recommended).

- Malicious exit relays can do several attacks like sniffing, TLS MitM, SSLstrip, ...

- Winter et al. found 40 exit relays doing active attacks like TLS MitM or SSLstrip and 27 exit relays doing passive sniffing of login data (2 exit relays appeared in both lists).

- Tor is actively looking for malicious relays and voting these relays out of the directory authorities!
An Attacker who can observe traffic entering (entry node) and leaving (exit node) the Tor network, can do correlation based on e. g. timing, volume, ...

Nations state attacker or strong group of cyber criminals.

Long known problem and long history of research
- Levine, et al., „Timing Attacks in Low-Latency Mix-Based Systems“, 2004
- Murdoch & Zielinski, „Sampled TA by IX-Level Adversaries“, 2007

July 2014: Several malicious relays (guard and exit relays) were discovered doing traffic confirmation (= correlation) by injecting signals into the Tor network and looking for these signals at the end of the circuits.
- Goal: Identifying users using hidden services
Chakravarty et al. uses NetFlow sampling for correlation and were able to achieve 81.4% accuracy with 6.4% false positive rate in real-world experiments.

- FPR 6.4% (base rate fallacy) leaves a lot of work to do!
Censorship circumvention

- Tor on one hand can be used to **circumvent state-based censorship** measures (e.g. blocking certain websites like Facebook, Google, ...).

- Tor on the other hand can be "easily" blocked (blocking known directory authorities, relays, DPI, ...).
  - Solution: Tor bridges (publicly unknown relays) + Pluggable transports

- Current research/surveys/talks
  - Winter, Measuring and circumventing Internet censorship, PhD, 2014
  - Dingledine & Applebaum, How governments have tried to block Tor, 28C3, 2011
Should we still use Tor? => YES!
- Don’t be afraid of the NSA, be afraid of the guy next-door!

HOW to use it is important!
- End-to-end encryption
- No personal (login) data
- Use tools like Tor Browser, Tails, ...
- Be careful with active technologies (e.g. Java, Flash) and P2P/Torrent!

Certain problems with Tor remain (e.g. end-to-end correlation), future research is necessary!

And finally ... privacy matters!
„I do not want to live in a world where everything I do and say is recorded.

That is not something I am willing to support or live under.“

Danke für Ihr Interesse!