TOP SECRET // COMINT // REL TO USA, AUS, CAN, GBR, NZL

# Roger Dingledine at NSA NOV 2007

From PE

Contents

## (U) Talk by Roger Dingledine at NSA, 11/01/2007 at R&E (Sponsored by NSA RT)

(U) Roger Dingledine, now of Torproject.org, was one of the principle inventors or TOR. Current usage statistics quoted are 200K users and 1K servers. When asked about trends, he had no concrete data - Being a non-profit open-source effort, the collector of statistics has not been active recently.

(U) The obligatory “Anonymity is not equal to Cryptography” and “Anonymity is not equal to Steganography” admonishments were given early on.

### (U) Who are TOR Customers?

(U) Mr. Dingledine mentioned that the way TOR is spun is dependent on who the “spinee” is. Using the typical (in the cryptography world), Alice and Bob as communicants, he described several Alices:

(U) 1. Blogger Alice, who wants to be able to write to a blog in an anonymous way.

(U) 2. 8 yr. old Alice, who wants to be able to post to sites for children in a way insuring her true name and location are not discovered.

(U) 3. Sick Alice, who want to research information on her illness on the Internet while not enabling anyone to determine her true name and location.

(U) 4. Consumer Alice, who wants to research possible purchases without having a database of her marketing habits being built without (or with her weak) consent.

(U) 5. Oppressed Alice, who lives in a repressive country (no or limited free speech) and wants to talk about things contrary to her governments positions. The countries he used as examples were France, Germany (prohibitions on fascist writings?) and the US (not sure what he meant here?).

(U) 6. Turning to “Business Alice”, we had examples of companies not wanting to give up their business secrets to competitors via their Internet usage patterns. An anecdote was given of some business getting a different HTML page displayed when the same URL was accessed with and without TOR.

(U) 7. “Law Enforcement Alice” was concerned with the ability of anonymous agents/informants to really main anonymous when contacting their law enforcement ties.

### (U) Anonymity System Concepts

(U) Running ones own anonymity service vs. Using a 3rd party service: If one uses one’s own service, its pretty obvious who the user is :-)

(U) Low Latency Anonymity Service vs. High Latency Anonymity Service: The difference is in how paranoid someone really is. In a Low Latency Anonymity Service (all common proxies, TOR, others), there is a rerouting through some number of proxies, but there is no attempt to reorder packets or artificially introduce latencies. The result is something which can be used for most web and instant messaging / chat applications with only minimal notice of delays by the user. In a high latency service, proxies attempt to randomly reorder an delay packet so that it is harder to track traffic. Such systems are really only useful for such protocols as email.

(U) The most recent and advanced High Latency anonymity service was the /*MixMinion*/ family of open source projects. Mr. Dingledine was one of the key developers of these. His opinion is that the very limited utility of such projects has caused them to wither on the vine. He does *not* see any major development in such services for other than research in the forseeable future. Another key point is that the degree of anonymity in any system is proportional to the number of users. If noone is using any of the high latency systems, why bother. This proportionality is one of the ideas Mr. Dingledine refers to as a /tension/ in the world of anonymity systems.

(U) TOR Issues

(U) The short description of TOR for the reader is as follows: The user, via his/her TOR client, queries one of 5 directory servers for the current list of TOR nodes. Using metrics such as availability and bandwidth in conjunction with random choice, a set of 3 proxies is chosen for a “circuit”. It is this circuit which is used, with a unique layer of encryption on each link, for anonymous Internet interactions.

(U) The lifetime of a circuit, a tuneable parameter, is another /tension/, this one specific to TOR. The longer the circuit life, the more various traffic that may transit it, forming a knowable relationship between the traffic streams. Too short of a lifetime means too much time/CPU is spent building circuits. The original default lifetime was 30 seconds but is now 10 minutes. Everything is tweakable in TOR, so a user if free to choose his/her own circuit lifetime. But this is dangerous, as a unique circuit lifetime could easily become a user identification feature :-).

(U) Mr. Dingeldine was asked about the concrete choice of a 3-long circuit. This is unlikely to change soon, as it appears to be a very suitable tradeoff.

(U) The mention of SOCKS proxies, such as /*Privoxy*/ as a bump in the

chain before TOR was mentioned. These proxies can intercept and cleanup things such as cookies to further help anonymity.

(U) The current “owner” of TOR is torproject.org, a US registerd 501(C) non-profit organization, of which Mr. Dingledine is a principal. In addition to specific technology issues such as scaling, other categories of work are:

(U) 1. Usability (Targetting the ability of other than tech-savvy users to embrace the technology)

2. Incentives (Trying to get more people to run TOR servers)

3. Design for Scalability/Decentralization

3a. Regarding scalability of the TOR network, Mr. Dingledine proffered the guess that 2000-3000 is a rough upper limit on the number of nodes in the pool before a new topology may be advised.

3b. Decentralization means less reliance on a very small set of trusted Directory Servers (curently 5)

4. Continued research on attacks and the mitigation thereof.

5. Continued provision of documentation and user technical support.