Unidirectional Tunnels - I2P

5-7 minutes

Ity pejy ity dia navaozina tamin'ny November 2016 ary mifanaraka amin'ny router modely 0.9.27.

Overview

This page describes the origins and design of I2P's unidirectional tunnels. For further information see:

- Tunnel overview page
- Tunnel specification
- Tunnel creation specification
- Tunnel design discussion
- Fifidianana Akama
- Meeting 125 (~13:12-13:30)

Review

While we aren't aware of any published research on the advantages of unidirecdtional tunnels, they appear to make it harder to detect a request/response pattern, which is quite possible to detect over a bidirectional tunnel. Several apps and protocols, notably HTTP, do transfer data in such manner. Having the traffic follow the same route to its destination and back could make it easier for an attacker who has only timing and traffic volume data to infer the path a tunnel is taking. Having the response come back along a different path arguably makes it harder.

When dealing with an internal adversary or most external adversaries, I2P's undirectional tunnels expose half as much traffic data than would be exposed with bidirectional circuits by simply looking at the flows themselves - an HTTP request and response would follow the same path in Tor, while in I2P the packets making up the request would go out through one or more outbound tunnels and the packets making up the response would come back through one or more different inbound tunnels.

The strategy of using two separate tunnels for inbound and outbound communication is not the only technique available, and it does have anonymity implications. On the positive side, by using separate tunnels it lessens the traffic data exposed for analysis to participants in a tunnel - for instance, peers in an outbound tunnel from a web browser would only see the traffic of an HTTP GET, while the peers in an inbound tunnel would see the payload delivered along the tunnel. With bidirectional tunnels, all participants would have access to the fact that e.g. 1KB was sent in one direction, then 100KB in the other. On the negative side, using unidirectional tunnels means that there are two sets of peers which need to be profiled and accounted for, and additional care must be taken to address the increased speed of predecessor attacks. The tunnel pooling and building process (peer selection and ordering strategies) should minimize the worries of the predecessor attack.

Anonymity

A recent paper by Hermann and Grothoff declared that I2P's unidirectional tunnels "seems to be a bad design decision".

The paper's main point is that deanonymizations on unidirectional tunnels take a longer time, which is an advantage, but that an attacker can be more certain in the unidirectional case. Therefore, the paper claims it isn't an advantage at all, but a disadvantage, at least with long-living I2P Sites.

This conclusion is not fully supported by the paper. Unidirectional tunnels clearly mitigate other attacks and it's not clear how to trade off the risk of the attack in the paper with attacks on a bidirectional tunnel architecture.

This conclusion is based on an arbitrary certainty vs. time weighting (tradeoff) that may not be applicable in all cases. For example, somebody could make a list of possible IPs then issue subpoenas to each. Or the attacker could DDoS each in turn and via a simple intersection attack see if the I2P Site goes down or is slowed down. So close may be good enough, or time may be more important.

The conclusion is based on a specific weighting of the importance of certainty vs. time, and that weighting may be wrong, and it's definitely debatable, especially in a real world with subpoenas, search warrants, and other methods available for final confirmation.

A full analysis of the tradeoffs of unidirectional vs. bidirectional tunnels is clearly outside the scope of the paper, and has not been done elsewhere. For example, how does this attack compare to the numerous possible timing attacks published about onion-routed networks? Clearly the authors have not done that analysis, if it's even possible to do it effectively.

Tor uses bidirectional tunnels and has had a lot of academic review. I2P uses unidirectional tunnels and has had very little review. Does the lack of a research paper defending unidirectional tunnels mean that it is a poor design choice, or just that it needs more study? Timing attacks and distributed attacks are difficult to defend against in both I2P and Tor. The design intent (see references above) was that unidirectional tunnels are more resistant to timing attacks. However, the paper presents a somewhat different type of timing attack. Is this attack, innovative as it is, sufficient to label I2P's tunnel architecture (and thus I2P as a whole) a "bad design", and by implication clearly inferior to Tor, or is it just a design alternative that clearly needs further investigation and analysis? There are several other reasons to consider I2P currently inferior to Tor and other projects (small network size, lack of funding, lack of review) but is unidirectional tunnels really a reason?

In summary, "bad design decision" is apparently (since the paper does not label bidirectional tunnels "bad") shorthand for "unidirectional tunnels are unequivocally inferior to bidirectional tunnels", yet this conclusion is not supported by the paper.