Loopix Anonymity System - Write-up*

Avishek Mondal

I. How does Loopix work?

Loopix is a mixnet, that routes messages anonymously from senders and receivers using a network of mix servers that act as relays. As compared to previous mixed networks where clients directly injected traffic into a set of nodes, Loopix utilises service providers. Service providers act as entry and exit nodes for the Loopix infrastructure, and also have the functionality of offline storage. Thus a client can go offline, and then go online and retrieve traffic meant for him from these providers. To achieve indistinguishability of messages, there are several kinds of traffic in the network -

1) End-to-end messages: The messages the client want to send to the recipients
2) Drop cover traffic: Similar to end-to-end message, but is dropped by recipient service provider on the recipient's side. These messages are sent to random providers, and are dropped after being decrypted.
3) Client loop cover traffic: Originates and terminates with the same client. This means there are two kinds of cover traffic - outgoing and incoming. An adversary will not be able to distinguish between genuine messages and cover traffic. This provides a defence against the n-1 attack, because a client will be able to detect that it is not getting back its client loop traffic
4) Mix loop cover traffic: Similar to client loop cover traffic, except that it originates and terminates in the mix net.

Each of these streams of messages follows a Poisson process, and the resultant aggregate is also a Poisson process. A global passive adversary is unable to distinguish if the client is genuinely trying to communicate with a receiver or simply sending fake messages. When the recipient is retrieving his messages, the service provider also always sends a fixed number of messages which will be padded to ensure it is the same each time.

II. What are the strengths and weaknesses of the system

A. Strengths

1) Single honest node property: Loopix has the advantage of a mixnet's single honest node property, i.e. as long as a single mix node is honest, the entire mix network is honest.

2) Low latency with scaling: Compared to other mixnet systems, Loopix achieves low latency using Poisson mixing. The paper shows only a 0.37ms increase in latency when the number of clients increases from 50 to 500, which is promising for the scalability of the infrastructure. A low latency system with many users can guarantee greater security and privacy then a perfect mixnet system with high latency and a low number of users.

3) Unobservability and anonymity: Compared to the Tor network, this system provides a greater level of defence against the strong passive adversary that the Tor network does not defend against.

4) Offline retrieval: This enhances user experience and utility which will lead to more users, and thus greater anonymity for all those who do use it.

B. Weaknesses

1) Requirement for the receiver to be part of the network: The Loopix system requires all entities to be participants of the Loopix infrastructure, i.e. the user is unable to visit websites that are not in the Loopix structure. This could affect the number of users who use this structure, and as a result compromise anonymity for everyone due to the small anonymity set.

2) Possibility of subpoenas on service providers and other compromises: While the system works well against a passive adversary who observes traffic, it doesn't guard against service providers colluding with a global passive adversary. In a real world setting, this is the most likely form of compromise, where service providers are forced to collude with nation state level adversaries. However, this risk is mitigated by the fact that the compromised provider still cannot decrypt the message payload. Also, if a sender provider is compromised, the adversary still has a limited ability to carry out traffic co-relation, since client coverloop messages will make it difficult for the adversary to distinguish between genuine traffic and cover traffic

3) Connection-less path selection: This limits the network conditions under which Loopix can operate. A connection-less service means that packets can arrive out of order, can be dropped and subject to mis-delivery etc. Thus, the channel quality of the network must be very good. This also limits the uses of Loopix, and restricts it to sending/receiving emails etc. instead of say, watching videos or visiting dynamic websites

*Paper is [1]

References

[1] Ania M. Piotrowska et al. "The Loopix Anonymity System". In: *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association, 2017, pp. 1199–1216. ISBN: 978-1-931971-40-9. URL: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/piotrowska.