Karaoke: Distributed Private Messaging Immune to Passive Traffic Analysis - Write-up*

Avishek Mondal

I. How does Karaoke work?

Karaoke is a low-latency, metadata-private communication. The system makes no claims to be able to achieve anything more than be a medium for exchange of messages, and thus, rules other online activities such as browsing dynamic webcontent etc. for its users. When two users want to communicate, they arrange a dead-drop, which is arranged by a shared secret. At a dead-drop, the messages are swapped. The route is chosen by the sender at random, and uses the same "tunnelling" as that used in the Tor protocol. Each server that the message passes through changes the order of the messages, so that traffic co-relation cannot be carried out. This ensures any malicious adversary cannot bypass the shuffling of an honest server. User privacy is guaranteed by the following ways -

1) Requiring users to always send two messages in a round. Users communicate with themselves if they are not actively communicating with another user. This means a passive adversary monitoring dead drop patterns is unable to come up with a deterministic relationship between dead drop location and users
2) Noise generated by servers at the beginning of each round. Servers generates messages to random dead drops through random paths, and thus obscure genuine message information. Karaoke requires all servers to generate noise, to detect malicious servers not generating noise. To detect if noise signals were dropped, and in comparison to previous work, Karaoke uses Bloom filter to check if noise signals were not lost, and does not verify if genuine messages were lost. This saves it computational overhead, and thus reduced latency
3) Message swap. The path suffixes of the messages from one user to another are swapped at a dead drop

II. What are the strengths and weaknesses of the paper?

A. Strengths

1) Strong threat model: Not only does Karaoke guard against a global passive adversary, it also assumes a portion of its servers are compromised. This is a stronger adversary model than that of Tor. The paper has analysed many points of failure and possible compromised and shown the system to be resilient to them, for example, a compromised co-ordinator.

2) User alertness to attacks: Users are alerted to possible attacks. This is desirable, as it could prevent the further leaks of sensitive information and metadata that could help an adversary uncover the identity of users.

3) Of the paper - Substantial proofs: The paper provides numerous theoretic proofs of its claims. This shows that many of its guarantees have a firm grounding, that are unlikely to be undone once the system scales and is deployed.

B. Weaknesses

The paper does not claim to be able to defend against DoS attacks. This could be an issue for users, for example journalists etc. using it to cover breaking stories in countries who require it to be online all the time.

1) Dependence on network quality: The paper assumes that users would not be transmitting private messages over a lossy channel. However, this may not be a valid assumption in light of real world network conditions of geographical locations where this system will be deployed.

2) Dependence on many users using the system: The latency value provided by the paper is 6.8 second for 2M users, and 28 seconds of latency for 16 million users. This may be acceptable for emails etc. However, this will not be acceptable for instant messaging. This could hamper the number of users who will use this system, and thus affect the system's ability to generate enough traffic to provide significant privacy and anonymity guarantees to its users.

References

[1] David Lazar, Yossi Gilad, and Nickolai Zeldovich. "Karaoke: Distributed Private Messaging Immune to Passive Traffic Analysis". In: *13th USENIX Symposium on Operating Systems Design and Implementation*. 2018, pp. 711–725.

*Paper is [1]