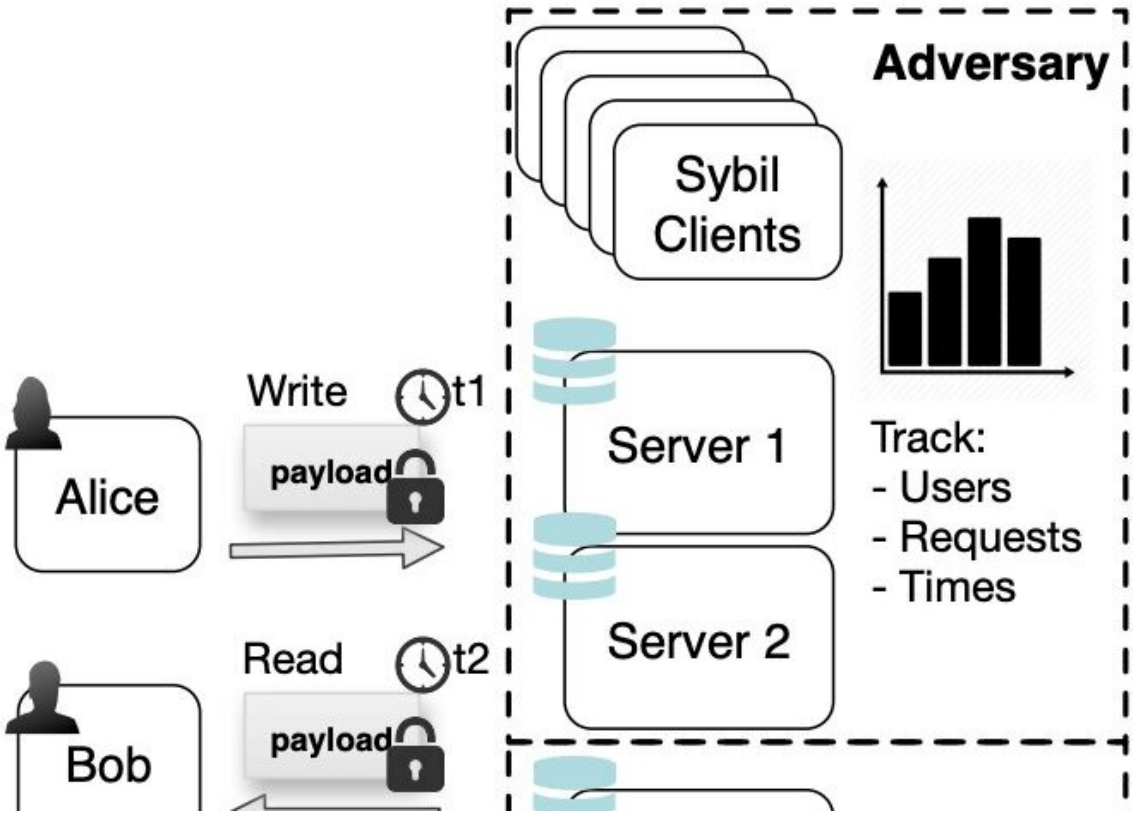
Talek: A private messaging system that hides message contents and user communication patterns

February 11 2020, by Ingrid Fadelli



Talek's system and threat model. The researchers assume the adversary can control all but one of the l servers in the system (here, l=3). Clients send network requests directly to the servers. Adversarial servers are free to record additional data, such as the source, type, parameters, timing, and size of all requests to link users who are likely to be communicating together. Credit: Cheng et al.

Encrypted messaging services, which prevent cyberattackers from reading the contents of messages exchanged by their users, have become increasingly popular over the past decade or so. While these services hide message content, malicious users can often use the network metadata to infer other information, such as the identity of users exchanging messages, when they are communicating, where their messages are sent, and how much data is transferred between them.

To prevent this from happening and ensure even greater security, researchers at the University of Washington and Carnegie Mellon University have recently developed Talek, a messaging system that hides both the content of messages and general patterns of communication between users, including their identity. This new messaging system, presented in a paper pre-published on arXiv, employs a technique called "private information retrieval" (PIR), designed to further enhance the safety of online communications.

The researchers who developed Talek have been investigating techniques that could improve user privacy and security online for several years now. In the past, they also collaborated with teams at Google on the development of uProxy (now known as Outline), a private VPN solution.

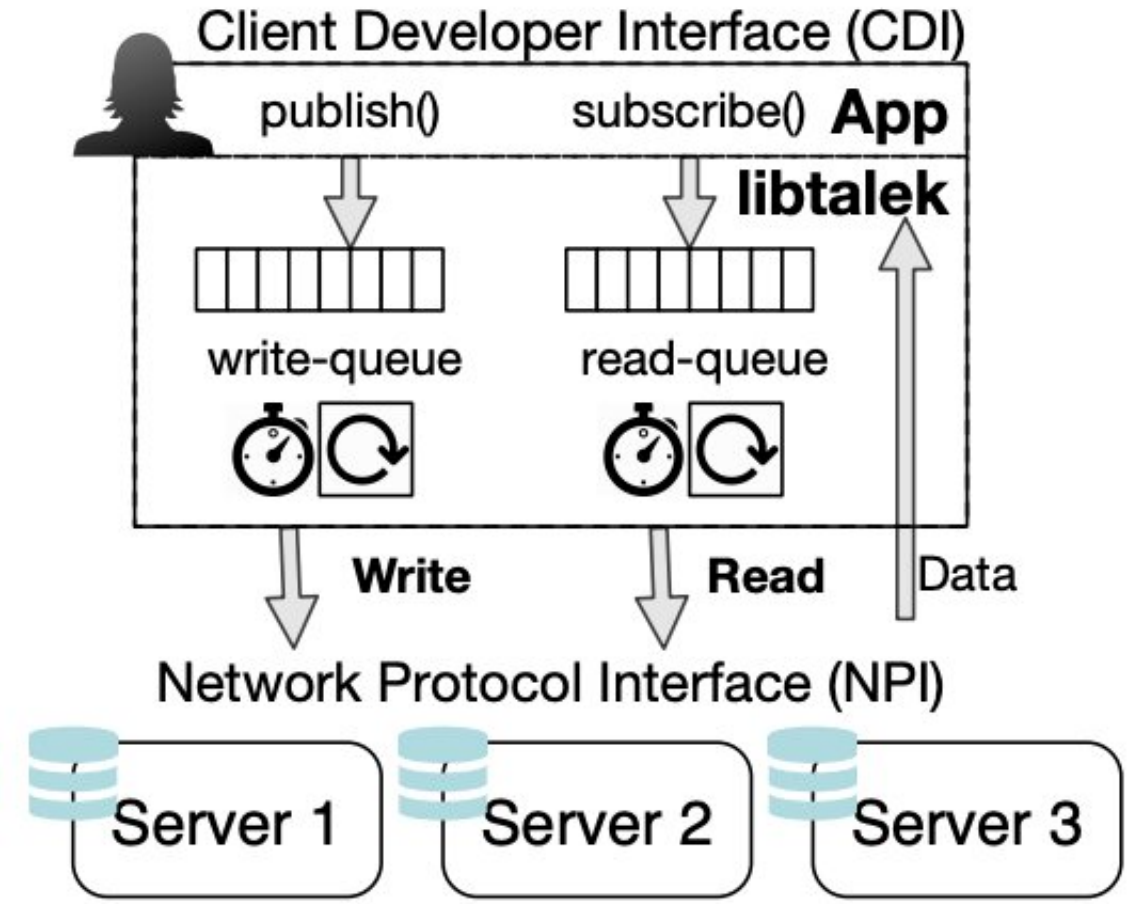
"More and more of our communications online are encrypted, which makes it harder for adversaries to see the contents of what we say," Raymond Cheng, one of the researchers who carried out the study, told TechXplore. "Talek takes this a step further, making it harder for those same adversaries to learn who is talking with whom."

The new messaging system developed by Cheng and his colleagues allows users to communicate with one another without sharing their identities with the server. It achieves this by hiding requests for information within random-looking requests.

Executing the theoretical constructs at the core of Talek's functioning has traditionally required substantial computational processes. A key advantage of Talek is that while realizing it may be computationally expensive, it can be done efficiently on GPUs. In addition to this, its unique design allows users to hide both ongoing conversations and their overall communication patterns.

"Prior work aimed at developing new messaging systems either offered strong security guarantees with prohibitive computational costs, or weaker security guarantees with practical performance," Cheng said. "Our work strives to provide a middle ground, bringing strong security guarantees (i.e., a security goal where any two access patterns between users is indistinguishable to the server), with performance that would satisfy many real messaging workloads."

To hide user communication patterns, Talek employs a technique known as PIR, which securely reads messages from a server without revealing what message was read. On its own, however, PIR is not enough to create a fully functioning messaging service. The researchers thus added a new component to their system, called the "oblivious log."



Talek's client interface. Application calls are translated by the client library into scheduled messages with equal-sized parameters and contents that appear random to an adversary. Clients behave identically from the perspective of any l-1 servers. Credit: Cheng et al.

Essentially, on Talek, messaging groups share secret log handles with one another, which are then used to create a random-looking sequence of addresses. Users can then store the messages they write to others according to this sequence of addresses, much like a digital dead drop. Those receiving the messages, on the other hand, can read them privately and securely using PIR.

"Compared to existing mixnet-based systems, we prove that we provide a stronger security goal of access sequence indistinguishability, as compared to security goals based on k-anonymity or differential privacy, which leak information by definition," Cheng explained.

Cheng and his colleagues have already built a working prototype of Talek with three servers and showed that it can be scaled to support real messaging workloads, achieving a throughput of 9,433 messages per second with 32,000 active users and an end-to-end latency of 1.7 seconds. Moreover, unlike most other private messaging systems, Talek can achieve a remarkable performance while maintaining a high level of user privacy.

"We are excited by the prospect of being able to provide a messaging service with strong security goals based on indistinguishability of access patterns, with sufficient performance to handle real-world messaging workloads," Cheng said. "We hope that these ideas can be directly applied to messaging services to improve the user privacy."

The messaging system comes with additional features. For instance, it allows users to learn when their private logs and conversations have new messages without polling (i.e., continuously checking the status of their device).

In the future, Talek could be used to create new secure, discrete and high-performing messaging services that can hide both the content of messages and user metadata. These services may prove to be particularly advantageous for people who carry out activities that require a high degree of anonymity, such as investigative journalists and activists.

"Privacy-preserving technology has come a long way, but there remain a number of difficult technical challenges to bringing strong security guarantees to the multitude of applications that we depend on a daily

basis," Cheng said. "We look forward to continuing our research into privacy-preserving technologies."

More information: Talek: private group messaging with hidden access patterns. arXiv: 2001.08250 [cs.CR]. arxiv.org/abs/2001.08250