OrgAn: Organizational Anonymity with Low Latency

Debajyoti Das*
Purdue University
U.S.A.
das48@purdue.edu

Easwar Vivek Mangipudi*
Purdue University
U.S.A.
emangipu@purdue.edu

Aniket Kate
Purdue University
U.S.A.
aniket@purdue.edu

Abstract

There is a growing demand for network-level anonymity for delegates at global organizations such as the UN and Red-Cross. Numerous anonymous communication (AC) systems have been proposed over the last few decades to provide anonymity over the internet; however, they either introduce high latency overhead, provide weaker anonymity guarantees, or are difficult to be deployed at the organizational networks. Recently, the PriFi system introduced a client/relay/server model that suitably utilizes the organizational network topology and proposes a low-latency, strong-anonymity AC protocol. Using an efficient (almost) key-homomorphic pseudorandom function in lattice-based cryptography and Netwon's power sums, we present a novel AC protocol OrgAn in this client/relay/server model that provides strong anonymity against a global adversary controlling the majority of the network. OrgAn's cryptographic design allows it overcomes several major problems with any realistic PriFi instantiation: (a) unlike PriFi, OrgAn avoids frequent, interactive, slots and key agreement protocol among the servers; (b) a PriFi relay has to receive frequent communication from the servers which can not only become a latency bottleneck but also reveal the access pattern to the servers and increases the chance of server collusion/coercion, while OrgAn servers are absent from any real-time process; (c) finally, unlike PriFi, OrgAn can handle absentees and churn without re-running the setup. Our protocol provides strong anonymity guarantees with resistance against intersection attacks and active attacks under Discrete Log (DL) and Ring Learning-with-rounding (R-LWR) assumptions.

As another key contribution, we demonstrate how to make this public-key cryptographic solution scale equally well as the symmetric-cryptographic PriFi using practical precomputation and storage requirements. We find that OrgAn provides similar end-to-end latency guarantees as PriFi, while still ignoring the PriFi's setup challenges. Our evaluation shows that network anonymity is feasible for latency-sensitive applications like VoIP, Skype video calls for organizations with a few hundred clients. Using a prototype implementation we show that OrgAn achieves reasonable round-trip-time (RTT) of 61 milliseconds for a system of 100 clients when they are communicating to the outside world compared to typical RTT of 20 milliseconds; it can support 1.9 Mbps throughput for every client in an organization with 100 clients.

Talk Proposal

In our talk we are going to present the protocol design of OrgAn and how it solves the following three key problems associated with PriFi and other existing DC-net based protocols: (i) In DC-net based protocols, all the users need to run a key agreement protocol among themselves to agree on shared secrets keys; such an agreement protocol is not scalable as it comes with high communication overhead and has to be repeated often towards stopping linkability/co-relations across multiple rounds. (ii) Most DC-net based protocols require all the users to participate in a slot agreement protocol before every round; otherwise two or more messages may collide as only one user is supposed to send a message in any given round. (iii) Finally, the DC-net designs draws their efficiency gains over mixnets through the fixed user setup and co-ordination among them: Unlike for mixnets, any user arrival, absentees and departure mandates re-running the setup with the new group. Then we present a preliminary performance analysis based on our prototype implementation. Finally, we talk about the different application scenarios where OrgAn can be employed.

If accepted, this will be the first time we are going to present our work to the scientific community.

Why is this a good topic for HotPETs?

We believe that out work is very suitable to be presented at HotPETs because we provide a solution to a very important problem of organizational anonymity — except PriFi, there are no suitable solutions in this area in the current literature. While improving upon the existing solution (PriFi) for privacy in an organizational network, our protocol OrgAn also solves several fundamental problems associated with the existing DC-net based protocols as mentioned above. Moreover, we are the first to consider the churn in the DC-net setting and offer practical solution to the problem. Despite solving the above problems using a public key cryptographic primitive (i.e., key-homomorphic PRF), OrgAn also shows how to keep the latency overhead in milliseconds using a storage vs. computation tradeoff associated with the R-LWR setting — which can of independent interest to many protocol developers.

How will we make the talk engaging?

Since the problem is real-world, we will present examples and data to bring out its relevance further. Colourful and animated presentation combined with crisp explanation of the solution is the topping on the cake.

[*] Both authors contributed equally to this research.