Practical Private Information Aggregation in Large Networks

Gunnar Kreitz, Mads Dam, Douglas Wikström
KTH CSC

With the continuous increase of network complexity and attacker sophistication, the subject of network and security monitoring becomes increasingly important. Traditionally, organizations have performed network and security monitoring based only on data they can collect themselves. One of the reasons for this is a reluctance to share traffic data and security logs between organizations, as such data is sensitive.

There is much to be gained from collaboration in security monitoring. Attacks range from being targeted at specific individuals or organizations, to global scale attacks such as botnets. Naturally, the response measures depends on the type of attack. The same situation applies to network monitoring, where the complexity of networks, and large amount of applications can make it difficult to distinguish between local and global disruptions with access only to local data.

A natural path towards a solution is to apply multi-party computation (MPC) techniques, which have been long studied within the field of cryptography. The goal of MPC is to allow a group of mutually distrusting parties to jointly evaluate a function of their private inputs, while leaking nothing but what can be deduced from the output of the function. Furthermore, protocols built on MPC techniques are generally secure, even if several parties (up to a fraction of the parties involved in the computation) collude to break the privacy of the other participants.

The traditional setting of MPC is one where the number of parties is relatively small and the network is assumed to be full mesh. Sadly, this precludes the immediate application of such techniques in the large, partial mesh networks which are prevalent today.

Towards a general solution to the problem of collaborative network and security monitoring we present efficient and scalable protocols for privately computing a large range of aggregation functions based on addition, disjunction, and max/min. Our protocols can be run on any network structure, and we characterize the resiliency to adversaries in terms of graph theoretical properties of the network on which the protocol is executed.

For addition, we give a protocol that is information-theoretically secure against a passive adversary, and which requires only one additional round compared to non-private protocols for computing sums. For disjunctions, we present both a computationally secure, and an information-theoretically secure solution. The latter uses a general composition approach which executes the sum protocol together with a standard multi-party protocol for a complete subgraph of ``trusted servers''. This can be used, for instance, when a large network can be partitioned into a smaller number of provider domains.