IXP++: Towards Securing IXPs

Muhammad Muqsit Nawaz, Faizan Safdar Ali, Dr. Muhammad Fareed Zaffar, Waqar Aqeel, Usman Nazir
LUMS School of Science and Engineering Pakistan

During the last few years, thousands of medium-to-large Internet Exchange Points (IXP) have emerged around the world. They operate a route server and offer its use as a free value-added service to their members. Original architects of IXPs and SDX (next generation Software Defined Exchange Points) paid less attention to accountability and security. Hence, this poses fundamental questions regarding the privacy concerns of confidential business information that is exchanged between members and Route Server (RS) services. Due to such reasons, Autonomous Systems (ASes) deter from providing intra-domain routing information, consequently resulting in an un-optimized traffic engineering. We have designed IXP++, a domain privacy-preserving security mechanism that employs homomorphic encryption and private set intersection in complex networks with SDXs to prevent leaking of crucial business information.

With newer Internet Exchange Points (IXPs) being established every day for mutual benefits of Autonomous Systems (ASes) involved, new privacy concerns arise. There are currently some 350+ Internet Exchange Points (IXPs) worldwide, and some of the largest and most successful IXPs have more than 500-600 members and carry as much traffic as some of the global Tier-1ISPs. Due to being densely connected physical components in today's Internet, many of them have started to use route servers (RSes) as a free valued-added service to their members. An RS greatly simplifies routing for its members, that is, most members use an IXP's RS to establish multi-lateral peerings as compared to bi-lateral peerings.

Our main aim is to answer the question of verifiability i.e. the questions for example, whether the chosen route was the best one available, or whether it was consistent with the networks peering agreements, and privacy of crucial information (for example the route policies of the ASes) in SDXes. Since more and more IXPs are moving towards SDXes, we believe that implementing IXP++ in a software defined environment is the most viable option. When we want to exchange intra-domain routing information for the purpose of verifiability and an optimized route selection, privacy concerns arise and some network administrators avoid it for precisely this reason. For example a couple of Internet providers in the Nairobi central business district offered to host the IXP. The challenges were (1) how to choose between the two ISPs and (2) the high levels of dissatisfaction expressed by the other ISPs about having to trust a competitor to handle the IXP without seeking for itself an undue advantage.

In this paper, we are trying to propose solution to how the Centralized Controller in SDXs (acting as a Route Server) can allow the ASs connected to it to verify a number of nontrivial properties about inter-domain routing decisions without leaking confidential information. If all the properties hold, the peers learn nothing beyond what the inter-domain routing protocol already reveals; if a property does not hold, at least one peer can detect this and prove the violation. Furthermore, since we are ensuring privacy the two ASs who have peering agreements can provide information about their intra-domain routing which will result in better traffic engineering.