Does Scale, Size, and Locality Matter?
Evaluation of Collaborative BGP Security Mechanisms

Rahul Hiran, Linköping University, Sweden
Supervisors: Nahid Shahmehri and Niklas Carlsson

The Border Gateway Protocol (BGP), the de-facto inter-domain routing protocol used over the Internet, is vulnerable to many attacks, including prefix/subprefix hijacks, interception attacks, and imposture Attacks. In a (sub)prefix hijack, the attacker announces a (sub)prefix that is actually allocated to a different AS without authority to do so. These attacks may lead to imposture attacks, where the attacker impersonates the victim network, or interception attacks, where the attacker redirects the traffic to its intended destination, after making a copy or modifying the data, for example.

Despite many protocols having been proposed to detect or prevent such attacks, no solution has been widely deployed. Yet, the effectiveness of most proposals relies on large scale adoption and cooperation between many large Autonomous Systems (ASes). In this paper, we use measurement data to evaluate some promising, previously proposed techniques in cases where they are implemented by different subsets of ASes, and answer questions regarding which ASes need to collaborate, the importance of the locality and size of the participating ASes, and how many ASes are needed to achieve good efficiency when different subsets of ASes collaborate. For our evaluation we use topologies and routing information derived from real measurement data. We consider collaborative detection and prevention techniques that use (i) prefix origin information, (ii) route path updates, or (iii) passively collected round-trip time (RTT) information.

Our results and answers to the above questions help determine the effectiveness of potential incremental rollouts, incentivized or required by regional legislation, for example. While there are differences between the techniques and two of the three classes see the biggest benefits when detection/prevention is performed close to the source of an attack, the results show that significant gains can be achieved even with only regional collaboration.

This presentation is based on our paper "**Does Scale, Size, and Locality Matter? Evaluation of Collaborative BGP Security Mechanisms**" presented at the IFIP Networking conference, May 2016