

## **Collaboration For Better Routing Security**

Routing security incidents occur every day. And although there are well-known best practices for routing security, the distributed architecture of the global routing system requires voluntary actions from all network operators to improve the security of the global routing system. Since many of these actions improve the security of others, rather than the network operators who implement them, there can be little incentive for any individual network operators to take action.

How do we improve those incentives? What are the simplest actions network operators can take, with the greatest impact. And just how bad is the state of routing security, both in Canada, and the world?

Using data from the forthcoming MANRS Observatory, we will look at the state of routing security in Canada over the course of 2019. We will identify the actions that three main categories of actors: ISPs, IXPs, and cloud/content providers, can take to have the biggest impact on the security of inter-domain routing. We will also identify the collective actions the routing community are taking to improve the incentives for implementing routing security best practices, including the Mutually Agreed Norms for Routing Security.