Towards Data-Driven Internet Routing Security

Cecilia Testart, ctestart@csail.mit.edu

Background
- The Border Gateway Protocol (BGP) – the de-facto inter-domain routing protocol of the Internet—lacks route authentication and validation.
- BGP security flaws have been known for a very long time. In 1982, RFC 827 pointed out problems if a router sends a message with false information.
- There have been many security proposals from the research, industry and standardization communities, but there are fundamental disagreements that hinder the adoption of technical solutions [1].
- Lack of empirical data to characterize BGP problems and evaluate defenses and proposals to increase BGP security. Only anecdotal evidence of attacks and other problems with BGP, most events are not disclosed.
- BGP security is far from solved.

Research Question
Can we design automated solutions that discover hijacks and other routing problems in the Internet?

Approach
- Large-scale Internet measurements
- Manually gathered ground truth
- Data analysis
- Domain knowledge
- New body of evidence
- New insights

Finding and Profiling BGP Serial Hijackers [2]
- BGP serial hijackers: Networks repeatedly hijacking over long periods of time.

Main Contributions
- First longitudinal analysis of BGP serial hijackers.
- New data for network reputation scoring systems and metrics for assessment of network-wide BGP behavior.
- Passive method for continuous monitoring of operational security practices.
- First study to measure the benefit of security practices.

Future Research
- How are malicious networks connected? How are their routes propagated?
- What are the more advanced/stealthy attacks on BGP?
- How is BGP misbehavior linked with misbehavior in DNS and other protocols?

- The Resource Public Key Infrastructure (RPKI) is a framework to secure BGP using cryptographic records to validate prefix and origin in BGP announcements.
- The operational adoption of RPKI security practices has significantly increased in 2020.
- RPKI effectively reduces illicit announcement propagation.

References