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**.

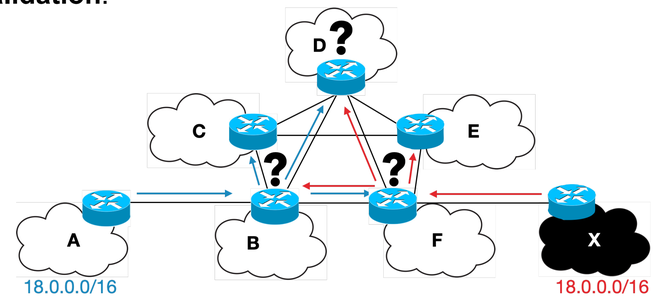


Fig.1 : Using only BGP, routers cannot determine which of the two announcements (from A and X) of prefix 18.0.0.0/16 is the legitimate one.

- **BGP security flaws have been known for a very long time.** In 1982, RFC 827 pointed out problems if a router send 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**.

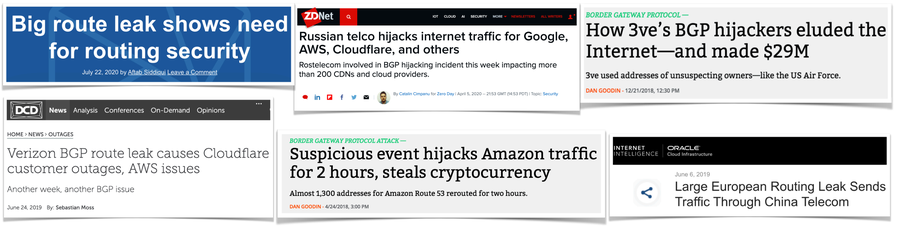
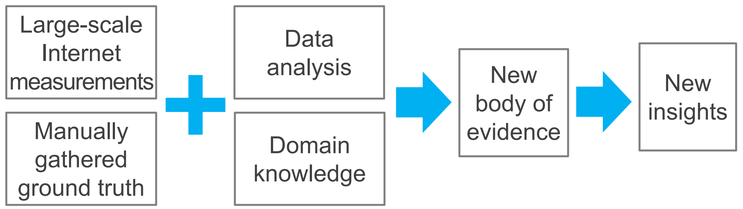


Fig.2 : BGP route leaks and hijacks that made the news between 2018 and 2020.

Research Question

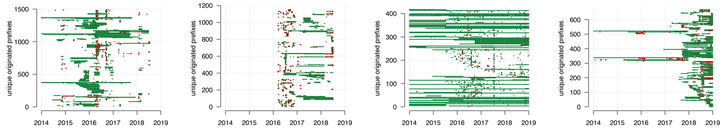
Can we design **automated solutions** that **discover hijacks** and other **routing problems** in the **Internet?**

Approach



Finding and Profiling BGP Serial Hijackers [2]

BGP serial hijackers: Networks repeatedly hijacking over long periods of time.



Legitimate networks: from Mutually Agreed Norms for Routing Security (MANRS).

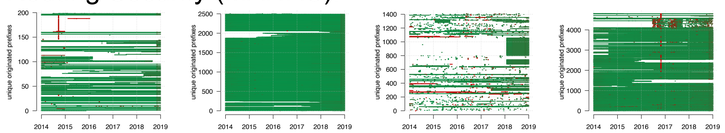


Fig.3: BGP origination behavior of selected networks from 5 years of BGP data (Jan 2014 – Dec 2018).

ML classifier output: 934 Networks (Autonomous Systems) with similar BGP behavior to serial hijackers.

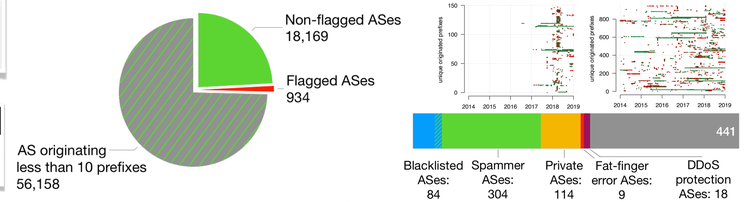


Fig.4: ML classifier outcome (left), selected networks BGP behavior (upper right) and categories of flagged networks (lower right).

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?

Measuring Operational Security Practices[3]

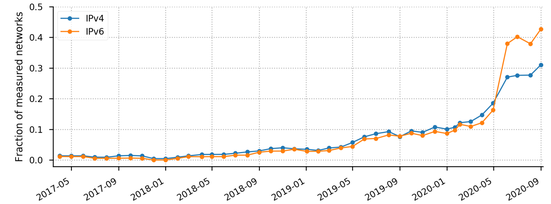


Fig.5: Fraction of networks adopting security practices.

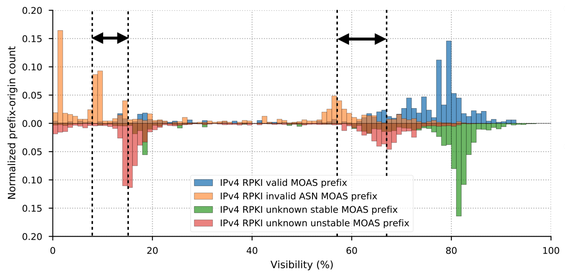


Fig.6: Benefit of RPKI: Comparison of prefix-origin visibility in the case of Multi-Origin AS (MOAS) conflicts.

- 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

[1] C Testart. *Reviewing a historical Internet vulnerability: why isn't BGP more secure and what can we do about it?* Research Conference on Communication, Information and Internet Policy (TPRC46), September 2018.

[2] C. Testart, P. Richter, A. Dainotti, D. Clark. *Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table*. ACM Internet Measurement Conference (IMC), October 2019. **Distinguished Paper Award**

[3] C. Testart, P. Richter, A. Dainotti, D. Clark. *To Filter or not to Filter: Measuring the Benefits of Registering in the RPKI Today*. Passive and Active Measurement Conference (PAM), April 2020.