

KIRIN: attacking BGP with IPv6

Lars Prehn

Max Planck Institute for Informatics

lprehn@mpi-inf.mpg.de



Pawel Foremski

IITiS PAN

pjf@iitis.pl



Oliver Gasser

Max Planck Institute for Informatics

oliver.gasser@mpi-inf.mpg.de



1. KIRIN: Killing Internet Routers in IPv6 Networks

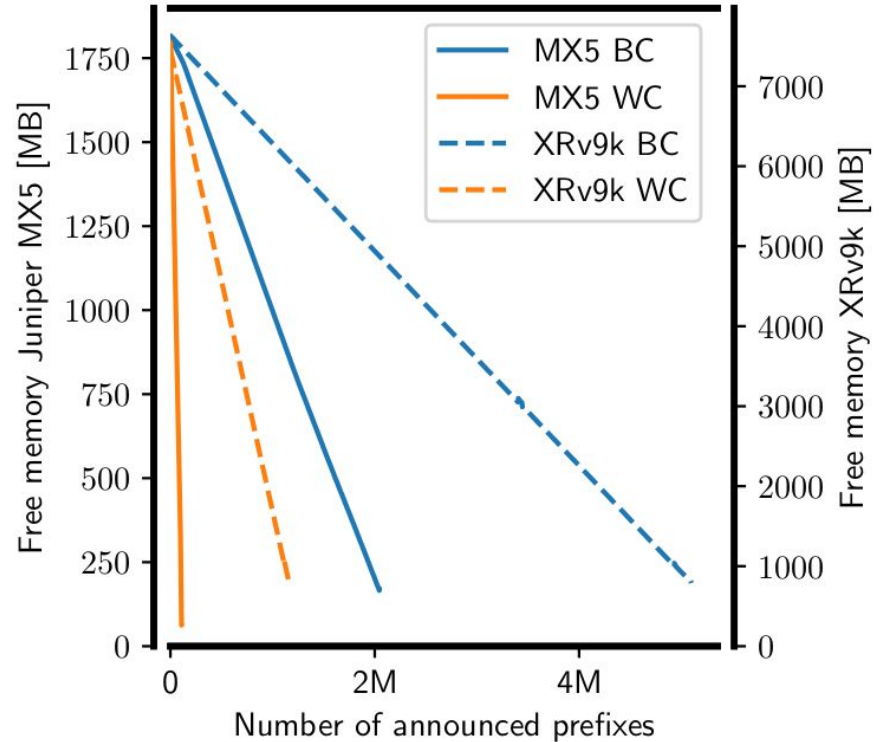
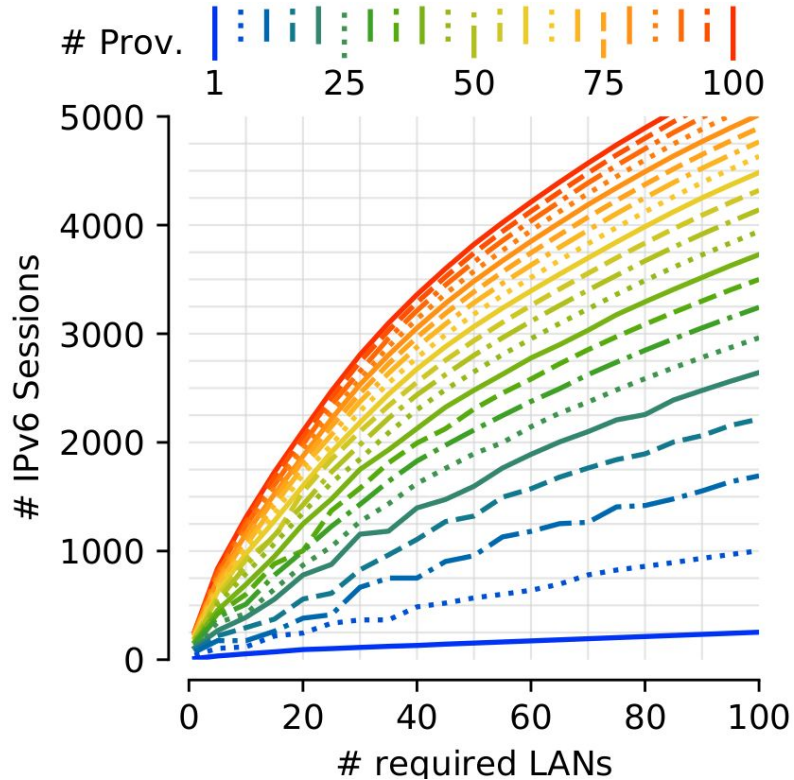
- Internet routers' FIB/RIB tables have *limited capacity* [1]
 - **What if we announce *too many prefixes*, and overflow them?**
- Let's re-visit *prefix de-aggregation attacks*, but also consider:
 - **IPv6**
 - Easy /29 allocation = 1 million possible sub-prefixes good for BGP
 - **Instant and “cheap” BGP sessions**
 - No more need for physical presence: remote peering, network-as-a-service, VPSes, ... [2]
 - **BGP max-prefix limits and prefix aggregation**
 - Establish many BGP sessions + unique, non-aggregatable announcements for each
 - **...and RPKI can actually “help”**
 - Parent ROA with a maxLength = route filter accept for each sub-prefix [3]

1. <https://blog.apnic.net/2021/03/03/what-will-happen-when-the-routing-table-hits-1024k/>

2. <https://www.ixreach.com/services/remote-peering/> | <https://www.megaport.com/> | <https://www.vultr.com/> | <https://bgp.services/>

3. <https://routing.he.net/algorithm.html>

2. Is it possible to launch KIRIN *today*?



3. What should I do?

- KIRIN is easily detectable
 - **Needs monitoring - area for researchers**
- Recommendations for operators
 - **Establish tight and dynamic max-prefix limits**
 - 1.5-2x daily growth for peers and customers
 - 1.2x daily growth of routing table size (transit providers)
 - **Redistribute a certain number of...**
 - ...routes per origin (eg. AS9808 = ~4k IPv6 prefixes)
 - ...more-specifics per each assigned block (eg. 2409:8000::/20 = ~10k more-specifics)
- Read our paper for more!



kirin-attack.github.io

Thank you!

Lars Prehn

lprehn@mpi-inf.mpg.de

[@mydamnhandle1](https://twitter.com/mydamnhandle1)

Pawel Foremski

pjf@iitis.pl

[@pforemski](https://twitter.com/pforemski)

Oliver Gasser

oliver.gasser@mpi-inf.mpg.de