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” remote BGP sessions**
    - No need for physical presence: remote peering, network-as-a-service, VPSes, … (eg. [2])
  - **BGP max-prefix limits and prefix aggregation**
    - Establish many BGP sessions + unique, non-aggregatable announcements for each
  - …and RPKI can sometimes “help”
    - Parent ROA with a maxLength = route filter accept for each sub-prefix (eg. [3])

1. [https://blog.apnic.net/2021/03/03/what-will-happen-when-the-routing-table-hits-1024k/](https://blog.apnic.net/2021/03/03/what-will-happen-when-the-routing-table-hits-1024k/)
3. [https://routing.he.net/algorith.html](https://routing.he.net/algorith.html)
2. Is it possible to launch KIRIN *today*?
2. Is it possible to launch KIRIN today? Yes!

\[
v_4 + v_6 = \sim 1.1M
\]
3. What should I do?

- KIRIN is easily detectable
  - Needs monitoring

- Recommendations for operators
  - More tight yet dynamic max-prefix limits
    - 1.5x growth per day - peers and customers sessions
    - A few thousand new prefixes per day - transit sessions
  - Introduce limits on
    - Routes per origin (max now: AS9808 = ~4k IPv6 prefixes)
    - More-specifics per each assigned block (max now: 2409:8000::/20 = ~10k more-specifics)
  - Don’t blindly rely on PeeringDB max-prefix limits (add sanity checks)

- …read much more in our paper!
Thank you!

Lars Prehn
lprenh@mpi-inf.mpg.de
@mydamnhandle1

Pawel Foremski
pjf@iitis.pl
@pforemski

Oliver Gasser
oliver.gasser@mpi-inf.mpg.de

kirin-attack.github.io
Backup slides
ONE DOES NOT SIMPLY

ANNOUNCE A MILLION NEW ROUTES