Privacy & Security Issues in IPv6 Deployment

Dave Plonka, **Tobias Fiebig**

IPv6 Security & Privacy Implications: Known and considered solved?

- EUI64
  - RFC4941 default: SHOULD be off
  - Identify devices/device types
  - Track users (physically)
  - More exposed addresses

Example: Privacy implications

- Example 1:
  - 45% of responding hosts replied with EUI-64 addresses for ICMP-Time-Exceeded messages in a measurement study
- Example 2:
  - 8am – 1pm: Working in Building 1

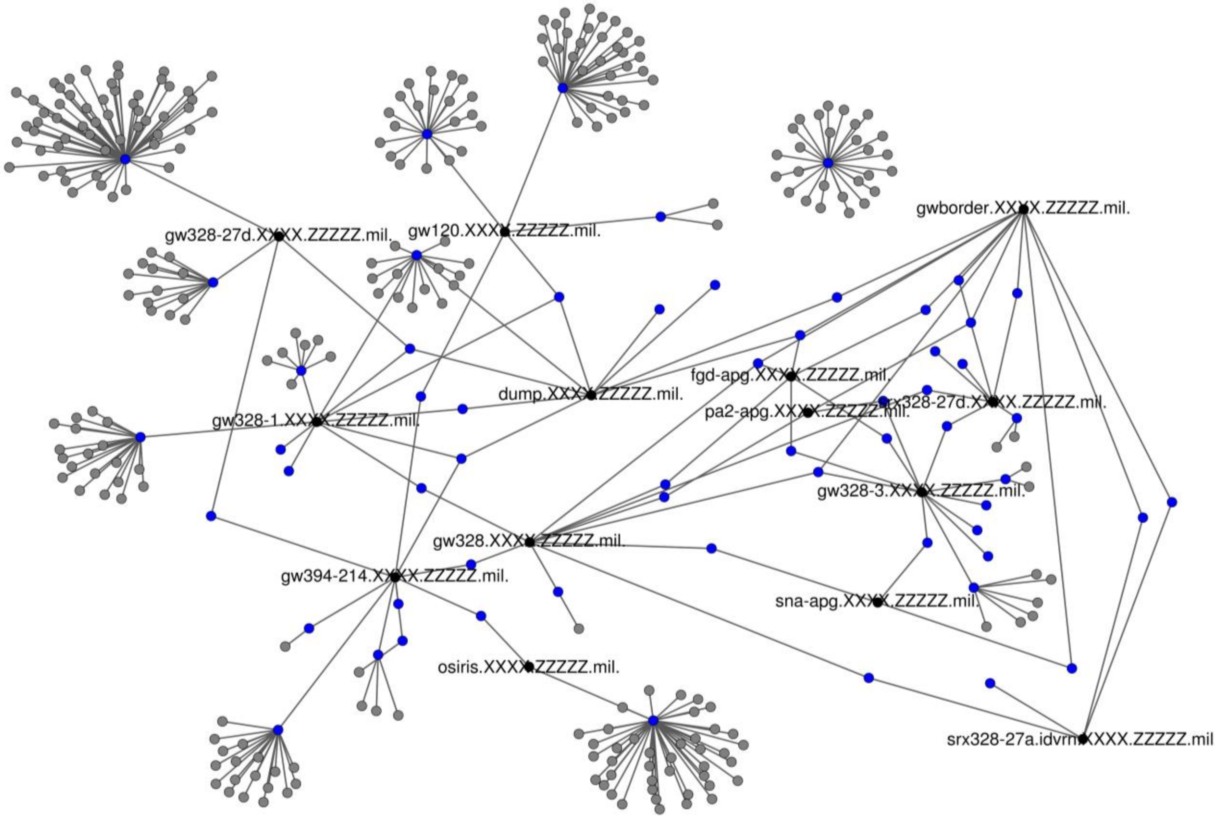
    2001:0db8:85a3:b1d1:020c:29ff:fe0c:47d5
  - 2pm – 5pm: Working in Building 2

    2001:0db8:85a3:b1d2:020c:29ff:fe0c:47d5

IPv6 Security & Privacy Implications: Known and considered solved?

- EUI64
  - RFC4941 default: SHOULD be off
  - Identify devices/device types
  - Track users (physically)
  - More exposed addresses
- Addressing practices
  - Privacy leaks
  - Address anonymization
  - Topology discovery

Example: Fine-grained topology



TUDelft

IPv6 Security & Privacy Implications: Different in the wild

- Beverly, Robert, et al. "In the IP of the Beholder: Strategies for Active IPv6 Topology Discovery", *ACM Internet Measurement Conference (IMC),* 2018

  https://conferences.sigcomm.org/imc/2018/papers/imc18-final151.pdf

- Borgolte, Kevin, et al. "Enumerating active IPv6 hosts for large-scale security scans via DNSSEC-signed reverse zones", *IEEE Symposium on Security and Privacy (Oakland)*, 2018

  https://homepage.tudelft.nl/2x09j/pdf/sp2018-dnssec-ipv6.pdf

Draft-Plan

- Document real measurement results
  - Real, measurable issues
  - Contrast what should be done with what is done
  - Have a basis for comparison with continuous measurements

Call for measurement observations

- Additional data-sets, experiences, and observations
- Input on experiences and anecdotes
- Drop us a line to dave@plonka.us and t.fiebig@tudelft.nl