Attribution of Internet Probes

draft-vyncke-opsec-probe-attribution-latest

Éric Vyncke, Cisco
Benoît Donnet, University of Liège
Justin Iurman, University of Liège
What are we trying to solve?

Many research projects require sending ‘strange’ sometimes unsolicited packets over the Internet e.g., JAMES or RFC 7872

Those packets may trigger security alerts or even cause network harm...

How can the impacted parties contact the sender?
Probe Description URI

The URI may be:

- A probe description
  https://example.net/measurement.txt
  based on RFC 9116 draft-foudil-securitytxt

- An email address
  mailto:eric@example.net

- A phone number
  tel:+1-201-555-0123
In-band probe attribution

Insert the attribution URI *in* all packets

Examples:
ICMPv6 echo request, in the optional data
UDP in the data payload
TCP SYN can also have data payload
IPv6 destination / hop-by-hop options header can have non standard options
Format of in-band probe attribution

If the URI can be placed at the beginning of the data, it MUST be terminated by 0x00.

If the URI can only be placed at the end of the data, it MUST be preceded and terminated by 0x00 octets.
Out-of-band probe attribution

Let’s rely on the source address...

E.g., for a source address of 2001:db8::dead

Reverse DNS exists:
https://example.net/.well-known/probing.txt

Reverse DNS does not exist:
https://[2001:db8::dead]/.well-known/probing.txt
Next steps?

This I-D was used by draft-vyncke-v6ops-james-latest (cfr V6OPS agenda)

Suggestions / comments welcome

If interest by OPSEC, even if pretty simple/obvious, then call for adoption?