Security and Privacy Implications of Numeric Identifiers Employed in Network Protocols

(draft-gont-predictable-numeric-ids)

Fernando Gont
Iván Arce

IETF 104
Prague, Czech Republic. March 23-29, 2019

Why talk about this?

- For the last 30 years, many protocol specifications and/or implementations got them wrong.
- Examples:
  - Predictable TCP sequence numbers
  - Predictable transport protocol numbers
  - Predictable IPv4 and IPv6 Fragment Identifiers
  - Predictable IPv6 IIDs
  - Predictable DNS TxIDs
- Lessons learned about numeric identifiers in one protocol were not leveraged/applied in others
- New protocols/specifications specified/built with same flaws

Root Cause of the Problem

Root cause of the problem

- Protocol specifications which under-specify the requirements for their identifiers
  - TCP port numbers and ISNs in [RFC0793]
  - DNS TxID in [RFC1035]
- Protocol specifications that over-specify their identifiers
  - IPv6 IIDs in [RFC4291]
  - IPv6 Frag ID in [RFC2460]
- Protocol implementations that simply fail to comply with the specified requirements

Numeric Identifiers

Numeric Identifiers

- A data object in a protocol specification that can be used to uniquely distinguish a protocol object from all others
- They usually have specific interoperability requirements, e.g.:
  - uniqueness
  - monotonically-increasing
  - Stable withing context
- They have different failure modes:
  - soft failure
  - hard failure

Categorizing Numeric Identifiers

Analysis of Some Numeric Identifiers

Identifier	Interoperability Requirements	Failure Severity
IPv6 Frag ID	Uniqueness (for IP address pair)	Soft/Hard
IPv6 IID	Uniqueness (and constant within IPv6 prefix)	Soft
TCP SEQ	Monotonically-increasing	Hard
TCP eph. port	Uniqueness (for connection ID)	Hard
IPv6 Flow L.	Uniqueness	None
DNS TxID	Uniqueness	None

Categorizing Numeric Identifiers

Cat #	Category	Sample Proto IDs
1	Uniqueness (soft failure)	IPv6 Flow L., DNS TxIDs
2	Uniqueness (hard failure)	IPv6 Frag ID, TCP ephemeral port
3	Uniqueness, constant within context (soft failure)	IPv6 IIDs
4	Uniqueness, monotonically increasing within context (hard failure)	TCP ISN

Some Possible Algorithms

Sample Algorithms

- Our I-D specifies algorithms for each category, that:
  - comply with interoperability requirements
  - minimize the security and privacy implications
- New specifications and/or implementations can use one of those by default, as needed

Advice on Numeric Identifiers

Protocols Specifications Must...

- Clearly specify the interoperability requirements for selecting the aforementioned identifiers.
- Provide a security and privacy analysis of the aforementioned identifiers.
- Recommend an algorithm for generating the aforementioned identifiers that mitigates security and privacy issues.

Moving Forward

Moving Forward

- Previous comments suggested to:
  - Split the I-D into informational and BCP parts
  - Incorporate recommendations in rfc3552bis? -- it didn’t happen
- How we should pursue this?

Questions?