Security and Privacy Implications of Numeric Identifiers Employed in Network Protocols

Fernando Gont
Iván Arce
Michael Richardson

IETF 97
Seoul, Korea. November 13-18, 2016

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 an associated failure severity
  - None
  - Soft Failure
  - Hard Failure

Issues with Numeric Identifiers

- 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 or 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

- 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

Ongoing work

- Original I-D (draft-gont-predictable-numeric-ids) now split into three documents.
- draft-gont-numeric-ids-history:
  - Sample timeline for a number of numeric identifiers
- draft-gont-numeric-ids-generation
  - Advice on the specification and generation of numeric identifiers
  - Categorize numeric IDs based on interoperability properties and associated failure severity
  - Propose algorithms for each category
- draft-gont-numeric-ids-sec-considerations
  - Advice on security considerations for numeric identifiers
  - Not pursued as an I-D anymore. Text to be considered for incorporation in rfc3552bis

Questions?