# Security and Privacy Implications of Numeric Identifiers Employed in Network Protocols

## (draft-gont-predictable-numeric-ids)

**Fernando Gont**
**Iván Arce**

**IETF 95**
Buenos Aires, Argentina. April 3-8, 2016

# 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 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

# Sample timeline: TCP ISNs

- **September 1981**:

  [RFC0793] suggests the use of a global 32-bit ISN generator.

- **February 1985**:

  [Morris1985] describes exploitation of predictable TCP ISNs.

- **April 1989**:

  [Bellovin1989] discusses security implication of this and other predictable IDs.

- **February 1995**:

  [Shimomura1995] reported a real-world exploitation of the attack described in 1985 (ten years before).

# Sample timeline: TCP ISNs (II)

- **May 1996**:

  [RFC1948] was the first IETF effort to mitigate the problem.

- **March 2001**:

  [Zalewski2001] shows statistical weaknesses in some ISN generators.

- **May 2001**:

  Vulnerability advisories [CERT2001] [USCERT2001] are released regarding statistical weaknesses in some ISN generators.

# Sample timeline: TCP ISNs (III)

- **March 2002**:

  [Zalewski2002] updates and complements [Zalewski2001]. It concludes that "***while some vendors [...] reacted promptly and tested their solutions properly, many still either ignored the issue and never evaluated their implementations, or implemented a flawed solution that apparently was not tested using a known approach***".

- **February 2012**:

  [RFC6528], after 27 years of Morris' original work [Morris1985], formally updates [RFC0793] to mitigate predictable TCP ISNs.

- **August 2014**:

  [I-D.eddy-rfc793bis-04], the upcoming revision of the core TCP incorporates [RFC6528] as the recommended algorithm for TCP ISN generation.

# 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

# Numeric Identifiers (II)

- They have an associated failure severity when requirements are not met:
  - **hard failure**: a non-recoverable condition in which a protocol does not operate in the prescribed manner or it operates with excessive degradation of service
  - **soft failure**: a recoverable condition in which a protocol does not operate in the prescribed manner but normal operation can be resumed automatically in a short period of time.

# 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

# 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
- Such that 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

- Where/how we should pursue this?

# Questions?