Security and Privacy Implications of Transient Numeric Identifiers
(RFC 9414, RFC 9415, RFC 9416)

F. Gont, SI6 Networks
I. Arce, Quarkslab

PEARG. IETF 117
July 22\textsuperscript{nd}-28\textsuperscript{th}, 2023
Introduction
What are “transient numeric identifiers”?

- “Data objects that can be used to distinguish one protocol object from all other objects of the same type” [RFC 9414]
- Examples: TCP ISNs, IP Identification, DNS ID, IPv6 IID, etc.
- They typically have:
  - Interoperability requirements
  - Associated failure severity
- The aforementioned properties are not always carefully spelled out in specs
Brief history of transient numeric identifiers

- Flawed numeric identifiers have plagued protocols for over 40 years
- **Examples:**
  - Predictable TCP Initial Sequence Numbers (ISNs)
  - Predictable ephemeral transport protocol numbers
  - Predictable IPv4 or IPv6 Fragment Identifiers
  - Predictable IPv6 IIDs
  - Predictable DNS TxIDs
- Lessons learned in one protocol were ignored for others
Motivation

- We had already helped fix several flawed numeric identifiers:
  - Transport-protocol ephemeral ports (RFC 6056)
  - TCP ISNs (RFC 6528)
  - IPv6 Identification (RFC 7739)
  - IPv6 Interface Identifiers (RFC 7217, RFC 8064, RFC 8941)
  - NTPv4 ephemeral ports (RFC 9109)
- So we wondered:
  - Why do we keep finding these issues in IETF protocols?
  - Is there anything we can do to stop playing whack-a-mole?
Our initial work on transient numeric identifiers

- draft-gont-predictable-numeric-ids-00 (2016)
  - Timeline of some sample transient numeric identifiers
  - A taxonomy for transient numeric identifiers and associated algorithms
  - Advice on the specification of transient numeric identifiers

- Our original document was split into three pieces:
  - draft-gont-pearg-numeric-ids-history → RFC 9414
  - draft-gont-pearg-numeric-ids-generation → RFC 9415
  - draft-gont-numeric-ids-sec-considerations → RFC 9416
RFC 9414: Unfortunate History of Transient Numeric Identifiers
Taxonomy for transient numeric identifiers

- Goal: Perform root-cause analysis
- Provides a timeline for some sample numeric IDs, considering:
  - Standardization work
  - Vulnerability advisories
  - Research work
- Transient numeric identifiers have usually been poorly specified:
  - Interoperability properties not clearly specified
  - Flawed algorithms recommended, or no algorithms recommended at all
  - In some cases, implementations simply ignored existing recommendations
RFC 9415: On the Generation of Transient Numeric Identifiers
Overview

- Introduce a taxonomy for transient numeric identifiers
- Suggest one good algorithm for each category
- Perform thread modeling for:
  - Specified algorithms
  - Common algorithms employed by popular implementations
## Taxonomy for transient numeric identifiers

<table>
<thead>
<tr>
<th>Cat #</th>
<th>Category</th>
<th>Sample numeric IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Uniqueness (soft failure)</td>
<td>IPv6 Flow Label, DNS ID</td>
</tr>
<tr>
<td>2</td>
<td>Uniqueness (hard failure)</td>
<td>IPv6 ID, TCP ephemeral port</td>
</tr>
<tr>
<td>3</td>
<td>Uniqueness, stable within context (soft failure)</td>
<td>IPv6 IID</td>
</tr>
<tr>
<td>4</td>
<td>Uniqueness, monotonically-increasing within context</td>
<td>TCP ISN, TCP initial timestamp</td>
</tr>
</tbody>
</table>
RFC 9416: Security Considerations for Transient Numeric Identifiers Employed in Network Protocols
Overview

- Introduces requirements for protocol specifications
- Specifications employing transient numeric Identifiers:
  - MUST specify their interoperability requirements (and associated failure severity)
  - MUST perform a vulnerability assessment of their transient numeric identifiers
  - SHOULD NOT employ predictable transient numeric identifiers
  - SHOULD recommend one algorithm for generating the IDs (possibly from RFC 9415)
  - MUST follow these recommendations even when cryptographic techniques are employed
Conclusions
Conclusions

- This has been a lot of work! (7+ years!)
- We hope this work will have a concrete impact on new protocol specifications and implementations
- A big “thank you!” to:
  - All those who provided valuable feedback
  - PEARG chairs, IRTF chair, and Security ADs for their guidance