

Network Working Group  
Internet-Draft  
Updates: [3552](#) (if approved)  
Intended status: Best Current Practice  
Expires: June 8, 2021

F. Gont  
SI6 Networks  
I. Arce  
Quarkslab  
December 5, 2020

**Security Considerations for Transient Numeric Identifiers Employed in  
Network Protocols  
draft-gont-numeric-ids-sec-considerations-06**

Abstract

Poor selection of transient numerical identifiers in protocols such as the TCP/IP suite has historically led to a number of attacks on implementations, ranging from Denial of Service (DoS) to data injection and information leakage that can be exploited by pervasive monitoring. To prevent such flaws in future protocols and implementations, this document updates [RFC 3552](#), requiring future RFCs to contain analysis of the security and privacy properties of any transient numeric identifiers specified by the protocol.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 8, 2021.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Issues with the Specification of Transient Identifiers . . .	<a href="#">4</a>
<a href="#">4.</a>	Common Flaws in the Generation of Transient Identifiers . . .	<a href="#">5</a>
<a href="#">5.</a>	Security and Privacy Requirements for Identifiers . . . . .	<a href="#">6</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">7</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">7</a>
<a href="#">8.</a>	Acknowledgements . . . . .	<a href="#">7</a>
<a href="#">9.</a>	References . . . . .	<a href="#">7</a>
<a href="#">9.1.</a>	Normative References . . . . .	<a href="#">7</a>
<a href="#">9.2.</a>	Informative References . . . . .	<a href="#">8</a>
	Authors' Addresses . . . . .	<a href="#">9</a>

## [1.](#) Introduction

Network protocols employ a variety of transient numeric identifiers for different protocol entities, ranging from DNS Transaction IDs (TxIDs) to transport protocol numbers (e.g. TCP ports) or IPv6 Interface Identifiers (IIDs). These identifiers usually have specific properties that must be satisfied such that they do not result in negative interoperability implications (e.g., uniqueness during a specified period of time), and an associated failure severity when such properties not met.

The TCP/IP protocol suite alone has been subject to variety of attacks on its numerical identifiers over the past 30 years or more, with effects ranging from Denial of Service (DoS) or data injection, to information leakage that could be exploited for pervasive monitoring [[RFC7258](#)]. The root of these issues has been, in many cases, the poor selection of identifiers in such protocols, usually as a result of insufficient or misleading specifications. While it is generally trivial to identify an algorithm that can satisfy the interoperability requirements for a given identifier, there exists practical evidence [[I-D.irtf-pearg-numeric-ids-history](#)] that doing so without negatively affecting the security and/or privacy properties of the aforementioned protocols is prone to error.

For example, implementations have been subject to security and/or privacy issues resulting from:



- o Predictable TCP sequence numbers
- o Predictable transport protocol numbers
- o Predictable IPv4 or IPv6 Fragment Identifiers
- o Predictable IPv6 IIDs
- o Predictable DNS TxIDs

Recent history indicates that when new protocols are standardized or new protocol implementations are produced, the security and privacy properties of the associated identifiers tend to be overlooked and inappropriate algorithms to generate such identifiers are either suggested in the specification or selected by implementers. As a result, advice in this area is warranted.

[Section 3](#) provides an overview of common flaws in the specification of transient numeric identifiers. [Section 4](#) provides an overview of the implications of predictable transient numeric identifiers. Finally, [Section 5](#) provides key guidelines for protocol designers.

## 2. Terminology

Transient Numeric Identifier:

A data object in a protocol specification that can be used to definitely distinguish a protocol object (a datagram, network interface, transport protocol endpoint, session, etc) from all other objects of the same type, in a given context. Transient numeric identifiers are usually defined as a series of bits, and represented using integer values. These identifiers are typically dynamically selected, as opposed to statically-assigned numeric identifiers (see e.g. [[IANA-PROT](#)]). We note that different identifiers may have additional requirements or properties depending on their specific use in a protocol. We use the term "transient numeric identifier" (or simply "numeric identifier" or "identifier" as short forms) as a generic term to refer to any data object in a protocol specification that satisfies the identification property stated above.

Failure Severity:

The consequences of a failure to comply with the interoperability requirements of a given identifier. Severity considers the worst potential consequence of a failure, determined by the system damage and/or time lost to repair the failure. In this document we define two types of failure severity: "soft" and "hard".

Hard Failure:



A hard failure is a non-recoverable condition in which a protocol does not operate in the prescribed manner or it operates with excessive degradation of service. For example, an established TCP connection that is aborted due to an error condition constitutes, from the point of view of the transport protocol, a hard failure, since it enters a state from which normal operation cannot be recovered.

#### Soft Failure:

A soft failure is 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. For example, a simple packet-loss event that is subsequently recovered with a retransmission can be considered a soft failure.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

### **3. Issues with the Specification of Transient Identifiers**

A recent survey of transient numerical identifier usage in protocol specifications and implementations [[I-D.irtf-pearg-numeric-ids-history](#)] revealed that most of the issues discussed in this document arise as a result of one of the following conditions:

- o Protocol specifications that under-specify the requirements for their identifiers
- o Protocol specifications that over-specify their identifiers
- o Protocol implementations that simply fail to comply with the specified requirements

Both under-specifying and over-specifying identifier contents is hazardous. TCP port numbers and sequence numbers [[RFC0793](#)] and DNS TxID [[RFC1035](#)] were under-specified, leading to implementations that used predictable values and thus were vulnerable to numerous off-path attacks. Over-specification, as for IPv6 Interface Identifiers (IIDs) [[RFC4291](#)] and Fragment Identification values [[RFC2460](#)], leaves implementations unable to respond to security and privacy issues stemming from the mandated algorithm -- IPv6 IIDs need not expose privacy-sensitive link-layer addresses, and predictable Fragment Identifiers invite the same off-path attacks that plague TCP.



Finally, there are protocol implementations that simply fail to comply with existing protocol specifications. That is, appropriate guidance is provided by the protocol specification (whether the core specification or an update to it), but an implementation simply fails to follow such guidance. For example, some popular operating systems (notably Microsoft Windows) still fail to implement transport-protocol port randomization, as specified in [[RFC6056](#)].

Clear specification of the interoperability requirements for the transient numeric identifiers will help identify possible algorithms that could be employed to generate them, and also make evident if such identifiers are being over-specified. A protocol specification will usually also benefit from a security and privacy analysis of the transient numeric identifiers they specify, to prevent the corresponding considerations from being overlooked.

#### **4. Common Flaws in the Generation of Transient Identifiers**

This section briefly notes common flaws associated with the generation of transient numeric identifiers. Such common flaws include, but are not limited to:

- o Employing trivial algorithms (e.g. global counters) that result in predictable identifiers
- o Employing the same identifier across contexts in which constancy is not required
- o Re-using identifiers across different protocols or layers of the protocol stack
- o Initializing counters or timers to constant values, when such initialization is not required
- o Employing the same increment space across different contexts
- o Use of flawed pseudo-random number generators (PRNGs).

Employing trivial algorithms for generating the identifiers means that any node that is able to sample such identifiers can easily predict future identifiers employed by the victim node.

When one identifier is employed across contexts where such constancy is not needed, activity correlation is made made possible. For example, employing an identifier that is constant across networks allows for node tracking across networks.





Re-using identifiers across different layers or protocols ties the security and privacy of the protocol re-using the identifier to the security and privacy properties of the original identifier (over which the protocol re-using the identifier may have no control regarding its generation). Besides, when re-using an identifier across protocols from different layers, the goal of isolating the properties of a layer from that of another layer is broken, and the privacy and security analysis may be harder to perform, since the combined system, rather than each protocol in isolation will have to be assessed.

At times, a protocol needs to convey order information (whether sequence, timing, etc.). In many cases, there is no reason for the corresponding counter or timer to be initialized to any specific value e.g. at system bootstrap. Similarly, there may not be a need for the difference between successive counted values to be a predictable.

A node that implements a per-context linear function may share the increment space among different contexts (please see the "Simple Hash-Based Algorithm" in [[I-D.irtf-pearg-numeric-ids-generation](#)]). Sharing the same increment space allows an attacker that can sample identifiers in other context to e.g. learn how many identifiers have been generated between two sampled values.

Finally, some implementations have been found to employ flawed PRNGs. See e.g. [[Klein2007](#)].

## 5. Security and Privacy Requirements for Identifiers

When a protocol specifies transient numerical identifiers, it is critical for the protocol specification to:

1. Clearly specify the interoperability requirements for the aforementioned identifiers (e.g., required properties such as uniqueness, along with the failure severity if such properties are not met).
2. Provide a security and privacy analysis of the aforementioned identifiers.
3. Recommend an algorithm for generating the aforementioned identifiers that mitigates security and privacy issues, such as those discussed in [[I-D.irtf-pearg-numeric-ids-generation](#)].



## **6. IANA Considerations**

There are no IANA registries within this document. The RFC-Editor can remove this section before publication of this document as an RFC.

## **7. Security Considerations**

This entire document is about the security and privacy implications of transient numeric identifiers, and formally updates [[RFC3552](#)] such that the security and privacy implications of transient numeric identifiers are considered when writing the "Security Considerations" section of future RFCs.

## **8. Acknowledgements**

The authors would like to thank Benjamin Kaduk for providing valuable comments and suggestions that have been incorporated into this document.

This document is based on the document [[I-D.gont-predictable-numeric-ids](#)] co-authored by Fernando Gont and Ivan Arce. Thus, the authors would like to thank (in alphabetical order) Steven Bellovin, Joseph Lorenzo Hall, Gre Norcie, for providing valuable comments on that document.

The authors would like to thank Diego Armando Maradona for his magic and inspiration.

## **9. References**

### **9.1. Normative References**

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", [BCP 72](#), [RFC 3552](#), DOI 10.17487/RFC3552, July 2003, <<https://www.rfc-editor.org/info/rfc3552>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.



## 9.2. Informative References

- [I-D.gont-predictable-numeric-ids]  
Gont, F. and I. Arce, "Security and Privacy Implications of Numeric Identifiers Employed in Network Protocols", [draft-gont-predictable-numeric-ids-03](#) (work in progress), March 2019.
- [I-D.irtf-pearg-numeric-ids-generation]  
Gont, F. and I. Arce, "On the Generation of Transient Numeric Identifiers", [draft-irtf-pearg-numeric-ids-generation-03](#) (work in progress), September 2020.
- [I-D.irtf-pearg-numeric-ids-history]  
Gont, F. and I. Arce, "Unfortunate History of Transient Numeric Identifiers", [draft-irtf-pearg-numeric-ids-history-03](#) (work in progress), October 2020.
- [IANA-PROT]  
IANA, "Protocol Registries",  
<<https://www.iana.org/protocols>>.
- [Klein2007]  
Klein, A., "OpenBSD DNS Cache Poisoning and Multiple O/S Predictable IP ID Vulnerability", 2007,  
<[https://dl.packetstormsecurity.net/papers/attack/OpenBSD\\_DNS\\_Cache\\_Poisoning\\_and\\_Multiple\\_OS\\_Predictable\\_IP\\_ID\\_Vulnerability.pdf](https://dl.packetstormsecurity.net/papers/attack/OpenBSD_DNS_Cache_Poisoning_and_Multiple_OS_Predictable_IP_ID_Vulnerability.pdf)>.
- [RFC0793] Postel, J., "Transmission Control Protocol", STD 7, [RFC 793](#), DOI 10.17487/RFC0793, September 1981,  
<<https://www.rfc-editor.org/info/rfc793>>.
- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), DOI 10.17487/RFC1035, November 1987, <<https://www.rfc-editor.org/info/rfc1035>>.
- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), DOI 10.17487/RFC2460, December 1998, <<https://www.rfc-editor.org/info/rfc2460>>.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", [RFC 4291](#), DOI 10.17487/RFC4291, February 2006, <<https://www.rfc-editor.org/info/rfc4291>>.



[RFC6056] Larsen, M. and F. Gont, "Recommendations for Transport-Protocol Port Randomization", [BCP 156](#), [RFC 6056](#), DOI 10.17487/RFC6056, January 2011, <<https://www.rfc-editor.org/info/rfc6056>>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", [BCP 188](#), [RFC 7258](#), DOI 10.17487/RFC7258, May 2014, <<https://www.rfc-editor.org/info/rfc7258>>.

#### Authors' Addresses

Fernando Gont  
SI6 Networks  
Evaristo Carriego 2644  
Haedo, Provincia de Buenos Aires 1706  
Argentina

Phone: +54 11 4650 8472  
Email: [fgont@si6networks.com](mailto:fgont@si6networks.com)  
URI: <https://www.si6networks.com>

Ivan Arce  
Quarkslab

Email: [iarce@quarkslab.com](mailto:iarce@quarkslab.com)  
URI: <https://www.quarkslab.com>



