Security Considerations for Transient Numeric Identifiers Employed in
Network Protocols

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) or data
   injection to information leakages that can be exploited by pervasive
   monitoring.  Due diligence in the specification of transient numeric
   identifiers is required even when cryptographic techniques are
   employed, since these techniques might not mitigate all the
   associated issues.  This document formally updates RFC 3552,
   incorporating requirements for transient numeric identifiers, to
   prevent flaws in future protocols and implementations.

Status of This Memo

   This memo documents an Internet Best Current Practice.

   This document is a product of the Internet Engineering Task Force
   (IETF).  It represents the consensus of the IETF community.  It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG).  Further information on
   BCPs is available in Section 2 of RFC 7841.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   https://www.rfc-editor.org/info/rfc9416.

Copyright Notice

Table of Contents

1.  Introduction

   Networking protocols employ a variety of transient numeric
   identifiers for different protocol objects, such as IPv4 and IPv6
   Identification values [RFC0791] [RFC8200], IPv6 Interface Identifiers
   (IIDs) [RFC4291], transport-protocol ephemeral port numbers
   [RFC6056], TCP Initial Sequence Numbers (ISNs) [RFC9293], NTP
   Reference IDs (REFIDs) [RFC5905], and DNS IDs [RFC1035].  These
   identifiers typically have specific requirements (e.g., uniqueness
   during a specified period of time) that must be satisfied such that
   they do not result in negative interoperability implications, and an
   associated failure severity when such requirements are not met
   [RFC9415].

   | NOTE: Some documents refer to the DNS ID as the DNS "Query ID"
   | or "TxID".

   For more than 30 years, a large number of implementations of IETF
   protocols have been subject to a variety of attacks, with effects
   ranging from Denial of Service (DoS) or data injection to information
   leakages that could be exploited for pervasive monitoring [RFC7258].
   The root cause of these issues has been, in many cases, the poor
   selection of transient numeric 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 of a given transient numeric
   identifier, empirical evidence exists that doing so without
   negatively affecting the security and/or privacy properties of the
   aforementioned protocols is prone to error [RFC9414].

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

   *  predictable IPv4 or IPv6 Identification values (e.g., see
      [Sanfilippo1998a], [RFC6274], and [RFC7739]),

   *  predictable IPv6 IIDs (e.g., see [RFC7217], [RFC7707], and
      [RFC7721]),

   *  predictable transport-protocol ephemeral port numbers (e.g., see
      [RFC6056] and [Silbersack2005]),

   *  predictable TCP Initial Sequence Numbers (ISNs) (e.g., see
      [Morris1985], [Bellovin1989], and [RFC6528]),

*   predictable initial timestamps in TCP timestamps options (e.g., see [TCPT-uptime] and [RFC7323]), and

*   predictable DNS IDs (see, e.g., [Schuba1993] and [Klein2007]).

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

We note that the use of cryptographic techniques for confidentiality and authentication might not eliminate all the issues associated with predictable transient numeric identifiers.  Therefore, due diligence in the specification of transient numeric identifiers is required even when cryptographic techniques are employed.

> NOTE: For example, cryptographic authentication can readily mitigate data injection attacks even in the presence of predictable transient numeric identifiers (such as "sequence numbers").  However, use of flawed algorithms (such as global counters) for generating transient numeric identifiers could still result in information leakages even when cryptographic techniques are employed.  These information leakages could in turn be leveraged to perform other devastating attacks (please see [RFC9415] for further details).

Section 3 provides an overview of common flaws in the specification of transient numeric identifiers.  Section 4 provides an overview of common flaws in the generation of transient numeric identifiers and their associated security and privacy implications.  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 (e.g., see [IANA-PROT]).  We note that different transient numeric 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 interoperability 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".

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

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. 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.

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 Numeric Identifiers

Recent work on transient numeric identifier usage in protocol specifications and implementations [RFC9414] [RFC9415] revealed that most of the issues discussed in this document arise as a result of one of the following conditions:

* protocol specifications that under specify their transient numeric identifiers

* protocol specifications that over specify their transient numeric identifiers

* protocol implementations that simply fail to comply with the specified requirements

Both under specifying and over specifying transient numeric identifiers is hazardous. TCP local ports [RFC0793], as well as DNS IDs [RFC1035], were originally under specified, leading to implementations that resulted in predictable values and thus were vulnerable to numerous off-path attacks. Over specification, as for IPv6 Interface Identifiers (IIDs) [RFC4291] and IPv6 Identification values [RFC2460], left implementations unable to respond to security and privacy issues stemming from the mandated or recommended algorithms -- IPv6 IIDs need not expose privacy-sensitive link-layer addresses, and predictable IPv6 Fragment Header Identification values 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 it be the core specification or an update to it), but an implementation simply fails to follow such guidance. For example, some popular operating systems 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 vulnerability assessment of the transient numeric identifiers they specify to prevent the corresponding considerations from being overlooked.

4.  Common Flaws in the Generation of Transient Numeric Identifiers

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

*   employing trivial algorithms (e.g., global counters) that result in predictable identifiers,

*   employing the same identifier across contexts in which constancy is not required,

*   reusing identifiers across different protocols or layers of the protocol stack,

*   initializing counters or timers to constant values when such initialization is not required,

*   employing the same increment space across different contexts, and

*   use of flawed Pseudorandom 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 possible. For example, employing an identifier that is constant across networks allows for node tracking across networks.

Reusing identifiers across different layers or protocols ties the security and privacy properties of the protocol reusing the identifier to the security and privacy properties of the original identifier (over which the protocol reusing the identifier may have no control regarding its generation). Besides, when reusing an identifier across protocols from different layers, the goal of isolating the properties of a layer from those of another layer is broken, and the vulnerability assessment 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 it be 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 counter values to be predictable.

A node that implements a per-context linear function may share the increment space among different contexts (please see the "Simple PRF-Based Algorithm" section in [RFC9415]).  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 (e.g., see [Klein2007]).

## 5.  Requirements for Transient Numeric Identifiers

Protocol specifications that employ transient numeric identifiers MUST explicitly specify the interoperability requirements for the aforementioned transient numeric identifiers (e.g., required properties such as uniqueness, along with the failure severity if such requirements are not met).

A vulnerability assessment of the aforementioned transient numeric identifiers MUST be performed as part of the specification process. Such vulnerability assessment should cover, at least, spoofing, tampering, repudiation, information disclosure, DoS, and elevation of privilege.

> NOTE: Sections 8 and 9 of [RFC9415] provide a general vulnerability assessment of transient numeric identifiers, along with a vulnerability assessment of common algorithms for generating transient numeric identifiers.  Please see [Shostack2014] for further guidance on threat modeling.

Protocol specifications SHOULD NOT employ predictable transient numeric identifiers, except when such predictability is the result of their interoperability requirements.

Protocol specifications that employ transient numeric identifiers SHOULD recommend an algorithm for generating the aforementioned transient numeric identifiers that mitigates the vulnerabilities identified in the previous step, such as those discussed in [RFC9415].

As discussed in Section 1, use of cryptographic techniques for confidentiality and authentication might not eliminate all the issues associated with predictable transient numeric identifiers. Therefore, the advice from this section MUST still be applied for cases where cryptographic techniques for confidentiality or authentication are employed.

## 6.  IANA Considerations

This document has no IANA actions.

## 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 addressed when writing the "Security Considerations" section of future RFCs.

## 8.  References

### 8.1.  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>.

### 8.2.  Informative References

[Bellovin1989]
           Bellovin, S., "Security Problems in the TCP/IP Protocol Suite", Computer Communications Review, vol. 19, no. 2, pp. 32-48, April 1989, <https://www.cs.columbia.edu/~smb/papers/ipext.pdf>.

[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", October 2007, <https://dl.packetstormsecurity.net/papers/attack/OpenBSD_DNS_Cache_Poisoning_and_Multiple_OS_Predictable_IP_ID_Vuln erability.pdf>.

[Morris1985]
           Morris, R., "A Weakness in the 4.2BSD UNIX TCP/IP Software", CSTR 117, AT&T Bell Laboratories, Murray Hill, NJ, February 1985, <https://pdos.csail.mit.edu/~rtm/papers/117.pdf>.

[PREDICTABLE-NUMERIC-IDS]
           Gont, F. and I. Arce, "Security and Privacy Implications of Numeric Identifiers Employed in Network Protocols",

                   Work in Progress, Internet-Draft, draft-gont-predictable-
                   numeric-ids-03, 11 March 2019,
                   <https://datatracker.ietf.org/doc/html/draft-gont-
                   predictable-numeric-ids-03>.

[RFC0791]    Postel, J., "Internet Protocol", STD 5, RFC 791,
                   DOI 10.17487/RFC0791, September 1981,
                   <https://www.rfc-editor.org/info/rfc791>.

[RFC0793]    Postel, J., "Transmission Control Protocol", 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>.

[RFC5905]    Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch,
                   "Network Time Protocol Version 4: Protocol and Algorithms
                   Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010,
                   <https://www.rfc-editor.org/info/rfc5905>.

[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>.

[RFC6274]    Gont, F., "Security Assessment of the Internet Protocol
                   Version 4", RFC 6274, DOI 10.17487/RFC6274, July 2011,
                   <https://www.rfc-editor.org/info/rfc6274>.

[RFC6528]    Gont, F. and S. Bellovin, "Defending against Sequence
                   Number Attacks", RFC 6528, DOI 10.17487/RFC6528, February
                   2012, <https://www.rfc-editor.org/info/rfc6528>.

[RFC7217]    Gont, F., "A Method for Generating Semantically Opaque
                   Interface Identifiers with IPv6 Stateless Address
                   Autoconfiguration (SLAAC)", RFC 7217,
                   DOI 10.17487/RFC7217, April 2014,
                   <https://www.rfc-editor.org/info/rfc7217>.

[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>.

[RFC7323]    Borman, D., Braden, B., Jacobson, V., and R.
                   Scheffenegger, Ed., "TCP Extensions for High Performance",
                   RFC 7323, DOI 10.17487/RFC7323, September 2014,

          <https://www.rfc-editor.org/info/rfc7323>.

[RFC7707]  Gont, F. and T. Chown, "Network Reconnaissance in IPv6
           Networks", RFC 7707, DOI 10.17487/RFC7707, March 2016,
           <https://www.rfc-editor.org/info/rfc7707>.

[RFC7721]  Cooper, A., Gont, F., and D. Thaler, "Security and Privacy
           Considerations for IPv6 Address Generation Mechanisms",
           RFC 7721, DOI 10.17487/RFC7721, March 2016,
           <https://www.rfc-editor.org/info/rfc7721>.

[RFC7739]  Gont, F., "Security Implications of Predictable Fragment
           Identification Values", RFC 7739, DOI 10.17487/RFC7739,
           February 2016, <https://www.rfc-editor.org/info/rfc7739>.

[RFC8200]  Deering, S. and R. Hinden, "Internet Protocol, Version 6
           (IPv6) Specification", STD 86, RFC 8200,
           DOI 10.17487/RFC8200, July 2017,
           <https://www.rfc-editor.org/info/rfc8200>.

[RFC9293]  Eddy, W., Ed., "Transmission Control Protocol (TCP)",
           STD 7, RFC 9293, DOI 10.17487/RFC9293, August 2022,
           <https://www.rfc-editor.org/info/rfc9293>.

[RFC9414]  Gont, F. and I. Arce, "Unfortunate History of Transient
           Numeric Identifiers", RFC 9414, DOI 10.17487/RFC9414, July
           2023, <https://www.rfc-editor.org/info/rfc9414>.

[RFC9415]  Gont, F. and I. Arce, "On the Generation of Transient
           Numeric Identifiers", RFC 9415, DOI 10.17487/RFC9415, July
           2023, <https://www.rfc-editor.org/info/rfc9415>.

[Sanfilippo1998a]
           Sanfilippo, S., "about the ip header id", message to the
           Bugtraq mailing list, December 1998,
           <https://seclists.org/bugtraq/1998/Dec/48>.

[Schuba1993]
           Schuba, C., "Addressing Weakness in the Domain Name System
           Protocol", August 1993,
           <http://ftp.cerias.purdue.edu/pub/papers/christoph-schuba/
           schuba-DNS-msthesis.pdf>.

[Shostack2014]
           Shostack, A., "Threat Modeling: Designing for Security",
           Wiley, 1st edition, February 2014.

[Silbersack2005]
           Silbersack, M., "Improving TCP/IP security through
           randomization without sacrificing interoperability",
           EuroBSDCon 2005 Conference, January 2005,
           <http://www.silby.com/eurobsdcon05/
           eurobsdcon_silbersack.pdf>.

[TCPT-uptime]
           McDanel, B., "TCP Timestamping - Obtaining System Uptime

Remotely", message to the Bugtraq mailing list, March
2001, <https://seclists.org/bugtraq/2001/Mar/182>.

## Acknowledgements

## Authors' Addresses

Fernando Gont
SI6 Networks
Segurola y Habana 4310 7mo piso
Ciudad Autonoma de Buenos Aires
Argentina
Email: fgont@si6networks.com
URI:   https://www.si6networks.com


Ivan Arce
Quarkslab
Segurola y Habana 4310 7mo piso
Ciudad Autonoma de Buenos Aires
Argentina
Email: iarce@quarkslab.com
URI:   https://www.quarkslab.com