Network Working Group   F. Gont
Internet-Draft   SI6 Networks / UTN-FRH
Updates: 3552 (if approved)   I. Arce
Intended status: Best Current Practice   Fundacion Sadosky
Expires: December 21, 2016   June 19, 2016

Security Considerations for Transient Numeric Identifiers Employed in Network Protocols

draft-gont-numeric-ids-sec-considerations-00

Abstract

For more than 30 years, a large number of implementations of the TCP/IP protocol suite have been subject to a variety of attacks, with effects ranging from Denial of Service (DoS) or data injection, to information leakage that could be exploited for pervasive monitoring. The root of these issues has been, in many cases, the poor selection of transient identifiers in such protocols, usually as a result of an insufficient or misleading specifications. This document formally updates RFC3552, such that RFCs are required to perform a security and privacy analysis of the transient numeric identifiers they specify.

Status of This Memo

Copyright Notice

Table of Contents

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 associated failure severities when such properties are not met.

For more than 30 years, a large number of implementations of the TCP/IP protocol suite have been subject to a variety of attacks, with effects ranging from Denial of Service (DoS) or data injection, to information leakage that could be exploited for pervasive monitoring [RFC7528]. The root of these issues has been, in many cases, the poor selection of identifiers in such protocols, usually as a result of an insufficient or misleading specification. While it is generally trivial to identify an algorithm that can satisfy the interoperability requirements for a given identifier, there exists practical evidence 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:

- Predictable TCP sequence numbers

- Predictable transport protocol numbers

- Predictable IPv4 or IPv6 Fragment Identifiers

- Predictable IPv6 IIDs

- 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 identifier values are either suggested in the specification or selected by implementators. As a result, we believe that advice in this area is warranted.

2. Terminology

Identifier:
A data object in a protocol specification that can be used to definetely 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. Identifiers are usually defined as a series of bits and represented using integer values. We note that different identifiers may have additional requirements or properties depending on their specific use in a protocol. We use the term "identifier" as a generic term to refer to any data object in a protocol specification that satisfies the identification property stated above. Throughout this document we refer as "transient network identifiers" (or simply as "identifiers") to the identifiers being dynamically selected by a protocol. Our use of "identifier" excludes static values such as "Protocol Numbers" and the like.

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", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Issues with the Specification of Identifiers

While assessing protocol specifications and implementations regarding the use of transient numeric identifiers, we found that most of the issues discussed in this document arise as a result of one of the following:

- Protocol specifications which under-specify the requirements for their identifiers

- Protocol specifications that over-specify their identifiers

- Protocol implementations that simply fail to comply with the specified requirements

A number of protocol implementations (too many of them) simply overlook the security and privacy implications of identifiers. Examples of them are the specification of TCP port numbers in [RFC0793], the specification of TCP sequence numbers in [RFC0793], or the specification of the DNS TxID in [RFC1035].

On the other hand, there are a number of protocol specifications that over-specify some of their associated protocol identifiers. For example, [RFC4291] essentially results in link-layer addresses being embedded in the IPv6 Interface Identifiers (IIDs) when the interoperability requirement of uniqueness could be achieved in other ways that do not result in negative security and privacy implications [RFC7721]. Similarly, [RFC2460] suggests the use of a global counter

for the generation of Fragment Identification values, when the interoperability properties of uniqueness per {Src IP, Dst IP} could be achieved with other algorithms that do not result in negative security and privacy implications.

Finally, there are protocol implementations that simply fail to comply with existing protocol specifications. For example, some popular operating systems (notably Microsoft Windows) still fail to implement randomization of transport protocol ephemeral ports, as specified in [RFC6056].

By requiring protocol specifications to clearly specify the interoperability requirements for the transient numeric identifiers they specify, the constraints in the possible algorithms to generate them, as well as possible over-specification of such identifiers, become evident. Furthermore, requiring specifications to include a security and privacy analysis of the transient numeric identifiers they specify prevents the corresponding considerations from being overlooked at the time a protocol is specified.

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 PRNGs.

Employing trivial algorithms for generating the identifiers means that any node that is able to sample the aforementioned identifier can easily predict future identifiers employed by the victim node. For example, the algorithm for Fragment Identification selection in [RFC2460] and the algorithm for TCP ISN selection in [RFC0793].

When one identifier is employed across contexts where such constancy is not needed, activity correlation is made made possible. For example, [RFC4291] essentially results in link-layer addresses being embedded in the IPv6 Interface Identifiers (IIDs) when the interoperability requirement of uniqueness could be achieved in other ways. 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 such 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 layer, this breaks the goal of layers of isolating the properties of a layer from that of another layer. The reuse of link-layer addresses in IPv6 addresses specified in [RFC4291] is one example of that.

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. For example, an implementations that employs a counter for the Fragment Identifier [RFC2460] that gets initialized to zero upon system bootstrapping will leak the amount of fragmented traffic that this node has transmitted. Similarly, a node that updates a timer to zero when bootstrapping will reveal the "uptime" of the node.

When 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.gont-predictable-numeric-ids]). 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. [Sanfilippo1998a] and [Sanfilippo1998b] employ shared increment spaces to leak the amount of fragmented traffic that has been transmitted by a target node.

Finally, some implementations have been found to emply flawed PRNGs. See e.g.[Klein2007].

5. Security and Privacy Requirements for Identifiers

Protocol specifications that specify transient numeric identifiers MUST:

1. Clearly specify the interoperability requirements for the aforementioned identifiers.

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.gont-predictable-numeric-ids].

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

The entire document is about the security and privacy implications of transient numeric identifiers, and formally updates [RFC3552] such that the "Security Considerations" sections of RFCs are required to perform a security and privacy analysis of the numeric identifiers they specify.

8. Acknowledgements

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.

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, <http://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, <http://www.rfc-editor.org/info/rfc3552>.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <http://www.rfc-editor.org/info/rfc793>.

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

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <http://www.rfc-editor.org/info/rfc4086>.

[RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, DOI 10.17487/RFC6151, March 2011, <http://www.rfc-editor.org/info/rfc6151>.

[RFC7098] Carpenter, B., Jiang, S., and W. Tarreau, "Using the IPv6 Flow Label for Load Balancing in Server Farms", RFC 7098, DOI 10.17487/RFC7098, January 2014, <http://www.rfc-editor.org/info/rfc7098>.

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

9.2. Informative References

[Sanfilippo1998a]
Sanfilippo, S., "about the ip header id", Post to Bugtraq mailing-list, Mon Dec 14 1998, <http://seclists.org/bugtraq/1998/Dec/48>.

[Sanfilippo1998b]
Sanfilippo, S., "Idle scan", Post to Bugtraq mailing-list, 1998, <http://www.kyuzz.org/antirez/papers/dumbscan.html>.

[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-00 (work in progress), February 2016.

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, DOI 10.17487/RFC1321, April 1992, <http://www.rfc-editor.org/info/rfc1321>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <http://www.rfc-editor.org/info/rfc4291>.

[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, <http://www.rfc-editor.org/info/rfc7721>.

[RFC7528] Higgs, P. and J. Piesing, "A Uniform Resource Name (URN) Namespace for the Hybrid Broadcast Broadband TV (HbbTV) Association", RFC 7528, DOI 10.17487/RFC7528, April 2015, <http://www.rfc-editor.org/info/rfc7528>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <http://www.rfc-editor.org/info/rfc1035>.

[Klein2007] Klein, A., "OpenBSD DNS Cache Poisoning and Multiple O/S Predictable IP ID Vulnerability", 2007, <http://www.trusteer.com/files/OpenBSD_DNS_Cache_Poisoning_and_Multiple_OS_Predictable_IP_ID_Vulnerability.pdf>.

Authors' Addresses

Fernando Gont
SI6 Networks / UTN-FRH
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
Email: fgont@si6networks.com
URI: http://www.si6networks.com

Ivan Arce
Fundacion Dr. Manuel Sadosky
Av. Cordoba 744 Piso 5 Oficina I
Ciudad Autonoma de Buenos Aires, Buenos Aires C1054AAT
Argentina

Phone: +54 11 4328 5164
Email: stic@fundacionsadosky.org.ar
URI: http://www.fundacionsadosky.org.ar