Network Time Protocol (ntp) Working Group
Internet-Draft
Obsoletes: rfc5905 (if approved)
Intended status: Standards Track
Expires: November 21, 2019

F. Gont
G. Gont
SI6 Networks

May 20, 2019

Port Randomization in the Network Time Protocol Version 4 draft-gont-ntp-port-randomization-01

Abstract

The Network Time Protocol can operate in several modes. Some of these modes are based on the receipt of unsolicited packets, and therefore require the use of a service/well-known port as the local port number. However, in the case of NTP modes where the use of a service/well-known port is not required, employing such well-known/service port unnecessarily increases the ability of attackers to perform blind/off-path attacks, since knowledge of such port number is typically required for such attacks. This document formally updates RFC5905, recommending the use of port randomization for those modes where use of the NTP service port is not required.

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 November 21, 2019.

Table of Contents

1. Introduction

The Network Time Protocol (NTP) is one of the oldest Internet protocols, and currently specified in [RFC5905]. Since its its original implementation, standardization and deployment, a number of vulnerabilities have been found both in the NTP specification and in some of its implementations [NTP-VULN]. Some of these vulnerabilities allow for off-path/blind attacks, where an attacker can send forged packets to one or both NTP peers for achieving Denial of Service (DoS), time-shifts, and other undesirable outcomes. Many of these attacks require the attacker to guess or know at least a target association, typically identified by the tuple {srcaddr, srcport, dstaddr, dstport, keyid}. Some of these parameters may be easily known or guessed.

NTP can operate in several modes. Some of these modes rely on the ability to receive unsolicited packets, and therefore require the use of a service/well-known port number. However, for modes where the use of a service/well-known port is not required, employing such well-known/service port improves the ability of an attacker to perform blind/off-path attacks (since knowledge of such port number is typically required for such attacks). A recent study [NIST-NTP] that analyzes the port numbers employed by NTP peers suggests that a considerable number of NTP peers employ the NTP service/well-known

port as their local port, or select predictable ephemeral port numbers, thus improving the ability of attackers to perform blind/ off-path attacks against NTP.

This document formally updates [RFC5905], recommending the use of port randomization for those NTP modes where use of the NTP service port is not required.

2. Terminology

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 [RFC2119].

3. Update to RFC5905

The specification of the "srcport" and "dstport" peer process variables from Section 9.1 ("Peer Process Variables") of [RFC5905] is updated as follows:

srcport: UDP port number of the server or reference clock. This becomes the destination port number in packets sent from this association. When operating in symmetric modes (1 and 2), this field must contain the NTP port number PORT (123) assigned by the IANA. In other modes, it SHOULD contain a randomized port number, as specified in [RFC6056].

dstport: UDP port number of the client. In the case of broadcast server mode (5) and symmetric modes (1 and 2), it must contain the NTP port number PORT (123) assigned by the IANA. In other cases, it SHOULD contain a randomized port number, as specified in [RFC6056]. The value in this variable becomes the source port number in packets sent from this association.

NOTES:

The port number is to be randomized on a per-association basis. That is, a random port number is selected when an association is first mobilized, and the selected port number is expected to remain constant during the life of an association.

On most current operating systems (that implement ephemeral port randomization [RFC6056]), an NTP peer may normally rely on the operating system for performing port randomization. For example, NTP implementations employing the Sockets API may achieve port randomization by *not* specifying the local port for the corresponding socket, or bind()ing the local socket to the "special" port 0 (which for the Sockets API has the special meaning of "any port").

4. Implementation Status

[RFC Editor: Please remove this section before publication of this document as an RFC.]

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [RFC7942]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

OpenNTPD:
: [OpenNTPD] has never explictly set the local port of NTP clients, and thus employs the ephemeral port selection algorithm implemented by the operating system. Thus, on all operating systems that implement port randomization (such as current versions of OpenBSD, Linux, and FreeBSD), OpenNTPD will employ port randomization for client ports.

chrony:
: [chrony] has never explictly set the local port of NTP clients, and thus employs the ephemeral port selection algorithm implemented by the operating system. Thus, on all operating systems that implement port randomization (such as current versions of OpenBSD, Linux, and FreeBSD), chrony will employ port randomization for client ports.

nwtime.org's sntp client:
: sntp does not explictly set the local port, and thus employs the ephemeral port selection algorithm implemented by the operating system. Thus, on all operating systems that implement port randomization (such as current versions of OpenBSD, Linux, and FreeBSD), it will employ port randomization for client ports.

5. 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.

6. Security Considerations

The security implications of predictable numeric identifiers [I-D.gont-predictable-numeric-ids] (and of predictable transport-protocol port numbers [RFC6056] in particular) have been known for a long time now. However, the NTP specification have traditionally followed a pattern of employing common settings and code even when not strictly necessary, which at times has resulted in negative security and privacy implications (see e.g. [I-D.ietf-ntp-data-minimization]). The use of the NTP service port (123) for the srcport and dstport variables is not required for all operating modes, and such unnecessary usage comes at the expense of reducing the amount of work required for an attacker to successfully perform off-path/blind attacks against NTP. Therefore, this document formally updates [RFC5905], recommending the use of transport-protocol port randomization when use of the NTP service port is not required.

This issue has been tracked by US-CERT with VU#597821, and has been assigned CVE-2019-11331.

7. Acknowledgments

The authors would like to thank (in alphabetical order) Miroslav Lichvar, and Steven Sommars, for providing valuable comments on earlier versions of this document.

The authors would like to thank Harlan Stenn for answering questions about nwtime.org's NTP implementation.

Fernando would like to thank Nelida Garcia and Jorge Oscar Gont, for their love and support.

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>.

[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>.

8.2. Informative References

[chrony] "chrony", <https://chrony.tuxfamily.org/>.

[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.ietf-ntp-data-minimization]
Franke, D. and A. Malhotra, "NTP Client Data Minimization", draft-ietf-ntp-data-minimization-04 (work in progress), March 2019.

[NIST-NTP]
Sherman, J. and J. Levine, "Usage Analysis of the NIST Internet Time Service", Journal of Research of the National Institute of Standards and Technology Volume 121, March 2016, <https://tf.nist.gov/general/pdf/2818.pdf>.

[NTP-VULN]
Network Time Foundation, "Security Notice", Network Time Foundation's NTP Support Wiki , <https://support.ntp.org/bin/view/Main/SecurityNotice>.

[OpenNTPD]
"OpenNTPD Project", <https://www.openntpd.org>.

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <https://www.rfc-editor.org/info/rfc7942>.

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
URI: https://www.si6networks.com

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

Phone: +54 11 4650 8472
Email: ggont@si6networks.com
URI: https://www.si6networks.com