

Operational Security Capabilities for IP Network InfrastructureE. Vyncke
Internet-DraftCisco
Intended status: InformationalB. Donnet
Expires: 4 September 2022J. Iurman

Université de Liège
3 March 2022

Attribution of Internet Probes
draft-vyncke-opsec-probe-attribution-01

Abstract

Active measurements at Internet-scale can target either collaborating parties or non-collaborating ones. This is similar scan and could be perceived as aggressive. This document proposes a couple of simple techniques allowing any party or organization to understand what this unsolicited packet is, what is its purpose, and more importantly who to contact.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at <https://evyncke.github.io/opsec-probe-attribution/draft-vyncke-opsec-probe-attribution.html>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-vyncke-opsec-probe-attribution/>.

Discussion of this document takes place on the Operational Security Capabilities for IP Network Infrastructure Working Group mailing list (<mailto:opsec@ietf.org>), which is archived at <https://mailarchive.ietf.org/arch/browse/opsec/>.

Source for this draft and an issue tracker can be found at <https://github.com/evyncke/opsec-probe-attribution>.

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-Draft

Probes Attribution

March 2022

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 4 September 2022.

Copyright Notice

Copyright (c) 2022 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 Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

Table of Contents

1.	Introduction	2
2.	Probe / Measurement Description	3
2.1.	Probe Description URI	3
2.2.	Probe Description Text	3
3.	Out-of-band Probe Attribution	4
4.	In-band Probe Attribution	4
5.	Ethical Considerations	5
6.	Security Considerations	5
7.	IANA Considerations	6
8.	References	6
8.1.	Normative References	6
8.2.	Informative References	7
	Acknowledgments	7
	Authors' Addresses	7

[1.](#) Introduction

Active measurements at Internet-scale can target either collaborating parties or non-collaborating ones. Such measurements include [[LARGE_SCALE](#)] and [[RFC7872](#)].

Sending unsolicited probes should obviously be done at a rate low enough to avoid wasting other parties resources. But even at a low rate, those probes could trigger an alarm that will request some investigation by either the party receiving the probe (i.e., when the

probe destination address is one address assigned to the receiving party) or by a third party having some devices where those probes are transiting (e.g., an Internet transit router).

This document suggests a couple of simple techniques allowing any party or organization to understand:

- * what this unsolicited packet is,
- * what is its purpose,
- * and more significantly who to contact for further information or stop the probing.

Note: it is expected that only good-willing researchers will use these techniques.

[2.](#) Probe / Measurement Description

[2.1.](#) Probe Description URI

This document defines a "probe description URI" (see [Section 2.2](#)) as a URI pointing to:

- * a "Probe Description", see [Section 2.2](#), e.g., "https://example.net/measurement.txt";
- * an email address, e.g., "mailto:eric@example.net";
- * a phone number to call, e.g., "tel:+1-201-555-0123".

[2.2.](#) Probe Description Text

Similarly, as in [I-D.[draft-foudil-securitytxt](#)], when a node probes other nodes over the Internet, it should create a text file following the syntax described in [section 3](#) of [I-D.[draft-foudil-securitytxt](#)]

and should have the following fields:

- * contact;
- * expires;
- * preferred-languages.

Plus, another one "description" which is a URI pointing a document describing the measurement.

[3.](#) Out-of-band Probe Attribution

When it is not possible to include the "probe description URI" in the probe packet itself, then a specific URI must be constructed based on the source address of the probe packet following [\[RFC8615\]](#), e.g., for a probe source address of 2001:db8::dead, the following URI are constructed:

- * if the reverse DNS record for 2001:db8::dead exists, e.g., "example.net", then the URI is "https://example.net/.well-known/probing.txt" ;
- * else (or in addition), the URI is "https://[2001:db8::dead]/.well-known/probing.txt". Of course, there will be a certificate verification issue.

The constructed URI must be a reference to the "Probe description Text" (see [Section 2.2](#)).

[4.](#) In-band Probe Attribution

When the desired measurement allows for it, one "probe description URI" should be included in the payload of all probes sent. This could be:

- * for a [\[RFC4443\]](#) ICMPv6 echo request: in the optional data (see [section 4.1 of \[RFC4443\]](#));
- * for a [\[RFC792\]](#) ICMPv4 echo request: in the optional data;

- * for a [\[RFC768\]](#) UDP datagram: in the data part;
- * for a [\[RFC793\]](#) TCP packet with the SYN flag: data is allowed in TCP packets with the SYN flag per [section 3.4 of \[RFC793\]](#) (2nd paragraph);
- * for a [\[RFC8200\]](#) IPv6 packet with either hop-by-hop or destination options headers, in the PadN option. Note that, per the informational [\[RFC4942\] section 2.1.9.5](#), it is suggested that PadN option should only contain 0x0 and be smaller than 8 octets, so the proposed insertion of the URI in PadN option could have influence on the measurement itself;
- * etc.

The URI should start at the first octet of the payload and should be terminated by an octet of 0x00, i.e., it must be null terminated. If the URI cannot be placed at the beginning of the payload, then it should be preceded also by an octet of 0x00.

Note: using the above technique produces a valid and legit packet for all the nodes forwarding the probe. The node receiving the probe may or may not process the received packet, but this should cause no harm if the probing rate is very low as compared to the network bandwidth and to the processing capacity of all the nodes. As the insertion of the URI in the packet may not respect the syntax of the protocol, responses may not be received (such a TCP SYN+ACK) and perhaps an ICMP should be expected or more probably an absence of reply.

[5.](#) Ethical Considerations

Executing some measurement experiences over the global Internet obviously require some ethical considerations when transit/destination non-solicited parties are involved.

This document proposes a common way to identity the source and the purpose of active probing in order to reduce the potential burden on

the non-solicited parties.

But there are other considerations to be taken into account: from the payload content (e.g., is the encoding valid ?) to the transmission rate (see also [[IPV6 TOPOLOGY](#)] and [[IPV4 TOPOLOGY](#)] for some probing speed impacts). Those considerations are out of scope of this document.

[6.](#) Security Considerations

While it is expected that only good-willing researchers will use these techniques, they will simplify and shorten the time to identify a probing across the Internet.

This information is provided to identify the source and intent of specific probes, but there is no authentication possible for the inline information. As a result, a malevolent actor could provide false information while conducting the probes, so that the action was attributed to a third party. The recipient of this information cannot, as a result, rely on this information without confirmation. If a recipient cannot confirm the information or does not wish to do so, they should treat the flows as if there were no attribution.

[7.](#) IANA Considerations

The "Well-Known URIs" registry should be updated with the following:

- * additional values (using the template from [[RFC8615](#)]):
- * URI suffix: probing.txt
- * Change controller: IETF
- * Specification document(s): this document
- * Status: permanent

[8.](#) References

8.1. Normative References

- [I-D.[draft-foudil-securitytxt](#)]
Foudil, E. and Y. Shafranovich, "A File Format to Aid in Security Vulnerability Disclosure", Work in Progress, Internet-Draft, [draft-foudil-securitytxt-12](#), 24 May 2021, <<https://datatracker.ietf.org/doc/html/draft-foudil-securitytxt-12>>.
- [RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, [RFC 4443](#), DOI 10.17487/RFC4443, March 2006, <<https://www.rfc-editor.org/rfc/rfc4443>>.
- [RFC768] Postel, J., "User Datagram Protocol", STD 6, [RFC 768](#), DOI 10.17487/RFC0768, August 1980, <<https://www.rfc-editor.org/rfc/rfc768>>.
- [RFC792] Postel, J., "Internet Control Message Protocol", STD 5, [RFC 792](#), DOI 10.17487/RFC0792, September 1981, <<https://www.rfc-editor.org/rfc/rfc792>>.
- [RFC793] Postel, J., "Transmission Control Protocol", STD 7, [RFC 793](#), DOI 10.17487/RFC0793, September 1981, <<https://www.rfc-editor.org/rfc/rfc793>>.
- [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/rfc/rfc8200>>.

- [RFC8615] Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", [RFC 8615](#), DOI 10.17487/RFC8615, May 2019, <<https://www.rfc-editor.org/rfc/rfc8615>>.

8.2. Informative References

- [IPV4_TOPOLOGY]
Beverly, R., "Yarrp'ing the Internet Randomized High-Speed

Active Topology Discovery", DOI 10.1145/2987443.2987479, 2016, <<http://www.cmand.org/papers/yarrp-imc16.pdf>>.

[IPV6_TOPOLOGY]

Beverly, R., Durairajan, R., Plonka, D., and J.P. Rohrer, "In the IP of the Beholder Strategies for Active IPv6 Topology Discovery", DOI 10.1145/3278532.3278559, 2018, <<http://www.cmand.org/papers/beholder-imc18.pdf>>.

[LARGE_SCALE]

Donnet, B., Raoult, P., Friedman, T., and M. Crovella, "Efficient Algorithms for Large-Scale Topology Discovery", DOI 10.1145/1071690.1064256, 2005, <<https://dl.acm.org/doi/pdf/10.1145/1071690.1064256>>.

[RFC4942] Davies, E., Krishnan, S., and P. Savola, "IPv6 Transition/ Co-existence Security Considerations", [RFC 4942](#), DOI 10.17487/RFC4942, September 2007, <<https://www.rfc-editor.org/rfc/rfc4942>>.

[RFC7872] Gont, F., Linkova, J., Chown, T., and W. Liu, "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World", [RFC 7872](#), DOI 10.17487/RFC7872, June 2016, <<https://www.rfc-editor.org/rfc/rfc7872>>.

Acknowledgments

The authors would like to thank Alain Fiocco, Fernando Gont, Ted Hardie, Mehdi Kouhen, and Mark Townsley for helpful discussions as well as Raphael Leas for an early implementation.

Authors' Addresses

Éric Vyncke
Cisco
De Kleetlaan 64
1831 Diegem
Belgium
Email: evyncke@cisco.com

Université de Liège
Belgium
Email: benoit.donnet@uliege.be

Justin Iurman
Université de Liège
Belgium
Email: justin.iurman@uliege.be