Internet Engineering Task Force (IETF)
Request for Comments: 9511
Category: Informational
ISSN: 2070-1721

É. Vyncke
Cisco
B. Donnet
J. Iurman
Université de Liège

November 2023

Attribution of Internet Probes

Установление авторства пробных пакетов Internet

Аннотация

Активные измерения в Internet могут производиться как между сотрудничающими, так и не сотрудничающими сторонами. Иногда такие измерения, называемые также зондами или пробами (probe) воспринимаются как нежелательные или агрессивные.

В этом документе предлагается несколько простых методов, позволяющих источнику (отправителю) идентифицировать свои зонды. Это позволяет любой стороне или организации понять, что собой представляет незапрошенный пакет-зонд, каково его назначение и, что наиболее важно, с кем следует связываться. Методы основаны на автономном (offline) анализе зондов, поэтому не требуют изменений в плоскости управления. Методы рассчитаны в основном на измерения L3.

Статус документа

Документ не относится к категории Internet Standards Track и публикуется для информации.

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc9511.

Оглавление

1. Введение

Большинство измерительных исследований (например, [LARGE_SCALE], [RFC7872], [JAMES]) включает отправку через общедоступную сеть Internet пакетов IP (иногда с заголовками расширения или L4), которые могут адресоваться как к сотрудничающим, так и не сотрудничающим сторонам. Такие пакеты в документе называются зондами или пробами.

[1]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

Очевидно, что незапрошенные зонды следует передавать с достаточно низкой скоростью, чтобы не оказывать чрезмерного влияния на ресурсы других сторон. Но даже при малой скорости такие пробы могут вызывать сигналы тревоги, которые потребуют расследования стороной, получившей зонд (в пробном пакете указан адрес получателя принявшей стороны), или третьей стороной, через устройства которой проходят пробные пакеты (например, транзитным маршрутизатором Internet). Расследование будет проводиться в автономном режиме (offline) с использованием захвата пакетов, поэтому для определения принадлежности зондов не требуется вносить изменений в плоскость управления или данных.

Этот документ предлагает несколько простых методов идентификации зондов их источником. Это позволит любой стороне или организации понять:

- что собой представляет незапрошенных пробный пакет;
- каково назначение зонда;
- к кому обращаться за дополнительной информацией (это наиболее важно).

Предполагается, что эти методы будут применяться исследователями только с добрыми намерениями, хотя методы доступны всем. Этот вопрос рассматривается в разделе 7.

Хотя метод подходит для маркировки измерений, выполняемых на любом уровне сетевого стека, он предназначен в основном для измерений на сетевом уровне (L3) и связанных с этим уровнем заголовков расширения и опций.

2. Описание пробных пакетов

В этом разделе описаны способы описания (идентификации) проных пакетов их источником.

2.1. URI описания

Этот документ определяет Probe Description URI как URI с одной из указанных ниже ссылок.

- Файл описания зонда (Probe Description File, параграф 2.2), как определено в разделе 8, например, "https://example.net/.well-known/probing.txt";
- Адрес электронной почты, например mailto:lab@example.net;
- Номер телефона, например, tel:+1-201-555-0123.

2.2. Файл описания зонда

Как указано в разделе 8, файл описания зонда должен быть доступен по ссылке /.well-known/probing.txt и должен иметь формат, заданный в разделе 4 [RFC9116]. В файл следует указывать поля, заданные в разделе 2 [RFC9116] и перечисленные ниже.

- Canonical
- Contact
- Expires
- Preferred-Languages

В описание измерения следует также включать поле Description. В соответствии с форматом, заданным в разделе 4 [RFC9116], это поле должно быть одной строкой без символов прерывания строки.

2.2.1. Пример

```
# Канонический URI (if при наличии)
Canonical: https://example.net/measurement.txt

# Адрес для контактов
Contact: mailto:lab@example.net

# Срок действия
Expires: 2023-12-31T18:37:07z

# Языки
Preferred-Languages: en, es, fr

# Описание пробного пакета
Description: Одна строка, описывающая пробные пакеты.
```

3. Автономное указание авторства

Возможность установить автора зонда основана на создании специальной ссылки URI, включающей адрес источника, как указано в [RFC8615]. Например, для зонда с адресом источника 2001:db8:dead::1 URI создаётся, как показано ниже.

- Если имеется обратная запись DNS для 2001:db8:dead::1, например, example.net, URI описания пробы будет иметь вид https://example.net/.well-known/probing.txt. Обратной записи DNS следует быть единственной, а при наличии нескольких записей идентичные файлы описания пробы следует обеспечивать для каждой из них.
- В ином случае (или в дополнение) URI описания имеет вид https://[2001:db8:dead::1]/.well-known/probing.txt.

Созданный идентификатор URI должен указывать файл описания пробы (см. параграф 2.2).

Национальный центр кибербезопасности Великобритании (UK National Cyber Security Centre [NCSC]) использует похожую форму указания авторства. Они сканируют на предмет уязвимостей все подключённые в Internet системы в Великобритании и публикуют сведения в [NCSC_SCAN_INFO], указывая адрес web-страницы в обратной записи DNS.

4. Указание авторства в пакетах

Другим вариантом является включение URI описания пробы в сами пробные пакеты, напримр, как указано ниже.

- Включение в поле данных пакетов ICMPv6 echo request [RFC4443].
- Включение в поле данных пакетов ICMPv4 echo request [RFC0792].
- Включение в данные (payload) дейтаграмм UDP datagram [RFC0768], если после транспортного протокола нет другого протокола вышележащего уровня.
- Включение в данные (payload) сегмента TCP [RFC9293], если после транспортного протокола нет другого протокола вышележащего уровня.
- Включение с опцию PadN внутри заголовка Hop-by-Hop или Destination Options пакета IPv6 [RFC8200].

URI описания зонда должен начинаться с первого октета данных (payload) и навершаться октетом 0x00 (null). Если URI описания невозможно поместить в начало данных, ему должен предшествовать октет 0x00. Вставка Probe Description URI может исказить измерение, если размер пакета превысит MTU. Некоторые примеры приведены в Приложении A.

Использовать «магическую строку» (специальный уникальный маркер) для указания наличия Probe Description URI не рекомендуется, поскольку некоторые транзитные узлы могут применять для таких пакетов особую обработку.

Указание автоства в пакетах применлось в [JAMES].

5. Эксплуатационные и технические вопросы

Использование любого из указанных методов (или обоих) сильно зависит от намерений и контекста. В этом разделе описаны плюсы и минусы каждого метода, чтобы владельны или изготовители пробных пакетов могли выбрать решение для себя.

Преимуществом автономного (out-of-band) метода является независимость результатов зондирования от указания автора зондов (т. е. запуска web-сервера на зондирующем устройстве). Однако в некоторых случаях применение этого метода может оказаться невозможным, например, при работе через NAT, слишком большом числе конечных точек для запуска web-серверов, неизвестности IP-адреса источника зондов (например, зонды RIPE Atlas [RIPE_ATLAS] передаются с адресов, не принадлежащих владельцу зонда), динамических адресах отправителя и т. п.

Основным достоинством метода in-band является возможность работы в тех ситуациях, когда метод out-of-band недоступен (см. выше). Основной недостаток заключается в возможности искажения измерений из-за того, что пакеты с Probe Description URI могут отбрасываться. Например, можно включать данные в сегменты TCP с флагом SYN [RFC9293], однако это может изменить способ их обработки, т. е. сегменты TCP SYN с Probe Description URI могут быть отброшены. Другим примером является включение Probe Description URI в опцию PadN заголовка Hop-by-Hop или Destination Options. В параграфе 2.1.9.5 [RFC4942] (Informational RFC) сказано, что в опцию PadN следует включать только нули и размер опции следует длать не более 8 октетов, что ограничивает её применения для атрибутирования зондов. Если опция PadN не следует этим рекомендациям, предлагается рассмотреть возможность отбрасывания пакетов. Например, ядро Linux, начиная с версии 3.5, следует этой рекомендации и отбрасывает такие пакеты.

Сочетание обоих методов может быть использовано как способ косвенной «аутентификации» Probe Description URI в пробном пакете (in-band) за счёт сопоставления с методом out-of-band (например, поиск обратной записи в DNS). Хотя сам метод out-of-band меньше подвержен подделкам, сочетание с in-band обеспечивает более полное решение.

6. Вопросы этики

Выполнение измерений в глобальной сети Internet, безусловно, требует соблюдения норм этики, рассматриваемых в [ANRW_PAPER], особенно при вовлечении чужих (unsolicited) транзитных и целевых точек. В этом документе предложены базовые способы указания источника и цели активного тестирования, чтобы минимизировать возможные издержки вовлечённых без запроса (unsolicited) сторон.

Однако следует учитывать и другие соображения, от содержимого данных (например, корректности их кодирования) до скорости передачи (см. [IPV6_TOPOLOGY] и [IPV4_TOPOLOGY], где рассмотрено влиения скорости тестов). Эти вопросы выходят за рамки данного документа.

7. Вопросы безопасности

В этом документе предложены простые методы указания авторства пробных пакетов. Предполагается, что они будут применяться только этичными исследователями, что упростит и ускорит идентификацию пробных пакетов в Internet. На деле эти методы может применять любой, поэтому полученным сведениям нельзя слепо доверять. Использование этих методов не следует считать признаком доверия к пробам и кто-либо может воспользоваться этим решением для получения сведений об источники и контексте зондирования. Решение не является идеальным, но обеспечивает способы атрибутирования пробных пакетов и это лучше, чем полное отсутствие решения.

Атрибутирование зондов позволяет идентифицировать источник и назначение конкретных зондов, но проверить подлинность информации невозможно. Злоумышленник может представить ложные сведения при проведении зондирования или подделать их так, чтобы пробные пакеты представлялись отправленными другой стороной. Эта сторона не только может быть ошибочно обвинена, но может подвергнуться нежелательным домогательствам (например, гневным письмам или телефонным звонкам, если злоумышленник указал соответствующий адрес или номер телефона). Поэтому получатель таких сведений не может доверять им без подтверждения. Если получатель не может или не хочет подтвердить сведения, ему следует считать, что их просто нет. Отметим, что атрибутирование пробных пакетов не открывает возможности для новых DDoS-атак, поскольку нет никаких оснований считать, что третья сторона будет автоматически подтверждать полученные сведения.

Поскольку Probe Description URI передаётся в открытом виде, а чтение файла Probe Description File доступно всем, не следует раскрывать персональные данные (Personally Identifiable Information или PII) в адресе электронной почты или

телефонном номере - лучше указывать групповой или общий адрес и номер телефона. Кроме того, в файл описания зондов можно включить вредоносные данные (например, ссылку), поэтому не следует слепо доверять этим файлам.

8. Взаимодействие с IANA

Агентство IANA включило приведённый ниже суффикс URI в реестр Well-Known URIs в соответствии с [RFC8615].

```
URI Suffix:  probing.txt
Change Controller:  IETF
Reference:  RFC 9511
Status:  permanent
```

9. Литература

9.1. Нормативные документы

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, DOI 10.17487/RFC0768, August 1980, <https://www.rfc-editor.org/info/rfc768>.

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, DOI 10.17487/RFC0792, September 1981, <https://www.rfc-editor.org/info/rfc792>.

[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/info/rfc4443>.

[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>.

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

[RFC9116] Foudil, E. and Y. Shafranovich, "A File Format to Aid in Security Vulnerability Disclosure", RFC 9116, DOI 10.17487/RFC9116, April 2022, <https://www.rfc-editor.org/info/rfc9116>.

[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>.

9.2. Дополнительная литература

[ANRW_PAPER] Fiebig, T., "Crisis, Ethics, Reliability & a measurement.network - Reflections on Active Network Measurements in Academia", DOI 10.1145/3606464.3606483, July 2023, <https://pure.mpg.de/rest/items/item_3517635/component/file_3517636/content>.

[IPV4_TOPOLOGY] Beverly, R., "Yarrp'ing the Internet: Randomized High-Speed Active Topology Discovery", DOI 10.1145/2987443.2987479, November 2016, <http://www.cmand.org/papers/yarrp-imc16.pdf>.

[IPV6_TOPOLOGY] Beverly, R., Durairajan, R., Plonka, D., and J. Rohrer, "In the IP of the Beholder: Strategies for Active IPv6 Topology Discovery", DOI 10.1145/3278532.3278559, October 2018, <http://www.cmand.org/papers/beholder-imc18.pdf>.

[JAMES] Vyncke, É., Léas, R., and J. Iurman, "Just Another Measurement of Extension header Survivability (JAMES)", Work in Progress, Internet-Draft, draft-vyncke-v6ops-james-03, 9 January 2023, <https://datatracker.ietf.org/doc/html/draft-vyncke-v6ops-james-03>.

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

[NCSC] UK NCSC, "The National Cyber Security Centre", <https://www.ncsc.gov.uk/>.

[NCSC_SCAN_INFO] UK NCSC, "NCSC Scanning information", <https://www.ncsc.gov.uk/information/ncsc-scanning-information>.

[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/info/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/info/rfc7872>.

[RIPE_ATLAS] RIPE Network Coordination Centre (RIPE NCC), "RIPE Atlas", <https://atlas.ripe.net/>.

[SCAPY] "Scapy", <https://scapy.net/>.

Приложение A. Примеры указания авторства через сеть

Ниже приведено несколько примеров, созданных с помощью генератора [SCAPY] и приведённых в формате tcpdump.

Пакет IP с Description URI внутри заголовка расширения Destination Options

```
IP6 2001:db8:dead::1 > 2001:db8:beef::1: DSTOPT 60878 > traceroute:
Flags [S], seq 0, win 8192, length 0

0x0000:  6000 0000 0044 3c40 2001 0db8 dead 0000  `....D<@........
0x0010:  0000 0000 0000 0001 2001 0db8 beef 0000  ................
0x0020:  0000 0000 0000 0001 0605 012c 6874 7470  ...........,http
0x0030:  733a 2f2f 6578 616d 706c 652e 6e65 742f  s://example.net/
```

```
0x0040:  2e77 656c 6c2d 6b6e 6f77 6e2f 7072 6f62  .well-known/prob
0x0050:  696e 672e 7478 7400 edce 829a 0000 0000  ing.txt.........
0x0060:  0000 0000 5002 2000 2668 0000            ....P...&h..
```

Пакет IP с URI в поле данных пакета TCP SYN

```
IP6 2001:db8:dead::1.15581 > 2001:db8:beef::1.traceroute:
Flags [S], seq 0:23, win 8192, length 23

0x0000:  6000 0000 002b 0640 2001 0db8 dead 0000  `....+.@........
0x0010:  0000 0000 0000 0001 2001 0db8 beef 0000  ................
0x0020:  0000 0000 0000 0001 3cdd 829a 0000 0000  ........<.......
0x0030:  0000 0000 5002 2000 c9b7 0000 6d61 696c  ....P.......mail
0x0040:  746f 3a6c 6162 4065 7861 6d70 6c65 2e6e  to:lab@example.n
0x0050:  6574 00                                  et.
```

Пакет IP echo request с другим URI в разделе данных ICMP ECHO_REQUEST

```
IP6 2001:db8:dead::1 > 2001:db8:beef::1: ICMP6, echo request, id 0,
seq 0, length 28

0x0000:  6000 0000 001c 3a40 2001 0db8 dead 0000  `.....:@........
0x0010:  0000 0000 0000 0001 2001 0db8 beef 0000  ................
0x0020:  0000 0000 0000 0001 8000 2996 0000 0000  ..........).....
0x0030:  7465 6c3a 2b31 2d32 3031 2d35 3535 2d30  tel:+1-201-555-0
0x0040:  3132 3300                                123.
```

Пакет IPv4 echo request с URI в разделе данных ICMP ECHO_REQUEST

```
IP 192.0.2.1 > 198.51.10.1: ICMP echo request, id 0, seq 0, length 31

0x0000:  4500 0033 0001 0000 4001 8e93 c000 0201  E..3....@.......
0x0010:  c633 0a01 0800 ea74 0000 0000 6d61 696c  .3d....t....mail
0x0020:  746f 3a6c 6162 4065 7861 6d70 6c65 2e6e  to:lab@example.n
0x0030:  6574 00                                  et.
```

Благодарности

Авторы благодарны Alain Fiocco, Fernando Gont, Ted Hardie, Mehdi Kouhen, Mark Townsley за полезные дискуссии, а также Raphael Leas - за раннюю реализацию.

Авторы также признательны за полезные рецензии и комментарии от Warren Kumari, Jen Linkova, Mark Nottingham, Prapanch Ramamoorthy, Tirumaleswar Reddy.K, Andrew Shaw, Magnus Westerlund.

Адреса авторов

Éric Vyncke
Cisco
De Kleetlaan 6A
1831 Diegem
Belgium
Email: evyncke@cisco.com

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

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

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru