Internet Engineering Task Force (IETF)
Request for Comments: 7343
Obsoletes: 4843
Category: Standards Track
ISSN: 2070-1721

J. Laganier
Luminate Wireless, Inc.
F. Dupont
Internet Systems Consortium

September 2014

An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers Version 2 (ORCHIDv2)

Префикс IPv6 для идентификаторов ORCHIDv2

Аннотация

Этот документ задаёт обновленный формат наложенных маршрутизируемых криптографических хэш-идентификаторов (Overlay Routable Cryptographic Hash Identifier или ORCHID), отменяющий определённые в RFC 4843 идентификаторы. Эти идентификаторы предназначены для использования в качестве идентификаторов конечных точек в приложениях и интерфейсах прикладных программ (Application Programming Interface или API), а не для указания местоположения уровня IP в сети (локатор). Идентификаторы выглядят как объекты прикладного уровня в имеющихся IPv6 API, но их не следует включать в реальные заголовки IPv6. Для большего сходства с обычными адресами IPv6 предполагается, что идентификаторы будут маршрутизироваться в наложенном уровне. Следовательно, хоть идентификаторы и не считаются маршрутизируемыми адресами с точки зрения уровня IPv6, от всех имеющихся приложений IPv6 ожидается способность использовать эти идентификаторы в манере, совместимой с текущей адресацией IPv6. Идентификаторы ORCHID, изначально определённые в RFC 4843, не обеспечивали гибкости криптографического алгоритма. Описанный здесь обновленный формат ORCHID снимает это ограничение путём кодирования в самом идентификаторе индекса применяемого набора криптоалгоритмов.

Статус документа

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 5741.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc7343.

Оглавление

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

1. Введение

Этот документ вводит ORCHID - новый класс идентификаторов, похожих на адреса IP. Эти идентификаторы должны быть глобально уникальными в статистическом смысле (см. Приложение A), немаршрутизируемыми на уровне IP и маршрутизируемыми на неком наложенном уровне. Идентификаторы надёжно привязываются с помощью безопасной хэш-функции к конкатенации входной строки битов и тега контекста. Обычно (но не обязательно) входная строка битов будет включать должным образом закодированный открытый криптографический ключ.

1.1. Обоснование и назначение

Предполагается, что эти идентификаторы будут использоваться в имеющихся IPv6 API и прикладных протоколах между согласившимися узлами. Примерами таких идентификаторов являются теги отождествления хостов (Host Identity Tag или HIT) в протоколе отождествления хостов (Host Identity Protocol или HIP) [HIPv2] и временные мобильные идентификаторы (Temporary Mobile Identifier или TMI) для Mobile IPv6 Privacy Extension [PRIVACYTEXT].

Поскольку предполагается использование этих идентификаторов вместе с адресами IPv6 в приложениях и API, желательна координация, позволяющая предотвратить неподобающее использование ORCHID как обычных адресов IPv6 и наоборот. На практике представляется достаточным выделение отдельного префикса для ORCHID, что делает их совместимыми с адресами IPv6 на верхних уровнях и одновременно препятствует их использованию на уровне IP.

Хотя технически возможно применять ORCHID между согласными хостами без координации с IETF и IANA, в IETF такую практику сочли бы потенциально опасной. Конкретная опасность возникнет, если позднее сообщество IETF решит использовать префикс ORCHID для какой-либо иной цели. В этом случае использующие префикс ORCHID хосты не смогут воспользоваться этим префиксом для новой (другой) цели. Это привело бы к частичной «балканизации» в Internet, похожей на то, что произошло в результате захвата адресов IPv4, не выделенных в RFC 1918 [RFC1918] для приватного использования.

Потребность в предложенном выделении префикса растёт из-за желания применять ORCHID с имеющимися приложениями и API. Это желание ведёт к отмеченному выше потенциальному конфликту, для разрешения которого следует выделить предложенный префикс.

Можно утверждать, что желание использовать этот тип идентификаторов через имеющиеся API является архитектурной ошибкой и это будет отчасти верно. На деле было бы лучше создать новые API и обновить все приложения для использования идентификаторов взамен «локаторов» (адресов) через новые API. Именно это ожидается в долгосрочной перспективе.

Однако с учётом текущего состояния Internet не представляется разумным вносить изменения, которые требуют сразу переписывания приложений и обновления стека протоколов на хостах. Вместо этого предполагается постепенное изменение архитектуры, которое будет требовать изменения лишь одного из имеющихся активов. Идентификаторы ORCHID были разработаны с учётом этого и они позволяют реализовать расширения стека протоколов, такие как защищённая наложенная маршрутизация, HIP или расширения приватности Mobile IP без изменения имеющихся приложений. Целью является облегчение широкомасштабного развёртывания с минимальными усилиями пользователей.

Например, в момент разработки этого документа уже были реализации HIP полностью в пространстве пользователя с использованием операционной системы для перенаправления некоторой части адресного пространства IPv6 демону пользовательского уровня для обработки HIP. На практике в таких реализациях уже применяется тот или иной префикс IPv6 для разделения идентификаторов HIP и адресов IPv6, позволяющего использовать те и другие в имеющихся приложениях через существующие API.

Наложенные маршрутизируемые криптографические хэш-идентификаторы ORCHID, изначально определённые в [RFC4843], не обеспечивали гибкости криптографических алгоритмов. Обновленный формат ORCHID, заданный в этом документе, снимает это ограничение за счёт кодирования применяемого набора криптоалгоритмов в самом идентификаторе.

Поскольку обновленный формат ORCHIDv2 не совместим с прежним, агентство IANA выделило новый 28-битовый префикс из блока специального назначения IANA IPv6 Special Purpose Address Block (2001:0000::/23, как указано в [RFC6890]). Префикс, выделенный для экспериментов ORCHID, возвращён IANA в марте 2014 г. [RFC4843].

1.2. Свойства ORCHID

Идентификаторы ORCHID обладают рядом свойств, указанных ниже.

- Статистическая уникальность (см. Приложение A. Возможные конфликты).
- Защищённая привязка к входным параметрам, использованным при генерации (идентификатор контекста и строка битов).
- Агрегирование в один префикс IPv6. Отметим, что это нужно лишь в связи с отмеченной выше необходимостью координации, без которой пространство имён ORCHID может быть совершенно плоским.
- Немаршрутизируемость на уровне IP, встроенная изначально.
- Маршрутизируемость в наложенном уровне, делающая идентификаторы семантически похожими на адреса IPv6 с точки зрения приложений.

Как отмечено выше, идентификаторы ORCHID предназначены для генерации и применения в разных контекстах, подходящих для различных механизмов и протоколов. Идентификатор контекста предназначен для различения разных контекстов. В Приложении A обсуждаются связанные с этим вопросы реализации API, а в разделе 4 описаны причины использования идентификаторов контекста.

1.3. Предполагаемое применение ORCHID

Примерами идентификаторов и протоколов, для которых предполагается адаптация к формату ORCHID, включают теги идентификации хостов (HIT) в протоколе идентификации хостов [HIPv2] и временные мобильные идентификаторы (TMI) в расширении для приватности мобильных узлов (Simple Privacy Extension for Mobile IPv6 [PRIVACYTEXT]). Формат разработан с возможностью расширения, позволяющего использовать то же пространство имён для других экспериментов.

1.4. План действий

Этот документ запрашивает в IANA выделение префикса из адресного пространства IPv6 для идентификаторов ORCHID.

1.5. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с RFC 2119 [RFC2119].

2. Создание криптографических хэш-идентификаторов

Идентификаторы ORCHID создаются с помощью специального алгоритма генерации (ORCHID Generation Algorithm или OGA), принимающего на входе строку битов и идентификатор контекста, а на выходе дающего ORCHID. Используемая в OGA хэш-функция определяется для каждого идентификатора OGA в спецификации соответствующего контекста применения (например, HIPv2).

```
Input      :=  любая строка битов
OGA ID     :=  4-битовый идентификатор алгоритма OGA
Hash Input :=  Context ID | Input
Hash       :=  Hash_function(Hash Input)
ORCHID     :=  Prefix | OGA ID | Encode_96( Hash )
```

где

|
: обозначает конкатенацию битовых строк.

Input
: Битовая строка, уникальная или статистически уникальная в данном контексте и предназначенная для привязки к создаваемому идентификатору ORCHID в данном контексте.

Context ID
: Случайное значение, определяющее ожидаемый контекст использования для конкретного идентификатора ORCHID и хэш-функцию для генерации идентификаторов ORCHID в этом контексте. Значения выделяются из пространства имён тегов типа криптографически создаваемых адресов (Cryptographically Generated Address или CGA), см. RFC 3972 и http://www.iana.org/assignments/cga-message-types.

OGA ID
: 4-битовый идентификатор функции Hash_function, применяемой в конкретном контексте.

Hash_function
: Необратимая хэш-функция (т. е. функция, устойчивая к прообразу и второму прообразу), которая будет использоваться в соответствии с идентификатором OGA ID в контексте применения, заданном Context ID. Например, версия 2 спецификации HIP определяет усечённый вариант SHA1 [RFC3174] в качестве хэш-функции для генерации ORCHIDv2 в протоколе HIPv2, когда OGA ID имеет значение 3 [HIPv2].

Encode_96( )
: Функция извлечения, результатом которой является строка из 96 битов, взятых из средней части аргумента.

Prefix
: Постоянный префикс размером 28 биотов (2001:20::/28).

Для формирования ORCHID нужны 2 входных значения. Первая часть может быть любой строкой битов, но обычно предполагается, что это открытый криптографический ключ и некоторые иные данные. Второй частью является идентификатор контекста размером 128 битов, выделенный в соответствии с разделом 6. Предполагается, что для каждого конкретного применения ORCHIDv2 (например, HIP HIT или MIP6 TMI) будет выделен свой идентификатор контекста.

Строка битов и идентификатор контекста объединяются (конкатенация) для формирования входных данных, которые передаются криптографической хэш-функции для использования в качестве идентификатора OGA в соответствии с документом, определяющим контекст применения, указанный Context ID. Результат хэш-функции обрабатывается функцией кодирования (извлечения), дающей на выходе значение размером 96 битов. Перед этим значением помещается (prepend) конкатенация 28-битового префикса ORCHID и 4-битового OGA ID. Результатом является идентификатор ORCHID, представляющий собой строку из 128 битов, которая может применяться в IPv6 API на хостах, участвующих в конкретном эксперимента.

Префикс ORCHID выделяется из глобального блока индивидуальных (unicast) адресов IPv6, поэтому идентификаторы ORCHID не отличимы от глобальных unicast-адресов IPv6. Однако следует отметить, что ORCHID не соответствуют формату глобальных индивидуальных адресов IPv6, заданному с параграфе 2.5.4 [RFC4291], поскольку они не включают 64-битового идентификатора интерфейса, как указано в параграфе 2.5.1. [RFC4291].

3. Вопросы маршрутизации и пересылки

Идентификаторы ORCHID предназначены для независимого от местоположения указания конечных точек вместо «локаторов» уровня IP (адресов). Поэтому на маршрутизаторах можно отключить пересылку пакетов, содержащих ORCHID в качестве адреса источника или получателя. Для пакетов, где в качестве адреса получателя указан идентификатор ORCHID, а отправитель задан действительным индивидуальным адресом, на маршрутизаторе можно настроить генерацию сообщений ICMP Destination Unreachable, Administratively Prohibited.

Идентификаторы ORCHID не предназначены для использования в протоколах маршрутизации IPv6, поскольку эти протоколы основаны на архитектурном определении адресов IPv6. Будущие системы маршрутизации, отличные от IPv6 (такие как наложенные системы маршрутизации) могут работать на основе ORCHID, однако такие системы выходят за рамки данного документа.

В программы маршрутизации недопустимо включать код для специальной обработки идентификаторов ORCHID. Иными словами, немаршрутизируемость ORCHID реализуется на уровне настройки, а не встраивается жёстко в программный код. Например, префикс ORCHID можно просто блокировать правилом конфигурации, таким как запись списка управления доступом (Access Control List или ACL).

4. Устройство идентификаторов

Устройство этого пространства имён связано с двумя противоречивыми требованиями:

- сохранение как можно большего числа битов результата хэширования;
- возможность совместного использования пространства разными механизмами.

Желание иметь длинный результат хэширования требует использования как можно более короткого префикса и малого количества дополнительных битов кодирования или полного отказа от них. Описанное здесь решение использует максимальное число битов, остающихся после включения префикса и идентификатора алгоритма OGA. Это не оставляет в ORCHID битов для идентификации контекста, однако 4 бита кодирования OGA обеспечивают криптографическую гибкость в части используемой в данном контексте хэш-функции (см. 5. Вопросы безопасности).

Желание использовать пространство имён для нескольких механизмов исполнено путём включения идентификатора контекста во входные данные хэш-функции. Хотя это не позволяет напрямую вывести механизм из ORCHID, можно с высокой вероятностью проверить, ч входная строка битов и ORCHID относятся к данному контексту (см. 5. Вопросы безопасности).

5. Вопросы безопасности

Идентификаторы ORCHID созданы для защищённой привязки к контексту (Context ID) и строке битов, используемым в качестве входных параметров при генерации идентификаторов. Для обеспечения этого алгоритм OGA полагается на устойчивость применяемой хэш-функции ко второму прообразу (необратимости) [RFC4270]. Для получения этого свойства и предотвращения конфликтов важно использовать как можно более короткий префикс, оставляющий больше битов хэш-значения.

Для данного Context ID все механизмы, использующие ORCHID, **должны** применять один способ генерации ORCHID из входной строки битов. Поддержка разных механизмов без явного указания механизма в Context ID или самом ORCHID приведёт к так называемым атакам с понижением цены (bidding-down). Если для создания ORCHID разрешается применять несколько хэш-функций с одним Context ID и одна из этих функций окажется небезопасной, это позволит атаковать даже те действительные в данном контексте идентификаторы ORCHID, которые были созданы с использованием достаточно защищённых хэш-функций.

Идентификатор хэш-функции для использования при генерации ORCHID кодируется в самом идентификаторе ORCHID, хотя семантика принимаемых идентификатором значений определяется отдельно для каждого Context ID. Поэтому предложенное решение позволяет использовать разные функции хэширования при создании ORCHID из входных строк битов в данном контексте. Цель заключается в том, чтобы применяющие ORCHIDv2 протокол или приложение выделяли Context ID для этого использования и определяли в области действия Context ID реестр идентификаторов OGA. Это сделано для того, чтобы позволить разным приложениям использовать хэш-функции, которые лучше подходят к конкретным требованиям, так что сравнительно малое пространство идентификаторов OGA (4 бита, 16 значений) не вносило существенных ограничений. При появлении более защищённых хэш-функций для данного контекста можно определить новые значения идентификаторов алгоритма OGA.

Для сохранения достаточно малой вероятности конфликтов (см. Приложение A. Возможные конфликты) каждый метод **должен** использовать механизм, гарантирующий уникальность или статистическую уникальность входных строк битов в данном контексте. Имеется несколько возможных методов, например, можно применять в качестве входной строки битов значение глобально поддерживаемого счётчика, псевдослучайное значение с достаточной энтропией (не меньше 96 битов) или случайно создаваемый открытый криптографический ключ. Context ID гарантирует, что входные строки битов из разных контекстов не будут совпадать. Вместе это гарантирует, что вероятность конфликтов (совпадений) определяется только вероятностью естественных конфликтов в хэш-пространстве и не увеличивается в результате совпадения входных строк битов.

Генерация идентификаторов ORCHIDv2 из входных строк битов включает отсечку выходного хэш-значения для создания идентификаторов фиксированного размера аналогично схеме из «Naming Things with Hashes» [RFC6920]. Поэтому вопросы безопасности, рассмотренные в [RFC6920] и связанные с отсечкой хэш-значений при генерации идентификаторов, применимы и к созданию ORCHIDv2.

6. Взаимодействие с IANA

Поскольку обновленный формат ORCHIDv2 не совместим с прежним, агентство IANA выделило новый 28-битовый префикс из блока адресов специального назначения IANA IPv6 Special Purpose Address Block 2001:0000::/23 в соответствии с [RFC6890]. Префикс, выделенный временно для экспериментов с ORCHID, возвращён IANA с марте 2014 г. [RFC4843]. Для выделенного префикса в реестре указан приведённая ниже информация.

- Блок адресов: 2001:20::/28
- Имя: ORCHIDv2
- RFC: RFC 7343
- Дата выделения: 2014-07
- Срок действия: N/A (не определён)

- Источник: True
- Получатель: True
- Возможность пересылки: True
- Глобальное действие: True
- Резерв для протокола: False

Идентификатором контекста (Context ID) является случайное значение, определяющее контекст применения ORCHID и хэш-функцию для создания идентификаторов ORCHID в этом контексте. Этот документ не задаёт определённого значения. Для Context ID используется пространство имён, введённое для тегов типа CGA (CGA Type Tag), поэтому при определении новых значений нужно следовать правилам раздела 8 в [RFC3972], т. е. выделят значения в порядке поступления запросов (First Come, First Served). Действий IANA для этого не требуется.

7. Участники работы

Pekka Nikander (pekka.nikander@nomadiclab.com) был соавтором экспериментального варианта спецификации [RFC4843].

8. Благодарности

Большое спасибо Geoff Huston за резкую, но конструктивную критику в процессе работы над документом. Tom Henderson помог прояснить множество вопросов. Документ также был улучшен рецензиями, комментариями и обсуждением в сообществах IPv6, Internet Area, IETF.

9. Литература

9.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

9.2. Дополнительная литература

[HIPv2] Moskowitz, R., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", Work in Progress[1], July 2014.

[PRIVACYTEXT] Dupont, F., "A Simple Privacy Extension for Mobile IPv6", Work in Progress, July 2006.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC3174] Eastlake, D. and P. Jones, "US Secure Hash Algorithm 1 (SHA1)", RFC 3174, September 2001.

[RFC4270] Hoffman, P. and B. Schneier, "Attacks on Cryptographic Hashes in Internet Protocols", RFC 4270, November 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4843] Nikander, P., Laganier, J., and F. Dupont, "An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID)", RFC 4843, April 2007.

[RFC6890] Cotton, M., Vegoda, L., Bonica, R., and B. Haberman, "Special-Purpose IP Address Registries", BCP 153, RFC 6890, April 2013.

[RFC6920] Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Keranen, A., and P. Hallam-Baker, "Naming Things with Hashes", RFC 6920, April 2013.

Приложение A. Возможные конфликты

Как отмечено выше, цель состоит в обеспечении статистической глобальной уникальности идентификаторов ORCHID, пока ключи не применяются повторно. Это значит, что для ORCHID, указывающего данный объект, достаточно мала вероятность наличия в масштабе Internet другого объекта с таким же ORCHID и её можно пренебречь на практике. Есть надежда, что предложенное решение соответствует этой цели (см. 4. Устройство идентификаторов).

Предполагается, что идентификаторы ORCHID будут применяться в унаследованных IPv6 API между согласными на это хостами. Context ID предназначен для различения разных экспериментов или контекстов, использующих общее пространство ORCHID. Однако Context ID не включается в ORCHID, а применяется лишь в начале битовой строки на входе функции хэширования. Хотя это может создавать некоторые сложности, относящиеся к реализациям, предполагается, что удлинение используемого в ORCHID результата хэширования принесёт больше пользы, нежели включение идентификатора контекста.

Поскольку идентификаторы ORCHID не маршрутизируются на уровне IP, для передачи пакетов с применением ORCHID на уровне API передающий хост должен иметь в стеке дополнительное наложенное состояние для определения параметров (например, «локаторов»), используемых в исходящих пакетах. Базовое допущение (по сути, имеющееся в известных авторам предложениях) состоит в наличии наложенного протокола для организации и поддержки такого дополнительного состояния. Предполагается, что протокол установки состояния переносит входную битовую строку и результирующее состояние в стеке, относящееся к ORCHID, может быть связано с соответствующим контекстом и протоколом установки состояния.

[1]Работа опубликована в RFC 7401. *Прим. перев.*

Приложение B. Отличия от RFC 4843

- В ссылках на HIP указаны обновлённые спецификации.
- В идентификаторах ORCHID, изначально определённых в [RFC4843], не доставало механизма обеспечения гибкости криптоалгоритмов. Обновленный формат ORCHID, заданный в этом документе, снимает это ограничение путём указания в самом идентификаторе индекса применяемого набора криптоалгоритмов.
- Раздел «Возможные конфликты» перенесён в приложение и из него исключено ненужное обсуждение.
- Исключено обсуждение наложенной маршрутизации.

Адреса авторов

Julien Laganier
Luminate Wireless, Inc.
Cupertino, CA
USA
EMail: julien.ietf@gmail.com

Francis Dupont
Internet Systems Consortium
EMail: fdupont@isc.org

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru