Internet Engineering Task Force (IETF)
Request for Comments: 8005
Obsoletes: 5205
Category: Standards Track
ISSN: 2070-1721

J. Laganier
Luminate Wireless, Inc.

October 2016

Host Identity Protocol (HIP) Domain Name System (DNS) Extension

Расширение DNS для протокола HIP

Аннотация

Этот документ задаёт запись о ресурсе (resource record или RR) для системы доменных имён (Domain Name System или DNS) и способ её использования в протоколе идентификации хостов (Host Identity Protocol или HIP). Эта запись RR позволяет узлу HIP сохранять в DNS своё отождествление (Host Identity или HI), открытый ключ асимметричной пары, тег отождествления хоста (Host Identity Tag или HIT), усечённое хэш-значение HI и доменные имена своих серверов встречи (rendezvous server или RVS). Документ отменяет действие RFC 5205.

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 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc8005.

Авторские права

Авторские права (Copyright (c) 2016) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, перечисленные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (http://trustee.ietf.org/license-info), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

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 задаёт запись RR для DNS [RFC1034] и способ её использования с протоколом HIP [RFC7401]. Эта запись позволяет узлу HIP сохранить в DNS своё отождествление (Host Identity или HI), открытую часть пары асимметричных ключей, тег отождествления (Host Identity Tag или HIT), усечённый хэш своего идентификатора HI и доменные имена своих серверов встречи (rendezvous server или RVS) [RFC8004].

В настоящее время большинству приложений Internet для взаимодействия с удаленным хостом нужно сначала транслировать его доменное имя (зачастую получаемое от пользователя) в один или несколько адресов IP. Этот этап происходит до взаимодействия с удаленным хостом и основан на поиске в DNS.

В HIP адреса IP предназначены для использования в основном для беспроводной связи, тогда как большинство протоколов верхнего уровня (Upper Layer Protocol или ULP) и приложений используют идентификаторы HI или теги HIT (ICMP может служить примером ULP, не использующего их). Поэтому нужны способы трансляции доменных имён в HI. Использование для этого DNS достаточно просто и для этого определяется запись HIP RR. При получении запроса от приложения или ULP для поиска сопоставления имени с адресом IP распознаватель дополнительно выполняет поиск сопоставления имени с HI и использует его для создания отображения HI на адрес IP (внутреннее для уровня HIP). Уровень HIP использует сопоставления HI-IP для трансляции HI и HIT в адреса IP и обратно.

Спецификация HIP [RFC7401] задаёт базовый обмен между инициатором (HIP Initiator) и ответчиком (HIP Responder) на основе обмена 4 пакетами HIP (I1, R1, I2, R2). Поскольку пакеты HIP включают теги HIT инициатора и ответчика, инициатору нужно знать HI и HIT ответчика до начала базового обмена (передача пакета I1).

Расширение HIP Rendezvous [RFC8004] позволяет достичь узла HIP по стороннему адресу IP (RVS узла). Инициатор, желающий организовать ассоциацию HIP с ответчиком, обслуживаемым сервером RVS, обычно будет инициировать базовый обмен HIP, передавая начальный пакет I1 по IP-адресу RVS, а не ответчика. Поэтому нужны средства определения имени RVS для данного имени хоста.

Документ вводит запись HIP DNS RR для хранения RVS, HI и HIT.

2. Уровни требований

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

3. Варианты применения

В этом разделе кратко описаны многочисленные варианты использования DNS в HIP.

При использовании HIP большинство приложений и ULP не знают адресов IP, используемых для передачи пакетов в линии. Поэтому узел HIP может использовать несколько адресов IP для отказоустойчивости, надёжности, мобильности или смены адресов (renumbering) так, что большинство ULP и приложений просто не заметят этого, поскольку они связаны с HI и не знают о смена адресов IP.

В таких ситуациях для обеспечения доступности узла по полному имени (Fully Qualified Domain Name или FQDN) в системе DNS следует хранить:

- адреса IP в наборах записей (Resource Record Set или RRSet) A [RFC1035] и AAAA [RFC3596] [RFC2181];
- HI, HIT и возможно набор серверов RVS в записях HIP RR.

Записи HIP RR не зависят от класса.

Когда узел HIP хочет взаимодействовать с другим узлом HIP, ему нужно сначала выполнить базовый обмен HIP для создания ассоциации HIP с партнёром. Хотя такой обмен можно инициировать, не зная HI ответчика, в этом случае для обоих хостов возникает риск вмешательства в обмен HIP (man-in-the-middle или MitM). Для предотвращения таких атак инициатору рекомендуется сначала узнать отождествление HI для ответчика, а затем начинать обмен. Это можно сделать, например, настройкой вручную или поиском в DNS. Для такого поиска предложена запись HIP RR.

Если узел HIP часто меняет свои адреса IP, естественная задержка распространения изменений через DNS может помешать публикации новых адресов IP в DNS. Для решения этой задачи в архитектуре HIP [RFC4423] служат серверы встречи (RVS) [RFC8004]. Хост HIP использует RVS как «точку встречи» для поддержки своей доступности для возможных инициаторов HIP при перемещениях [RFC5206]. Такой узел HIP будет публиковать в DNS доменное имя своих RVS в записях HIP RR, сохраняя на этих RVS фактические сведения о своих текущих адресах IP.

Если узел HIP хочет инициировать обмен HIP с ответчиком, он выполняет запросы к DNS, порядок которых может меняться в зависимости реализации. Например, реализации, применяющие HIT в интерфейсах прикладных программ (Application Programming Interface или API) обычно могут сначала запросить HIP RR по FQDN ответчика, а при использовании в API адресов IP обычно сначала выполняются запросы записей A и/или AAAA.

Далее предполагается, что инициатор сначала запрашивает HIP RR по FQDN ответчика.

Если на запрос для типа HIP служба DNS возвратила RCODE=3 (ошибка имени), это говорит об отсутствии в DNS сведений об ответчике и дополнительных запросов для того же имени владельца передавать **не следует**. Если запрос записей HIP в DNS возвращает RCODE=0 (нет ошибок) с пустым разделом ответов, это говорит об отсутствии данных HIP для имени ответчика. В таком случае при настройке ответчика на гибкое использование (opportunistic) HIP с инициированием без HI ответчика или работу по IP, он будет передавать дополнительные запросы для получения записей A и AAAA по FQDN ответчика.

В зависимости от комбинации откликов выполняются действия, описанные в параграфах 3.1 и 3.2.

Отметим, что хранение HIP RR в DNS по FQDN, назначенному узлу, не являющемуся HIP, может негативно влиять на его доступность для узлов HIP.

3.1. Простой конечный хост с одним статическим адресом

В дополнение к адресу IP или адресам (IP-R) узел HIP (R) с одним статическим подключением к сети, желающий обеспечить свою доступность по имени FQDN (www.example.com) в качестве ответчика, будет сохранять в DNS запись HIP RR со своим отождествлением Host Identity (HI-R) и тегом (HIT-R).

Инициатор, желающий связаться с узлом, обычно будет использовать показанные ниже запросы.

- Запрос #1: QNAME=www.example.com, QTYPE=HIP

  (QCLASS=IN предполагается по умолчанию и не указывается в примерах)

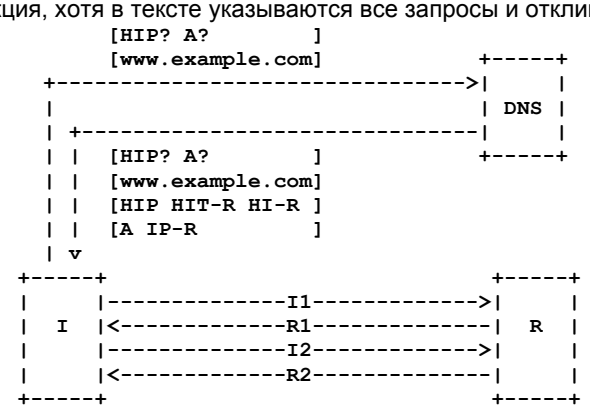
  Этот запрос возвращает пакет DNS с RCODE=0 и одной или несколькими HIP RR с HIT и HI (например, HIT-R и HI-R) ответчика в разделе ответов (answer), но не возвращает RVS.

- Запрос #2: QNAME=www.example.com, QTYPE=A

- Запрос #3: QNAME=www.example.com, QTYPE=AAAA

  Эти запросы будут возвращать пакеты DNS с RCODE=0 и записями A или AAAA, содержащими IP-адреса ответчика (например, IP-R) в разделе ответов (answer).

Примечание. Далее в документе для простоты и лаконичности рисунков несколько запросов и откликов DNS представляются как одна транзакция, хотя в тексте указываются все запросы и отклики на ниже.

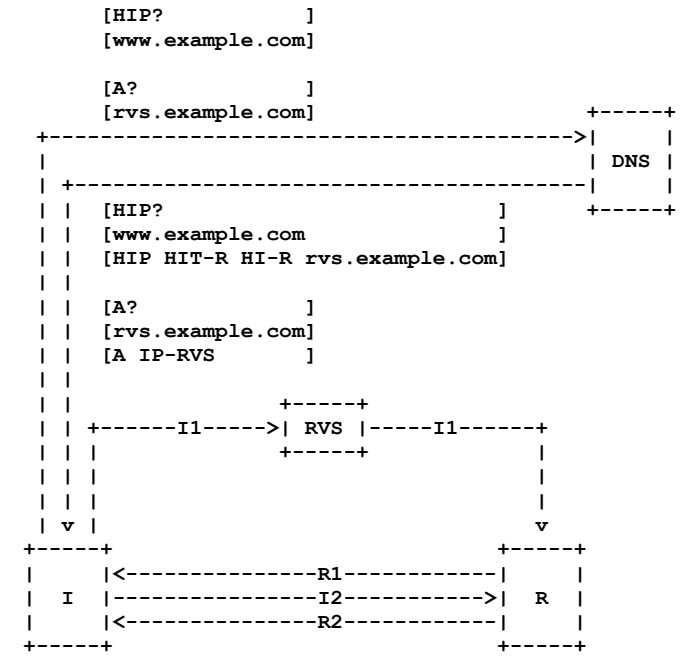


Статический хост с одним адресом.

После этого инициатор будет отправлять пакет I1 по IP-адресам ответчика (IP-R).

3.2. Мобильный конечный хост

Мобильный узел HIP (R), желающий быть доступным по своему имени FQDN (www.example.com), будет сохранять в DNS в дополнение к адресам IP (IP-R) своё отождествление HI (HI-R), HIT (HIT-R) и доменные имена своих RVS (например, rvs.example.com) в записях HIP RR. Мобильному хосту HIP также требуется уведомлять свои RVS о смене адресов IP.



Мобильный конечный хост.

Инициатор, желающий связаться с таким мобильным узлом, будет обычно передавать показанные ниже запросы.

- Запрос #1: QNAME=www.example.com, QTYPE=HIP

  Возвращает пакет DNS с RCODE=0 и одну или несколько записей HIP RR с HIT, HI и доменными именами RVS (например, HIT-R, HI-R, rvs.example.com) для ответчика в разделе ответов (answer).

- Запрос #2: QNAME=rvs.example.com, QTYPE=A

- Запрос #3: QNAME=rvs.example.com, QTYPE=AAAA

  Эти запросы будут возвращать пакеты DNS с RCODE=0 и записями A или AAAA, содержащими IP-адреса RVS ответчика (например, IP-RVS) в разделе ответов (answer).

После этого инициатор будет отправлять пакет I1 по IP-адресу RVS (IP-RVS), а RVS будет транслировать пакет I1 мобильному узлу по его адресу IP (IP-R) для завершения обмена HIP.

4. Обзор использования DNS с HIP

4.1. Хранение HI, HIT и RVS в DNS

Для любого узла HIP его отождествление HI, связанный тег HIT и FQDN возможных серверов RVS могут сохраняться в записи DNS HIP RR. Любая соответствующая спецификации реализация может сохранять HI и связанный тег HIT в формате DNS HIP RDATA. HI и HIT определены в разделе 3 спецификации HIP [RFC7401].

После возврата HIP RR хост всегда **должен** рассчитывать тег HIT на основе HI для использования в обмене HIP, как указано в разделе 3 спецификации HIP [RFC7401], тогда как тег HIT из HIP RR **следует** применять лишь для оптимизации (например, при поиске в таблице).

Запись HIP RR может также включать доменные имена серверов RVS, которым могут отправляться пакеты HIP I1 для запуска создания ассоциации с объектом, указанным этой записью RR [RFC8004].

Поле Rendezvous Server из записи HIP RR, хранящейся для данного имени владельца, **может** включать это имя. Семантически эквивалентная ситуация возникает, когда RVS не включается в HIP RR, хранящуюся для этого имени владельца. Это возможно в двух случаях.

- Хост является мобильным и записи A и/или AAAA RR, хранящиеся с его именем, содержат IP-адреса сервера RVS, а не самого хоста.
- Хост является стационарным и доступен напрямую по адресам IP из записей A и/или AAAA RR, хранящихся с его именем. Это вырожденный случай службы встречи, где хост выступает в качестве своего сервера RVS.

Сервер RVS, получивший такой пакет I1, транслирует его соответствующему ответчику (владельцу HIT получателя I1). Ответчик завершает обмен с инициатором обычно без участия RVS.

4.2. Инициирование соединения по имени DNS

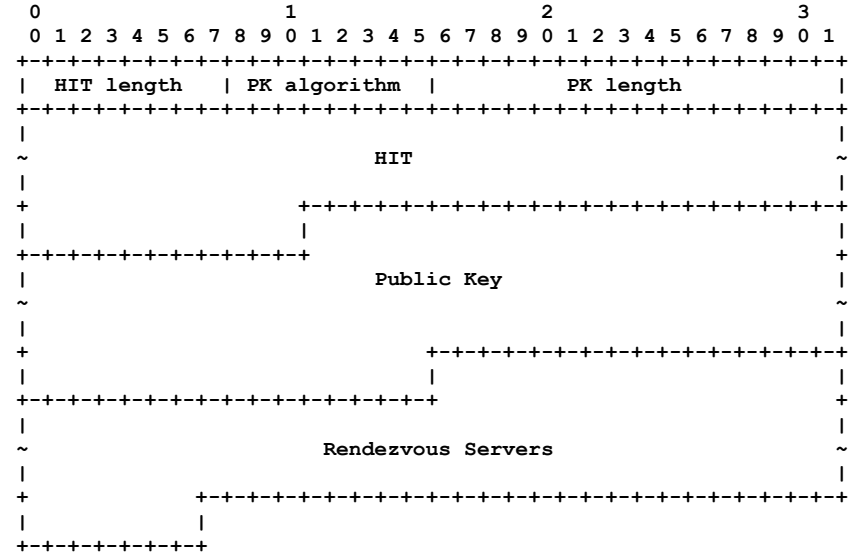
На узле HIP следует запускать обмен HIP всякий раз, когда ULP пытается взаимодействовать с объектом и запрос возвращает записи HIP RR.

С записями HIP RR связано поле срока действия (Time To Live или TTL). Когда число секунд с момент извлечения записи превышает значение TTL для этой записи, получивший запись объект **должен** считать её недействительной и удалять. Если доступ к записи требуется для инициирования взаимодействия с объектом, которому запись соответствует, **должен** передаваться новый запрос DNS для получения свежей копии записи.

С одним именем может быть связано несколько записей HIP RR. Выбор хостом записи из нескольких предоставленных выходит за рамки этой спецификации. Сведения об RVS могут копироваться и согласовываться для нескольких RR или содержаться отдельно для каждого сервера. При наличии нескольких серверов хост **должен** убедиться, что выбранный сервер RVS связан с используемым отождествлением HI.

5. Формат хранения HIP RR

RDATA для HIP RR включает PK Algorithm Type, HIT length, HIT, PK (т. е. HI) и может включать 1 или несколько RVS.



Поля HIT length, PK algorithm, PK length, HIT, Public Key **требуются** , поле Rendezvous Server **не обязательно**.

5.1. Формат HIT Length

Поле HIT length указывает размер поля HIT в байтах 8-битовым целым числом без знака.

5.2. Формат PK Algorithm

Поле PK algorithm указывает криптографический алгоритм PK и подразумеваемый формат поля Public Key 8-битовым целым числом без знака. В документе используются значения, заданные для Algorithm Type в записи IPSECKEY RR [RFC4025].

Определённые в настоящий момент значения перечислены в разделе 9.

5.3. Формат PK Length

Поле PK указывает размер поля Public Key в байтах 16-битовым целым числом без знака.

5.4. Формат HIT

Тег HIT представляется двоичным значением с сетевым порядком байтов.

5.5. Формат открытого ключа

Два из заданных в этом документе типов PK (RSA и DSA) используют форматы PK из IPSECKEY RR [RFC4025].

Формат ключей DSA задан в RFC 2536 [RFC2536].

Формат ключей RSA задан RFC 3110 [RFC3110], а ограничение размера ключей RSA (4096 битов) смягчено в IPSECKEY RR [RFC4025].

В дополнение к этому данный документ определяет формат PK с алгоритмом подписи на основе эллиптических кривых (Elliptic Curve Digital Signature Algorithm или ECDSA) как зависимую от алгоритма часть DNSKEY RR RDATA для ECDSA [RFC6605], т. е. DNSKEY RR DATA после первых 4 октетов, что соответствует той же части записи DNSKEY RR, которая задана в документах, определяющих алгоритм DNSSEC.

5.6. Формат записей о серверах встречи

Поле Rendezvous Server указывает одно или несколько доменных имён в формате передачи в линию (wire-encoded) для одного или нескольких серверов RVS. Конкатенация и кодирование имён выполняются в соответствии с параграфом 3.3 в RFC 1035 [RFC1035]: «<domain-name> указывает доменное имя в форме последовательности меток, завершаемое меткой нулевого размера». Поскольку формат wire-encoded является самоописывающим, размер каждого доменного имени является неявным, а метка нулевого размера служит разделителем доменных имён RVS, объединяемых в поле Rendezvous Server одной записи HIP RR. Поскольку размер другой части RRDATA в записи RR известен, как и общий размер RDATA в RR (RDLENGTH), вся информация, требуемая для раздора HIP RR, доступна.

Доменные имена **недопустимо** сжимать. RVS или серверы указываются в порядке предпочтения (первый наиболее предпочтительней), задавая неявный порядок RVS в одной записи RR. При наличии нескольких HIP RR с одним именем **недопустимо** использовать этот неявный порядок RVS в записи RR для упорядочения RVS из разных RR.

6. Формат представления HIP RR

Этот раздел задаёт представление HIP RR в первичном файле зоны.

Поле HIT length не указывается, поскольку оно неявно задаётся представлением поля HIT.

Поле PK algorithm представляется целым числом без знака.

Поле HIT представляется в формате Base16 [RFC4648] (hex) для значения HIT. В представление **недопустимо** включать пробелы для того, чтобы отделить это поле от поля Public Key.

Поле Public Key представляется Base64-кодированием PK, как указано в разделе 4 [RFC4648]. В представление **недопустимо** включать пробелы для того, чтобы отделить это поле от поля Rendezvous Server.

Поле PK length не указывается, поскольку оно неявно задано представлением поля Public Key, не содержащим пробелов.

Поле Rendezvous Server содержит одно или несколько доменных имён, разделённых пробелами. Эти пробелы применяются лишь в формате представления HIP RR и отсутствуют при передаче HIP RR в линию).

Полное представление записи HIP имеет вид

```
IN  HIP   ( pk-algorithm
            base16-encoded-hit
            base64-encoded-public-key
            rendezvous-server[1]
                    ...
            rendezvous-server[n] )
```

Если серверы RVS не присутствуют, запись HIP имеет вид

```
IN  HIP   ( pk-algorithm
            base16-encoded-hit
            base64-encoded-public-key )
```

7. Примеры

В приведённых ниже примерах поле Public Key, не содержащее пробелов, разделено на несколько строк в соответствии с требованиями к форматированию документа.

Пример для узла с HI и HIT но без RVS

```
www.example.com.      IN  HIP ( 2 200100107B1A74DF365639CC39F1D578
                                AwEAAbdxyhNuSutc5EMzxTs9LBPCIkOFH8cI
vM4p9+LrV4e19WzK00+CI6zBCQTdtWsuxKbWIy87UOoJTwkUs7lBu+Upr1gsNrut79ry
```

```
   ra+bSRGQb1slImA8YVJyuIDsj7kwzG7jnERNqnWxZ48AWkskmdHaVDP4BcelrTI3rMXd
   XF5D )
```

Пример для узла с HI, HIT и одним именем RVS

```
   www.example.com.      IN  HIP ( 2 200100107B1A74DF365639CC39F1D578
                                   AwEAAbdxyhNuSutc5EMzxTs9LBPCIkOFH8cI
   vM4p9+LrV4e19WzK00+CI6zBCQTdtWsuxKbWIy87UOoJTwkUs7lBu+Upr1gsNrut79ry
   ra+bSRGQb1slImA8YVJyuIDsj7kwzG7jnERNqnWxZ48AWkskmdHaVDP4BcelrTI3rMXd
   XF5D
                                   rvs.example.com. )
```

Пример для узла с HI, HIT и двумя RVS

```
   www.example.com.      IN  HIP ( 2 200100107B1A74DF365639CC39F1D578
                                   AwEAAbdxyhNuSutc5EMzxTs9LBPCIkOFH8cI
   vM4p9+LrV4e19WzK00+CI6zBCQTdtWsuxKbWIy87UOoJTwkUs7lBu+Upr1gsNrut79ry
   ra+bSRGQb1slImA8YVJyuIDsj7kwzG7jnERNqnWxZ48AWkskmdHaVDP4BcelrTI3rMXd
   XF5D
                                   rvs1.example.com.
                                   rvs2.example.com. )
```

8. Вопросы безопасности

В этом разделе рассматриваются известные угрозы, связанные с использованием расширения HIP DNS.

Подобно IPSECKEY RR [RFC4025], расширение DNS Extension позволяет двум узлам HIP предоставить один другому открытый ключевой материал (HI). Эти отождествления HI будут затем использоваться при обмене ключами между партнёрами. Поэтому расширение HIP DNS, как и IPSECKEY RR, подвержено угрозам атак на незащищённые записи RR, как описано ниже.

Узлу HIP **следует** получать записи HIP RR от доверенной стороны по защищённому каналу, обеспечивающему целостность и подлинность RR. Такой защищённый канал обеспечивает DNSSEC [RFC4033] [RFC4034] [RFC4035]. Однако следует подчеркнуть, что DNSSEC обеспечивает защиту целостности и аутентификацию данных лишь для канала между публикующим зону сервером DNS и узлом HIP, не гарантируя доверия к объекту, публикующему зону. Поэтому RRSIG из HIP RRSet **недопустимо** считать сертификатом привязки HI и/или HIT к имени владельца.

При отсутствии подходящего защищённого канала обе стороны уязвимы для атак MitM и DoS (Denial-of-Service — отказ в обслуживании), а несвязанные стороны также могут подвергаться DoS-атакам. Эти угрозы рассмотрены ниже.

8.1. Вмешательство атакующего в незащищённую запись HIP RR

HIP RR содержит открытый ключевой материал в форме PK (HI) указанного именем партнёра и его защищённого хэша (HIT). Они нечувствительны к атакам, в которых злоумышленник может раскрыть содержимое. Однако злоумышленник, способный организовать активную атаку DNS, т. е. подменит HIP RR (например, путём подмены DNS), сможет организовать MitM-атаку на криптографическое ядро обмена HIP (переписать HIP RR ответчика).

HIP RR может включать доменное имя RVS, преобразованное в IP-адрес получателя, где указанный именем партнёр доступен для I1 в соответствии с расширением HIP Rendezvous [RFC8004]. Таким образом, атакующий, способный вмешаться в RR, сможет перенаправить пакеты I1, отправленные указанному именем партнёру, на выбранный адрес IP для атаки DoS или MitM. Отметим, что этот вид атак возможен не только для HIP и существует независимо от использования HIP и HIP RR. Такой злоумышленник может вмешаться и в записи A или AAAA RR.

Атакующий очевидно сможет использовать отмеченные атаки в комбинации, заменяя HI ответчика и IP-адрес RVS своими значениями в подменных пакетах DNS, передаваемых по HI инициатора, а затем перенаправив на него все пакеты обмена для организации MitM-атаки на HIP. В этом случае HIP не обеспечивает конфиденциальности и защиты HI инициатора от перехвата.

8.2. Конфликты хэш-значений и HIT

Как и в других криптографических алгоритмах, некоторые хэш-значения (например, SHA1, применяемые в HIP для создания HIT из HI) могут оказаться незащищёнными в результате обнаружения эксплойта, позволяющего злоумышленнику с достаточными вычислительными ресурсами нарушить одну из защитных функций хэша (например, его предполагаемую устойчивость к конфликтам - совпадениям). Поэтому реализациям конечного узла HIP **не следует** аутентифицировать своих партнёров HIP на основе лишь тега HIT, полученного от DNS, а **следует** выполнять проверку подлинности на основе отождествления HI.

8.3. DNSSEC

При отсутствии DNSSEC записи HIP RR подвержены угрозам, описанным в RFC 3833 [RFC3833].

9. Взаимодействие с IANA

В [RFC5205], отменённом этим документом, определено и зарезервировано указанное в таблице значение в субреестре Resource Record (RR) TYPEs реестра Domain Name System (DNS) Parameters.

Значение	*Тип*
55	HIP

В субреестре Resource Record (RR) TYPEs реестра Domain Name System (DNS) Parameters ссылка на [RFC5205] заменена ссылкой на данный документ.

Как и [RFC5205], данный документ использует Algorithm Type из [RFC4025] для записей IPSEC KEY RR. Для справки определённые к настоящему моменту значения приведены в таблице.

Значение	*Описание*
1	Присутствует ключ DSA в формате [RFC2536]
2	Присутствует ключ RSA в формате [RFC3110]

Агентство IANA Добавило указанное в таблице значение в субреестр Algorithm Type Field реестра IPSECKEY Resource Record Parameters [RFC4025].

Значение	*Описание*
1	Присутствует ключ ECDSA в формате [RFC6605]

10. Литература

10.1. Нормативные документы

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <http://www.rfc-editor.org/info/rfc1034>.

[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>.

[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>.

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, DOI 10.17487/RFC2181, July 1997, <http://www.rfc-editor.org/info/rfc2181>.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, DOI 10.17487/RFC3596, October 2003, <http://www.rfc-editor.org/info/rfc3596>.

[RFC4025] Richardson, M., "A Method for Storing IPsec Keying Material in DNS", RFC 4025, DOI 10.17487/RFC4025, March 2005, <http://www.rfc-editor.org/info/rfc4025>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <http://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <http://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <http://www.rfc-editor.org/info/rfc4035>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <http://www.rfc-editor.org/info/rfc4648>.

[RFC6605] Hoffman, P. and W. Wijngaards, "Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC", RFC 6605, DOI 10.17487/RFC6605, April 2012, <http://www.rfc-editor.org/info/rfc6605>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <http://www.rfc-editor.org/info/rfc7401>.

[RFC8004] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", RFC 8004, DOI 10.17487/RFC8004, October 2016, <http://www.rfc-editor.org/info/rfc8004>.

10.2. Дополнительная литература

[RFC2536] Eastlake 3rd, D., "DSA KEYs and SIGs in the Domain Name System (DNS)", RFC 2536, DOI 10.17487/RFC2536, March 1999, <http://www.rfc-editor.org/info/rfc2536>.

[RFC3110] Eastlake 3rd, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", RFC 3110, DOI 10.17487/RFC3110, May 2001, <http://www.rfc-editor.org/info/rfc3110>.

[RFC3833] Atkins, D. and R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, DOI 10.17487/RFC3833, August 2004, <http://www.rfc-editor.org/info/rfc3833>.

[RFC4423] Moskowitz, R. and P. Nikander, "Host Identity Protocol (HIP) Architecture", RFC 4423, DOI 10.17487/RFC4423, May 2006, <http://www.rfc-editor.org/info/rfc4423>.

[RFC5205] Nikander, P. and J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions", RFC 5205, DOI 10.17487/RFC5205, April 2008, <http://www.rfc-editor.org/info/rfc5205>.

[RFC5206] Nikander, P., Henderson, T., Ed., Vogt, C., and J. Arkko, "End-Host Mobility and Multihoming with the Host Identity Protocol", RFC 5206, DOI 10.17487/RFC5206, April 2008, <http://www.rfc-editor.org/info/rfc5206>.

Приложение A. Отличия от RFC 5205

- Обновлены ссылки на HIP с указанием пересмотренных спецификаций протокола HIP.
- Расширены записи DNS HIP RR для поддержки Host Identity на основе ECDSA.
- Уточнено, что запрос должен повторяться после завершения срока действия (TTL) записи RR.
- Добавлены разъяснения для случая нескольких HIP RR, связанных с одним именем.
- Указано применение кодирования Base64 в соответствии с разделом 4 в [RFC4648].
- Указан формат передачи (wire format) при включении нескольких RVS в одну запись RR.
- Указано использование пробела (whitespace) в качестве разделителя для человеко-читаемого представления RR, но не для передачи в линию.

Благодарности

Как обычно в IETF, этот документ является результатом работы многих людей. Автор благодарен разработчику (Michael Richardson), участникам и рецензентам спецификации IPSECKEY RR [RFC4025], позволившей создать этот документ. Автор также признателен людям, которые предоставили вдумчивые и полезные комментарии и предложения, оказавшие помощь при подготовке документа: Jeff Ahrenholz, Rob Austein, Hannu Flinck, Olafur Gudmundsson, Tom Henderson, Peter Koch, Olaf Kolkman, Miika Komu, Andrew McGregor, Gabriel Montenegro, Erik Nordmark. Некоторые части этого документа заимствованы из спецификации HIP [RFC7401]. Спасибо также Sheng Jiang за рецензирование документа для Internet Area Directorate в процессе его публикации.

Участник работы

Teemu Koponen был соавтором ранней экспериментальной версии этой спецификации [RFC5205].

Адрес автора

Julien Laganier
Luminate Wireless, Inc.
Cupertino, CA
United States of America
Email: julien.ietf@gmail.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru