Network Working Group
Request for Comments: 3007
Updates: 2535, 2136
Obsoletes: 2137
Category: Standards Track

B. Wellington
Nominum

November 2000

Secure Domain Name System (DNS) Dynamic Update

Защищённое динамическое обновление DNS

Статус документа

Данный документ содержит спецификацию стандартного протокола Internet, предложенного сообществу Internet, и является приглашением к дискуссии в целях развития этого протокола. Сведения о текущем состоянии стандартизации протокола вы найдёте в документе «Internet Official Protocol Standards» (STD 1). Документ можно распространять без ограничений.

Авторские права

Аннотация

Этот документ предлагает метод защищённого динамического обновления для системы доменных имён (Domain Name System или DNS). Описываемый метод предполагается гибким и полезным, а также не требует значительных изменений протокола. Проверка подлинности сообщений об обновлении отделена от последующей проверки данных с помощью DNSSEC. Защищённое взаимодействие основано на аутентифицированных запросах и транзакциях для проверки полномочий.

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].

1. Введение

С этом документе определяются средства защиты динамических обновлений DNS, позволяющие вносить изменения в содержимое зон лишь уполномоченным сторонам. Основой для работы послужили имеющиеся незащищённые операции динамического обновления.

Предполагается будет знакомство читателя с системой DNS [RFC1034, RFC1035] и её динамическим обновлением [RFC2136]. Кроме того, рекомендуется ознакомиться с защитными расширениями DNS [RFC2535], защитой транзакций SIG(0) [RFC2535, RFC2931] и TSIG [RFC2845].

Документ частично обновляет RFC 2535 (параграф 3.1.2) и RFC 2136. Документ отменяет RFC 2137, предоставляя другой вариант защищённых динамических обновлений.

1.1. Обзор динамического обновления DNS

Динамическое обновление DNS задаёт новый код операции DNS (opcode) и новую интерпретацию сообщений DNS с таким кодом операции. Обновления могут задавать вставку или удаление данных, а также предварительные условия, необходимые для внесения изменений. Все проверки и изменения для запроса обновления DNS относятся лишь к одной зоне и выполняются на первичном сервере этой зоны. Первичный сервер динамической зоны инкрементирует серийный номер SOA, когда выполняется обновление или при следующем извлечении SOA.

1.2. Обзор защиты транзакций DNS

Обмен сообщениями DNS с записями TSIG [RFC2845] или SIG(0) [RFC2535, RFC2931] позволяет двум субъектам DNS проверить подлинность запросов и откликов DNS, передаваемых между ними. Код аутентификации сообщения TSIG MAC (message authentication code) выводится из общего секрета, а SIG(0) создаётся из секретного ключа, открытый ключ для которого хранится в DNS. В обоих случаях запись подпись или MAC включается как финальная запись о ресурсе в сообщении DNS. Хэш-значения на основе ключа, применяемые в TSIG недороги в плане расчёта и проверки. Шифрование с открытым ключом, применяемое в SIG(0), лучше расширяется, поскольку открытые ключи хранятся в DNS.

1.3. Сравнение аутентификации данных и сообщений

Аутентификация на основе сообщений с использованием TSIG или SIG(0) обеспечивает защиту всего сообщения с помощью одной подписи и одной проверки, которая в случае TSIG является сравнительно недорогими созданием и проверкой MAC. Для запросов обновления подпись может определять на основе политики или согласования ключей полномочия на подачу запросов.

Записи DNSSEC SIG можно применять для защиты целостности отдельных RR или RRset в сообщении DNS с полномочиями владельца зоны. Однако это не обеспечивает должной защиты запросов динамического обновления.

Применение записей SIG для защиты RRset в запросах обновления несовместимо с устройством обновления, как описано ниже, и в любом случае будет требовать множества дорогостоящих подписей с открытым ключом и проверок.

Подписи SIG не охватывают заголовок сообщения, который включает число записей. Поэтому можно добавлять и удалять RRset, не вызывая отказов при проверке.

Если бы записи SIG применялись для защиты раздела предварительных условий, было бы невозможно определить, являются ли сами SIG предварительными условиями или просто служат для проверки.

В разделе обновления запроса обновления подпись запросов на добавление RRset не вызывает сложностей и может постоянно применяться для защиты данных, как указано в [RFC2535]. Однако при удалении RRset для SIG не будет данных.

1.4. Подписи данных и сообщений

Как указано в [RFC3008], процессу проверки DNSSEC на проверяющем распознавателе **недопустимо** обрабатывать не относящиеся к зоне ключи, пока этого не разрешает локальная политика. При защищённом динамическом обновлении все изменённые данные в подписанной зоне **должны** быть подписаны с соответствующим ключом зоны. Это полностью отделяет проверку подлинности запроса на обновление пот аутентификации самих данных.

Основная польза ключей хоста и пользователя применительно к DNSSEC заключается в проверке подлинности сообщений, включая динамические обновления. Ключи хоста и пользователя **могут** применяться для создания записей SIG(0) с целью аутентификации обновлений, а также **могут** использоваться в процессе TKEY [RFC2930] для генерации общих секретов TSIG. В обоих случаях записи SIG, созданные с не относящимися к зоне ключами, не будут применяться в процессе проверки DNSSEC, пока этого не требует локальная политика.

Проверка подлинности данных при их представлении в DNS включает лишь ключи DNSSEC для зоны и созданные с этими ключами подписи.

1.5. Поле signatory

В параграфе 3.1.2 [RFC2535] поле signatory для ключа определено как 4 финальных бита поля флагов, но значение поля не задано. В соответствии с обновлением [RFC2535] в этом поле записей KEY **следует** устанавливать значение 0, которое **должно** игнорироваться.

2. Проверка подлинности

Подписи TSIG или SIG(0) **должны** включаться во все сообщения динамического обновления. Это позволяет серверу достоверно определить источник сообщения. При использовании аутентификации SIG(0) отправителем (владельцем) будет владелец записи KEY RR, послужившей для создания SIG(0). Если сообщение содержит подпись TSIG, созданную с помощью заданного статически общего секрета, владелец будет тем же, что и для общего секрета или производным от него. Если сообщение содержит подпись TSIG, созданную с помощью динамического общего секрета, владельцем будет тот, кто аутентифицировал процесс TKEY, если же процесс не был аутентифицирован, сведений о владельце не будет и соответствующий общий секрет TSIG **недопустимо** применять для защищённых динамических обновлений.

Подписи SIG(0) **не следует** генерировать с ключами зон, поскольку транзакцию инициирует хост или пользователь, а не зона.

В сообщения обновления **можно** включать записи DNSSEC SIG (отличные от SIG(0)), но их **недопустимо** использовать для проверки подлинности запросов обновления.

При отказе обновления из-за его подписания с несанкционированным ключом сервер **должен** указать ошибку, вернув сообщение RCODE REFUSED. Другие ошибки TSIG, SIG(0) или динамического обновления возвращаются в соответствии со спецификацией протокола.

3. Политика

Правила политики настраиваются администратором зоны и применяются первичным ведущим сервером зоны. Правила определяют разрешённые действия для аутентифицированного участника. Проверка правил учитывает участников и желаемые действия, при этом участник определяется по ключу подписи сообщения и правила применяются к сообщениям динамического обновления, подписанным с этим ключом.

Политика сервера определяет критерии, показывающие, разрешено ли для ключа в подписи обновления выполнять запрошенное обновление. По умолчанию **недопустимо** разрешать участнику менять какие-либо данные в зоне, а все разрешения **должны** быть указаны в конфигурации.

Политика полностью реализуется в конфигурации первичного сервера зоны по нескольким причинам. Это снимает ограничения, накладываемые кодированием правил в фиксированном числе битов (например, в поле signatory KEY RR). Правила относятся лишь к применяющему их серверу, поэтому нет причин раскрывать политику. Изменениям политики или новому типу правил **не следует** влиять на протокол DNS или формат данных, а также вызвать проблемы функциональной совместимости.

3.1. Стандартные правила

Реализациям **следует** разрешать правилам контроля доступа использовать участника в качестве маркера проверки полномочий и **можно** разрешать правилам предоставлять полномочия для подписанных сообщений без учёта участника. Общепринятой практикой является ограничение полномочий участника по доменному имени, т. е. участнику может быть разрешено добавлять, удалять и изменять записи для одного или нескольких соответствующих доменов. Реализациям **следует** разрешать управление доступом по именам, а также **следует** разрешать краткое представление принадлежащего участнику имени, его субдоменов и всех имён в зоне.

Кроме того, серверу **следует** разрешать ограничение обновлений по типу RR, чтобы участник мог добавлять, изменять или удалять записи определённого типа для некоторых имён. Реализациям **следует** разрешать контроль доступа на основе типа, а также **следует** разрешать краткое представление всех типов и всех пользовательских типов, где пользовательскими считаются типы, не способные сами влиять на работу DNS.

3.1.1. Пользовательские типы

Пользовательскими считаются все типы, кроме SOA, NS, SIG и NXT. Записи SOA и NS **не следует** изменять обычным пользователям, поскольку эти типы создают или изменяют точки делегирования. Добавление записей SIG может приводить к атакам, создающим дополнительную нагрузку на распознаватели, а удаление SIG для зоны может приводить к дополнительной нагрузке на сервер. Отметим, что доступ к этим записям обычных пользователей не запрещён, но не рекомендуется.

Динамическим обновлениям **недопустимо** создавать, изменять или удалять записи NXT, поскольку их обновление может приводить к нестабильности протокола. Это является обновлением RFC 2136.

Вопросы, связанные с обновлением записей KEY рассматриваются в разделе 5.

3.2. Дополнительные правила

Пользователи могут реализовать любые правила. Политика может быть сколь угодно конкретной или общей, а также сколь угодно сложной. Правила могут зависеть от участников или иных характеристик подписанных сообщений.

4. Взаимодействие с DNSSEC

Хотя этот документ не меняет способа обработки защищённых обновлений зон, некоторые вопросы нужно прояснить.

4.1. Добавление SIG

Полномочный запрос **может** включать записи SIG в каждом RRset. Поскольку записи SIG (кроме SIG(0)) **недопустимо** применять для проверки подлинности сообщений обновления, такие записи не требуются. Если участник уполномочен обновлять записи SIG и в обновлении имеются такие записи, они добавляются без проверки. Сервер **может** проверять записи SIG и отбрасывать SIG с истекшим сроком действия.

4.2. Удаление SIG

Если участник уполномочен обновлять записи SIG и обновление задаёт удаление SIG, сервер **может** переопределить полномочия и отклонить обновление. Например, сервер может разрешать удаление всех записей SIG, не созданных с ключом зоны.

4.3. Неявные обновления SIG

Если обновляемая зона защищена, набор RRset, затронутый обновлением, по завершении обновления **должен** быть подписан в соответствии с политикой зоны. Для этого обычно требуется создать одну или несколько записей SIG с одним или разными ключами зоны, закрытые компоненты которых **должны** быть доступны через сеть (online) [RFC3008].

При обновлении содержимого RRset сервер **может** удалять связанные записи SIG, поскольку они станут недействительными.

4.4. Воздействие на зону

При внесении каких-либо изменений сервер **должен** (если необходимо) создавать новую запись SOA и новые записи NXT, подписывая их с соответствующими ключами зоны. Изменения записей NXT путём защищённого динамического обновления явно запрещены. Обновления SOA разрешаются, поскольку поддержка параметров SOA выходит за рамки протокола DNS.

5. Вопросы безопасности

Этот документ требует, чтобы ключ зоны и, возможно, иные криптографические материалы хранились на подключённом к сети хосте, скорей всего, на сервере имён. Эти материалы относятся к зоне защиты хоста и должны храниться в секрете. Раскрытие этих секретов подвергает данные DNS риску атак с маскированием. Под угрозу попадают данные зон, обслуживаемых машиной и делегированных с неё.

Разрешение обновлять записи KEY может приводить к нежелательным результатам, поскольку участнику может быть разрешена вставка открытого ключа, не имея секретного ключа, и, возможно, выдача себя за владельца ключа.

6. Благодарности

Авторы благодарят указанных ниже в алфавитном порядке людей за рецензии и содержательные комментарии.

Harald Alvestrand
Donald Eastlake
Olafur Gudmundsson
Andreas Gustafsson
Bob Halley
Stuart Kwan
Ed Lewis

7. Литература

[RFC1034] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987.

[RFC2136] Vixie (Ed.), P., Thomson, S., Rekhter, Y. and J. Bound, "Dynamic Updates in the Domain Name System", RFC 2136, April 1997.

[RFC2137] Eastlake, D., "Secure Domain Name System Dynamic Update", RFC 2137, April 1997.

[RFC2535] Eastlake, G., "Domain Name System Security Extensions", RFC 2535, March 1999.

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake, D. and B. Wellington, "Secret Key Transaction Signatures for DNS (TSIG)", RFC 2845, May 2000.

[RFC2930] Eastlake, D., "Secret Key Establishment for DNS (TKEY RR)", RFC 2930, September 2000.

[RFC2931] Eastlake, D., "DNS Request and Transaction Signatures (SIG(0)s)", RFC 2931, September 2000.

[RFC3008] Wellington, B., "Domain Name System Security (DNSSEC) Signing Authority", RFC 3008, November 2000.

8. Адрес автора

Brian Wellington
Nominum, Inc.
950 Charter Street
Redwood City, CA 94063
Phone: +1 650 381 6022
EMail: Brian.Wellington@nominum.com

9. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru