Network Working Group
Request for Comments: 4033
Obsoletes: 2535, 3008, 3090, 3445, 3655, 3658,
3755, 3757, 3845
Updates: 1034, 1035, 2136, 2181, 2308, 3225,
3007, 3597, 3226
Category: Standards Track

R. Arends
Telematica Instituut
R. Austein
ISC
M. Larson
VeriSign
D. Massey
Colorado State University
S. Rose
NIST

March 2005

Защита DNS - введение и требования

DNS Security Introduction and Requirements

Статус документа

Этот документ содержит спецификацию стандартного протокола, предложенного сообществу Internet, и служит приглашением к дискуссии в целях развития. Текущее состояние стандартизации и статус описанного здесь протокола можно узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться без ограничений.

Аннотация

Расширение DNSSEC[1] добавляет поддержку аутентификации источника и проверку целостности данных для системы доменных имён DNS. В данном документе содержится вводная информация и описание возможностей и недостатков расширения. В документе также рассматриваются типы сервиса, которые расширение DNS может и не может обеспечивать. И, наконец, в документе приводится описание связей между набором документов, описывающих DNSSEC.

Оглавление

1. Введение

Этот документ является введением для серии RFC, описывающих расширение DNSSEC для системы доменных имен. Документ вместе с [RFC4034] и [RFC4035] служит обновлением и совершенствованием расширений в целях безопасности, описанных в [RFC2535] и предшествующих документах. Расширения включают набор новых типов записей RR[2] и изменение существующего протокола DNS ([RFC1035]). Новые записи и обновление протокола не описываются в данном документе полностью, но они подробно описаны в документах, перечисленных в главе 10. В главах 3 и 4 описываются более детально возможности и ограничения предложенного расширения. В главе 5 обсуждается сфера действия описывающего расширение набора документов. В глава 6 - 9 обсуждается воздействие

[1]Domain Name System Security Extensions - расширение системы доменных имён в целях безопасности.
[2]Resource record - запись для ресурса.

этого документа на серверы преобразования (resolver), оконечные серверы преобразования (stub resolver), зоны и серверы имён.

Данный документ в комбинации в двумя другими документами серии отменяет действие документов [RFC2535], [RFC3008], [RFC3090], [RFC3445], [RFC3655], [RFC3658], [RFC3755], [RFC3757] и [RFC3845]. Кроме того, этот набор документов служит обновлением (но не отменяет) для документов [RFC1034], [RFC1035], [RFC2136], [RFC2181], [RFC2308], [RFC3225], [RFC3007], [RFC3597] и части [RFC3226], относящейся к DNSSEC.

Расширение DNS в целях безопасности обеспечивает аутентификацию источника и обеспечение целостности данных DNS, а также рассматривает вопрос распространения открытых ключей. Расширение протокола не обеспечивает конфиденциальности.

2. Определения важнейших терминов DNSSEC

В этой главе приводятся определения множества терминов, используемых в описывающем расширение наборе документов. Эта глава будет полезна, как справочник по используемым в серии документов терминам, поэтому при первом чтении может оказаться достаточно бегло просмотреть определения и вернуться к ним при работе с соответствующими разделами данного набора документов.

Authentication Chain - цепочка аутентификации.

Чередующаяся последовательность наборов открытых ключей DNS (DNSKEY) и Delegation Signer (DS), формирующая подписанные данные - каждая связь в цепочке служит поручительством для следующей. Запись DNSKEY RR используется для верификации сигнатуры, покрывающей DS RR, и позволяет проверить запись DS RR. Запись DS RR содержит хэш другой записи DNSKEY RR и эта новая запись DNSKEY RR проверяется по соответствию хэшу в записи DS RR. Эта новая запись DNSKEY RR, в свою очередь, аутентифицирует другой набор DNSKEY RR и, в свою очередь, некая запись DNSKEY RR из этого набора может использоваться для аутентификации другой DS RR и т. д., пока цепочка не завершится записью DNSKEY RR, которая соответствует приватному ключу, подписывающему желаемые данные DNS. Например, корневой набор DNSKEY RR может использоваться при аутентификации набора DS RR для "example.". Набор DS RR "example." содержит хэш для некой записи из "example.". DNSKEY и соответствующий приватный ключ подписывают DNSKEY RR для "example.". Дополнение приватного ключа "example." DNSKEY RR подписывает данные (такие, как ("www.example.") и DS RR для делегирования "subzone.example."

Authentication Key - ключ аутентификации.

Открытый ключ, который защищенный распознаватель[1] проверяет и может, следовательно, использовать для аутентификации данных. Защищенный распознаватель может получить ключи аутентификации тремя способами. Во-первых, распознаватель обычно настроен так, что ему известен по крайней мере один открытый ключ - в конфигурационных параметрах указывается сам ключ или его хэш, который находится в DS RR (см. "trust anchor"). Во-вторых, распознаватель может использовать аутентифицированный открытый ключ для верификации записей DS RR и DNSKEY RR, на которые указывает DS RR. В-третьих, распознаватель может определить, что новый открытый ключ был подписан секретным ключом, соответствующим другому публичному ключу, который был уже верифицирован распознавателем. Отметим, что распознаватель всегда должен следовать локальной политике при определении необходимости аутентификации нового открытого ключа, даже если локальная политика состоит состоит лишь из аутентификации любого нового открытого ключа, для которого распознаватель способен проверить подпись.

Authoritative RRset - аутентичный набор RRset.

В контексте отдельной зоны RRset является аутентичным тогда и только тогда, когда имя владельца RRset входит в подмножество пространства имен, которое находится на уровне вершины (апекса) зоны или ниже его и на уровне или выше границы, отделяющей зону от ее потомков, если таковые имеются. Все наборы RRset на уровне вершины зоны являются аутентичными, за исключением отдельных RRset на уровне доменного имени, которое (если оно имеется), относится к родителю данной зоны. Этот набор RRset может включать DS RRset, набор NSEC RRset, указывающий на данный набор DS RRset (“родительский NSEC”) и записи RRSIG RR, связанные с этими RRset, каждый из которых является аутентичным в родительской зоне. Аналогично, если эта зона содержит любые точки делегирования, только родительский набор NSEC RRset, наборы DS RRset и все записи RRSIG RR, связанные с этими наборами RRset, являются аутентичными для этой зоны.

Delegation Point - точка делегирования[2].

Этот термин используется для обозначения имени на родительской стороне среза зоны. Т. е., точкой делегирования для "foo.example" в зоне "example" будет узел foo.example (апекс зоны для "foo.example"). См. также zone apex.

Island of Security - островок безопасности

Этот термин используется для обозначения подписанной, делегированной зоны, которая не имеет цепочки аутентификации от делегировавшего эту зону родителя. Т. е., здесь нет записи DS RR, содержащей хэш DNSKEY RR для островка в делегирующей родительской зоне (см. [RFC4034]). Островки безопасности обслуживаются защищенными[3] серверами имен и могут обеспечивать цепочки аутентификации для любых делегированных дочерних зон. Ответы от островка безопасности или его наследников могут быть аутентифицированы только в тех случаях, когда аутентификационные ключи могут быть аутентифицированы тем или иным доверенным способом за пределами протокола DNS.

Key Signing Key (KSK) - ключ подписывания ключа

Аутентификационный ключ, который соответствует закрытому (private) ключу, использованному для подписания одного или множества других аутентификационных ключей, которые, в свою очередь, имеют соответствующие закрытые ключи для подписывания других данных зоны. Локальная политика может требовать частой смены ключа, подписывающего зону, тогда как ключ подписывания ключа может использоваться в течение большего срока для обеспечения более стабильной защищённой точки входа в зону. Обозначение аутентификационного ключа в качестве ключа подписывания других ключей является рабочим вопросом - проверка достоверности DNSSEC не делает различий между ключами подписывания ключей и другими аутентификационными ключами

[1] В оригинале - security-aware resolver.
[2] Передачи полномочий.
[3] В оригинале - security-aware. Использованный здесь перевод не совсем точен, но суть отражает достаточно верно. Корректным и точным переводом будет «понимающий методы защиты, описанные в настоящем наборе документов». *Прим. перев.*

DNSSEC и можно использовать один ключ для подписывания зоны и других ключей. Более детальное обсуждение ключей для подписывания других ключей приведено в документе [RFC3757]. См. также zone signing key.

Non-Validating Security-Aware Stub Resolver - не проверяющий достоверность защищенный оконечный распознаватель

Защищенный оконечный распознаватель, который доверяет одному или более защищенному рекурсивному серверу имен для выполнения от его имени большинства задач, обсуждающихся в данном наборе документов. В частности, такой распознаватель является объектом, передающим запросы DNS, получающим отклики DNS и способным создавать подобающим образом защищённый канал к защищённому серверу имён, который будет выполнять эти задачи от имени оконечного защищённого распознавателя. См. также security-aware stub resolver, validating security-aware stub resolver.

Non-Validating Stub Resolver - не проверяющий оконечный распознаватель

Менее утомительный термин для обозначения non-validating security-aware stub resolver.

Security-Aware Name Server - защищённый сервер имён

Объект, действующий в роли сервера имён (определён в параграфе 2.4 документа [RFC1034]), который понимает защитные расширения DNS, определённые в данном наборе документов. В частности, защищённый сервер имён представляет собой объект, получающий запросы DNS, передающий отклики DNS, поддерживающий расширение размера сообщения EDNS0 ([RFC2671]) и бит DO ([RFC3225]), а также типы RR и биты заголовка сообщения, определённые в данном наборе документов.

Security-Aware Recursive Name Server- защищённый рекурсивный сервер имён

Объект, выступающий одновременно в качестве security-aware name server и security-aware resolver. Более громоздким, но эквивалентным термином является a security-aware name server that offers recursive service[1].

Security-Aware Resolver - защищённый распознаватель

Объект, играющий роль распознавателя (см. определение в параграфе 2.4 документа [RFC1034]) и понимающий защитные расширения DNS, определенные в данном наборе документов. В частности, защищенный распознаватель представляет собой объект, передающий запросы DNS, получающий отклики DNS, поддерживающий расширения размера сообщений EDNS0 ([RFC2671]) и бит DO ([RFC3225]), а также способный использовать типы RR и биты заголовка сообщения, определенные в настоящем наборе документов, для предоставления сервиса DNSSEC.

Security-Aware Stub Resolver - защищенный оконечный распознаватель

Объект, действующий в качестве оконечного распознавателя (см. определение в параграфе 5.3.1 документа [RFC1034]), который в достаточной степени понимает защитные расширения DNS, определенные в данном наборе документов, для предоставления дополнительных услуг, которые невозможно получить от обычного (не защищенного) оконечного распознавателя. Защищённые распознаватели могут быть проверяющими (validating) и не проверяющими (non-validating) достоверность в зависимости от того, проверяет ли распознаватель подписи DNSSEC сам или доверяет такую проверку дружественному защищённому серверу имен. См. также validating stub resolver, non-validating stub resolver.

Security-Oblivious <anything> - обычное <нечто>

Нечто, не относящееся к числу понимающего защищенного (security-aware).

Signed Zone - подписанная зона

Зона с подписанными наборами Rrset, содержащая корректно созданный ключ DNSKEY, подпись RRSIG[2], записи NSEC[3] и (необязательно) DS.

Trust Anchor - доверенная привязка

Сконфигурированная запись DNSKEY RR или хэш DS RR записи DNSKEY RR. Проверяющий защищенный оконечный распознаватель использует этот открытый ключ или хэш а качестве стартовой точки для построения аутентификационной цепочки отклика DNS. В общем случае проверяющий распознаватель будет получать начальные значения таких привязок с помощью того или иного защищенного или доверенного способа, не входящего в протокол DNS. Присутствие доверенной привязки также подразумевает, что распознавателю следует ожидать наличия подписи для зоны, на которую указывает такая привязка.

Unsigned Zone - неподписанная зона

Зона, не имеющая подписи.

Validating Security-Aware Stub Resolver - проверяющий достоверность оконечный распознаватель

Защищённый распознаватель, который передаёт запросы в рекурсивном режиме, но выполняет проверку сигнатур самостоятельно, не полагаясь на доверие к вышестоящему защищённому рекурсивному серверу имён. См. также security-aware stub resolver, non-validating security-aware stub resolver.

Validating Stub Resolver - проверяющий оконечный распознаватель

Менее утомительный термин для validating security-aware stub resolver.

Zone Apex - апекс (вершина) зоны

Этот термин используется для имени на дочерней стороне среза зоны. См. также delegation point.

Zone Signing Key (ZSK) - ключ для подписывания зоны

Аутентификационный ключ, который соответствует закрытому ключу, используемому для подписывания зоны. Обычно такой ключ является частью того же набора DNSKEY RRset, к которому относится ключ для подписывания ключей, чей закрытый ключ подписывает данного набора DNSKEY RRset, но ключ подписывания зоны используется для иных задач и может отличаться от ключа подписывания ключей (например, временем жизни). Назначение аутентификационного ключа для подписывания зоны является локальным рабочим вопросом; проверка достоверности DNSSEC не делает различий между ключами для подписывания зоны и другими аутентификационными ключами DNSSEC и можно использовать один ключ в качестве ключа для подписывания зоны и подписывания других ключей. См. также key signing key.

3. Службы, обеспечиваемые DNS Security

Защитные расширения DNS обеспечивают аутентификацию источника и гарантию целостности для данных DNS, включая механизмы аутентифицированного запрета на существование данных DNS. Защитные механизмы описаны ниже.

[1]Защищенный сервер имен, предоставляющий рекурсивный сервис.
[2]Resource Record Signature
[3]Next Secure

Эти механизмы требуют изменения протокола DNS. DNSSEC добавляет 4 новых типа записей о ресурсах - RRSIG[1], DNSKEY[2], DS[3] и NSEC[4]. Добавлены также два новых бита заголовков - CD[5] и AD[6]. Для поддержки сообщений DNS большего размера в связи с добавлением записей DNSSEC RR это расширение также требует поддержки EDNS0 ([RFC2671]). И, наконец, DNSSEC требует поддержки битов заголовка DNSSEC OK (DO) EDNS ([RFC3225]), чтобы защищенный распознаватель мог указать в своих запросах, желает ли он получать записи DNSSEC RR в откликах.

Перечисленные меры обеспечивают защиту от большинства угроз системе DNS, описанных в [RFC3833]. В главе 12 обсуждаются ограничения, присущие этим расширениям.

3.1. Аутентификация источника данных и проверка целостности

DNSSEC обеспечивает аутентификацию путем связывания криптографических цифровых подписей с наборами данных DNS RRset. Эти цифровые подписи хранятся в новых записях RRSIG. Обычно имеется один закрытый (ключ для подписывания данных зоны, но можно использовать и множество ключей. Например, могут использоваться отдельные ключи для каждого из различных алгоритмов создания цифровой подписи. Если защищённый распознаватель надёжным путём получает открытый ключ зоны, он может аутентифицировать подписанные данные зоны. Важной концепцией DNSSEC является то, что ключ, подписывающий данные зоны, связывается с самой зоной, а не с уполномоченными серверами этой зоны. Открытые ключи для механизмов аутентификации транзакций DNS также могут появляться в зонах, как описано в [RFC2931], но расширения DNSSEC сами по себе не имеют дела с защитой объектов данных DNS и каналов для выполнения транзакций DNS. Ключи, связанные с защитой транзакций, могут храниться в различных типах RR. Дополнительную информацию можно найти в [RFC3755].

Защищённый распознаватель может получить открытый ключ зоны с помощью доверенной привязки, заданной в конфигурации распознавателя или полученной обычными средствами преобразования DNS. Для второго варианта ключи хранятся в записях нового типа - DNSKEY RR. Отметим, что закрытые ключи, используемые для подписывания зоны, должны храниться отдельно с обеспечением защиты. Для надёжного получения публичных ключей с помощью преобразования DNS, сам ключ подписывается с помощью аутентификационного ключа, заданного в конфигурации, или другого ключа, который был заранее аутентифицирован. Защищённые распознаватели аутентифицируют данные зоны для формирования аутентификационной цепочки от полученного последним публичного ключа обратно к ранее известному аутентификационному ключу, который, в свою очередь, задаётся в конфигурации распознавателя или должен быть получен и проверен заранее. Следовательно, в конфигурации распознавателя должна быть задана по крайней мере одна доверенная привязка.

Если заданная в конфигурации доверенная привязка является ключом подписывания зоны, она будет аутентифицировать соответствующую зону; если заданный в конфигурации ключ является ключом для подписывания, он будет аутентифицировать ключ подписывания зоны. Если заданная в конфигурации доверенная привязка представляет собой хэш ключа, а не сам ключ, распознаватель может получить ключ с помощью запроса DNS. Чтобы помочь защищенным распознавателям создавать аутентификационные цепочки, защищённые серверы имён пытаются передавать сигнатуру (сигнатуры), требуемую для аутентификации открытого ключа зоны, в сообщении DNS вместе с самим ключом, благо в сообщении для этого имеется место.

Записи типа DS RR упрощают решение некоторых административных задач, связанных с подписыванием делегирования через организационные границы. Набор DS RRset находится в точке делегирования родительской зоны и показывает открытый ключ (ключи), используемый для самоподписывания DNSKEY RRset на вершине делегированной дочерней зоны. Администратор дочерней зоны, в свою очередь, использует закрытый ключ (ключи), соответствующий одному или нескольким открытым ключам в данном наборе DNSKEY RRset, для подписывания данных дочерней зоны. Типовая цепочка аутентификации, следовательно, будет иметь вид DNSKEY->[DS->DNSKEY]*->RRset, где символ * обозначает субцепочки DS->DNSKEY (0 или более). DNSSEC разрешает и более сложные цепочки аутентификации (такие, как дополнительные уровни DNSKEY RR, подписывающие другие DNSKEY RR внутри зоны).

Защищённый распознаватель обычно создаёт цепочку аутентификации от корня иерархии DNS вниз к ветвям зон, на основе заданных в конфигурации данных о корневом открытом ключе. Локальная политика может также позволять защищённому распознавателю использовать один или множество открытых ключей (или их хешей), отличных от корневого открытого ключа, не обеспечивать данных о корневом открытом ключе или запрещать распознавателю использовать открытые ключи по любым причинам, даже если эти ключи корректно подписаны и подписи проверены. DNSSEC обеспечивает механизмы, посредством которых защищенный распознаватель может определить, является ли подпись RRset достоверной с точки зрения DNSSEC. Однако последнее слово при анализе аутентификации для ключей и данных DNS остается за локальной политикой, которая может расширить или переназначить расширения протокола, определенные в этом наборе документов (см. также главу 5).

3.2. Аутентификация в случаях отсутствия имени или типа

Механизм защиты, описанный в параграфе 3.1, обеспечивает лишь способ подписывания существующих в зоне наборов RRset. Проблема возврата негативных откликов с таким же уровнем аутентификации и целостности требует использования еще одного нового типа записи - NSEC. Запись NSEC позволяет защищенному распознавателю аутентифицировать негативный отклик в случаях отсутствия имени или типа с использованием того же механизма, который применяется при аутентификации других откликов DNS. Использование NSEC требует канонического представления и упорядочения имен в зонах. Цепочки записей NSEC явно описывают пропуски или «пустое пространство» между доменными именами в зоне, а для существующих имен присутствует список типов RRset. Каждая запись NSEC подписывается и аутентифицируется, как описано в параграфе 3.1.

[1]Resource Record Signature - подпись RR
[2]DNS Public Key - открытый ключ DNS.
[3]Delegation Signer
[4]Next Secure
[5]Checking Disabled - проверка запрещена.
[6]Authenticated Data - аутентифицированные данные.

4. Сервис, не поддерживаемый DNS Security

Система DNS изначально разрабатывалась в предположении, что DNS будет возвращать одинаковый отклик на данный запрос независимо от того, кем был подан этот запрос. Таким образом, все данные DNS были доступными для каждого. Соответственно, расширения не предназначены для обеспечения конфиденциальности, поддержки списков контроля доступа или иных способов дифференциации запрашивающих данные сторон.

DNSSEC не обеспечивает защиты от DoS-атак. Защищенные распознаватели и серверы имен уязвимы также для DoS-атак на основе криптографических механизмов. Более детальное обсуждение этого вопроса содержится в главе 12.

Расширения DNS обеспечивают аутентификацию данных и источника для операций DNS. Описанный выше механизм не предназначен для защиты таких операций, как перенос зон или динамическое обновление ([RFC2136], [RFC3007]). Для таких транзакций защиту можно организовать с помощью схем, описанных в [RFC2845] и [RFC2931].

5. Сфера действия документов и проблема последнего интервала

Спецификации этого набора документов определяют поведение узлов, подписывающих зону, а также защищенных серверов имен и распознавателей таким образом, чтобы проверяемые объекты могли однозначно определять состояние данных.

Проверяющий распознаватель может определять 4 перечисленных ниже состояния:

Secure - защищенное
: Проверяющий распознаватель имеет доверенную привязку или цепочку доверия или способен проверить все подписи в отклике.

Insecure - незащищенное
: Проверяющий распознаватель имеет доверенную привязку или цепочку доверия и (в некой точке делегирования) подписанное подтверждение отсутствия записи DS. Это показывает, что последующие ветви дерева могут оказаться незащищенными. Проверяющий распознаватель может иметь локальное правило для маркировки части доменного пространства, как незащищенной.

Bogus - подделка
: Проверяющий распознаватель имеет доверенную привязку и защищенное делегирование, показывающие, что дополнительные данные подписаны, но проверка отклика по той или иной причине дала отрицательный результат (отсутствие подписи, просроченная подпись, отсутствие данных, которые должны присутствовать в соответствующей NSEC RR и т. п.).

Indeterminate - неопределенное
: Нет доверенной привязки, которая показывает, что определенная часть дерева защищена. Это состояние принимается по умолчанию.

Эта спецификация определяет лишь, как защищенные серверы имен могут сигнализировать не проверяющим достоверность оконечным распознавателям, что данные были квалифицированы как подставные (с помощью RCODE=2, "Server Failure", см. [RFC4035]).

Существует механизм, с помощью которого защищенный сервер имен может сообщить защищенному оконечному распознавателю о том, что данные были сочтены защищенными (с помощью бита AD; см. [RFC4035]).

Данная спецификация не определяет формат обмена информацией о причинах, по которым отклики были сочтены поддельными или помечены, как незащищенные. Текущий механизм сигнализации не делает различий между неопределённым и незащищённым состоянием.

Метод расширенной сигнализации об ошибках и политике между защищенными распознавателями и защищенными серверами имен является темой дальнейшей работы, равно как интерфейс между защищенным распознавателем и использующими его приложениями. Отметим, однако, что отсутствие спецификации для такого типа взаимодействий не запрещает развертывание подписанных зон или защищенных рекурсивных серверов имен, которые будут предотвращать передачу приложениям подставных данных.

6. Распознаватели

Защищенный распознаватель способен выполнять криптографические функции, требуемые для проверки цифровых подписей, используя по крайней мере обязательные для реализации алгоритмы. Защищенные распознаватели должны также уметь формировать аутентификационные цепочки от последней полученной зоны к ключу аутентификации, как описано выше. Этот процесс может потребовать дополнительных запросов к промежуточным зонам DNS для получения требуемых записей DNSKEY, DS и RRSIG. В конфигурации защищенного распознавателя следует указывать по крайней мере одну доверенную привязку в качестве стартовой точки, в которой будут начинаться попытки формирования цепочек аутентификации.

Если защищенный распознаватель отделен от уполномоченного сервера имен любым промежуточным устройством, играющим роль посредника для DNS, если рекурсивный сервер имен или промежуточное устройство не являются защищенными, распознаватель может оказаться неспособным работать в защищенном режиме. Например, если пакеты защищенного распознавателя маршрутизируются через систему трансляции адресов и устройство, включающее DNS-прокси, не является защищенным, для защищенного распознавателя может оказаться сложным или невозможным получение или проверка подписанных данных DNS. Особые сложности могут возникать у защищенного распознавателя при получении DS RR в таких ситуациях, поскольку DS RR не следуют обычным правилам DNS для принадлежности RR на срезе зоны. Отметим, что такие проблемы не являются спецификой NAT - не понимающие защиты программы DNS любого типа между защищенным распознавателем и уполномоченным сервером имен будут вызывать проблемы с DNSSEC.

Если защищенный распознаватель должен полагаться на не подписанную зону или сервер имен, который не понимает защитных расширений, этот распознаватель может оказаться неспособен проверить отклики DNS и ему потребуется локальная политика на основе которой будет приниматься решение о судьбе непроверенных откликов.

Защищенному распознавателю следует принимать во внимание период проверки подписи при рассмотрении времени жизни (TTL) данных в своем кэше, чтобы избежать кэширования подписанных данных на период, превышающий срок

действия подписи. Однако ему следует также допускать возможность некорректности показаний своих часов. Таким образом, защищенный распознаватель, который является часть защищенного рекурсивного сервера имен, должен аккуратно принимать во внимание бит DNSSEC CD ([RFC4034]). Это нужно для того, чтобы предотвратить блокирование достоверных подписей, передаваемых другим защищенным распознавателям, которые являются клиентами данного рекурсивного сервера имен. Обработка защищенным рекурсивным сервером запросов с битом CD описана в [RFC4035].

7. Оконечные распознаватели

Хотя протокол не требует этого жестко, большинство запросов DNS приходит от оконечных распознавателей. Такие распознаватели по определению являются минимальными распознавателями DNS, которые используют режим рекурсивных запросов для передачи большей части работы по преобразованию имен DNS рекурсивным серверам имен. Исходя из такого повсеместного использования оконечных распознавателей, архитектура DNSSEC принимает такие распознаватели во внимание, но средства защиты, требуемые от оконечного распознавателя, отличаются в некоторых аспектах от требований к защищенным итеративным распознавателям.

Хотя обычные оконечные распознаватели могут получить некоторые преимущества DNSSEC, если используемые ими рекурсивные серверы имен являются защищенными, для реального доверия к службам DNSSEC оконечный распознаватель должен доверять как используемым серверам имен, так и коммуникационным каналам, связывающим его с этими серверами. Первый вопрос определяется локальной политикой - обычный распознаватель, по сути, не имеет выбора кроме как положиться на используемый рекурсивный сервер, поскольку распознаватель не может выполнять операций DNSSEC по проверке достоверности. Второй вопрос требует того или иного механизма защиты канала - надлежащего использования механизмов аутентификации транзакций DNS (таких, как SIG(0) ([RFC2931]) или TSIG ([RFC2845]) будет вполне достаточно, подойдет и использование IPsec. Конкретные реализации могут выбирать и другие доступные варианты (например, поддерживаемые операционной системой механизмы обмена данными между процессами). Конфиденциальность для канала не требуется, но нужна аутентификация и обеспечение целостности данных.

Защищенный оконечный распознаватель который доверяет как рекурсивному серверу, так и коммуникационному каналу, может проверить бит AD в заголовке полученного отклика. Оконечный распознаватель может использовать этот флаг в качестве рекомендации по определению возможности рекурсивного сервера проверять подписи для всех данных в разделах отклика Answer и Authority.

Если защищенный оконечный распознаватель по какой-либо причине не может организовать доверительные отношения с рекурсивными серверами имен, он может самостоятельно проверить подписи, устанавливая при этом бит CD в своих запросах. Проверяющий достоверность оконечный распознаватель способен трактовать подписи DNSSEC как доверительные отношения между администратором зоны и собой.

8. Зоны

Существуют некоторые различия между подписанными и неподписанными зонами. Подписанная зона будет содержать дополнительные записи, связанные с защитой (RRSIG, DNSKEY, DS, NSEC). Записи RRSIG и NSEC могут генерироваться подписывающим процессом до обслуживания зоны. Записи RRSIG, сопровождающие данные зоны, имеют время начала и завершения действия, определяющие период достоверности подписей и данных зоны.

8.1. Значения TTL и срок действия RRSIG

Важно отметить различия между временем жизни RRset TTL и периодом достоверности, заданным записью RRSIG RR для этого набора RRset. DNSSEC не изменяет определение и функции значений TTL, которые предназначены для поддержки когерентности кэшированных баз данных. Кэширующий распознаватель удаляет наборы RRset из своего кэша не позже, чем истечет время, заданное значением поля TTL данного набора RRset, независимо от того, понимает ли распознаватель защитные расширения.

Поля начала и завершения срока действия в RRSIG RR ([RFC4034]), с другой стороны, задают временной интервал, в течение которого подписи могут применяться для проверки соответствующего набора RRset. Сигнатуры, связанные с подписанными данными зоны, достоверны лишь в течение периода, заданного полями записи RRSIG RR. Значения TTL не могут расширять период достоверности подписанных наборов RRset в кэше распознавателя, но распознаватель может использовать время, остающееся до истечения срока действия сигнатуры подписанного набора RRset, в качестве верхней границы для значения TTL подписанного набора RRset и связанной с ним записи RRSIG RR в кэше распознавателя.

8.2. Новые временные зависимости для зон

Информация в подписанной зоне имеет зависимость от времени, которой не существовало в исходном протоколе DNS. Подписанная зона требует регулярного обслуживания для обеспечения достоверности текущего значения RRSIG RR для каждого набора в зоне. Период достоверности подписи RRSIG RR представляет собой интервал, в течение которого сигнатура для одного подписанного набора RRset может считаться корректной. Срок действия подписей разных наборов RRset в зоне может различаться. При подписывании заново одного или нескольких наборов RRset в зоне будут изменяться соответствующие записи RRSIG RR, что, в свою очередь, потребует увеличения порядкового номера в записи SOA, которое показывает, что в зоне произошли изменения, и создания новой подписи для самого набора SOA RRset. Таким образом, создание новой подписи для любого набора RRset в зоне может также инициировать сообщение DNS NOTIFY и операции по переносу зоны.

9. Серверы имен

Защищенным серверам имен следует включать соответствующие записи DNSSEC (RRSIG, DNSKEY, DS и NSEC) во все отклики на запросы от распознавателей, которые указали свое желание получать такие записи путем установки бита DO в заголовке EDNS, с учетом ограничений на размер сообщений. Поскольку включение записей DNSSEC RR может привести к усечению сообщений UDP и переходу на использование протокола TCP, защищенные серверы имен должны также поддерживать механизм EDNS "sender's UDP payload".

По возможности закрытую часть каждой пары ключей DNSSEC следует держать в недоступном месте, но такой подход невозможен для зон, в которых разрешена функция динамического обновления DNS. В случае динамического обновления, первичный ведущий сервер для зоны будет заново подписывать зону при ее обновлении, поэтому серверу нужен доступ к закрытому ключу для подписывания зоны. Это пример ситуации, когда может быть полезна возможность разделения DNSKEY RRset для зоны на подписывающие ключи и ключи для подписывания ключей - в этом случае можно сохранять ключи в недоступном месте, имея время жизни, превышающее срок жизни ключей для подписывания зоны.

Расширений DNSSEC, как таковых, еще недостаточно для обеспечения целостности всей зоны при операциях переноса, поскольку даже подписанная зона содержит некоторые не подписанные и не полномочнные (nonauthoritative) данные, если эта зона имеет какие-либо дочерние зоны. Следовательно, операции по поддержке зоны будут требовать дополнительных механизмов (обычно это средства защиты каналов типа TSIG, SIG(0) или IPsec).

10. Серия документов DNS Security

Набор документов DNSSEC можно разделить на несколько основных групп, находящихся под большим зонтом документов, определяющих протокол DNS.

Словами "Набор документов DNSSEC" обозначаются три документа, описывающих расширение DNS security:

1. DNS Security Introduction and Requirements (данный документ)
2. Resource Records for DNS Security Extensions [RFC4034]
3. Protocol Modifications for the DNS Security Extensions [RFC4035]

К этой категории будут относится также все документы, дополняющие или изменяющие любой из входящих в данную категорию документов. Сюда могут быть отнесены будущие работы по обмену данными между защищенными конечными распознавателями и расположенными выше в иерархии защищенными рекурсивными серверами имен.

Словами "Спецификация алгоритма цифровой подписи" обозначается группа документов, описывающих работу конкретных алгоритмов цифровой подписи, которые следует реализовать для заполнения формата записей о ресурсах DNSSEC. Каждый документ этой группы связан с определенным алгоритмом создания цифровой подписи. Список таких алгоритмов на момент создания настоящей спецификации приведен в приложении "DNSSEC Algorithm and Digest Types" документа [RFC4034].

Словами "Протокол аутентификации транзакций" обозначается группа документов, описывающих аутентификацию сообщений DNS, включая создание и верификацию секретных ключей. Не будучи существенной частью спецификации DNSSEC, эта группа, тем не менее, указана в списке, благодаря ее тесной связи с DNSSEC.

И, наконец, словами "Новые защищенные приложения" будут обозначаться документы, в которых рассматривается использование предложенного расширения DNS Security для иных приложений, связанных с безопасностью. DNSSEC не обеспечивает прямых механизмов защиты для таких новых приложений, но может использоваться для их поддержки. К этой категории относятся документы, описывающие использование DNS в системах хранения и распространения сертификатов ([RFC2538]).

11. Согласование с IANA

Этот обзорный документ не требует согласования с IANA. Полный обзор требующих согласования с IANA вопросов, связанных с DNSSEC, приведен в [RFC4034].

12. Вопросы безопасности

Этот документ включает защитные расширения DNS и описывает набор документов, содержащий новые защитные записи и изменения протокола DNS. Расширения обеспечивают аутентификацию источника данных и их целостность за счет применения цифровых подписей для наборов записей о ресурсах. В этом параграфе рассматриваются присущие расширениям ограничения.

Для того, чтобы защищенный распознаватель мог проверить отклик DNS, все зоны на пути от доверенной стартовой точки до зоны, содержащей зону из отклика, должны быть подписаны, а все серверы имен и распознаватели, вовлеченные в процесс преобразования, должны быть защищенными, как описано в данном наборе документов. Защищенный распознаватель не может проверить отклики, происходящие из не подписанной зоны, из зоны, не обслуживаемой защищенным сервером имен, или в тех случаях, когда данные DNS распознаватель может получить лишь через рекурсивный сервер имен, который не является защищенным. При наличии разрыва в цепочке аутентификации защищенный распознаватель не может получить и проверить нужные ключи аутентификации, следовательно, он не способен проверить достоверность соответствующих данных DNS.

В этом документе кратко обсуждаются другие методы защиты запросов DNS (такие, как использование защищенных каналов IPsec или применение механизмов защиты транзакций DNS типа TSIG [RFC2845] или SIG(0) [RFC2931]), но защита транзакций не входит в задачи DNSSEC.

Не проверяющий достоверность защищенный оконечный распознаватель по определению не проверяет достоверность сигнатур DNSSEC и, вследствие этого, открыт для атак на (или со стороны) защищенные рекурсивные серверы имен, которые выполняют проверку от имени этого распознавателя, а также для атак на соединения распознавателя с такими рекурсивными серверами имен. Единственной известной защитой от первого типа атак является проверка сигнатур самим защищенным распознавателем. Но в этом случае распознаватель (по определению) перестанет быть не проверяющим подписи защищенным оконечным распознавателем.

DNSSEC не защищает от DoS-атак. DNSSEC делает протокол DNS уязвимым к новому классу атак на службы, основанных на использовании криптографических механизмов, против защищенных распознавателей и серверов имен - в таких атаках могут предприниматься попытки использования механизмов DNSSEC для потребления значительных ресурсов атакуемой системы. Этот класс атак принимает как минимум две формы. Атакующий может поглотить значительные ресурсы на проверку подписей в защищенном распознавателе путем подмены записей RRSIG RR в

откликах или путем создания чрезмерно сложных цепочек сигнатур. Атакующий может также потребить ресурсы защищенных серверов имен, поддерживающих динамические обновления, передавая им поток обновлений, заставляющих сервер заново подписывать некоторые наборы RRset с более высокой частотой, нежели это нужно при нормальной работе.

В результате обдуманного выбора разработчиков DNSSEC не обеспечивает защиты конфиденциальности.

DNSSEC позволяет недружественной стороне найти все имена в зоне, следуя по цепочке NSEC. Записи NSEC RR обеспечивают связь существующего в зоне имени со следующим существующим именем в каноническом порядке. Таким образом, атакующий может последовательно запросить записи NSEC RR для получения всех имен в зоне. Хотя это не будет атакой на DNS, атакующий получает возможность узнать имена хостов и других ресурсов, имеющихся в зоне.

DNSSEC значительно усложняет DNS и, следовательно, добавляет новые возможности внесения ошибок в реализации протокола и конфигурацию зон. В частности, включение проверки достоверности подписей DNSSEC на распознавателях может привести к тому, что некоторые легитимные зоны целиком станут нечитаемыми в результате конфигурационных ошибок DNSSEC или ошибок в реализации DNSSEC.

DNSSEC не защищает от подмены данных неподписанных зон. Неуполномоченные данные на срезах зон (склеивающие записи и NS RR в родительской зоне) не подписываются. Это не создает проблем при проверке достоверности аутентификационной цепочки, но означает, что неуполномоченные данные сами по себе уязвимы для подмены при операциях переноса зон. Таким образом, хотя DNSSEC может обеспечить аутентификацию источника данных и целостность данных в RRset, такие функции не обеспечиваются для зон и требуется использовать другие механизмы (такие, как TSIG, SIG(0) IPsec) для защиты операций переноса зон.

Дополнительная информация по вопросам безопасности приведена в [RFC4034] и [RFC4035].

13. Благодарности

Этот документ был создан на основе идей и результатов работы членов группы DNS Extensions. Указать полный список всех, кто внес свой вклад за десятилетие разработки DNSSEC, не представляется возможным. Редакторы хотят поблагодарить и отметить вклад в подготовку документа таких людей, как Jaap Akkerhuis, Mark Andrews, Derek Atkins, Roy Badami, Alan Barrett, Dan Bernstein, David Blacka, Len Budney, Randy Bush, Francis Dupont, Donald Eastlake, Robert Elz, Miek Gieben, Michael Graff, Olafur Gudmundsson, Gilles Guette, Andreas Gustafsson, Jun-ichiro Itojun Hagino, Phillip Hallam-Baker, Bob Halley, Ted Hardie, Walter Howard, Greg Hudson, Christian Huitema, Johan Ihren, Stephen Jacob, Jelte Jansen, Simon Josefsson, Andris Kalnozols, Peter Koch, Olaf Kolkman, Mark Kosters, Suresh Krishnaswamy, Ben Laurie, David Lawrence, Ted Lemon, Ed Lewis, Ted Lindgreen, Josh Littlefield, Rip Loomis, Bill Manning, Russ Mundy, Thomas Narten, Mans Nilsson, Masataka Ohta, Mike Patton, Rob Payne, Jim Reid, Michael Richardson, Erik Rozendaal, Marcos Sanz, Pekka Savola, Jakob Schlyter, Mike StJohns, Paul Vixie, Sam Weiler, Brian Wellington и Suzanne Woolf.

Приведенный список, вне всяких сомнений, неполон и мы извиняемся перед всеми, кто оказался за его пределами.

14. Литература

14.1. Нормативные документы

[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.

[RFC2535] Eastlake 3rd, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[RFC2671] Vixie, P., "Extension Mechanisms for DNS (EDNS0)", RFC 2671, August 1999.

[RFC3225] Conrad, D., "Indicating Resolver Support of DNSSEC", RFC 3225, December 2001.

[RFC3226] Gudmundsson, O., "DNSSEC and IPv6 A6 aware server/resolver message size requirements", RFC 3226, December 2001.

[RFC3445] Massey, D. and S. Rose, "Limiting the Scope of the KEY Resource Record (RR)", RFC 3445, December 2002.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

14.2. Информационные документы

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

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, March 1998.

[RFC2538] Eastlake 3rd, D. and O. Gudmundsson, "Storing Certificates in the Domain Name System (DNS)", RFC 2538, March 1999.

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake 3rd, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[RFC2931] Eastlake 3rd, D., "DNS Request and Transaction Signatures (SIG(0)s)", RFC 2931, September 2000.

[RFC3007] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.

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

[RFC3090] Lewis, E., "DNS Security Extension Clarification on Zone Status", RFC 3090, March 2001.

[RFC3597] Gustafsson, A., "Handling of Unknown DNS Resource Record (RR) Types", RFC 3597, September 2003.

[RFC3655] Wellington, B. and O. Gudmundsson, "Redefinition of DNS Authenticated Data (AD) bit", RFC 3655, November 2003.

[RFC3658] Gudmundsson, O., "Delegation Signer (DS) Resource Record (RR)", RFC 3658, December 2003.

[RFC3755] Weiler, S., "Legacy Resolver Compatibility for Delegation Signer (DS)", RFC 3755, May 2004.

[RFC3757] Kolkman, O., Schlyter, J., and E. Lewis, "Domain Name System KEY (DNSKEY) Resource Record (RR) Secure Entry Point (SEP) Flag", RFC 3757, April 2004.

[RFC3833] Atkins, D. and R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, August 2004.

[RFC3845] Schlyter, J., "DNS Security (DNSSEC) NextSECure (NSEC) RDATA Format", RFC 3845, August 2004.

Адреса авторов

Roy Arends
Telematica Instituut
Brouwerijstraat 1
7523 XC Enschede
NL
EMail: roy.arends@telin.nl

Rob Austein
Internet Systems Consortium
950 Charter Street
Redwood City, CA 94063
USA
EMail: sra@isc.org

Matt Larson
VeriSign, Inc.
21345 Ridgetop Circle
Dulles, VA 20166-6503
USA
EMail: mlarson@verisign.com

Dan Massey
Colorado State University
Department of Computer Science
Fort Collins, CO 80523-1873
EMail: massey@cs.colostate.edu

Scott Rose
National Institute for Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899-8920
USA
EMail: scott.rose@nist.gov

Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru