Network Working Group
Request for Comments: 3118
Category: Standards Track

R. Droms, Editor
Cisco Systems
W. Arbaugh, Editor
University of Maryland
June 2001

Проверка подлинности сообщений DHCP

Authentication for DHCP Messages

Статус документа

Этот документ содержит проект стандартного протокола Internet для сообщества Internet и служит запросом к обсуждению в целях развития и совершенствования. Текущее состояние стандартизации и статус протокола можно узнать из документа «Internet Official Protocol Standards» (STD 1). Документ можно распространять без ограничений.

Авторские права

Тезисы

Этот документ определяет новую опцию протокола DHCP[1], с помощью которой можно легко генерировать маркеры полномочий и недавно подключенные хосты с нужными полномочиями могут быть настроены автоматически с помощью полномочного сервера DHCP. Протокол DHCP обеспечивает основу для передачи конфигурационной информации хостам сети TCP/IP. В некоторых ситуациях сетевые администратору могут захотеть ограничить выделение адресов лишь хостам, имеющим полномочия. Кроме того, некоторые администраторы могут захотеть аутентифицировать источник и содержимое сообщений DHCP.

1. Введение

Протокол DHCP [1] передает конфигурациоонные параметры стека протоколов от централизованно администрируемых серверов хостам TCP/IP. Среди этих параметров присутствуют адреса IP. Сервер DHCP можно настроить на динамическое выделение адресов из пула, что позволяет избавиться от этапа ручной настройки хостов TCP/IP.

Некоторые сетевые администраторы могут захотеть проверки подлинности источника и содержимого сообщений DHCP. Например, клиенты могут быть подвержены DoS[2]-атакам с использованием обманных серверов DHCP или могут быть некорректно настроены в результате непреднамеренного запуска сервера DHCP. Сетевые администраторы могут пожелать ограничить выделение адресов, предоставляя их лишь уполномоченным хостам, для предотвращения DoS-атак во «враждебных» средах, где физическая среда не имеет достаточной защиты, таких как беспроводные сети или студенческие общежития.

В этом документе определен метод, который может обеспечить проверку подлинности объектов и сообщений. Текущий протокол объединяет исходный механизм аутентификации Schiller-Huitema-Droms с отложенной аутентификацией, предложенной Bill Arbaugh.

1.1 Модель угроз DHCP

Угрозы DHCP по своей сути являются внутренними (предполагается корректно настроенная сеть, где порты BOOTP блокируются на периметре корпоративной сети). Однако независимо от настройки шлюзов возможные атаки извне и изнутри одинаковы.

Специфичной для клиентов DHCP атакой является организация «мошеннического» сервера с целью предоставить клиентам некорректную конфигурацию. Мотивом этого может служить организация MITM[3]- или DoS-атаки.

Существует и другая угроза для клиентов DHCP от ошибочно настроенных или случайно запущенных серверов DHCP, которые отвечают на запросы клиентов, сообщая им (непреднамеренно) неверные параметры конфигурации.

Специфичной для серверов DHCP угрозой является маскировка «подставных» клиентов под лигитимных. Мотивом этого может быть «кража услуг» или обход аудита с той или иной неблаговидной целью.

Общей для клиентов и серверов угрозой является DoS-атака на ресурсы. Такие атаки обычно ведут к истощению адресов, а также ресурсов CPU или пропускной способности сети и возможны при наличии любого общего ресурса. В современной практике для смягчения таких атак лучше всего подходит избыточность ресурсов (резервирование).

1.2 Цели разработки

Ниже перечислены в порядке важности цели, которые послужили разработке протокола аутентификации.

1. Устранение угроз, отмеченных в параграфе 1.1.
2. Сохранение в неизменном виде текущего протокола.
3. Ограничение числа состояний, требуемых от сервера.

[1]Dynamic Host Configuration Protocol - протокол динамической настройки конфигурации хоста.
[2]Denial of service - отказ в обслуживании.
[3]Man in the middle - перехват и изменение пакетов с участием человека.

4. Ограничение сложности, которая порождает ошибки при разработке и реализации.

1.3 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 [5].

1.4 Терминология DHCP

DHCP client - клиент DHCP

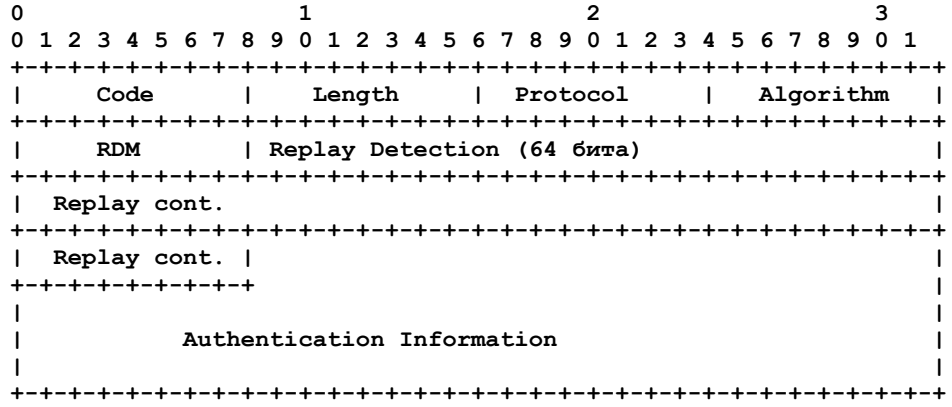
Клиентом DHCP или просто клиентом называется хост Internet, использующий DHCP для получения конфигурационных параметров, таких как сетевой адрес.

DHCP server - сервер DHCP

Сервером DHCP или просто сервером называется хост Internet, возвращающий параметры конфигурации по запросам клиентов DHCP.

2. Формат аутентификационной опции

На рисунке показан формат опции DHCP для проверки подлинности.



Опция имеет код 90, а поле размера учитывает поля Protocol, RDM, Algorithm, Replay Detection и Authentication Information.

Поле Protocol определяет конкретный метод проверки подлинности, используемый опцией. Определение новых протоколов описано в разделе 6.

Поле Algorithm указывает конкретный алгоритм, используемый методом, указанным в поле Protocol.

Поле Replay Detection относится к RDM, а поле Authentication Information - к используемому протоколу.

Поле RDM[1] указывает тип детектирования повторного использования, используемого Replay Detection.

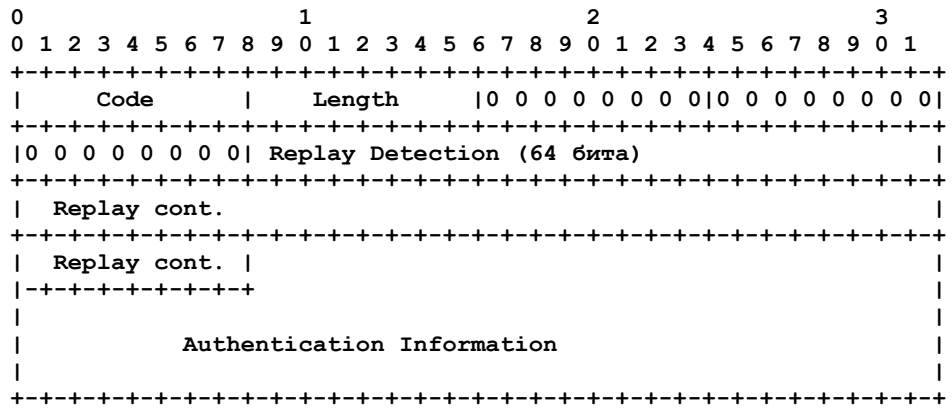
Если RDM = 0x00, поле Replay Detection **должно** содержать монотонно возрастающее значение счетчика. Применение таких счетчиков, как время суток (например, метка времени в формате NTP [4]) может снизить риск атак с воспроизведением. Этот метод **должен** поддерживаться всеми протоколами.

3. Взаимодействие с ретрансляторами

Поскольку ретранслятор DHCP может менять значения полей giaddr и hops в сообщении DHCP, для этих двух полей при расчете хэш-функции для заголовка сообщения **должно** приниматься значение 0. Кроме того, ретрансляторы DHCP могут добавлять свою информационную опцию 82 [7] в качестве последней опции сообщения серверу. Если сервер видит опцию 82 в принятом сообщении, он **должен** рассчитывать хэш-функцию без учета этой опции, не изменяя порядка других опций. Всякий раз, когда сервер возвращает ретранслятору опцию 82, он **должен** пропускать эту опцию при расчете хэш-функции для сообщения.

4. Маркер конфигурации

Если Protocol = 0, поле Authentication Information содержит простой конфигурационный маркер, показанный на рисунке.



[1]Replay Detection Method - метод обнаружения повторного использования.

Маркер конфигурации представляет собой неанализируемое (opaque), некодированное значение, известное отправителю и получателю. Отправитель помещает маркер конфигурации в сообщение DHCP, а получатель сравнивает полученный в сообщении маркер с известным ему общим маркером. При наличии конфигурационной опции и расхождении значений маркеров получатель **должен** отбросить сообщение.

Маркер конфигурации передается в открытом и обеспечивает лишь слабую аутентификацию объекта, а сообщение не аутентифицируется совсем. Этот протокол полезен лишь для элементарной защиты от непреднамеренно организованных серверов DHCP.

Обсуждение.

Намерение заключается в передаче постоянного, не вычисляемого маркера, такого как нешифрованный пароль. Другие типы аутентификации объектов с использованием рассчитываемых маркеров, таких как квитанции Kerberos или одноразовые пароли, будут определены в отдельных протоколах.

5. Отложенная аутентификация

Если Protocol = 1, сообщение использует механизм отложенной аутентификации. В этом случае клиент запрашивает проверку подлинности в своем сообщении DHCPDISCOVER, а сервер отвечает сообщением DHCPOFFER и данными аутентификации. Эти данные содержат одноразовое значение (nonce), создаваемое источником как код аутентификации сообщения (MAC[1]) для проверки подлинности сообщения и объекта.

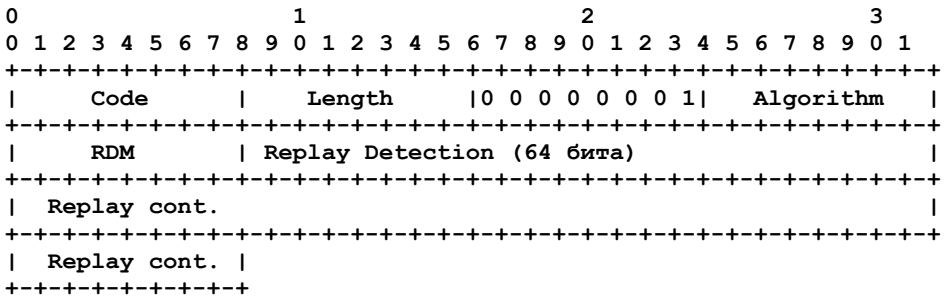
Этот документ задает использование конкретного метода на основе протокола HMAC [3] с хэш-функцией MD5 [2].

5.1 Вопросы управления

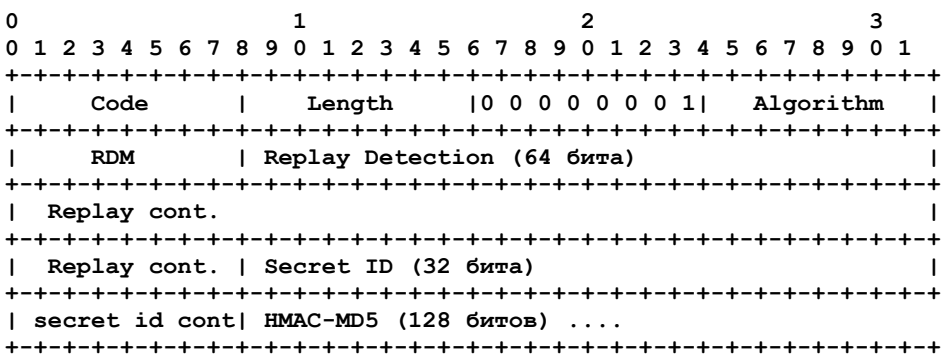
Протокол отложенной аутентификации не пытается обрабатывать ситуации, когда клиент может перемещаться из одного административного домена в другой (междоменный роуминг). Этот протокол ориентирован на решение проблемы внутри домена, где возможен обмен общим секретом по отдельному каналу (out-of-band).

5.2 Формат

Формат запроса аутентификации в сообщении DHCPDISCOVER или DHCPINFORM для отложенной аутентификации показан ниже.



Формат данных аутентификации в сообщении DHCPOFFER, DHCPREQUEST или DHCPACK для отложенной аутентификации показан ниже.



Ниже приведены определения, используемые при описании аутентификационных данных для отложенной аутентификации с алгоритмом 1.

Replay Detection
В соответствии с полем RDM.

K
Значение общего секрета для отправителя и получателя сообщения. Каждый секрет имеет уникальный идентификатор (secret ID).

secret ID
Уникальный идентификатор секретного значения, использованного при создании MAC для этого сообщения.

HMAC-MD5
Функция генерации кода MAC [3, 2].

Отправитель рассчитывает MAC используя алгоритм генерации HMAC [3] и хэш-функцию MD5 [2]. Все сообщение DHCP (исключения рассмотрены ниже), включая заголовок DHCP и поле опций служит входными данными функции расчета HMAC-MD5. Поле secret ID **должно** содержать идентификатор секрета, используемого для генерации MAC.

[1]Message authentication code.

Обсуждение.

Algorithm=1 задает использование HMAC-MD5. Другие методы (например, HMAC-SHA) будут описаны в отдельном протоколе.

Отложенная аутентификация требует общего секрета для каждого клиента и каждого сервера DHCP, с которым клиент может захотеть использовать протокол DHCP. Каждый секрет имеет уникальный идентификатор, который может использоваться получателем для выбора секрета, применяемого при генерации MAC в сообщении DHCP. Поэтому отложенная аутентификация слабо расширяема в архитектуре, где клиенты DHCP подключаются к множеству административных доменов.

5.3 Проверка сообщения

Для проверки входящего сообщения получатель сначала проверяет приемлемость значения поля Replay Detection в соответствии с методом детектирования, заданным полем RDM. Затем получатель рассчитывает MAC, как описано в [3]. При расчете MAC получатель **должен** установить 0 в поле MAC аутентификационной опции, а поскольку ретрансляторы DHCP могут менять значения полей giaddr и hops в сообщении DHCP, в этих полях при расчете также должны быть установлены нулевые значения. Если рассчитанное значение MAC отличается от принятого в аутентификационной опции, получатель **должен** отбросить сообщение DHCP.

В разделе 3 представлена дополнительная информация по части обработки сообщений с опцией 82 (ретрансляторы).

5.4 Использование ключа

Каждый клиент DHCP имеет ключ K, который применяется для кодирования всех сообщений, передаваемых серверу, а также для аутентификации и проверки всех полученных от сервера сообщений. Клиентские ключи **следует** передавать с использованием отдельного механизма (out-of-band), а хранить их **следует** локально у клиентов для использования со всеми аутентифицированными сообщениями DHCP. Когда клиент получает свой ключ, его **следует** применять для всех транзакций, даже при изменении конфигурации клиента (например, смена сетевого адреса).

Каждый сервер DHCP **должен** знать или иметь возможность защищенно получить ключи всех уполномоченных клиентов. Если все клиенты применяют один ключ, они могут проверить подлинность объекта и сообщения для всех получаемых от серверов сообщений. Однако применение общего ключа настоятельно не рекомендуется, поскольку это позволяет неуполномоченным клиентам представиться уполномоченными, просто получив копию общего ключа. Для проверки подлинности отождествления отдельных клиентов каждому клиенту **должен** настраиваться уникальный ключ. Метод управления ключами рассмотрен в приложении A.

5.5 Поведение клиентов

В этом параграфе рассматривается поведение клиента DHCP, использующего отложенную аутентификацию.

5.5.1 Состояние INIT

В состоянии INIT клиент использует отложенную аутентификацию в соответствии с приведенным ниже описанием.

1. Клиент **должен** включить опцию запроса аутентификации в свое сообщение DHCPDISCOVER вместе с опцией идентификации клиента [6] для однозначного представления себя серверу.

2. Клиент **должен** выполнять проверочные тесты (параграф 5.3) для любых сообщений DHCPOFFER, включающих данные аутентификации. Если одно или несколько сообщений DHCPOFFER проходит проверку, клиент выбирает одну из предложенных конфигураций.

   Поведение клиента при отсутствии сообщений DHCPOFFER с данными аутентификации или отрицательном результате проверки всех сообщений определяется локальной политикой клиента. В соответствии с этой политикой клиент **может** принять решение об ответе на сообщение DHCPOFFER, которое не аутентифицировано.

   Установку локальной политики с возможность восприятия не аутентифицированных сообщений следует выбирать с осторожностью. Восприятие сообщения DHCPOFFER без проверки подлинности может сделать клиента уязвимым к подмене серверов и другим атакам. Если локальные пользователи явно не уведомлены о том, что клиент воспринял неаутентифицированное сообщение DHCPOFFER, они могут ошибочно считать, что клиент получил аутентифицированный адрес и не подвержен атакам DHCP с неаутентифицированными сообщениями.

   На клиенте **должна** быть возможность настройки на отклонение неаутентифицированных сообщений и по умолчанию такие сообщения **следует** отвергать. Клиент может выбрать разный подход для сообщений DHCPOFFER без данных аутентификации и сообщений DHCPOFFER, которые не прошли проверку подлинности. Например, клиент может воспринимать первые и отбрасывать вторые. Если клиент воспринимает сообщение без проверки подлинности, ему **следует** уведомить об этом всех локальных пользователей, а событие **следует** записать в системный журнал.

3. Клиент отвечает сообщением DHCPREQUEST, которое **должно** включать данные аутентификации, закодированные с применением того же секрета, который сервер использовал в выбранном сообщении DHCPOFFER.

4. Если клиент проверил подлинность воспринятого сообщения DHCPOFFER, он **должен** проверить сообщение DHCPACK от сервера. Клиент **должен** отбросить DHCPACK, если сообщение не прошло проверку и **может** записать это событие в системный журнал. Если сообщение DHCPACK не прошло проверку, клиент **должен** восстановить состояние INIT и вернуться к п. 1. Клиент **может** запомнить сервер, чье сообщение DHCPACK не прошло проверку и отбрасывать последующие сообщения от него.

   Если клиент воспринял сообщение DHCPOFFER, которое не включало данных аутентификации или не прошло проверку, он **может** воспринять неаутентифицированное сообщение DHCPACK от сервера.

5.5.2 Состояние INIT-REBOOT

В состоянии INIT-REBOOT клиент **должен** применять секрет, использованный в его сообщении DHCPREQUEST, чтобы получить свою текущую конфигурацию для создания аутентификационных данных, помещаемых в сообщение DHCPREQUEST. Клиент **может** выбрать восприятие неаутентифицированных сообщений DHCPACK/DHCPNAK, если не было получено аутентифицированных сообщений. Клиент **должен** обрабатывать прием (или отсутствие) сообщений DHCPACK/DHCPNAK в соответствии с параграфом 3.2 в [1].

5.5.3 Состояние RENEWING

В состоянии RENEWING клиент применяет секрет, который он использовал в исходном сообщении DHCPREQUEST, получить свою текущую конфигурацию для создания аутентификационных данных, помещаемых в сообщение DHCPREQUEST. Если клиент не получил сообщения DHCPACK или ни одно из таких сообщений не прошло проверку, клиент ведет себя как при отсутствии сообщений DHCPACK, описанном в параграфе 4.4.5 спецификации DHCP [1].

5.5.4 Состояние REBINDING

В состоянии REBINDING клиент применяет секрет, который он использовал в исходном сообщении DHCPREQUEST, получить свою текущую конфигурацию для создания аутентификационных данных, помещаемых в сообщение DHCPREQUEST. Если клиент не получил сообщения DHCPACK или ни одно из таких сообщений не прошло проверку, клиент ведет себя как при отсутствии сообщений DHCPACK, описанном в параграфе 4.4.5 спецификации DHCP [1].

5.5.5 Сообщение DHCPINFORM

Поскольку клиент уже имеет некую конфигурационную информацию, он может иметь с сервером общий секрет K. Поэтому клиенту **следует** использовать запрос аутентификации как в сообщении DHCPDISCOVER при наличии общего секрета. Клиент **должен** трактовать все полученные сообщения DHCPACK, как указано для сообщений DHCPOFFER в параграфе 5.5.1.

5.5.6 Сообщение DHCPRELEASE

Поскольку клиент уже находится в состоянии BOUND, у него имеется защищенная связь с сервером. Поэтому клиент **должен** включить данные аутентификации в сообщение DHCPRELEASE.

5.6 Поведение сервера

В этом параграфе описано поведениесервера при получении от клиента сообщений, использующих отложенную аутентификацию.

5.6.1 Общие вопросы

Каждый сервер поддерживает список секретов и их идентификаторов, которые он использует совместно с имеющимися и возможными клиентами. Эта информация должна поддерживаться так, чтобы сервер мог выполнить указанные ниже действия.

- Определить подходящий секрет и его идентификатор для использования с клиентом, с которым сервер раньше мог не взаимодействовать.
- Найти секрет и идентификатор, используемый клиентом, для которого раньше сервер предоставил конфигурационную информацию.

Каждый сервер **должен** сохранять счетчик для предшествующего аутентифицированного сообщения. Сервер **должен** отбрасывать любое входящее сообщение, которое не прошло проверку на повторное использование в соответствии с RDM, для предотвращения атак с воспроизведением сообщений.

Обсуждение.

Аутентифицированное сообщение DHCPREQUEST от клиента в состоянии INIT-REBOOT может быть проверено только сервером, использующим тот же секрет, который применялся в его сообщении DHCPOFFER. Другие серверы будут отбрасывать такие сообщения DHCPREQUEST. Поэтому только сервер, использующий секрет, выбранный клиентом, сможет определить, что предложенная им конфигурационная информация не была выбрана и предложенный адрес можно вернуть в пул доступных адресов на сервере. Серверы, которые не могут проверить сообщение DHCPREQUEST, в конечном итоге вернут предложенные адреса в свои пулы доступных адресов, как описано в параграфе 3.1 спецификации DHCP[1].

5.6.2 После приема сообщения DHCPDISCOVER

Сервер выбирает для клиента секрет и включает аутентификационные данные в сообщение DHCPOFFER как указано выше в параграфе 5. Сервер **должен** записать идентификатор выбранного для клиента секрета и впредь использовать его для проверки сообщений от клиента.

5.6.3 После приема сообщения DHCPREQUEST

Сервер использует указанный в сообщении секрет и проверяет сообщение в соответствии с параграфом 5.3. Если проверка завершается отказом или сервер не знает секрета, указанного полем secret ID, он **должен** отбросить сообщение и **может** записать событие в системный журнал.

Если сообщение прошло процедуру проверки, сервер отвечает в соответствии со спецификацией DHCP. Сервер **должен** включить аутентификационную информацию, созданную в соответствии с параграфом 5.2.

5.6.4 После приема сообщения DHCPINFORM

Сервер **может** воспринимать неаутентифицированные или только аутентифицированные сообщения DHCPINFORM в соответствии со своей локальной политикой.

Если клиент включил запрос аутентификации в сообщение DHCPINFORM, сервер **должен** ответить аутентифицированным сообщением DHCPACK. Если у сервера нет общего секрета с отправителем DHCPINFORM, он **может** ответить неаутентифицированным сообщением DHCPACK или DHCPNAK, если не воспринимает неаутентифицированных клиентов в соответствии с политикой сайта, а **может** просто не ответить на сообщение DHCPINFORM.

6. Взаимодействие с IANA

В разделе 2 определена новая опция DHCP - Authentication Option с кодом 90.

Этот документ задает три новых пространства имен, связанных с Authentication Option, которые создаются и поддерживаются IANA - Protocol, Algorithm и RDM.

Начальными значениями для пространства имен Protocol служат 0 (конфигурационный маркер, раздел 4) и 1 (отложенная аутентификация, размел 5). Дополнительные значения Protocol будут выделяться по процедуре IETF Consensus в соответствии с RFC 2434 [8].

Пространство имен Algorithm связано с отдельными значениями Protocol. Т. е. каждый протокол имеет свое пространство имен алгоритмов. Рекомендации по выделению значений Algorithm для конкретного протокола следует включать в документ, определяющий новый протокол.

Для протокола конфигурационных маркеров поле Algorithm **должно** иметь значение 0. Для протокола отложенной аутентификации значение Algorithm = 1 выделено для функции генерации HMAC-MD5, как указано в разделе 5. Дополнительные значения в пространстве имен алгоритмов для Algorithm = 1 будут выделяться по процедуре IETF Consensus в соответствии с RFC 2434.

Начальное значение 0 из пространства имен RDM выделено для использования монотонно возрастающих значений, как указано в разделе 2. Дополнительные значения из пространства имен RDM будут выделяться по процедуре IETF Consensus в соответствии с RFC 2434.

7. Литература

[1] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[2] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[3] Krawczyk H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[4] Mills, D., "Network Time Protocol (Version 3)", RFC 1305, March 1992.

[5] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2219, March 1997.

[6] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[7] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

[8] Narten, T. and H. Alvestrand, "Guidelines for Writing and IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

8. Благодарности

Jeff Schiller и Christian Huitema разработали исходный вариант этого протокола проверки подлинности для терминального зала BOF на конференции IETF в Далласе в декабре 1995 г. Один из редакторов (Droms) расшифровал заметки с того обсуждения, которые послужили основой для этого документа. Редакторы высоко ценят терпение Jeff и Christian при рассмотрении этого документа и ранних черновиков.

Механизм отложенной аутентификации, используемый в разделе 5, принадлежит Bill Arbaugh. Модель угроз и требования параграфов 1.1 и 1.2 взяты из предложения Bill по протоколу согласования. Участники промежуточного совещания рабочей группы DHC в июне 1998 г., включая Peter Ford, Kim Kinnear, Glenn Waters, Rob Stevens, Bill Arbaugh, Baiju Patel, Carl Smith, Thomas Narten, Stewart Kwan, Munil Shah, Olafur Gudmundsson, Robert Watson, Ralph Droms, Mike Dooley, Greg Rabil и Arun Kapur разработали модель угроз и рассмотрели несколько дополнительных вариантов.

Метод защиты от воспроизведения принадлежит Vipul Gupta.

С благодарностью отмечается вклад Bill Sommerfield.

Спасибо также John Wilkins, Ran Atkinson, Shawn Mamros и Thomas Narten за рецензирование ранних версий документа.

9. Вопросы безопасности

В документе описаны механизмы аутентификации и проверки для протокола DHCP.

9.1 Уязвимости протокола

Механизм аутентификации с конфигурационным маркером уязвим для перехвата и обеспечивает лишь элементарную защиту от непреднамеренно созданных серверов DHCP.

Описанный в документе механизм отложенной аутентификации уязвим для DoS-атак с лавинной рассылкой сообщений DHCPDISCOVER, которые не аутентифицируются этим протоколом. Такие атаки могут полностью нарушить работу компьютера с сервером DHCP и могут исчерпать адреса, доступные для распределения сервером DHCP.

Отложенная аутентификация может также быть уязвима для DoS-атак с лавинной рассылкой аутентифицированных сообщений, которые могут перегружать компьютер с сервером DHCP расчетами ключей аутентификации для входящих сообщений.

9.2 Ограничения протокола

Отложенная аутентификация не поддерживает работу в разных доменах.

Реальный механизм цифровой подписи, такой как RSA, обеспечил бы нужную защиту, но в настоящее время невозможен по причине значительных объемов вычислений.

10. Адреса редакторов

Ralph Droms

Cisco Systems

300 Apollo Drive

Chelmsford, MA 01824

Phone: (978) 244-4733

EMail: rdroms@cisco.com

Bill Arbaugh

Department of Computer Science

University of Maryland

A.V. Williams Building

College Park, MD 20742

Phone: (301) 405-2774

EMail: waa@cs.umd.edu

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

Приложение A - метод управления ключами

Чтобы избавиться от централизованного управления списком случайных ключей, предположим, что K для каждого клиента создается из пары (идентификатор клиента [6], маска подсети - например, 192.168.1.0), которая должна быть уникальна для каждого клиента. Т. е. K = MAC(MK, unique-id), где MK - секретный первичный ключ, а MAC - необратимая хэш-функция с ключом, такая как HMAC-MD5.

Не зная MK, клиент без полномочий не сможет создать свой ключ K. Сервер может быстро проверить входящее сообщение от нового клиента путем регенерации K из идентификатора клиента. Для известных клиентов сервер может выбрать динамическое восстановление клиентского ключа K из client-id в сообщении DHCP или заранее рассчитать и кэшировать все K.

Благодаря выводу всех ключей из одного первичного ключа, серверу DHCP не нужен доступ к открытым паролям и он может рассчитать и проверить MAC с ключом без обращения к централизованному серверу аутентификации.

Для предотвращения рисков компрометации этой системы управления ключами первичный ключ MK **недопустимо** хранить у клиентов. Клиенту **следует** знать лишь свой ключ K. При компрометации MK **следует** выбрать новый ключ и предоставить индивидуальные ключи всем клиентам.

Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.