Network Working Group
Request for Comments: 4255
Category: Standards Track

J. Schlyter
OpenSSH
W. Griffin
SPARTA

January 2006

Использование DNS для защищенной публикации отпечатков ключей SSH

Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints

Тезисы

В этом документе описан метод верификации ключей хостов SSH (Secure Shell) с использованием DNSSEC[1]. Документ определяет новую запись DNS, которая содержит стандартный отпечаток ключа SSH.

Оглавление

1. Введение

Протокол SSH [6] обеспечивает защищенный вход в удаленные системы (remote login) и другие защищенные услуги в сетях без защиты. Защита соединений базируется на идентификации сервера для клиентов, а также идентификации пользователя на сервере.

Если соединение организуется с сервером, открытый ключ которого еще не известен клиенту, пользователю предоставляется отпечаток ключа (fingerprint) для его верификации. Если пользователь примет решение о корректности отпечатка и восприятии ключа, этот ключ сохраняется локально и будет использоваться для верификации последующих соединений. Хотя некоторые, озабоченные безопасностью пользователи проверяют отпечаток независимыми путями (out-of-band) до восприятия ключа, многие пользователи слепо доверяют представленному ключу.

Описанный здесь метод может обеспечить независимый канал верификации за счет поиска отпечатка открытого ключа сервера в DNS [1][2] и использования DNSSEC [5] для верификации такого поиска.

Для распространения отпечатков с использованием DNS в этом документе определяется новая запись DNS "SSHFP", позволяющая передавать отпечатки.

Предполагается, что читатель имеет базовые знания в области DNS [1][2] и защитных расширений DNS [5].

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с RFC 2119 [3].

[1]Domain Name System Security - защита системы доменных имен.

2. Верификация ключа хоста SSH

2.1. Метод

При соединении с сервером SSH клиент SSH **может** отыскать запись(и) SSHFP для хоста, к которому он подключается. Если алгоритм и отпечаток, полученные от сервера SSH, соответствуют алгоритму и отпечатку одной из записей SSHFP, полученных от DNS, клиент **может** воспринять идентификацию сервера.

2.2. Замечания по реализации

Реализациям клиентов **следует** обеспечивать настраиваемое правило, используемое для выбора порядка методов верификации ключей хостов. В этом документе определяется один из таких методов - хранение отпечатка ключа в DNS. Другой метод, определенный в архитектуре SSH [6], использует локальные файлы для хранения сравниваемых ключей. Иные методы, которые могут быть определены в будущем, могут включать хранение отпечатков в LDAP или других базах данных. Настраиваемые правила позволяют администратору определить, какие методы он желает использовать и задать порядок применения выбранных методов. Это позволит администраторам определить уровень доверия к различным методам.

Одним из сценариев с настраиваемой политикой относится к случаю, когда клиенты не используют полные имена хостов для обращения к серверам. В этом сценарии реализациям **следует** сравнивать ключ хоста с локальной базой данных до верификации ключа с использованием отпечатка, полученного от DNS. Это поможет предотвратить атаки, связанные со вставкой пути поиска в DNS в локальный преобразователь (resolver) для принудительного подключения клиента к другому хосту.

2.3. Соответствие отпечатков

Открытый ключ и запись SSHFP сравниваются путем сопоставления номера алгоритма и отпечатка ключа.

алгоритм открытого ключа и алгоритм в записи SSHFP **должны** совпадать;
цифровая подпись открытого ключа с использованием алгоритма, указанного в типе отпечатка SSHFP, **должна** совпадать с отпечатком в SSHFP.

2.4. Аутентификация

Открытому ключу, проверенному с использованием этого метода, **недопустимо** доверять, если запись SSHFP RR[1] не была аутентифицирована с помощью доверенной записи SIG RR.

Клиентам, самостоятельно выполняющим валидацию подписей DNSSEC, **следует** использовать стандартные процедуры валидации DNSSEC.

Клиенты, которые не выполняют самостоятельно валидацию подписей DNSSEC, **должны** использовать защищенный транспорт (например, TSIG [9], SIG(0) [10] или IPsec [8]) до элемента, выполняющего валидацию подписей.

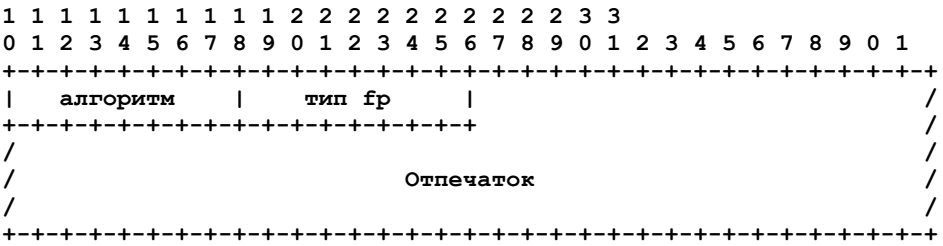
3. Запись SSHFP

Запись SSHFP RR используется для хранения отпечатка открытого ключа хоста SSH, связанного с именем DNS[2].

Код типа RR для записи SSHFP RR имеет значение 44.

3.1. Формат SSHFP RDATA

Поле RDATA записи SSHFP RR включает номер алгоритма, тип отпечатка и сам отпечаток (fingerprint) открытого ключа хоста.



3.1.1. Спецификация номера алгоритма

Октет номера алгоритма указывает алгоритм открытого ключа. Выделенные значения номеров алгоритмов показаны в таблице.

Значение	Имя алгоритма
0	резерв
1	RSA
2	DSS

Резервирование других значений требует согласования с IETF [4].

3.1.2. Спецификация типа отпечатка

Октет типа отпечатка указывает алгоритм цифровой подписи, используемый для получения отпечатка открытого ключа. Выделенные значения приведены в таблице.

[1]Resource record - запись о ресурсе.
[2]Domain Name System - система доменных имен.

Значение	Тип отпечатка
0	резерв
1	SHA-1

Резервирование других значений требует согласования с IETF [4].

Из соображений интероперабельности следует минимизировать число используемых типов отпечатков. Единственной причиной выделения новых типов может служить повышение уровня безопасности.

3.1.3. Отпечаток

Отпечаток рассчитывается для открытого ключа (blob), как описано в [7].

Предполагается, что алгоритм создания цифровой подписи дает на выходе строку октетов, которая без дополнительной обработки помещается в поле RDATA fingerprint.

3.2. Формат представления SSHFP RR

Поле RDATA в формате представления SSHFP состоит из двух целых чисел (номер алгоритма и тип отпечатка), за которыми следует сам отпечаток, представленный в шестнадцатеричном формате:

```
host.example.  SSHFP 2 1 123456789abcdef67890123456789abcdef67890
```

Использование вместо номеров мнемонических имен не допускается.

4. Вопросы безопасности

В настоящее время уровень доверия пользователей к серверным ключам пропорционален усилиям по проверке соответствия представленного открытого ключа секретному ключу сервера. Если пользователь воспринимает ключ без верификации отпечатка с помощью средств, использующих защищенный канал, соединение становится уязвимым для MITM-атак[1].

Общий уровень безопасности при использовании SSHFP для ключа хоста SSH зависит от правил безопасности, заданных администратором хоста SSH и администратором зоны DNS (в части передачи отпечатков), деталей процесса верификации в реализации SSH и уровня защиты доступа клиента к DNS.

Одним из аспектов безопасности является порядок просмотра отпечатков (например, сначала просматривается локальный файл, а потом SSHFP). Отметим, что в дополнение к защите изначального переноса ключей хоста SSHFP опционально может применяться для более сильной защиты ключа хоста.

Если сначала проверяется SSHFP, новые ключи хостов SSH могут быть распространены путем замены соответствующих записей SSHFP в DNS.
Если верификация ключей хостов SSH может быть настроена так, чтобы требовалось использование SSHFP, отзыв ключа хоста SSH может быть реализован путем удаления соответствующей записи SSHFP из DNS.

Как было отмечено в параграфе 2.2, разработчикам SSH рекомендуется обеспечивать механизм правил для управления порядком использования методов верификации ключей хостов. Одним из сценариев, требующих таких правил, является случай использования неполных имен хостов для подключения к серверам. В этом случае разработчикам SSH рекомендуется сначала сравнивать ключ хоста с локальной базой данных и только после этого проверять по отпечатку, полученному от DNS. Это поможет предотвратить атаки со вставкой пути поиска в DNS в локальный преобразователь для того, чтобы вынудить клиента подключаться к другому хосту.

Другим вариантом решения вопроса с подменой пути поиска в DNS является использование клиентами доверенного пути поиска в DNS, который получен не от DHCP или иных механизмов автоматической настройки. Поскольку в современных API для поиска в DNS нет способа проверки доверенности пути поиска, всю клиентскую систему потребуется настроить на использование доверенного пути поиска в DNS.

Другая зависимость связана с реализациями DNSSEC. Как отмечено в параграфе 2.4, требуется использовать защищенные методы поиска, а записи SSHFP RR должны подтверждаться доверенными записями SIG RR. Это особенно важно в тех случаях, когда SSHFP используется в качестве основы для возобновления и/или отзыва ключей хостов, как описано выше.

Поскольку DNSSEC лишь защищает целостность отпечатка после того, как он был подписан администратором зоны DNS, требуется обеспечить защищенную передачу отпечатков от администратора хоста SSH к администратору зоны DNS. Это можно сделать вручную или автоматически с использованием защищенного динамического обновления DNS [11] между сервером SSH и сервером имен. Отметим, что это не отличается от других ситуаций с обновлением ключей (например, клиенты отправляют запросы сертификатов уполномоченным агентствам для подписания).

5. Согласование с IANA

Агентство IANA выделило код типа RR со значением 44 для записей SSHFP из стандартного пространства типов RR.

Агентство IANA создало новый реестр для алгоритмов открытых ключей в записях типа SSHFP RR, включающий три элемента:

0 - резерв

1 - RSA

2 - DSA

Добавление новых значений требует согласования с IETF [4].

Агентство IANA создало новый реестр типа отпечатков для записей SSHFP RR, включающий два элемента:

[1]Man-in-the-middle attack - атака с перехватом трафика на пути и участием человека в точке перехвата.

0 - резерв

1 - SHA-1

Добавление новых значений требует согласования с IETF [4].

6. Нормативные документы

[1] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[2] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

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

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

[5] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

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

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

[6] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006.

[7] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, January 2006.

7. Дополнительная литература

[8] Thayer, R., Doraswamy, N., and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.

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

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

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

8. Благодарности

Авторы выражают свою благодарность:

Martin Fredriksson
Olafur Gudmundsson
Edward Lewis
Bill Sommerfeld

Адреса авторов

Jakob Schlyter

OpenSSH

812 23rd Avenue SE

Calgary, Alberta T2G 1N8

Canada

EMail: jakob@openssh.com

URI: http://www.openssh.com/

Wesley Griffin

SPARTA

7075 Samuel Morse Drive

Columbia, MD 21046

USA

EMail: wgriffin@sparta.com

URI: http://www.sparta.com/

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

Полное заявление авторских прав

Интеллектуальная собственность

Подтверждение

Финансирование функций RFC Editor обеспечено IETF Administrative Support Activity (IASA).