ISSN 2226-3780

УДК 681.3.06:519.248

Радивилова Т. А.,
Бушманов В. С.

АНАЛИЗ ОСНОВНЫХ АТАК НА DNS-СЕРВЕР И МЕТОДЫ ИСПОЛЬЗОВАНИЯ DNSSEC ПРИ ЗАЩИТЕ DNS-СЕРВЕРА

Проведен подробный анализ уязвимостей и атак, осуществляемых на DNS-сервер. Описан принцип работы DNSSEC и варианты его настройки и использования. Осуществлены, проанализированы и описаны атаки на DNS-сервер без использования DNSSEC и при его использовании. Проведены исследования защищенности DNS-сервера и влияние DNSSEC на уровень его защищенности. Проведено исследование влияния использования DNSSEC на нагрузку сети.

Ключевые слова: *DNS-сервер, DNSSEC, домен, шифрование, цифровая подпись, атаки, уязвимости.*

1. Введение

DNSSEC (DomainNameSystemSecurityExtensions) представляет собой группу спецификаций из InternetEngineeringTaskForce (IETF), которые обеспечивают проверку подлинности происхождения DNS (DomainNameSystem) данных, отрицание существования данных при проверке их подлинности и целостности (не обеспечивает доступность и конфиденциальность данных) [1].

Целью DNSSEC является защита DNS посредством использования цифровых подписей. DNSSEC по сути представляет собой собрание новых компонентов, добавленных во взаимодействие между клиентом и сервером DNS, которое поможет повысить безопасность основных протоколов DNS.

Корректное функционирование DNS является критически важным для сети предприятия, подсоединенной к Интернету, и для Интернета в целом. Действительно, если злоумышленнику удастся сделать так, чтобы атакуемый хост получил из DNS сфальсифицированную информацию, то хост будет отправлять данные на подложный IP-адрес (InternetProtocol). В лучшем случае результатом будет отказ в обслуживании, в худшем — злоумышленник получит возможность перехвата трафика со всеми вытекающими последствиями [1, 3].

Принцип работы DNSSEC можно сравнить с цифровой подписью. Используется два типа ключей, закрытым ключом данные подписываются, а открытым сверяются. Но главное отличие в том, что — одним подписывается зона (ZSK, zonesigningkey), другим подписывается набор ключей (KSK, keysigningkey). Сделано это из следующих соображений: зона может быть достаточно большой, чтобы удалось подобрать закрытый ключ ZSK, поэтому его необходимо чаще менять, и можно сделать его менее длинным, чтобы зоны подписывались быстрее; открытый ключ KSK используется для небольших объемов данных, поэтому его можно сделать длиннее и реже изменять. Тем более, что хэш от открытой части KSK требуется отправить в родительскую зону, что слишком часто делать не целесообразно [3—5].

Вся информация о защищенном домене в системе DNSSEC определенным образом зашифрована, поэтому может быть изменена только при помощи закрытого ключа шифрования. В процессе защищенного делегирования домена генерируется пара ключей. Информация о ключах хранится на первичном DNS-сервере. Закрытый ключ используется для подписи зоны после каждого изменения. Цифровая подпись закрытого ключа (DS-запись) передается администратору родительской зоны и подписывается его закрытым ключом. Таким образом, организуется цепочка доверия. Зная открытый ключ администратора родительской зоны, можно проверить «валидность» открытого ключа любой из дочерних зон [6—8].

Каждый узел в дереве DNS связан с некоторым открытым ключом. Каждое сообщение от DNS-серверов подписывается под соответствующим закрытым ключом. Эти ключи используются для генерации сертификатов или подписей, которые сохраняют идентификационные данные о каждом домене верхнего уровня на соответствующий открытый ключ.

Такие криптографические подписи обеспечивают целостность за счет вычисления криптографического хэша (т. е. уникальной контрольной суммы) данных и, затем, защиты вычисленной величины от несанкционированных изменений посредством ее шифрования. Хэш шифруется с помощью личного ключа из пары ключей, чтобы любой желающий мог воспользоваться открытым ключом для его дешифровки. Если дешифрованное получателем значение хэша совпадает с вычисленным, то данные достоверны (не подвергались несанкционированному изменению).

Цифровые подписи хранятся в зоне DNS в новых записях ресурсов RRSIG (подпись записи ресурса). Когда сопоставитель выдает запрос на имя, в ответе возвращаются одна или несколько RRSIG-записей. Для проверки подписи используется открытый криптографический ключ, который хранится в DNSKEY-записи ресурса. В ходе проверки DNS-сервер извлекает DNSKEY-запись.

KSK означает ключ подписи ключа (ключ долговременного пользования), а ZSK означает ключ подписи зоны (ключ кратковременного пользования).

В случае асимметричной криптографии или шифрования с открытым ключом, используемой в DNSSEC, атакующему необходимо определить, посредством прямого перебора или других методов, закрытую половину в паре открытый-закрытый ключ, используемой

для создания подписи, подтверждающей достоверность DNS-записи. Это позволит ему обойти защиту DNSSEC. DNSSEC предотвращает эти попытки взлома, используя ключ кратковременного пользования — ключ подписи зоны (ZSK) — для регулярного вычисления подписей DNS-записей и ключ долговременного пользования — ключ подписи ключа (KSK) — для вычисления подписи ZSK, дающей возможность проверки. Ключ ZSK часто изменяется, чтобы атакующему было тяжелее «угадать» его, в то время, как более длинный ключ KSK изменяется гораздо реже (лучше всего — раз в год). Так как ключ KSK подписывает ключ ZSK, который подписывает DNS-записи, для проверки DNS-записи в зоне необходимо знать только ключ KSK. Ключ KSK в форме записи DelegationSigner (DS) передается выше по дереву записей — родительской зоне. Родительская зона (например, корень) подписывает дочернюю запись DS (например, .org) своим ключом ZSK, который подписывается своим ключом KSK [3—9].

Это значит, что если DNSSEC полностью приняла ключ KSK для корневой зоны, то она становится частью цепочки проверки для каждого проверяемого доменного имени DNSSEC (или разрабатываемого приложения).

2. Уязвимости DNS

DNS-протокол может работать как поверх TCP (TransmissionControlProtocol), так и поверх UDP (UserDatagramProtocol), причем в 99 % случаев используется именно UDP — как более быстрый, менее ресурсоемкий, но, в тоже время, и менее защищенный. Чтобы послать подложный пакет, который будет воспринят жертвой как правильный, достаточно угадать (подобрать) идентификатор последовательности и номер порта-отправителя [3, 7, 10].

В простейшем случае злоумышленник может отправить подложный DNS-ответ с подложным IP-адресом некоторого узла, на который жертва пытается зайти. Сложность реализации атак подобного рода в том, что рабочие станции кэшируют DNS запросы. Более того, система не принимает DNS-ответов, которые не запрашивались. Хакер должен дождаться момента, когда жертва пошлет DNS-запрос, и сгенерировать подложный ответ прежде, чем это сделает настоящий DNS-сервер. На самом деле, обе проблемы имеют решение. DNS-кэш обычно невелик, а потому, послав жертве HTML-письмо с кучей картинок, лежащих на внешних серверах с разными доменными именами, хакер может вытеснить из кэша все старые записи. После чего, последняя ссылка в письме, ведущая на сервер обновлений, гарантированно пошлет обозначенный запрос в Сеть. Предшествующая ей ссылка на Web-сервер, подконтрольная хакеру, подскажет точное время, когда следует начинать генерацию подложных пакетов. Если хотя бы один из них будет воспринят как правильный, в DNS-кэш попадет «левый» адрес сервера с обновлениями, имеющий все шансы «дожить» до очередной сессии обновлений [2, 11].

Атаки на DNS можно условно разделить на два вида:

— Пассивные — атакующий получает необходимую информацию без заметного влияния на систему; система при этом продолжает функционировать как прежде.

— Активные — атакующий реализует некоторое воздействие на систему, в результате которого изменяется ее поведение. Такое изменение может быть и неопределимым для атакуемой системы, но криптоаналитик в состоянии определить и использовать эту информацию.

3. Реализация атак на DNS

Тестовая среда представляет собой два сервера с развернутой операционной системой WindowsServer 2008R2 и клиентским ПК на базе WindowsXP. Тестирование защиты DNS сервера проводится путем организации разного рода атак при стандартной защите DNS сервера и при дополнительно развернутой системе защиты DNSSEC.

3.1. Пример 1. Организация MITM-атак с помощью «dsniff». Служба DNS использует простые UDP-пакеты, обмен которыми происходит через порт 53. Так как UDP является протоколом, не ориентированным на установление соединений, то можно подменить информацию его пакетов.

В состав пакета «dsniff» (http://www.monkey.org/~dugsong/dsniff), входит средство под названием «dnsspoof» [6]. Эта программа содержит в себе простой анализатор пакетов, который отслеживает запросы DNS относительно информации записей «A» или «PTR». При использовании параметра -f, запушенная на компьютере хакера программа «dnsspoof» будет выполнять чтение локального файла, который записан в стандартном формате /etc/hosts, и будет отвечать на все перехваченные «A» или «PTR» DNS-запросы.

```
testb$ host www.victim.com
www.victim.com has address 192.168.1.25
c rackerbox# cat /ete/dnssnifff.hosts
crackerbox# dnssniff -f /etc/dnssniff.hosts
testb$ host www.victim.com
www.victim.com has address 192.168.1.3
```

Если параметр -f не указан, ответом на все «A» и «PTR» запросы DNS будет IP-адрес или имя хоста, на котором запущена «dnsspoof». Это приведет к тому, что все запросы на поиск IP-адресов будут проходить через хост нарушителя, т. е. можно выполнять перехват трафика, маршрутизацию или изменение данных, еще до того, как они попадут по действительному адресу назначения.

Суть атаки заключается в том, что если пакет от «dnsspoof» поступит раньше, чем пакет от реального DNS-сервера, то предпочтение получит первый, фальшивый пакет, а действительный ответ будет отброшен. Поэтому успех работы программы «dnsspoof» зависит от скорости передачи пакета запросившему узлу. Так как «dnsspoof» не нуждается в выполнении поиска действительной информации по запросу, то вероятнее всего, что ее пакет поступит первым.

3.2. Пример 2. DNShijacking. Данная атака также часто используется для изменения принципа работы систем DNS. В данном случае не вносится никаких изменений в кэш DNS клиента, но производятся изменения в настройках, после которых все запросы разрешения имен адресуются личному DNS-серверу взломщика. Обычно данная атака ставит своей целью не похищение данных, а сбор статистической информации с компьютера клиента. Все запросы разрешения имен, отправляемые

серверу взломщика, выполняются корректно, но при этом взломщик получает информацию о сайтах, посещаемых клиентом.

Пакет для проведения атаки «DNSHijacker» представляет собой сочетание sniffer& DNS spoofed [4].

Рассмотрим пример проведения атаки.

1. Злоумышленник запускает набор для проведения атаки «DNSHijacker».

./dnshijacker —i eth0 —v —f ftable

2. Злоумышленник прослушивает DNS запросы исходящие от жертвы к DNS серверу.

3. Жертва отправляет запрос DNS серверу на получение адреса www.xxxxx.com.

13:59:20.042628 192.168.1.2732839 > 192.168.1.60. domain: [udp sum ok] 24959+ A? www.xxxxx.com [|domain] (DF) (ttl 64, id 30800, len 61)

Запрос содержит в себе следующие части:

1. 192.168.1.27: адресWeb-сайта.
2. 192.168.1.60: IP адрес внутреннего DNS.
3. 24949:DNSID запроса отправленного жертвой на внутренний DNS.
4. (DF):Флаг.
5. Time to live64.
6. IPID 30800.
7. length61.

Внутренний DNS сервер пытается обработать ответ, не находя запроса в свой базе, он посылает запрос к вышестоящему DNS-серверу.

4. «Dnshijackertool» отправляет ответ с подмененной информацией об IP адресе DNS сервера и IP-адресе запрашиваемого ресурса, до того как внутренний DNS сервер получит ответ.

Результатом данной атаки является перенаправление жертвы на подделанный веб-ресурс.

3.3. Пример 3. Подмена DNS ID (DNS ID Spoofing). Заголовок пакета DNS-протокола содержит идентификационное поле для соответствия запросов и ответов. Целью подмены DNS ID является посылка своего ответа на DNS-запрос до того, как ответит настоящий DNS-сервер. ID — это единственный способ различить различные запросы DNS. Серверы DNS используют ID, чтобы определить каков был первоначальный запрос. Для выполнения этого, нужно спрогнозировать идентификатор запроса. Локально это реализуется простым прослушиванием сетевого трафика, но удаленно выполнить эту задачу можно путем проверки всех доступных значений идентификационного поля (общее количество возможных значений составляет 65535), или же посылкой нескольких сотен DNS-запросов в правильном порядке. Очевидно, что этот метод не очень надежен. Еще одной задачей для злоумышленника является то, что он должен иметь возможность прослушивать пакеты, идущие от произвольного DNS, для чего злоумышленник должен контролировать DNS-сервер, который является авторитетным для этой зоны.

Для этого типа атаки будет использован пакет «ADMIDtools, который обычно используется для тестирования уровня защиты DNS [5].

Утилита «ADMkill» прослушивает ответы, отправляемые DNS сервером, и отсылает неверные ответы с подделанным IP-адресом уполномоченного сервера имен.

Для проведения атаки, нужно угадать DNSID. Инструмент «dnshijackertool» может быть использован для прослушивания DNS трафика, после чего злоумышленник может оценить диапазон ID для запросов сервера имен [4]. Атакующий должен выполнить следующие действия:

1. Злоумышленник посылает DNS-запрос на разрешение имени www.test.com целевому серверу ns.dnstest.com.
2. Целевой DNS-сервер перенаправляет поученный запрос к серверу доменans.test.com.
3. Злоумышленник прослушивает запросы, получаемые ns.test.com и определяет ID.
4. Злоумышленник посылает DNS-запрос на разрешение имени www.victim.com серверу ns.dnstest.com. И сразу же шлет группу фальсифицированных DNS-ответов (передавая в качестве IP-адреса, один из адресов злоумышленника — 10.0.0.1) на свой же запрос с подмененным IP-адресом источника на адрес одного из DNS-серверов victim.com. В каждом ответе ID увеличивается на 1 по сравнению с идентификатором, полученным во время второго этапа атаки, для увеличения вероятности нахождения правильного номера ID. Сервер ns.dnstest.com мог ответить на запросы других клиентов и, соответственно, увеличить свой DNS ID. Для этого может быть использована утилита «ADMkill», которая будет отсылать серию подделанных ответов с IP-адресом с заданным диапазоном ID (т.е. мы отсылаем пакеты с ID от 27300 до 27330):

./ADMkillDNS 10.0.0.1 192.168.1.60 ns2.victim.com 27300 27330

В результате такой атаки по подложным IP-адресам будет ходить не отдельный клиент-жертва, а все пользователи будут обращаться к машине злоумышленника.

4. DNSSEC и нагрузка на сеть

Как уже упоминалось выше, в основе протокола DNSSEC лежит метод цифровой подписи ответов на запросы, в результате чего пакеты DNSSEC несут больше информации, что увеличивает нагрузку на память, процессор и полосу пропускания сервера. Внедрение DNSSEC увеличивает объем передаваемых данных, за счет использования цифровой подписи. Для того, чтобы это проверить, были прослушаны запросы отправляемые пользователями. Проанализировав их можно однозначно сделать вывод, что объем трафика увеличивается при развернутом DNSSEC почти на 20 %. Также следует знать, что если пакет превысит 512 байт, то могут возникнуть проблемы с его приемом. Конечно, у этой проблемы есть решение. Согласно протоколу DNS клиент должен сообщить об этом серверу, который, в свою очередь, постарается уместить ответ в установленные 512 байт. При этом часть информативных данных может быть обрезана. В случае, если даже необходимая информация не помещается, сервер сообщит об этом клиенту установкой бита «обрезания» (truncationbit). Однако, сжатие не безгранично, и если после него размер пакета все еще большой, то клиент автоматически

переключится из транспортного протокола UDP в TCP, в котором нет подобных ограничений [12]. Некоторые маршрутизаторы или устройства безопасности могут работать на правиле об ограничении пакета в 512 байт, что в свою очередь требует переконфигурации.

5. Выводы

В этой статье были исследованы и реализованы атаки на сервер имен, в результате чего было выяснено, что оригинальный DNS стандарт не заботится о безопасности. При проведении атак на сервер с развернутым DNSSEC методы, которые использовались при атаке на «чистый» DNS, оказались безуспешными. Причиной этого является то, что в основе протокола DNSSEC лежит метод цифровой подписи ответов на запросы. В ходе анализа проведенных атак, было выяснено, что DNSSEC может бороться с таким уязвимостями DNS как «отравление кэша» или «человек посередине». Это объясняется тем, что DNSSEC защищает DNS путем проверки подлинности и целостности системы DNS-сообщений. Атаки, ориентированые на DNS сообщения, невозможны при использовании DNSSEC, так как клиенты проверяют цифровую подпись предоставляемую в ответ. Расширения безопасности DNS SecurityExtensions защищают клиентов и сервера от атак, при которых модифицируется кэш DNS, путем подписывания записи с использованием шифрования с открытым ключом.

В ходе работы было выявлено, что внедрение DNSSEC увеличивает объем передаваемых данных, нагрузку на память, процессор и полосу пропускания сервера на 20 %, что не является критичным, с учетом уровня осуществляемой безопасности.

Литература

1. Мамаев, М. А. Технологии защиты информации в Интернете [Текст] / М. А. Мамаев, С. К. Петренко. — СПб.: Питер, 2002. — 243 с.
2. Карпов, Г. А. Атака на ДНС [Электронный ресурс] / Г. А. Карпов. — Режим доступа: \www/ URL: http://www.hackzone.ru/articles/dns-poison.html. — Загл. с экрана.
3. Arends, R. L. DNSSecurity Introduction and Requirement [Text] / R. L. Arends, R. U. Austein // RFC 4033. — 2005. — 47 p.
4. DNS ID Hacking — ADM Crew [Электронный ресурс] — Режим доступа: \www/ URL: http://packetstorm.securify.com/groups/ADM/ADM-DNS-SPOOF/ADMID.txt — Загл. с экрана.
5. Abley, J., Larson, M. DNSSEC for the Root Zone — Update [Text] / J. Abley, M. Larson // IETF 78, Maastricht, Нидерланды. — 2010. — 44 p.
6. Waterman, S. UPI Analysis: Owning the keys to the Internet. [Электронный ресурс] / S. Waterman. — Режим доступа: \www/ URL: http://www.mail-archive.com/osint@yahoogroups.com/msg39697.html — Загл. с экрана.
7. Kerner, S. M. ORG the Most Secure Domain? [Электронный ресурс] / S. M. Kerner. — Режим доступа: \www/ URL: http://www.internetnews.com/security/article.php/3774131/ORG+the+Most+Secure+Domain.htm — Загл. с экрана.
8. Singel, R. Feds Start Moving on Net Security Hole. [Text] / R. Singel. — Wired News (CondéNet). — 2006. — 76 p.
9. Eklund-Löwinder, Anne-Marie. Swedish ISP TCD Song Adopts DNSSEC. [Text] / Eklund-Löwinder, Anne-Marie // DNS-wg mailing list, RIPE NCC. — 2012. — 8 p.
10. Andrews, M., Weiler, S. The DNSSEC Lookaside Validation (DLV) DNS Resource Record. [Text] // M. Andrews, S. Weiler // RFC 4431. — 2006. — 22 p.
11. Metzger, Perry, Simpson, W. A. and Vixie, P. Improving TCP security with robust cookies. [Text] / P. Metzger, W. A. Simpson, P. Vixie // 26th Large Installation System Administration Conference (LISA'12), volume 34, № 6. — 2009. — pp. 86—97.

АНАЛІЗ ОСНОВНИХ АТАК НА DNS-СЕРВЕР І МЕТОДИ ВИКОРИСТАННЯ DNSSEC ПРИ ЗАХИСТІ DNS-СЕРВЕРА

Проведено грунтовний аналіз вразливостей і атак, які здійснюються на DNS-сервер. Описано принцип роботи DNSSEC і варіанти його налаштування і використання. Здійснені, проаналізовані та описані атаки на DNS-сервер без використання DNSSEC і при його використанні. Проведено дослідження захищеності DNS-сервера і вплив DNSSEC на рівень його захищеності. Проведено дослідження впливу використання DNSSEC на навантаження мережі.

Ключові слова: DNS-сервер, DNSSEC, домен, шифрування, цифровий підпис, атаки, уразливості.

***Радивилова Тамара Анатольевна**, кандидат технических наук, доцент, кафедра телекоммуникационных систем, Харьковский национальный университет радиоэлектроники,*
***e-mail: lmd@kture.kharkov.ua**.*
***Бушманов Виктор Сергеевич**, кафедра телекоммуникационных систем, Харьковский национальный университет радиоэлектроники, **e-mail: bu6manov@gmail.com**.*

***Радівілова Тамара Анатоліївна**, кандидат технічних наук, доцент, кафедра телекомунікаційних систем, Харківський національний університет радіоелектроніки.*
***Бушманов Віктор Сергійович**, кафедра телекомунікаційних систем, Харківський національний університет радіоелектроніки.*

***Radivilova Tamara**, Kharkiv National University of Radioelectronics,*
***e-mail: lmd@kture.kharkov.ua**.*
***Bushmanov Viktor**, Kharkiv National University of Radioelectronics,*
e-mail: bu6manov@gmail.com