УДК 623.618

А.В. Снегуров, В.Х. Чакрян

Харьковский национальный университет радиоэлектроники, Харьков

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТЕКА ПРОТОКОЛОВ IPv6

Проведен анализ уязвимостей протокола IPv6 и других протоколов, которые входят в его реализацию и необходимые для его корректной работы, к примеру: протоколы NDP, IMCPv6, DHCPv6 и т.п. Также в статье проведен анализ возможных векторов атак на семейство протоколов IPv6 и принципов их реализации, среди них: атак на уязвимости протокола NDP, CGA DoS атак, ICMPv6 DoS атак, DoS атак путем манипуляции полями пакета MTU либо Current Hop Limit, атак на протокол DHCPv6, атак скрытой передачи данных в полях пакета и др. В дополнение приведены программные средства реализации перечисленных атак.

Ключевые слова: *уязвимости протокола IPv6, атаки на семейство протоколов IPv6, ICMPv6, NDP, DHCPv6.*

Введение

Все крупные компании, которые занимаются производством сетевого оборудования уже давно говорят о сетях без границ. С необычайно быстрым ростом сети Интернет увеличилось и количество потребляемых IP адресов. IANA распределила последние пулы IPv4 адресов 3 февраля 2011 года [1]. Такие регистраторы как APNIC [2], RIPE [3] и ARIN [4], на данный момент, распределяют последний /8 блок IPv4 адресов, планируется, что остальные два регистратора, LACNIC и AFRINIC, также достигнут этого состояния в ближайшие годы. С 2006 года IPv6 протокол перешел в фазу активного внедрения после прохождения тестов и необходимых проверок [5, 6], которые проводила группа 6bone [7]. Сейчас мир находится в состоянии, когда IPv6 становится неотъемлемой частью сетевого окружения.

Несмотря на то, что основная функция протоколов IPv4 и IPv6 остается одинаковой, все же новый протокол претерпел значительных изменений, например:

- в IPv6 отсутствует такое понятие как широковещательная рассылка (англ. “broadcast”), которая заменена на групповую рассылку (англ. “multicast”);
- вместо протокола ARP используется ICMPv6;
- изменена структура заголовка пакета;
- добавлена возможность автоматической конфигурации IPv6-адреса;
- добавлены новые функции безопасности, такие как: Cryptographic Generated Address (CGA) и Secure ND (SEND), а также добавлена поддержка IPSec по умолчанию;
- изменение размера IP-адреса с 32 до 128 битов и многие другие.

С изменениями правил взаимодействия и добавлением нового функционала появились и новые уязвимости. Большой упор в IPv6 ставился на безопасность. Именно это стало причиной появления новых механизмов защиты от различных атак, которые можно было реализовать на сетевом уровне модели OSI. Стоит отметить, что подобные механизмы безопасности начали появляться на свет в виде RFC еще начиная с 2005 года, однако в протоколе IPv4 они не применялись и разрабатывались исключительно для протокола IPv6.

Целью данной статьи является анализ существующих уязвимостей стека протоколов IPv6 к информационным атакам, а также анализ таких атак и принципов их реализации.

Общие сведения функционирования стека протоколов IPv6

Последние годы протокол IPv6 стал постоянным объектом исследований хакеров и специалистов по информационной безопасности. Найдено множество уязвимостей, которые позволяют осуществить атаки перехвата данных и атаки отказа в обслуживании, причем, исключительно на протокол IPv6 в силу его функциональных особенностей.

Обнаружение слабых мест позволило разработать подходы к обеспечению безопасности протокола IPv6, о которых будет рассказано в следующей статье. Однако далеко не всегда пользователями используются предложенные методы безопасности. Кроме того, согласно отчету NIST [8, 9], многие аспекты IPv6 протокола еще не исследованы и требуют более тщательного анализа.

Атаки на протокол IPv6 возможно осуществить по нескольким причинам:

1. В сети Интернет стало намного проще найти необходимое для атаки программное обеспечение.
2. В сети появилось множество статей, в которых открыто описываются известные типы атак.
3. В сети можно найти множество видеороликов, в которых показано, как произвести процесс атаки.
4. IPv6 все чаще и чаще употребляется в реальной жизни, что привлекает внимание хакеров, которые исследуют безопасность протокола и находят уязвимости нулевого дня, о которых не осведомлены официальные органы.

Исходя из вышеизложенных пунктов можно утверждать, что атаки на протокол IPv6 осуществимы и представляют большой риск. Для того, чтобы детально разобрать процесс осуществления подобных атак, сперва следует рассмотреть принцип работы нескольких протоколов, которые стали неотъемлемой частью IPv6.

NDP протокол

Протокол обнаружения соседей (англ. “Network Discovery Protocol, NDP”) – используется в IPv6 для проверки IPv6 адреса на уникальность, автоматической настройки IPv6 адреса на конечных узлах, обнаружение адреса канального уровня соседних устройств, поиск доступных путей и DNS-серверов.

Существует 5 типов NDP сообщений:

1. Запрос на доступность маршрутизаторов (англ. “Router Solicitation”, RS).
2. Ответ маршрутизатора (англ. “Router Advertisement”, RA).
3. Запрос доступных соседей (англ. “Neighbor Solicitation”, NS).
4. Ответ соседа (англ. “Neighbor Advertisement”, NA).
5. Перенаправление (англ. “Redirect”).

Стоит отметить, что эти сообщения рассылаются в сети в открытом виде при помощи ICMPv6 протокола и могут быть свободно перехвачены злоумышленником.

Автоматическая настройка IPv6 адреса

В IPv6 существует такое понятие как SLAAC (англ. “Stateless address autoconfiguration”) - данный механизм позволяет конечному устройству автоматически получить все необходимые IPv6 настройки: префикс, длину префикса, адрес шлюза по умолчанию. Для этих целей NDP протокол.

SLAAC может работать в трех режимах:

1. Все настройки клиент получает от маршрутизатора (только SLAAC). Данный процесс изображен на рис. 1.
2. Часть настроек клиент получает от маршрутизатора, а часть от DHCPv6 сервера (SLAAC и DHCPv6). Данный процесс изображен на рис.2.
3. Все настройки клиент получает от DHCPv6 сервера (только DHCPv6).

На рис. 1 и 2 изображены первые два случая динамической получения настроек IPv6. Как видно в первом случае (рис. 1) клиент сперва обращается групповой рассылкой ко всем маршрутизаторам в сети с просьбой выдать настройки IPv6 (отправляет RS), и тот маршрутизатор, который ответит первым (англ. “Router Advertisement”, RA), того настройки клиент и применит.

Во втором случае (рис. 2) клиент проходит те же фазы, что и в первом случае. Однако в ответе от маршрутизатора он получает специальный флаг, который свидетельствует о том, что дополнительные настройки клиент может получить с DHCPv6 сервера. В третьем случае, клиент должен пройти те же фазы, что и в первом случае, только в ответе от маршрутизатора он получит специальный бит, который укажет на то, что клиент должен запросить настройки IPv6 у DHCPv6 сервера.

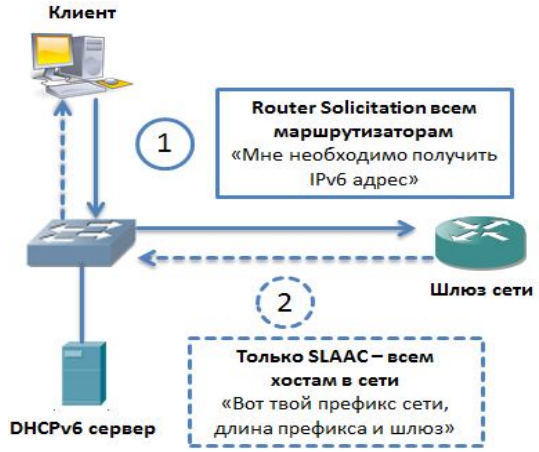

Рис. 1. Динамическая настройка IPv6 с применением настроек только от маршрутизатора сети

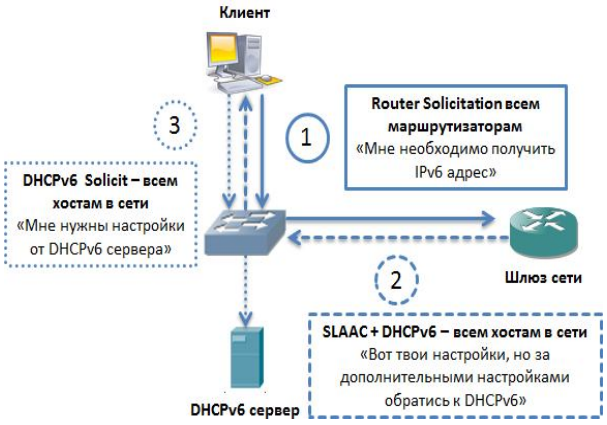

Рис. 2. Динамическая настройка IPv6 с применением части настроек от маршрутизатора и части настроек от DHCPv6 сервера

Специальные биты, которые оповещают клиента о том, откуда следует брать настройки IPv6 называются M/O:

- “O” бит – указывает на то, что дополнительные настройки следует получить у DHCPv6 сервера;
- “M” бит – указывает на то, что все настройки необходимо получить у DHCPv6 сервера.

Данные биты пользователь получает в первом ответном сообщении от маршрутизатора.

NDP как протокол общения с соседями

Выше приведен функционал протокола NDP, который относится к общению с маршрутизаторами Однако на этом функции данного протокола не заканчиваются.

В качестве протокола общения с соседями NDP может выполнять несколько функций, перечислим основные:

- Обнаружение дублирующего IPv6 адреса в сети.
- Обнаружение MAC адреса по IPv6 адресу (замена протокола ARP в IPv4 сетях).

Для того, чтобы избежать конфликтов в ситуациях, когда на двух различных устройствах установлен одинаковый IPv6 адрес, используется протокол DAD (англ. “Duplicate Address Detection”). Для того, чтобы проверить уникальность IPv6 адреса, клиент отправляет всем другим клиентам в сети NA запрос, объявляя в нем свой IPv6 адрес. Если ни один другой клиент не откликнулся NS ответом на этот запрос, это означает, что клиент может его использовать.

Другая важная функция NDP это обнаружение MAC адреса по IPv6 адресу. В локальной сети, где клиенты объединены коммутатором и не разделены устройствами L3-уровня, решения о передаче данных принимаются на основе MAC адресов. Однако, когда клиент только загрузился, MAC адресов удаленных соседей у него нет. Каждый раз, когда клиенту необходимо отправить информацию на IPv6 адрес, MAC адрес которого он не знает, запускается процесс NDP. В сеть отправляется специальный NS запрос, в котором указан IPv6 адрес устройства, MAC адрес которого клиент хочет узнать. В результате устройство отвечает NA ответов, котором указывает свой MAC адрес.

Атаки на стек протоколов IPv6 в пределах локальной сети

Перехват сообщений RA, RS, NA, NS позволяет злоумышленнику контролировать процесс установления новых настроек IP на конечном устройстве. Также уязвимости NDP могут быть использованы и для осуществления DoS атак, в том числе атак на процесс проверки дублирующегося адреса в сети.

Помимо широко распространенных атак на NDP протокол, IPv6 может быть атакован и с множества других сторон. Также механизмы безопасности, которые призваны снизить риски эксплуатации стека протоколов IPv6 открывают злоумышленнику новые возможности для атаки.

Следует отметить, что в данной статье рассматривают атаки, которые возможно реализовать в пределах локальной сети и, вследствие, не рассматривают атаки направленные на Mobile IPv6, множественную адресацию (англ. “Multihoming”) IPv6 и атаки связанные с туннелированием IPv6-IPv4 трафика.

Атаки на процесс обнаружения маршрутизатора

В IPv6 за обнаружение маршрутизатора в сети ответственен протокол ICMPv6. Поиск клиент производит путем отправки в сеть на адрес групповой рассылки маршрутизаторов RS пакета. Тот маршрутизатор, который первым ответил RA сообщением, будет выбран в качестве шлюза по умолчанию.

Злоумышленник, перехватив данный информационный обмен, может отправить поддельный RA ответ, указав в качестве шлюза по умолчанию себя. Таким образом, весь трафик, направленный во внешние сети будет проходить через устройство злоумышленника. Компьютер атакующего, в таком случае, будет выступать в качестве прокси-сервера.

Механизм осуществления данной атаки в простом варианте представлен на рис. 3. Данная атака может быть модифицирована, путем отправки на шаге 3 поддельного RA пакета, в котором указан настоящий MAC адрес маршрутизатора и время жизни записи равное нескольким часам.

Таким образом, клиент через назначенное время удалит запись из своей таблицы, а злоумышленник передаст уже поддельный RA пакет со своим MAC адресом. Подобная атака может быть проведена в случае, если на клиенте уже установлен корректный шлюз, либо для обхода некоторых механизмов безопасности.

Рис. 3. Механизм атаки на процесс обнаружения маршрутизатора в IPv6

Атака на SLAAC

Как было видно из рис. 1, для того, чтобы автоматически настроить IPv6 адрес, клиент сперва обращается к маршрутизаторам сети, отправляя RS сообщение на адрес групповой рассылки маршрутизаторов. Маршрутизатор либо выдает настройки, либо отправляет клиента за получением настроек к DHCPv6 серверу, отправляя ему ответ в RA сообщении.

Перехватив RS запрос клиента, злоумышленник может подменит RA ответ маршрутизатора и указать в ответе поддельные настройки. В качестве шлюза по умолчанию злоумышленник указывает свое устройство и весь трафик клиента, который передается во внешние сети, будет проходить через атакующего. Как и в прошлой атаке, устройство злоумышленника выступает в качестве прокси-сервера между клиентом и внешними сетями.

Атака на процесс обнаружения MAC адреса

Предположим, что клиент хочет передать информацию Клиенту 2 (рис. 4). Он знает IPv6 адрес, но не знает MAC адреса данного устройства. Клиент

отправляет в сеть NS запрос в надежде получить MAC адрес необходимого устройства.

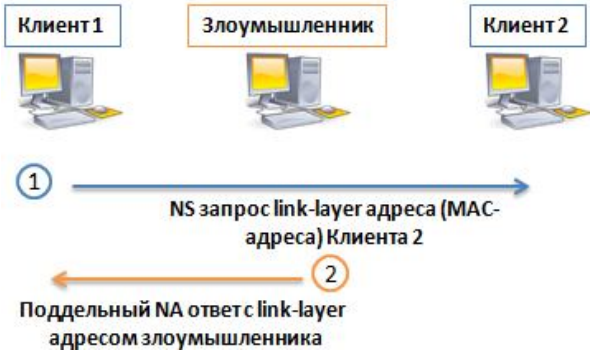

Рис. 4. Механизм атаки на процесс обнаружения MAC адреса в IPv6

Злоумышленник перехватывает данный запрос и отправляет поддельный ответ, указав в NA ответе MAC адрес собственного устройства (шаг 2 на рис. 4). Данный процесс называется подменой (англ. “spoofing”). В результате, вся информация, которая должна передаваться Клиенту 2, теперь будет передаваться на устройство злоумышленника.

Атака на процесс обнаружения дублирующегося IPv6 адреса

Предположим, что клиент с целью проверки собственного IPv6 адреса на уникальность отправляет в сеть NS запрос с указанием своего адреса. Если на запрос ни одно другое устройство не ответит – значит IPv6 адрес уникальный и его можно использовать. Злоумышленник перехватывает NS запрос клиента и отправляет поддельный NA ответ, в котором утверждает, что данный IPv6 адрес уже занят (шаг 2 на рис. 5). Клиент снова генерирует новый IPv6 адрес и снова проверяет его на уникальность. Злоумышленник снова повторяет свои действия. Данная атака приводит к отказу в обслуживании клиента, на которого она совершается, так как клиент никогда не сможет установить такой IPv6 адрес, который прошел бы проверку уникальности.

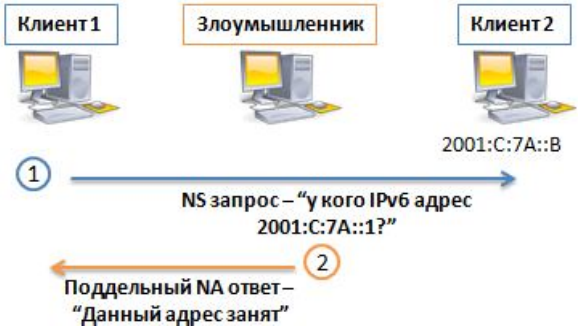

Рис. 5. Механизм атаки на процесс обнаружения дублирующегося IPv6 адреса

Атака на кеш соседа

Каждое устройство хранит у себя специальную таблицу, в которую записываются сопоставления MAC адреса с IP адресов. Новые ячейки в данной таблице появляются при каждом новом NDP запросе для установления MAC адреса удаленного устройства. В IPv4 сети ее называли ARP-таблицей, однако, так как в стеке протоколов IPv6 отсутствует ARP протокол, то данную таблицу принято называть просто кешем. Уязвимость состоит в том, что если записать в таблицу большое количество сопоставлений, то устройство не сможет сохранять новые сопоставления, либо и вовсе выйдет из строя.

В примере, приведенном на рис. 6, злоумышленник отправляет запросы в сеть с префиксом 2001:A:A::/64. Так как маршрутизатор (шлюз на рис. 6) имеет прямое подключение к этой сети, то для каждого нового запроса он формирует запись в кеше. В случае, если в сканируемой сети существует устройство, на которое направлен запрос злоумышленника, то маршрутизатор запишет сопоставление IPv6 и MAC адреса данного устройства. Если данное устройство в сети отсутствует, то запись в кеше все равно будет создана и просуществует несколько секунд.

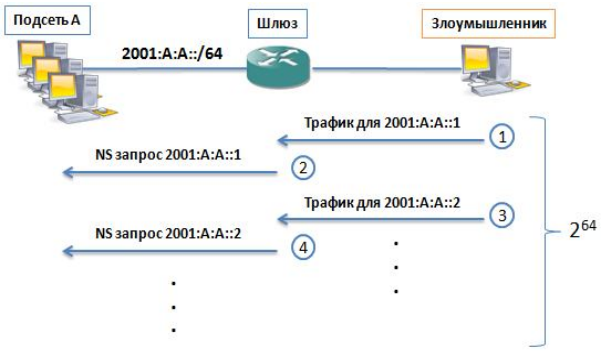

Рис. 6. Механизм осуществления атаки на кеш шлюза сети

Если устройство злоумышленника достаточно быстрое, то кеш маршрутизатора (шлюза на рис. 6) забьется, что приведет к отказу в обслуживании.

Осуществление DoS посредством ICMPv6 протокола

Классическая smurf атака - реализуется путем отправки злоумышленником multicast сообщения всем хостам в сети от адреса устройства-жертвы. Все устройства сети, получив multicast сообщение отправляют ответ. Устройство-жертва испытывает недостаток ресурсов, вследствие невозможности обработки такого большого количества откликов.

Распространение большого количества RA [9] и NA запросов. Удаленное устройство-жертва зависает, получая большое количество подобных запросов, к примеру, здесь представлен список операционных систем, которые подвержены атаке RA flood [10].

Осуществление DoS атаки при помощи CGA

Протокол CGA позволяет создать криптографический IPv6 адрес для подтверждения подлинно-

сти устройства источника. При получении CGA адреса получатель должен пройти процедуру его проверки, что может оказаться достаточно трудоемким процессом. Злоумышленник отправляет жертве пакеты с большого количества различных CGA адресов, что заставляет устройство жертвы многократно инициировать процесс проверки CGA адреса и истощает его ресурсы (рис. 7).

Рис. 7. Механизм осуществления DDoS атаки с использования некорректных CGA

Более подробно о CGA написано в разделе “Механизмы обеспечения информационной безопасности стека протоколов IPv6”.

DoS атака путем манипуляции параметром MTU

MTU (англ. “Maximum Transmission Unit”) – определяет какое количество байт может обработать каждый узел на пути от передающего до принимающего хоста. MTU выбирается наименьшим из возможных, чтобы каждый хост в пути мог обработать его не фрагментируя пакет на несколько частей.

В IPv6 сетях, если какой-то хост на выбранном для маршрутизации трафика пути, не может обработать MTU определенного размера, то он отправляет узлу-отправителю ICMPv6 Packet Too Big (Type 2) запрос, который содержит тот MTU, который он в силах обработать без фрагментации.

Атака осуществляется путем отправки узлу-отправителю MTU очень маленького размера, заставляя его передавать определенный объем информации крайне маленькими порциями, что приводит к лишнему потреблению ресурсов как на источнике так и на получателе. Чтобы передать поддельный MTU злоумышленнику необходимо каким-либо образом организовать атаку человека-по-середине, которая может быть осуществлена при использовании незащищенного NDP протокола.

Dos атака путем изменения Current Hop Limit

В IPv6 сети маршрутизатор может отправить хостам RA сообщение с выставленным значением в поле Current Hop Limit – это поле указывает какое значение хосты в локальной сети должны указывать в поле Hop Limit каждого IPv6-пакета.

В IPv6 пакете поле Hop Limit играет ту же роль, что и поле TTL в IPv4 пакете и указывает на то, сколько прыжков может совершить заданный пакет (сколько устройств L3 уровня может пройти пакет) до того как он будет отброшен. Каждое L3 устройство отнимает от данного поля 1 перед его отправкой. Когда поле Hop Limit становится равным нулю пакет отбрасывается.

Злоумышленник может указать очень маленький Current Hop Limit и это приведет к тому, что пакеты с маленьким Hop Limit будут отбрасываться быстрее, чем достигнут конечного узла-получателя. Для осуществления данной атаки злоумышленнику необходимо каким-либо образом организовать атаку человека-по-середине, которая может быть осуществлена при использовании незащищенного NDP протокола.

Внедрение поддельного DHCPv6 сервера

Внедрив поддельный DHCP сервер в сеть злоумышленник может перехватывать запрос от клиентов на выдачу настроек от DHCP сервера и отвечать заведомо ложным ответом. В этом процессе на компьютер жертвы внедряется не легитимный DNS сервер, вследствие этого злоумышленник может управлять тем, куда будет переходить пользователь при запросе легитимных сайтов и порталов.

К примеру, злоумышленник может создать фишинговый сайт-копию оригинального сайта крупного банка, изменить параметры на фальшивом DNS сервера таким образом, что при переходе на сайта банка клиент будет перенаправлен на поддельную копию сайта, где введет чувствительные данные: номер кредитной карты, логин и пароль и т.п.

Данная атака возможна в случае, если маршрутизатор выдает не полный набор настроек либо не выдает настройки вообще, перенаправляя клиента за дополнительной информацией на DHCPv6 сервер. Это происходит путем выставления соответствующих M либо O битов в единицу, как описано в пункте “Автоматическая настройка IPv6 адреса”.

Истощение адресов на DHCPv6 сервере

Суть атаки состоит в том, чтобы создать большое количество запросов на выдачу IPv6 к DHCPv6 серверу. Каждая авторизованная операция предоставления IPv6 адреса записывается в специальной таблице, чтобы DHCP сервер знал какие адреса он уже выдал. Эти записи хранятся в данной таблице определенное время, которое задано в настройках самого сервера. Вследствие этого могут реализоваться две ситуации:

1. На DHCP сервере больше не останется свободных IPv6 адресов для выдачи и новые клиенты не смогут получить IPv6 адрес до тех пор пока один из них не освободится.

2. Таблица записи выданных IPv6 адресов станет настолько большой, что займет всю оперативную память и сервер зависнет, либо станет работать с очень большими задержками.

Упрощение процесса разведки по средствам multicast рассылок

Увеличение количества IPv6 адресов в рамках одной подсети значительно затрудняет возможности

злоумышленника по сканированию сети на наличие работающих хостов. Данный процесс происходит на этапе сканирования ресурсов системы, после выявления работающих устройств начинается фаза сканирования открытых портов и выявления деталей о службах, которые работают на этих хостах.

Так как количество хостов в одной подсети при использовании IPv6 может составлять 2^64, по сравнению с IPv4 - 2^8, то задача сканирования хостов становится крайне сложной.

Однако Multicast рассылка значительно упрощает этот процесс. Отправив ping запрос на multicast адрес ff02::1 можно получить отклик от работающих хостов.

Так же существует Nmap скрипт “target-ipv6-multicast-slaac” [11], который отправляет в сеть ICMPv6 Router Advertisement запрос со случайным адресным префиксом (рис. 8), что заставляет устройства в сети запустить процесс SLAAC. Получив новый IPv6 адрес, хост отправляет в сеть NS запрос (рассылается multicast рассылкой всем устройствам в сети), в рамках процесса обнаружения дублирующийся адресов DAD.

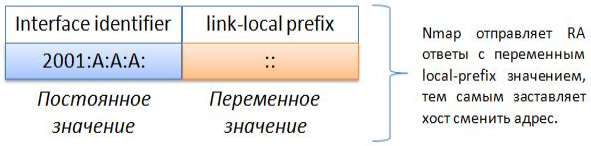

Рис. 8. Принцип работы Nmap скрипта для разведки IPv6 адресов

Затем атакующий угадывает IPv6 адреса путем совмещения идентификаторов интерфейсов (англ. interface identifier), полученных в NS сообщениях, с link-local префиксом (англ. link-local prefix). Процесс сопровождается рассылкой ND сообщений с целью обнаружения хостов, что позволяет проверить корректность угаданных IPv6 адресов.

В сборе инструментов THC IPv6 [12] для анализа безопасности протокола IPv6 существует скрипт (detect-new-ipv6), который позволяет в пассивном режиме узнать какие хосты находятся в сети. Это возможно благодаря тому, что NDP протокол использует DaD механизм для проверки неповторимости IPv6 адреса и рассылает реальный адрес хоста multicast сообщением на все устройства сети.

Также довольно интересным для целей разведки адресов в IPv6 сетях является стандарт [13], которому на смену в ближайшие месяцы должен прийти стандарт [14]. В нем описаны наработки сообщества относительно процесса разведки узлов с IPv6 адресами как в локальных, так и в удаленных сетях. Они выпущены организацией IETF и выложены в открытый доступ в виде RFC.

Скрытие данных в расширенных заголовках

IPv6 используется два типа заголовков: обычные и расширенные (англ. “extension”) [15, 16]. В отличии от IPv4 протокола, в заголовок которого входили поля для выполнения обширного набора функций, в обычном IPv6 заголовке полей гораздо меньше. Весь дополнительный функционал переброшен в расширенные заголовки. Обычный заголовок имеет длину 40 байт, в свою очередь расширенные заголовки могут иметь различную длину в зависимости от того какой из них применяется, а также могут применяться или не применяться в зависимости от необходимого функционала [17].

Используя расширенные заголовки можно легко организовать скрытый канал передачи данных [11, 18]. К примеру, в расширенном заголовке Hop-by-Hop, поле Options (на рис. 9 поле Options изображено как Options and Padding) согласно стандарту RFC 2460 должно содержать все нули, однако никто не мешает записать в это поле полезную информацию и по частям передавать ее в этих заголовках на удаленный узел при этом не затрагивая выше и нижележащие протоколы.

Как свидетельствует практика многие средства сетевой безопасности, такие как брандмауэры и IDS/IPS системы производства популярных вендоров не готовы к защите от подобного рода атак [19]. Решение, которое на данный момент предлагает IETF согласно стандарту RFC 6437 [20] – брандмауэр должен обнулить те поля расширенных заголовков, в которых должны быть установлены ноли.

Программные средства реализации атак на семейство протоколов IPv6

Nmap [21] – сетевой сканер, который используют как системные администраторы, так и хакеры для сканирования сетевых ресурсов на наличие открытых портов и распознания версии служб, которые работают на этих портах.

Offsets Octet	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Next Header								Hdr Ext Len								Options and Padding															
4	32	Options and Padding																															
8	64	Optional: more Options and Padding ...																															
12	96																																

Рис. 9. Формат расширенного заголовка Hop-by-Hop

THC-IPv6 [12] – довольно большой набор инструментов, собранных в одной программе Марком Хьюзом (Marc Heuse). Используется для атаки уязвимых протоколов IPv6 и ICMPv6. Один из самых популярных инструментов для атаки на IPv6.

SI6 Networks' IPv6 Toolkit [22] – набор инструментов для анализа безопасности и поиска неисправностей протокола IPv6. Содержит редактор и генератор пакетов ICMPv6 и IPv6, сканер сети и scanf6 и многое другое. Более сложный по сравнению с THC-IPv6.

Scapy [23] – редактор и генератор пакетов. При помощи данной программы можно создать пакет, вручную задав настройки каждого поля заголовков транспортного, сетевого и канального уровней. Используется для составления пакетов с нестандартными значениями полей, которые невозможно задать штатными средствами. Программа не имеет графической оболочки и довольна сложна для использования в непрофессиональных руках.

packETH [24] и Hping [25] – популярные генераторы пакетов. packETH создан для работы с Ethernet средой, также может помочь в создании IMCPv6 пакета. Hping в свою очередь имеет возможность редактирования лишь заголовка сетевого уровня. Hping3 в свою очередь также имеет обширные возможности по редактированию полей различных заголовков.

Parasite6 [26] – протокол NDP отправляет NS запрос для распознания MAC-адреса удаленного узла. Parasite6 внедряется в данный процесс и передает клиенту поддельный MAC адрес в ответ, таким образом клиент перенаправляет все пакеты, предназначенные для удаленного узла через устройства злоумышленника (через поддельный MAC адрес). Пример данной атаки приведен в разделе “Атака на процесс обнаружения MAC адреса”.

Smurf6 – программа для осуществления классической smurf атаки, эксплуатируя уязвимость ICMPv6 протокола. Пример данной атаки приведен в разделе “Осуществление DoS посредством ICMPv6 протокола”.

Выводы

Исходя из анализа всевозможных атак, в том числе и абсолютно новых способов компрометации, которые появились в силу принципов реализации и работы самого протокола IPv6, можно сделать вывод о его недостаточной защищенности без применения специальных защитных технологий.

Также следует отметить, что в сети Интернет появилось большое количество различных утилит, которые могут быть использованы для компрометации протокола IPv6. Учитывать также следует и тот факт, что данные программы становятся все проще в эксплуатации, что делает возможным реализацию атаки даже атакующим с базовым уровнем знаний и навыков.

Все вышеперечисленные факторы указывают на то, что для семейства протоколов IPv6 нуждается в дополнительных механизмах обеспечения информационной безопасности, в том числе и кардинально новых, так как протокол IPv6 имеет множество уникальных особенностей функционирования.

Список литературы

1. IANA issues final IP addresses, signals end of IPv4 [Электрон. ресурс]: Perle Article. – 4 Feb 2014. – Режим доступа: http://www.perle.com/articles/IANA-issues-final-IP-addresses-signals-end-of-IPv4-800382210.shtml

2. IPv4 exhaustion details [Электрон. ресурс]: ARIN Community – Режим доступа: http://www.apnic.net /community/ipv4-exhaustion/ipv4-exhaustion-details.

3. RIPE NCC Begins to Allocate IPv4 Address Space From the Last /8 [Электрон. ресурс]: RIPE News. – 14 Sep 2012 – Режим доступа: http://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8.

4. Arin enters phase four of the IPv4 countdown plan [Электрон. ресурс]: ARIN Announcements. – 23 Apr 2014. – Режим доступа: https://www.arin.net/announcements/2014/20140423.html

5. Postel J. IPv6 Testing Address Allocation / J. Postel, R. Fink, R. Hinden // ISI. – 1998.

6. Hinden R. M. 6bone (IPv6 Testing Address Allocation) Phaseout / R. M. Hinden, R. L. Fink. – 2004.

7. IPv6 Backbone (6bone) [Электрон. ресурс]: IETF. – Jan 1997 – Режим доступа: http://www.ietf.org/wg/ concluded/6bone.html.

8. Guidelines for the secure deployment of IPv6 / Frankel S., Gravmen R., Pearce J. [и др.] // NIST Special Publication. – 2010. – Т. 800. – С. 119.

9. Vulnerability Summary for CVE-2010-4669 [Электрон. ресурс]: National Vulnerability Database. – 1 Jul 2011 – Режим доступа: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4669.

10. Multiple Vendors IPv6 Neighbor Discovery Router Advertisement Remote Denial of Service Vulnerability [Электрон. ресурс]: Security Focus. – 11 Jan 2011 – Режим доступа: http://www.securityfocus.com/bid/45760/info.

11. File targets-ipv6-multicast-slaac [Электрон. ресурс]: NSEdoc Scripts – Режим доступа: http://nmap.org/nsedoc/scripts/targets-ipv6-multicast-slaac.html.

12. THC-IPV6 [Электрон. ресурс]: THC-IPV6 project site – Режим доступа: https://www.thc.org/thc-ipv6/

13. Chown T. IPv6 Implications for Network Scanning. – 2008.

14. Gont F. Network Reconnaissance in IPv6 Networks draft-ietf-opsec-ipv6-host-scanning-03 / F. Gont, T. Chown. – January, 2014.

15. A Uniform Format for IPv6 Extension Headers / Krishnan S., Woodyatt J., Kline E. [и др.]. – 2012.

16. Deering S. E. Internet protocol, version 6 (IPv6) specification. – 1998.

17. IPv6 Extension Headers Review and Considerations [Электрон. ресурс]: Cisco technology white paper. – Oct 2006 – Режим доступа: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900acd8054d37d.html.

18. Panajotov B. Covert Channels in TCP/IP Protocol Stack / B. Panajotov, A. Mileva – 2013.

19. Atlasis A. Security Impacts of Abusing IPv6 Extension Headers // Black Hat security conference. – 2012. – С. 1-10.

20. Rajahalme J. IPv6 flow label specification / Rajahalme J., Amante S., Jiang S. [и др.] // RFC. – 2011.

21. Nmap [Электрон. ресурс]: Nmap tool site. – Режим доступа: http://nmap.org/

22. SI6 Networks' IPv6 Toolkit [Электрон. ресурс]: Official SI6 Networks' IPv6 Toolkit site. – Режим доступа: http://www.si6networks.com/tools/ipv6toolkit/

23. Scapy [Электрон. ресурс]: Official Scapy project site. – Режим доступа: http://www.secdev.org/projects/scapy/

24. PACKETH [Электрон. ресурс]: Official PACKETH site – Режим доступа: ttp://packeth. sourceforge.net/packeth/Home.html

25. Hping [Электрон. ресурс]: Hping tool site. – Режим доступа: http://www.hping.org/

26. THC-IPv6-Attack-Toolkit/parasite6 [Электрон. ресурс]: Parasite6 tool site – Режим доступа: http://www.aldeid.com/wiki/THC-IPv6-Attack-Toolkit/parasite6.

27. Vulnerability Summary for CVE-2010-4669 [Электрон. ресурс]: National Vulnerability Database. – 1 Jul 2011 – Режим доступа: http://web.nvd.nist.gov/view/vuln/ detail?vulnId=CVE-2010-4669.

Поступила в редколлегию 7.10.2014

Рецензент: д-р тех. наук, проф. А.В. Лемешко, Харьковский национальный университет радиоэлектроники, Харьков.

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ СТЕКА ПРОТОКОЛІВ IPV6

А.В. Снігуров, В.Х. Чакрян

У наведеній статті проведений аналіз вразливостей протоколу IPv6 та інших протоколів, що входять в його реалізацію та необхідні для його коректної роботи, наприклад: протокол NDP, ICMPv6, DHCPv6 та ін. Також в статті розглядаються можливі вектори атак на сімейство протоколів IPv6 та принципи їх реалізації, серед них: атаки на вразливості протоколу NDP, CGA DoS атаки, ICMPv6 DoS атаки, DoS атаки шляхом маніпуляції полями пакету MTU або Current Hop Limit, атаки на протокол DHCPv6, атаки прихованої передачі даних в полях пакету та ін. Також наведені програмні засоби реалізації перерахованих атак.

Ключові слова: *вразливість протоколу IPv6, атаки на сімейство протоколів IPv6, ICMPv6, NDP, DHCPv6, DoS атаки.*

INFORMATION SECURITY THREATS IPV6 PROTOCOL STACK

A.V. Snigurov, V.K. Chakrian

In this paper are addressed the issues of vulnerabilities of IPv6 protocol and all other protocols that are parts of its implementation and are needed for IPv6 to work properly, for example: NDP, ICMPv6, DHCPv6, etc. Also in this paper the possible attack vectors on IPv6 protocols family and principles of its realization are shown, among them are: attacks on NDP protocol vulnerabilities, CGA DoS attacks, ICMPv6 DoS attacks, DoS attacks caused by manipulation of MTU or Current Hop Limit packet fields, attacks on DHCPv6 protocol, attacks of hidden information transmission using packet fields, etc. Additionally the software for realization of listed attacks is given.

Keywords: *vulnerabilities of IPv6 protocol, attacks on IPv6 protocols family, ICMPv6, NDP, DHCPv6, DoS attacks.*