УДК 681.3

О ПРОБЛЕМАХ АТАК В СЕТЕВЫХ СИСТЕМАХ

© 2018 А. С. Стешковой

Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия им. проф. Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж, Россия)

В статье рассматриваются некоторые угрозы безопасности в беспроводных компьютерных сетях. Проанализированы причины различных Dos-атак.

Ключевые слова: беспроводные сети, dos-атаки, защита информации, информационная безопасность.

Беспроводные сети предпочтительнее проводных сетей из-за их экономической эффективности и простоты использования. Но технологические инновации в беспроводных сетях открыли новые угрозы безопасности системы.

Отказ в обслуживании – это атака, которая нарушает доступ к сетевому ресурсу авторизованному пользователю.

Статистика правонарушений в области информационной безопасности свидетельствует о том, что самое дорогое компьютерное преступление за последние годы связаны с отказом в обслуживании. DoS-атака нацелена на разные уровни модели OSI [1]:

Физический уровень: обрыв кабеля связи, постановка шумовой помехи в определенном диапазоне частот, чтобы отключить сетевые сервисы.

Канальный уровень: отключить возможность доступа хостов к локальной сети.

Сетевой уровень: отправка большого количества IP-данных в сеть.

Транспортный уровень: отправив множество запросов TCP-соединения на хост

Прикладной уровень: отправка большого количества законных запросов к приложению.

Различные виды Dos-атак это [2] ARP отправка, MAC Спуфинг, Web Спуфинг, ICMP Flooding, атаки на функционирование процессора и памяти, задержка в эфире, атака Disassociation, атака распределенного отказа в обслуживании (DDoS), атака сообщения об аутентификации и т. д. WLAN сети используют протокол безопасности Wired Equivalent Privacy (WEP) [1], чтобы обеспечить службы проверки целостности и конфиденциальности. Поскольку WEP не обеспечивает необходимый уровень безопасности, IEEE предложил два других протокола безопасности, такие как Wi-Fi Protected Access (WPA) и 802.11i в качестве стандартов безопасности для локальных сетей WLAN. WPA был промежуточным протоколом безопасности для повышения уровня безопасности, предлагаемого WEP, до окончательного протокола безопасности в виде 802.11i. Кадры управления и контроля в беспроводных сетях на основе стандарта 802.11 по-прежнему остаются незащищенными. Следовательно, WLANсети, даже с развертыванием 802.11i, подвержены атакам с отказами в обслуживании (DoS).

DOS-атаки возникают, когда какой-либо системный ресурс недоступен для пользователей сети. DOS-атаки наполняют удаленную систему таким большим количеством трафика, что она не может обрабатывать обычные, действительные запросы, отправленные из других систем [3].

DOS-атаки не так легко обнаружить, поскольку удаленный компьютер не может легко отличить запросы и трафик, отправленные с DOS- атакующих машин и отправленные действительными средствами. DOS также может возникать из-за высокого легетимного спроса.

Атаки DoS можно грубо классифицировать в соответствии с моделью OSI [4, 5]:

1. DoS-атаки уровня приложения.
2. Атаки межсетевого и транспортного уровней.
3. DOS-атаки на уровене доступа к среде.
4. DoS уровня физического уровня.

Стешковой Анатолий Сергеевич – Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия им. проф. Н. Е. Жуковского и Ю. А. Гагарина», специалист, S9821steshkowoiy@yandex.ru.

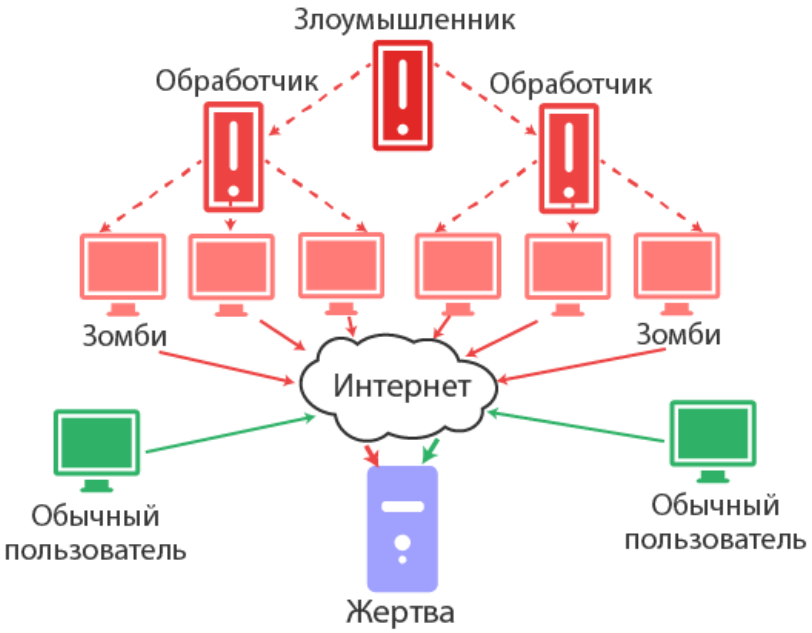

Рисунок 1. Структурная схема DOS атаки.

Атаки уровня приложений: здесь злоумышленник пытается использовать слабость протокола приложения, например DNS (кэширование), HTTP (переполнение стека и буфера) [6]. Это достигается путем отправки большого количества легитимных запросов в приложение. Например, [7] атака потоком HTTP может сделать сотни тысяч запросов страниц на веб-сервер, который может исчерпать всю возможность обработки сервера.

Атаки между сетевыми и транспортными уровнями. Атака DoS транспортного уровня включает отправку многих запросов на подключение к хосту. Очень эффективно и чрезвычайно сложно отследить атакующего из-за используемых методов IP-спуфинга. Сетевой уровень DoS-атаки [8] достигается путем отправки большого количества данных в беспроводную сеть.

Атаки уровня доступа к среде: атаки уровня множественного доступа к среде. Беспроводные сети особенно уязвимы для атак уровня MAC из-за использования совместно используемого канала связи [9]. Злоумышленник может передавать пакеты с использованием поддельного MAC-адреса источника – точки доступа. Получатель этих поддельных кадров не может отличить, являются ли они законными или незаконными запросами и будет их обрабатывать. Существует два основных уровня MAC:

1. Атака на аутентификацию/ассоциация.
2. Атаки на деактивацию/деассоциация.

Атаки на физическом уровне: основные две атаки - это помехи и интерференции. Зашумление беспроводной сети с шумовыми сигналами может снизить пропускную способность сети.

Вмешательство других радиопередатчиков – еще одна возможность понизить производительность беспроводной сети.

Различные DoS-атаки объясняются следующим образом.

Атаки кадра управления WLAN: устройства 802.11 используют кадры управления для обнаружения, аутентификации и объединения клиентов WLAN к точке доступа. Многие из этих типов фреймов управления не аутентифицируются и таким образом уязвимы для DoS-атак [8]. Например, злоумышленник может отправлять кадры деаутентификации с поддельными MAC-адресами источника кв точке доступа, тем самым делая недоступным клиентское устройство.

Teardrop Attack: Teardrop attack [10] использует сеть, отправляя пакеты фрагментов IP, которые трудно собрать. Сначала пакет фрагментов идентифицирует смещение, которое может быть использовано для сборки всего пакета, чтобы приемное устройство могло их собрать. В этой атаке IP-адрес злоумышленника помещает значение смещения в последующие фрагменты, которые смешивают принимающую систему, тем самым делая систему неспособной обрабатывать эту ситуацию, в свою очередь, приводящую к сбою системы.

Уязвимость режима сохранения мощности (Power save Exploits): В состоянии ожидания клиент сети WLAN отключается для экономии энергии и переходит в режим автономной работы; трафик, предназначенный для клиента, впоследствии отбрасывается. Злоумышленник может отправить сообщение об ошибке с отключением питания, в то время как клиент все еще спит, заставляя точку доступа передавать и отбрасывать любой буферный трафик [8]. Также буферизованные кадры на AP рекламируются на карте индикации трафика (TIM). Злоумышленник может подделать TIM, чтобы показать клиенту, что нет буферизованного трафика, заставляя клиента вернуться в состояние ожидания и в результате чего кадры для клиента в конечном итоге будут отброшены.

WPA 802.1i атаки: WPA и 802.11i, предназначенные для защиты сети WLAN, могут использоваться для запуска атаки [5]. В качестве меры защиты, если точка доступа сети WLAN получает более 1 сообщения с недопустимой контрольной суммой MIC, сеанс должен быть отключен на 1 минуту, а затем должен быть сгенерирован новый сеансовый ключ, это поведение может быть неправильно использовано для запуска DoS атака фактически отключает беспроводную услугу, неоднократно отправляя сообщения с поддельными контрольными суммами MIC.

Атака на аутентификацию/ассоциация: во время атаки на атаку аутентификации/ассоциации злоумышленник использует поддельные исходные MAC-адреса, которые пытаются аутентифицировать и связывать с целевой точкой доступа. Злоумышленник неоднократно делает запросы на аутентификацию/ассоциацию, в конечном итоге исчерпывая память и вычислительную мощность точки доступа, оставляя клиентов с небольшим или никаким подключением к беспроводной сети.

Атаки деаутентификации / диссоциации: они также известны как уязвимости идентификаторов [11]. Во время deaunthentication клиент сначала аутентифицируется у точки доступа, как показано на рисунке 3, одна часть структуры аутентификации - это сообщение, которое позволяет клиентам и точкам доступа явно запрашивать деаутентификацию друг от друга. Это сообщение не зашифровано. Таким образом, злоумышленник может легко обмануть это сообщение, либо притворившись точкой доступа, либо клиентом.

Фреймы диссоциации используются, когда клиент имеет множественную точку доступа. 802.11 Поскольку клиент может быть аутентифицирован из нескольких точек доступа, поэтому 802.11 предоставляет сообщение ассоциации, позволяющее клиенту и точке доступа согласовать, какая точка доступа несет ответственность за пересылку пакетов от имени клиента.

Наполнение авторизации на основных устройствах: кадры запроса используются в IEEE 802.11 для обнаружения беспроводной сети [6], если существует беспроводная сеть, тогда точка доступа реагирует на кадр ответа на запрос. Клиенты выбирают эту точку доступа, которая обеспечивает самый сильный сигнал. Злоумышленник может обманывать путем отправки потока кадров запроса, представляющих множество узлов, которые ищут беспроводную сеть; может перегружать точку доступа или беспроводной маршрутизатор. Если нагрузка превышает пороговое значение, это приведет к тому, что точкадоступа или беспроводной сетчатый маршрутизатор перестанут отвечать на запросы и могут создать недоступность службы.

Веб-спуфинг: при веб-спуфинге злоумышленник убеждает жертву, что он посещает законный веб-сайт, тогда как когда веб-страницы создаются злоумышленником для кражи информации, такой как пароли и номера кредитных карт [3]. Злоумышленник может достичь этого, поставив под угрозу сервер интрасети любой компании и перенаправляя некоторые ссылки на свой веб-сервер.

MAC Spoofing: злоумышленник изменяет назначенный изготовителем MAC-адрес беспроводного адаптера на MAC-адрес, который он хочет подделать. Злоумышленник может узнать MAC-адрес действительного пользователя, захватив беспроводные пакеты. При успешном спуфинге MAC IP-адрес, назначенный компьютеру злоумышленника, будет идентичен IP-адресу компьютера-жертвы, MAC-адрес которого был подделан [3]. Чтобы получить доступ к беспроводной сети, злоумышленник должен выполнить DoS-атаку, чтобы отключить целевой компьютер от своего беспроводного соединения.

ICMP Flooding: используется для сообщения о доставке эхо-пакетов интернет-протокола (IP), устранения неполадок, что-

бы показать, когда конкретная конечная станция не отвечает, когда сеть IP недоступна, когда узел перегружен или когда возникает ошибка в информации заголовка IP и т. д. Типичная атака DoS с использованием ICMP известна как наводнение ICMP [3]. Он включает в себя наводнение буфера целевого компьютера нежелательными пакетами ICMP и, наконец, отсутствие ответа или сбой системы.

Атака SYN Flooding: одна из наиболее распространенных DoS-атак - атака SYN Flooding Attack [10]. Реализации TCP разработаны с небольшим ограничением на максимальное количество полуоткрытых соединений на порт, которые возможны в любой момент времени. Злоумышленник инициирует атаку SYN-затопления, отправив на зараженный компьютер множество запросов на соединение с поддельными исходными адресами. В результате жертва выделяет ресурсы. Когда достигнут предел полуоткрытых соединений, все последующие попытки установления соединения отключаются, вне зависимости являются ли они законными или нет. Если злоумышленник хочет, чтобы условие отказа в обслуживании продолжалось дольше, чем период ожидания, ему необходимо постоянно запрашивать жертву для новых подключений. Размер полосы пропускания центрального процессора и сети, требуемый злоумышленником для длительной атаки, ничтожно мал [10].

Выводы. DoS-атаки намного легче осуществлять в беспроводных сетях, чем в проводных, как правило, из-за характера беспроводной связи, когда трафик открыто перемещается в беспроводном канале связи. После разработки многих безопасных протоколов, беспроводная сеть IEEE 802.11 попрежнему уязвима для атак. DoS-атаки могут вызывать серьезные проблемы у законных пользователей. DOS может инициироваться на физическом уровне, канальном уровне, сетевом уровне, прикладном уровне и т. д. разными способами. В будущем больше внимания следует уделять проблемам DoS, так как доступные решения не способны полностью остановить Dos-атаки. А гарантированный иммунитет от DoS-атак никогда не будет возможен из-за открытости канала связи.

ЛИТЕРАТУРА

1. Львович, И. Я. Основы информатики / И. Я. Львович, Ю. П. Преображенский, В. В. Ермолова. – Воронеж, Воронежский институт высоких технологий (Воронеж). – 2014. – 339 с.

2. Преображенский, Ю. П. Проблемы кодирования информации в каналах связи / Ю. П. Преображенский // Современные инновации в науке и технике; Отв. ред. А. А. Горохов. – 2018. – С. 180-182.

4. Преображенский, Ю. П. Применение программных средств для повышения защищенности компьютерных систем / Ю. П. Преображенский // Проблемы и перспективы развития России: Молодежный взгляд в будущее; Отв. ред. А. А. Горохов. – 2018. – С. 76-78.

3. Преображенский, Ю. П. О видах информационных систем в организации / Ю. П. Преображенский // Молодежь и системная модернизация страны; Отв. ред. А. А. Горохов. – 2018. – С. 131-134.

5. Преображенский, Ю. П. Проблемы управления в производственных организациях / Ю. П. Преображенский // В сборнике: Актуальные проблемы развития хозяйствующих субъектов, территорий и систем регионального и муниципального управления Материалы XIII международной научно-практической конференции. Под редакцией Ю. В. Вертаковой. – 2018. – С. 208-211.

6. Питолин, А. В. Исследование возможностей использования стеганографических способов защиты информации / А. В. Питолин, Ю. П. Преображенский, О. Н. Чопоров // Моделирование, оптимизация и информационные технологии. 2018. – Т. 6. – № 2 (21). – С. 336-353.

7. Преображенский, Ю. П. О возможности защиты информации на предприятиях / Ю. П. Преображенский // Современные материалы, техника и технология; Отв. ред. А. А. Горохов. – 2017. – С. 294-298.

8. Преображенский, Ю. П. Предложения по оптимизации систем защиты информации / Ю. П. Преображенский // Современные материалы, техника и технология; Отв. ред. А. А. Горохов. – 2017. – С. 298-302.

9. Воронов, А. А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А. А. Воронов, И. Я. Львович, Ю. П. Преображенский, В. А. Воронов // Информация и безопасность. – 2006. – Т. 9. – № 2. – С. 8-11.

10. Львович, И. Я. Применение методологического анализа в исследовании безопасности / И. Я. Львович, А. А. Воронов // Информация и безопасность. – 2011. – Т. 14. – № 3. – С. 469-470.

11. Преображенский, А. П. Комбинированный алгоритм шифрования данных в компьютерной системе / А. П. Преображенский, О. Н. Чопоров // International Journal of Advanced Studies. – 2018. – Т. 8. – № 2-2. – С. 38-47.

ABOUT ATTAK PROBLEMS AND NETWORK SYSTEMS

© 2018 A. S. Steshkowoy

Military training and research center of the air force «Air force Academy prof. E. Zhukovsky and Y. A. Gagarin» (Voronezh, Russia)

The paper is devoted to the consideration of some security threats in wireless computer networks. The causes of various Dos attacks are analyzed.

Key words: wireless networks, dos attacks, information protection, information security.