ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ ОТ ВЗЛОМА

Манукян Э.Г., студент гр. 110402-ИТСа-о19, II курс
Научный руководитель: Янченко Д.В., к.т.н., доцент
Южно-российский государственный политехнический университет
(новочеркасский политехнический институт) имени М.И. Платова
г.Новочеркасск

Беспроводные соединения окружают нас повсюду. Это пульт дистанционного управления телевизором, сотовый мобильный телефон и, конечно же, компьютер подключенный к беспроводному Интернету. Небольшой маршрутизатор с беспроводной точкой доступа теперь становится простым занятием дома, не говоря уже о небольшом офисе. Также, однако, ограничивающим фактором является то, что большинство пользователей не имеют представления об основных принципах работы этих устройств, об их возможностях и способах их использования. Мы хотели бы поделиться этими аспектами непосредственно в этой статье.

В чем разница между проводной сетью и беспроводной? В общем, проводная сеть, при условии, что ее пользователи абсолютно честны, может быть атакована только из Интернета – если она подключена к сети. Беспроводная связь открыта абсолютно всем ветрам, и кроме вторжений из Интернета, ей как минимум угрожает попытка "подслушать" со стороны сотрудников из соседнего офиса или с нижнего этажа. Но это важно – подобные действия могут не только принести удовлетворение от использования беспроводной сети, но и найти способы попасть в нее. Соответственно, если безопасности не будет уделено должного внимания, такая сеть вполне может считаться публичной, что неизбежно плохо скажется на ее функционировании.

Соответственно, если безопасности не будет уделено должного внимания, такая сеть может считаться публичной, что неизбежно плохо скажется на ее функционировании.

Общей тенденцией формирования компьютерных сетей в последние годы является постепенная замена проводных сетей их беспроводными аналогами. Это наблюдается на всех уровнях-от компьютерных и периферийных интерфейсов до магистральных сетей, от передачи данных до голосовой и видеотелефонии. Все многообразие современных беспроводных технологий можно разделить на следующие типы: 1.Для соединения оборудования внутри рабочего места, например, сотового телефона или ноутбука (либо ПК, либо принтера), предусмотрены индивидуальные беспроводные сети WPAN (Wireless Personal Area Network). Очевидно, что такие сети обслуживаются лично пользователем или системным (сетевым)

администратором при отсутствии участия оператора связи. Среди сетей WPAN наиболее известной является сеть Bluetooth, которая позволяет комбинировать портативные вычислительные или телекоммуникационные устройства (сотовые телефоны, КПК, смартфоны, планшеты, ноутбуки) с беспроводной периферией и аксессуарами, расположенными на небольшом расстоянии (до 10 м, но в некоторых случаях – до 100 м) от пользователя. Беспроводные локальные сети (WLAN), которые, согласно ассоциации с более распространенной беспроводной сетью, также называются Wi-Fi (сокращение от Wireless Fidelity) сетями, гарантируют расстояние соединения в закрытом режиме от пятидесяти до 150 м или до 300 м в открытом пространстве. Они предназначены в основном для развертывания беспроводных сетей в пределах 1 или нескольких помещений, хотя их также можно использовать на открытых площадках ограниченного размера. Также большой популярностью пользуются так называемые горячие точки-беспроводные сети, которые развертываются для обеспечения доступа в Интернет или корпоративную сеть в общественных местах (в гостиницах, аэропортах, кафе, ресторанах, выставочных залах и т. Д.). 3.Типичный радиус воздействия распределенных беспроводных сетей городского масштаба WMAN (Wireless Metropolitan Area Networks) составляет около 50 километров. Такие сети призваны расширяться (а в перспективе и полностью меняться) как "последняя миля" инфраструктуры проводных муниципальных сетей связи, которые служат для высокоскоростного доступа в Интернет и телефонии. К этой категории относятся широкополосные сети WiMAX.

Само название WiMAX является свободной аббревиатурой Всемирной интероперабельности для микроволнового доступа (Worldwide Network Association for Microwave Access). Основным отличием нового стандарта от всех предыдущих является радиус воздействия, который в зависимости от используемых передатчиков может достигать 50 километров, что позволяет говорить о WiMAX как своеобразном аналоге сотовой связи. Одной из его основных задач является обеспечение высокоскоростным доступом в Интернет небольших населенных пунктов или отдельных районов крупного города. Кроме того, данная методика позволяет передавать не только данные (пакетные и голосовые), но и видео-и аудиопотоки, что дает возможность интегрировать и унифицировать все существующие сети связи на единой базе WiMAX.

Само название WiMAX является свободной аббревиатурой Всемирной интероперабельности для микроволнового доступа (Worldwide Network Association for Microwave Access). Основное отличие нового стандарта от всех предыдущих заключается в дальности действия, которая в зависимости от используемых передатчиков может достигать 50 км, что позволяет говорить о WiMAX как своеобразном аналоге сотовой связи. Одной из его основных задач является обеспечение высокоскоростным доступом в Интернет небольших населенных пунктов или отдельных районов крупного города. Кроме того, данная технология позволяет передавать не только

данные (пакетные и голосовые), но и видео-и аудиопотоки, что дает возможность интегрировать и унифицировать все существующие сети связи на единой базе WiMAX.

Любая беспроводная сеть состоит как минимум из двух основных компонентов – беспроводной точки доступа и клиента беспроводной сети (режим ad-hoc, в котором клиенты беспроводной сети общаются друг с другом напрямую без точки доступа, мы рассматривать не будем). Стандарты беспроводной сети 802.11/b/g предусматривают несколько механизмов безопасности, которые включают в себя различные механизмы аутентификации пользователей и реализацию шифрования при передаче данных.

Основными преимуществами беспроводных сетей, по сравнению с традиционными кабельными сетями, являются простота развертывания и подключения к ним новых пользователей, а также мобильность пользователей в зоне ее покрытия. Только этих двух достоинств достаточно, чтобы говорить об их радужных перспективах, несмотря на имеющиеся (пока) недостатки. И действительно, если сегодня еще можно говорить о недостаточной пропускной способности наиболее популярных современных беспроводных сетей Bluetooth и Wi-Fi по сравнению с проводными сетями, то если первая действительно перейдет на UWB и широкое распространение спецификации 802.11 n для второй, то в ближайшем будущем их возможности как минимум сравняются. Но все же ожидается появление новых, довольно агрессивных игроков рынка, таких как Wireless USB и Wireless HD. А "дальнобойный" WiMAX, несмотря на то, что этот стандарт лучше всего подходит для интернет-провайдеров, еще не сказал своего последнего слова. Основные направления взлома беспроводных сетей.

Еще одна мера предосторожности, которая часто используется в беспроводных сетях, - это порядок скрытого идентификатора сети. Каждой беспроводной сети присваивается свой собственный оригинальный персональный номер (SSID), который является названием сети. Когда пользователь пытается войти в сеть, в этом случае программа драйвера беспроводного адаптера сначала сканирует широковещательную передачу на наличие в ней беспроводных сетей. При использовании режима секретного частного номера (обычно называемого Hide SSID) линия не отражается в списке доступных, и подключиться к ней можно только в том случае, если, во-первых, вы точно знаете ее SSID, а, во-вторых, заранее создан профиль подключения к этой сети.

Безопасности беспроводных сетей следует уделять особое внимание. Wi-Fi-это беспроводная сеть и с огромным радиусом влияния. Таким образом, злоумышленник может перехватить информацию или атаковать вашу систему с безопасного расстояния. В настоящее время уже существует множество различных способов защиты, и если вы правильно ее настроите, то можете быть уверены в обеспечении необходимого уровня безопасности:

-Протокол шифрования WEP

-Протокол шифрования WPA

-Протокол WPA2

- стандарт безопасности 802.1 X

- Фильтрация по MAC-адресу

- Скрытие SSID

- Запретить доступ к настройкам точки доступа или маршрутизатора через беспроводную сеть.

В арсенал злоумышленника, стремящегося взломать беспроводную сеть, входит следующее: в первую очередь вам понадобится портативный компьютер с беспроводным адаптером. Основной проблемой, возникающей при выборе средств для взлома беспроводных сетей, является обеспечение совместимости между чипом беспроводного адаптера, используемым программным обеспечением обеспечения, а также операционной системой. Программы для взлома также настраиваются операционной системой. Для преодоления всей системы безопасности беспроводной сети на основе WEP-шифрования не требуется практически никаких работ. Правда, многие скажут, что это малоинтересно, так как протокол WEP давно мертв — он не используется. Он был заменен самым стабильным протоколом WPA. Однако не будем спешить с выводами. Это верно, но лишь отчасти. Проблема заключается в том, что в некоторых случаях для увеличения радиуса воздействия беспроводной сети на базе определенных точек доступа возникают так называемые распределенные беспроводные сети (WDS). Самое интересное, что такие сети не поддерживают протокол WPA и единственной приемлемой мерой безопасности в этом случае является использование WEP-шифрования. В то же время сети WDS открываются точно так же, как и сети, основанные на одной точке доступа. Кроме того, КПК, оснащенные беспроводным модулем, также не поддерживают протокол WPA, по этой причине для внедрения в беспроводную сеть клиента на базе КПК в ней должен использоваться протокол WEP. Таким образом, протокол WEP будет востребован в беспроводных сетях еще долгое время. Рассмотренные примеры взлома беспроводных сетей очень наглядно демонстрируют их уязвимость. Если говорить о протоколе WEP, то в данном случае его можно сравнить с "надежной" защитой. Это примерно то же самое, что сигнализация на автомобиле — только она спасает вас от хулиганов. Что касается таких мер предосторожности, как фильтрация по MAC-адресам и режим секретного сетевого идентификатора, то их вообще нельзя рассматривать как защиту. Тем не менее, даже такие средства не следует игнорировать, хотя бы только в сочетании с другими мерами.

Таким образом, беспроводные сети формируют новые классы рисков также угроз, которые не могут быть защищены классическими проводными средствами. Даже если Wi-Fi официально запрещен в компании – это не означает, что один из пользователей не установит постороннего также этим

наиболее сведет все капиталовложения в сетевую безопасность к нулю. Помимо этого, в связи с отличительными чертами беспроводной связи немаловажно следить не только за безопасностью инфраструктуры доступа, но также за пользователями, которые могут быть предметом атаки злоумышленника либо попросту могут случайно или намеренно перейти с корпоративной сети на незащищенное соединение.

Хорошая новость, после такой удручающей презентации, заключается в том, что большинство перечисленных рисков можно свести к минимуму или даже свести к нулю. Для обеспечения безопасной работы беспроводной сети (включая инфраструктуру и пользователей) используется подход, в целом совпадающий с подходом "многоуровневой безопасности", используемым для традиционных проводных сетей (с поправкой на специфику WLAN). Но это тема для отдельной статьи не меньшего объема, которая последует позже.

Обеспечение безопасности беспроводных сетей-довольно сложная задача. Трудности вызваны невозможностью физически изолировать злоумышленников от сети или отследить их местоположение. В то же время следование простым рекомендациям позволяет значительно повысить уровень безопасности и минимизировать риски атак.

Основные рекомендации по защите беспроводных сетей:

Обеспечьте физическую защиту сетевого устройства. Маршрутизатор должен быть установлен таким образом, чтобы исключить помехи, например, от микроволновой печи. Также следует исключить возможность случайного нажатия кнопки сброса.

Измените имя пользователя и пароль по умолчанию. Данные для доступа к интерфейсу настройки маршрутизатора и сети Wi-Fi указаны в инструкции к устройству. Мы рекомендуем вам изменить эти данные, создав надежный пароль.

Отключите широковещательную передачу идентификатора сети. В этом случае только тот пользователь, который знает идентификатор беспроводной сети, сможет подключиться к вашей беспроводной сети.

Примените фильтрацию MAC-адресов. Фильтрация поможет вам ограничить количество подключенных устройств. В результате к сети смогут подключаться только определенные устройства, указанные в настройках MAC. Эта мера значительно усложнит доступ злоумышленников и поможет исключить возможность "левых" подключений.

Используйте эффективные протоколы безопасности беспроводной сети. Поэтому при настройке маршрутизатора рекомендуется установить протоколы безопасности WPA/ WPA2.

Используйте брандмауэр на вашем компьютере. Программный брандмауэр устанавливается по умолчанию в системах Windows, начиная с XP. Вы можете использовать сторонние брандмауэры. Брандмауэр обеспечивает мониторинг трафика и фильтрацию для защиты от сетевых угроз. Поэтому такая компания всегда должна находиться в активном состоянии.

Используйте регулярно обновляемый эффективный антивирус.

Ограничьте диапазон действия сети. В идеале лучше ограничить активность Wi-Fi только за пределами вашей квартиры или офиса. Это сделает невозможным или значительно затруднит злоумышленнику доступ к беспроводной сети.

Отключите доступ к настройкам маршрутизатора через Wi-Fi. В этом режиме для изменения настроек вам понадобится кабельное соединение, то есть физический доступ к сетевому устройству, который недоступен посторонним.

Избегайте использования незащищенных беспроводных сетей в общественных местах. Также не рекомендуется подключаться к чужой незащищенной сети внутри вашего дома. Это может быть ложная точка доступа, используемая хакерами для кражи данных.

Всегда выключайте маршрутизатор, когда вы не пользуетесь Интернетом. Эта мера снизит вероятность нападения.

Используйте Bluetooth осторожно. Эта функция должна быть постоянно отключена на телефоне. Рекомендуется включать Bluetooth только непосредственно перед использованием. Отклоняйте запросы на подключение к неизвестным устройствам и не принимайте от них никаких файлов.

Следование этим рекомендациям не дает стопроцентной гарантии безопасности беспроводных сетей, но позволяет значительно снизить уровень рисков.

Библиографическое описание.

1.Маркелов, К. С. Безопасность беспроводных сетей / К. С. Маркелов, А. Б. Нейман. — Текст : непосредственный // Молодой ученый. — 2012. — № 4 (39). — С. 63-66. — URL: https://moluch.ru/archive/39/4589/ (дата обращения:27.03.2021).

2. Патий Е. Проблемы безопасности в беспроводных сетях/ Е.Патий // Искусство управления информационной безопасностью [Электронный ресурс]. – Режим доступа: http://www.iso27000.ru/chitalnyi-zai/bezopasnost-besprovodnyh-setei/problemy-bezopasnosti-v-besprovodnyh-setyah/

3. Монин С. Защита информации и беспроводные сети / С. Монин // Компьютер Пресс #4/2005 [Электронный ресурс]. – Режим доступа: http://www.redcenter.ru/?did=822&p_realm=print1

4. Практика взлома беспроводных сетей / Сергей Пахомов, Максим Афанасьев // Компьютер Пресс [Электронный ресурс]. – Режим доступа: http://www.compress.ru/Article.aspx?id=17372