УДК 519-7

Атаки на беспроводные сети.

Г.Д.Асяев

(Челябинск,НИУ ЮУрГУ,asyaev1996@mail.ru)

Аннотация: с развитием беспроводных технологий учащаются и атаки на них. Расширение мобильного пространства, при котором возможен доступ как дома, как в университете, как и на улице ведёт к условиям при которых возможно перехватить пакеты данных, а также приводит к потери данных или даже проникновение в сеть различных вирусов. Беспроводные сети удобны тем на предприятиях, что имеют меньшую сложность развёртывания сети.

Ключевые слова: сети, атаки, беспроводные соединения.

При атаке на беспроводные соединения атакующий может выполнять действия, которые поглощают сетевые ресурсы, не позволяющие пользователю законно получать доступ к сетевым сервисам, это может привести к краже данных, нелегитимному использованию аккаунтов пользователей. При этом мотивы у злоумышленников могут быть разные от простой славы до промышленного терроризма и расизма. Отсюда следует, что нужно постоянно отслеживать уровень безопасности Wi-fi инфраструктуры.

Все многообразие протоколов беспроводной передачи данных можно классифицировать по максимальному радиуса действия беспроводной сети. Ниже приведена классификация рассматриваемых протоколов по порядку уменьшению радиуса.

* WWAN (Wireless Wide area network) – в основном это сети сотовой связи, их радиус действия составляет десятки километров. К этим сетям относятся следующие протоколы: GSM, CDMAone, iDEN, PDC, GPRS и UMTS.
* WMAN (Wireless Metropolitan Area Networks – это беспроводные сети масштаба города. Радиус действия таких сетей несколько километров. Примером протокола этой сети служит WiMAX.
* Wireless LAN (Wireless Local Area Network; WLAN) – это беспроводная локальная вычислительная сеть. Радиус действия этого класса сетей — несколько сотен метров. К ним относятся следующие протоколы: UWB, ZigBee, Wi-Fi.
* WPAN применяются для связи различных устройств, включая компьютеры, бытовые приборы и оргтехнику, средства связи и т. д. Радиус действия WPAN составляет от нескольких метров до нескольких десятков метров. WPAN используется как для объединения отдельных устройств между собой, так и для связи их с сетями более высокого уровня. Примером таких сетей могут служить протоколы RuBee, X10, Insteon, Bluetooth, Z-Wave, ANT, RFID.

Беспроводные сети работают в одном или нескольких вариантах топологии. На рис.1 приведены топологии беспроводных сетей различных конфигураций.

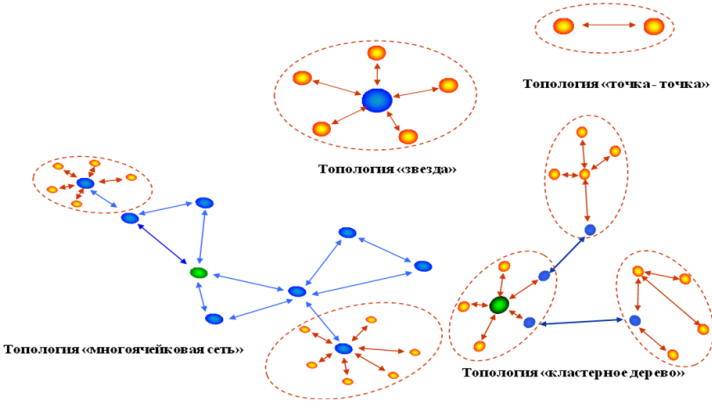


Рисунок 1. Топологии сетей.

Самым простым вариантом топологии является точка-точка. Это вариант организации сети из двух устройств. Как правило, узлы этой сети являются равноправными, то есть сеть одноранговая. Эта топология характерна для Bluetooth, ANT, RFID, RuBee, PDC, WI-FI, Insteon, UWB, ZigBee и прочих.

Топология «Звезда» служит основой организации всех современных сетей связи и вычислитель- ных сетей. Данную топологию используют протоколы WI-FI, Insteon, ZigBee, UWB, IDEN, CDMAOne, WIMAX, GSM, GPRS, UTMS.

Топология «многоячейковая сеть» — базовая полносвязная топология компьютерных сетей и сетей связи, в которой каждая рабочая станция сети соединяется со всеми другими рабочими станциями этой же сети. Достоинством этой топологии является высокая отказоустойчивость, а недостатками сложность настройки и избыточным расходом кабеля в проводных сетях. Каждый узел имеет несколько возможных путей соединения с другими узлами, за счет этого такая топология очень устойчива. Так как исчезновение одного из каналов не приводит к потере соединения между двумя компьютерами.

Топология «Кластерное дерево» образуется в основном в виде комбинаций вышеназванных топологий вычислительных сетей. Основание дерева вычислительной сети располагается в точке (корень), в которой собираются коммуникационные линии информации (ветви дерева). Вычислительные сети с древовидной структурой строятся там, где невозможно непосредственное применение базовых сетевых структур в чистом виде.

* Выделяют 2 типа сетевых атак:

- внешние атаки: выполняется группой хакеров или индивидуалами, которые владеют техникой для выполнения атаки. Выполняется атака путём сканирования системы и сбором информации. Для предотвращения атак можно выполнять трассирование портов на коммутаторах, к которым присоединены чужие устройства и блокировка данных портов;

- внутренние атаки: выполняются бывшими или действующими сотрудниками компании. Один из способов защиты является развёртывание системы обнаружения вторжений(IDS) и конфигурирования её для сканирования системы на предмет как внешних, так и внутренних атак.

Никто «в лоб» взламывать систему не будет. Первым делом взломщик пытается собрать как можно больше информации о сети, далее он создаёт карту сети для обнаружении открытых портов, типа операционных устройств и так далее. Хакер производит сбор информации о компании по доменному имени, используемому IP адресу, тестирование хостов в блоке IP адресов, использует такой инструмент как Nmap, которые позволяет определить какие операционные системы используются. Далее взломщик производит сканирование портов с целью найти открытые. Он это может сделать с помощью стробирования: когда атакующий пытается присоединиться к диапазону портов, которые открыты на хостах с операционными системами Linux, Windows. Для сканирования портов используется такой метод как развёртка, то есть огромный набор IP адресов сканируется с целью найти хотя бы один открытый порт. Также трафик может копироваться целиком, а потом анализироваться для поиска открытых портов. Используется такой метод как перебор. Атакующий пытается взломать пользовательские аккаунты, как правило, это аккаунты «по умолчанию», которые не имеют паролей, и производит сбор информации по приложениям на сети. Для получения доступа в систему программы типа Троян или специальные программы для взлома пароля (Wi-Lomster). Существует такой тип атак, как эскалация привилегий, то есть взломщик с минимальными правами пытается подняться до привилегий администратора, для контроля над системой. Это можно сделать с помощью документов с информаций об административных правах, паролей и ключей для регистрации паролей.

Нарушение работы беспроводной сети может вызвать атака типа Отказ в Обслуживании, основная задача которой не дать нормально пользоваться ресурсом. Эта атака может отправлять в сеть большое количество некорректных данных, запросов вследствие чего сеть становится перегруженной, физически повреждать сеть.

Рассмотрим варианты, которые помогут защитить которые беспроводную сеть от хакинга:

1. SSID Cloaking — скрытие имени сети. Доступ разрешается только клиентам, которые знают это имя.

2. MAC Filtering — фильтрация по MAC адресам. Доступ разрешается только клиентам, адреса сетевых адаптеров которых записаны в точке доступа.

Эти два метода помогут ограничить доступ к сети, то есть, но даже если все эти средства включены на точке доступа, злоумышленник сможет, включив свой беспроводной адаптер в «monitor mode», слушать эфир и вылавливать всю передаваемую информацию. Следующие методы криптографически защищают данные:

1. WEP — статистически самый используемый метод защиты беспроводной сети. Предоставляет шифрование всех передаваемых по сети данных. Аутентификации, как таковой не имеет — если вы не знаете ключа, вы не сможете расшифровать данные. Минусы метода — очень слабый алгоритм, ключ взламывается очень быстро.

2. WPA и WPA2 Pre-Shared Key — сильная система аутентификации и шифрования данных. Доступ производится через общий ключ. Уровень защиты равен сложности общего ключа, так как система подвержена brute force атакам.

3. WPA и WPA2 Enterprise — вариант предыдущей системы, но для подтверждения личности используется внешний аутентификатор 802.1x EAP, что позволяет использовать сертификаты, смарт карты и т.д.

Существуют атаки с использованием снифферов (Sniffer attacks): атаки сниффинга - это процесс, когда атакующий использует специальные программы для перехвата и анализа сетевого трафика. Снифферы перехватывают, копируют и т.п. сетевую информацию, как, например, пароли и открытые пользовательские данные. В случае, когда кто-либо имеет физический доступ к сети, он может легко установить анализатор протоколов в сеть и копировать трафик. Можно выделить следующие снифферы, которые часто используются атакующими:

-Dsniff  
-Ethereal  
-Sniffit  
-Snort  
- Windump.

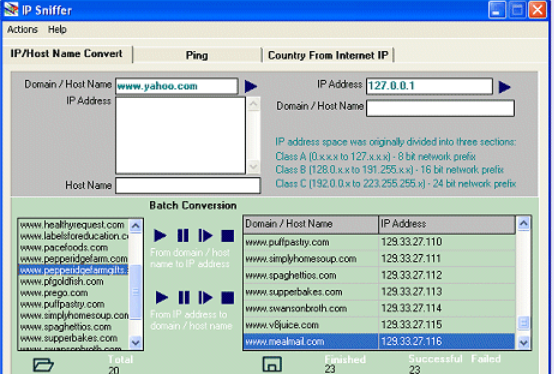


Рисунок 2. Прослушивание через сниффер.

Для защиты от снифферов используйте шифрование трафика, например, с помощью IPSec (Internet Protocol Security). В данном случае никакой перехваченный пакет не может быть интерпретирован в доступную форму.

Атаки на пароли (Password attacks): чаще всего основаны на подборе паролей для системы пока не будет определен верный. Одно из основных слабых мест в безопасности, связанных с контролем доступа по паролям, - то, что подход основан на корпоративном идентификаторе пользователя (user ID) и каком-либо пароле. Некоторые старые приложения не защищают передаваемые пароли. В таком случае пароли просто отправляются как обычный текст (не используется никакая форма шифрования). Огромная опасность, когда пользователь использует одни и те же логин и пароль ко всем системам. Тогда атакующий сразу получает доступ к целому ряду систем.

Итак, важно защищать не только пользовательские системы, но и хранилища с резервными копиями, так как при взломе возможна переустановка систем безопасности. Кроме того, важно определить систему определения вторжений для сбора данных, что пострадало, и кто за это стоит. Для защиты целостности данных, передаваемых по сети можно использовать цифровые подписи, для сохранения данных и их достоверности, постоянное резервное копирование информации, установка антивирусного программного обеспечения, использовать длинные пароли, конфигурирование фильтров на маршрутизаторах.

Список литературы:

1.     Дэвис Дж. Создание защищенных беспроводных сетей 802.11 в Microsoft Windows: справочник профессионала. Серия «Справочник профессионала»: пер. С англ. - М.: Издательство «ЭКОМ», 2006. -

2.     Пахомов Сергей, Афанасьев Максим. Беспроводные сети: ломаем, чтобы защищать / Компьютер Пресс. 06.2008.

3. <http://www.securitylab.ru>

4. <http://habrahabr.ru>

5. ТРУДЫ МФТИ. — 2012. — Том 4, № 2