ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ В БЕСПРОВОДНЫХ СЕТЯХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ковалев И.А, Радченко А.С., Ставров С.Д.
Бойправ О.В.. – к.т.н.

В современном мире беспроводные сети все более распространены за счет удобств, которые они предоставляют. Рост популярности этих сетей обуславливает увеличение количество выполняемых по отношению к ним атак. выделяют несколько причин реализации атак.

1. Взлом с целью похищения конфиденциальной информации.

2. Стремление воспользоваться чужим Интернет-соединением. В данном случае также происходит воровство, но не осязаемых конфиденциальных документов, а виртуальное - воровство Интернет-трафика. Если злоумышленник пользуется чужим интернет-каналом для сугубо утилитарных целей (электронная почта, веб-серфинг), то ощутимого материального урона он не нанесет, но, если локальная сеть организации используется как плацдарм для рассылки спама или последующей масштабной Интернет-атаки, последствия могут быть крайне неприятными как со стороны интернет-провайдера, так и со стороны контролирующих органов.

Поскольку радиосигналы имеют широковещательную природу, не ограничены стенами зданий и доступны всем приемникам, местоположение которых сложно или вообще невозможно зафиксировать – злоумышленникам особенно легко и удобно атаковать беспроводные сети. Поэтому, формально, даже случайный прохожий может заниматься радиоразведкой вашей сети – сугубо из любопытства. Огромное разнообразие готового инструментария анализа протоколов и уязвимостей, доступного в Интернете, позволяет ему без особых усилий совершить проникновение в корпоративную сеть.

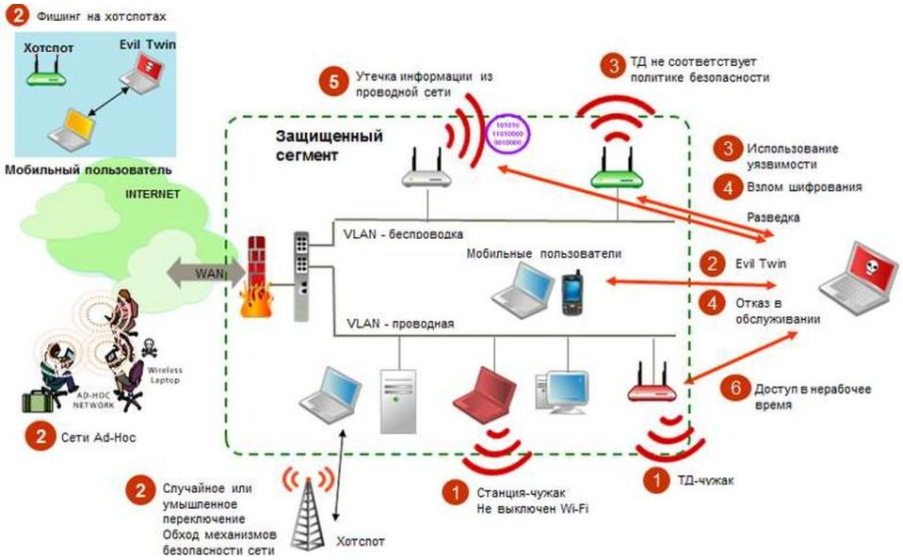

Рисунок 1 – Основные риски беспроводных сетей

Выделяют следующие основные причины реализации угроз информационной безопасности беспроводных информационных сетей.

1. Наличие в составе этой сети устройств, предоставляющих возможность неавторизованного доступа к корпоративной сети, зачастую в обход механизмов защиты, определенных корпоративной политикой безопасности. Чаще всего это те самые самовольно установленные точки доступа. Также в роли чужака могут выступить домашний роутер с Wi-Fi, программная точка доступа Soft AP, ноутбук с одновременно включенными проводным и беспроводным интерфейсом, сканер, проектор и т.д.

2. Нефиксированная природа связи, которая позволяет мобильным устройствам автоматически подключаться к сети. Таким образом, для доступа к информации злоумышленник имеет возможность переключить пользователя на свою точку доступа с последующей атакой или для поиска тонких мест в защите. Примерами являются фишинг на хотспотах, случайное или умышленное переключение, обход механизмов безопасности сети, сети Ad-Hoc, Evil Twin.

3. Уязвимости, связанные с конфигурацией сетей и подключаемых устройств. Некоторые сетевые устройства (точки доступа, беспроводные клиенты) могут быть более уязвимы, чем другие – неправильно сконфигурированы, использовать слабые ключи шифрования или методы аутентификации с известными уязвимостями.

4. Новые угрозы и атаки. Беспроводные технологии породили новые способы реализации старых угроз, а также некоторые новые, доселе невозможные в проводных сетях. Во всех случаях, бороться с атакующим стало гораздо тяжелее, т.к. невозможно ни отследить его физическое местоположение, ни изолировать его от сети. Злоумышленник как правило начинает атаки с предварительной разведки и зачастую совершает атаки типа «Отказ в обслуживании» (Denial of Service, DoS). Серьезной угрозой любой сети, не только беспроводной является имперсонация авторизованного пользователя и Identity Theft. Инструментарий для организации атак на беспроводные сети широко доступен и постоянно пополняется новыми средствами, начиная от всеми известного AirCrack и заканчивая облачными сервисами по расшифровке хешей.

5. Утечки информации из проводной сети. Практически все беспроводные сети в какой-то момент соединяются с проводными. Соответственно, любая беспроводная точка доступа может быть использована как плацдарм для атаки. Но это еще не все: некоторые ошибки в конфигурации точек доступа в сочетании с ошибками конфигурации проводной сети могут открывать пути для утечек информации. Наиболее распространенный пример – точки доступа, работающие в режиме моста (Layer 2 Bridge), подключенные в плоскую сеть (или сеть с нарушениями сегментации VLAN) и передающие в эфир широковещательные пакеты из проводного сегмента. Другой распространенный сценарий основывается на особенностях реализации протоколов 802.11. В случае, когда на одной точке доступа настроены сразу несколько ESSID, широковещательный трафик будет распространятся сразу во все ESSID. В результате, если на одной точке настроена защищенная сеть и публичный хот-спот, злоумышленник, подключенный к хот-споту, может нарушить работу протоколов DHCP или ARP в защищенной сети.

6. Особенности функционирования беспроводных сетей. Некоторые особенности функционирования беспроводных сетей порождают дополнительные проблемы, способные влиять в целом на их доступность, производительность, безопасность и стоимость эксплуатации. Для грамотного решения этих проблем требуется специальный инструментарий поддержки и эксплуатации, специальные механизмы администрирования и мониторинга, не реализованные в традиционном инструментарии управления беспроводными сетями. Такими проблемами являются активность в нерабочее время, точки доступа, разрешающие подключения на низких скоростях, интерференция радиосигналов, способная значительно ухудшить показатели пропускной способности и количества поддерживаемых пользователей, вплоть до полной невозможности использования сети.

Основные этапы, которые необходимо учитывать при построении системы безопасности беспроводных сетей:

– контроль доступа;

– аутентификация пользователей;

– шифрование трафика;

– система предотвращения вторжений в беспроводную сеть;

– система обнаружения чужих устройств и возможности их активного подавления;

– мониторинг радиоинтерференции и DoS-атак;

– мониторинг уязвимостей в беспроводной сети и возможности аудита уязвимостей;

– функции повышения уровня безопасности инфраструктуры беспроводной сетипо способу регистрации и усиления.

Методы повышения общего уровня безопасности беспроводной сети:

– аутентификация и авторизация всех пользователей сети WiFi;

– конфигурирование VLAN-ов для разделения трафика (например, гости/сотрудники, высокий уровень доступа/низкий уровень доступа и т.п.) и введения первичного, грубого сегментирования;

– использование межсетевых экранов на уровне портов для формирования более тонкого уровня безопасности;

– использование шифрования на всей сети для обеспечения секретности;

– определение опасности целостности сети и применение методов решения этих проблем;

– включение обеспечения безопасности конечных устройств в общую политику безопасности;

При использовании беспроводных сетей для передачи данных о держателях карт, следует использовать технологию WPA (WPA2), IPSEC VPN, либо SSL/TLS. Не следует полагаться только технологию WEP для защиты конфиденциальных данных в беспроводных сетях.