Безопасность беспроводных сетей

Выполнил: Теванян А.А.
Группа: ФК 1-3

Содержание

1.Что такое беспроводные сети?
2.Современные беспроводные технологии
3. Вопросы безопасности беспроводных соединений

Что такое беспроводные сети?

Беспроводные сети представляют собой недорогой метод соединения информационных систем, просты в установке и работе. Однако она ведет к возникновению серьезных вопросов безопасности в организациях, использующих данный тип соединений.

Современные беспроводные технологии

В беспроводных локальных сетях главным образом используется группа стандартов технологии 802.11x (a, b, g и т. д.). Эти стандарты позволяют соединять рабочие станции каналами, с пропускной способностью до 54 Мбит/с, с использованием беспроводной точки доступа, которая подключается к кабельной сети или напрямую к другой рабочей станции.

Стандартные архитектуры

Для эффективного использования беспроводных локальных сетей (WLAN) на предприятии необходимо обеспечить достаточную зону покрытия в областях, где сотрудники или посетители организации будут размещать свои компьютеры. В помещениях радиус действия обычной беспроводной системы стандарта 802.11x WLAN составляет, как правило, около 50 метров. Вне помещения радиус действия может достигать 500 метров. Следовательно, точки доступа (AP) должны размещаться так, чтобы обеспечивать область покрытия в соответствующих областях.

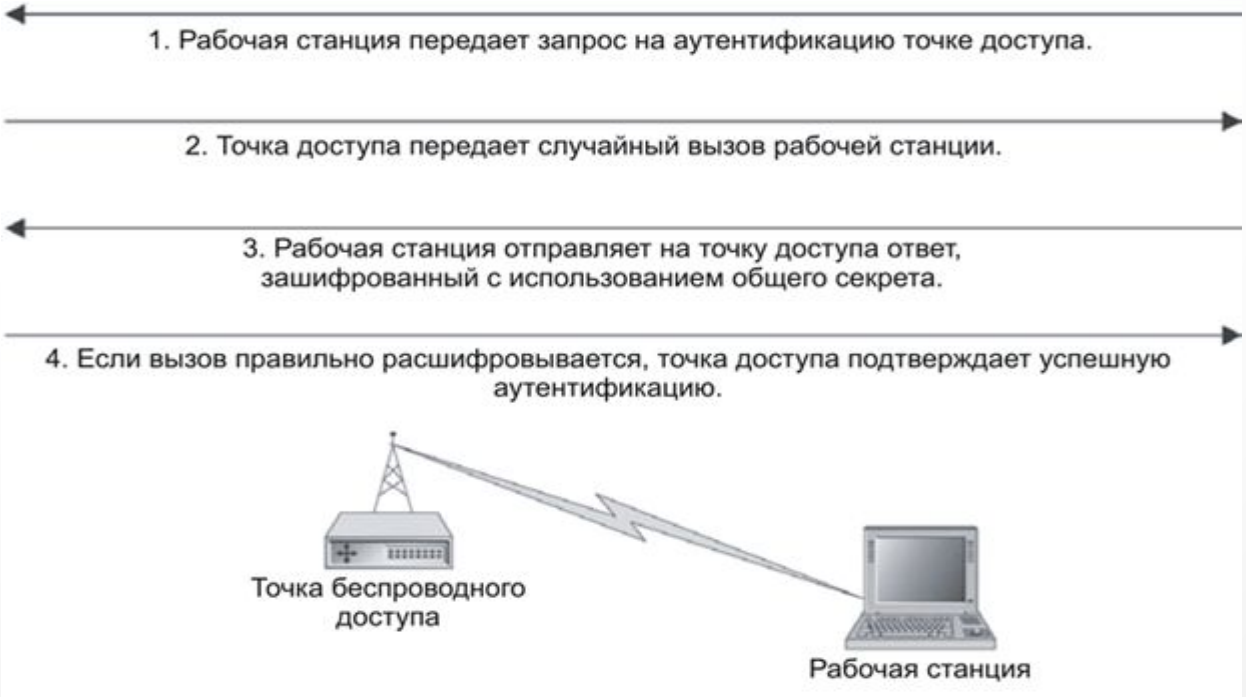
Реальный радиус действия определяется используемым оборудованием, а также формой и материалами, из которых сделаны окружающие физические объекты.

Безопасность передачи данных

Беспроводные сети используют воздух и пространство для передачи и приема информации (сигналы являются открытыми для любого лица, находящегося в зоне действия), что требует должной защиты конфиденциальности и целостности информации при ее передаче между рабочими станциями и точками доступа.

Стандарт 802.11x определяет протокол Wired Equivalent Privacy (WEP) для защиты информации при ее передаче через WLAN. WEP предусматривает обеспечение трех основных аспектов:

1) Аутентификация
2) Конфиденциальность
3) Целостность



Аутентификационный обмен WEP

Вопросы безопасности беспроводных соединений

Риски, связанные с использованием сетей WLAN, варьируются от прослушивания до направленных внутренних атак и даже атак, нацеленных на внешние сайты.

Обнаружение WLAN

NetStumber – утилита, которая работает в операционных системах семейства Windows и может использоваться совместно со спутниковым навигатором (ресивером глобальной системы позиционирования, GPS) для обнаружения беспроводных сетей WLAN. Она идентифицирует SSID сети WLAN, а также определяет, используется ли в ней WEP.

Обнаружить сети WLAN не составит особого усилия во время обхода нужного района или поездки по городу, обследование офисного здания с переносным компьютером в руках. Внешняя антенна не является необходимой, однако помогает расширить диапазон обнаружения, которым обладают утилиты.

Прослушивание

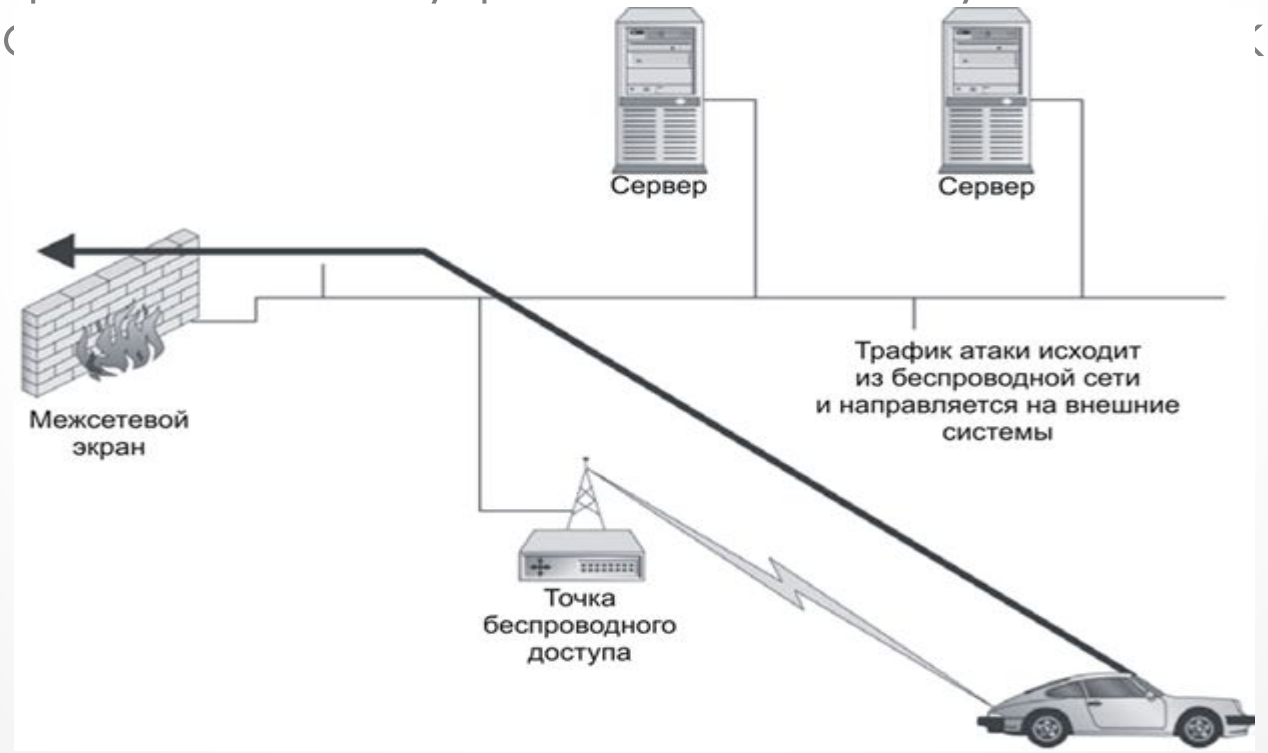
Беспроводные сети позволяют соединять с физической сетью компьютеры, находящиеся на некотором расстоянии от нее, как если бы эти компьютеры находились непосредственно в сети. Можно подключиться к беспроводной сети организации, располагающейся в здании, человеку, сидящему в машине на стоянке рядом с ним.

Даже при надежной аутентификации, которую должны проходить все пользователи для доступа к секретным файлам и системам, злоумышленник может без труда добыть секретные сведения посредством пассивного прослушивания сети. Атаку посредством пассивного прослушивания практически невозможно обнаружить.

Активные атаки

Преодоление периметра сетевой защиты организации, где размещают большую часть средств безопасности (межсетевые экраны, системы обнаружения вторжений и т. д.). Расположенные внутри периметра системы, как правило, защищены в гораздо меньшей степени.

Вместо проведения внутренних атак злоумышленник может ис и извне.



Атака на внешние системы

Реализация безопасности беспроводных сетей

Реализация WLAN должна предваряться полной оценкой рисков, связанных с проектом. Необходимо провести изучение потенциальных угроз, выявить любые имеющиеся контрмеры, принять дополнительные меры для снижения рисков.

Безопасность передачи данных

Даже, несмотря на серьезные уязвимости, присутствующие в WEP, необходимо использовать этот протокол. Защита WEP может быть преодолена, однако для этого потребуется много усилий, и нет никаких причин для того, чтобы позволять злоумышленнику действовать совершенно свободно.

Принимая во внимание, что WEP недостаточно защищает важную информацию, рекомендуется использовать иной тип системы шифрования, помимо WLAN. Следует применять VPN при соединении рабочих станций WLAN с внутренней сетью. Большая часть VPN-продуктов предусматривает надежные алгоритмы шифрования, в которых отсутствуют недостатки, присущие WEP.

Размещать WLAN, лучше всего, в зоне, защищаемой межсетевым экраном или другим устройством контроля доступа, и использовать VPN при соединении с этой системой.

Безопасность рабочей станции

Если злоумышленник хочет проникнуть в сеть WLAN, то будет использовать снифферы для обнаружения других рабочих станций. Даже если не получится проникнуть во внутренние системы или прослушать информацию, передаваемую в сети, он сможет атаковать другие рабочие станции.

Необходимо установить соответствующее антивирусное ПО. Но если риск велик, на рабочих станциях следует применить еще персональные межсетевые экраны.

Безопасность сайта

Не существует различия между сетями WLAN и подобными системами: их необходимо отделять от внутренней сети. Следовательно, сети WLAN необходимо развертывать в отдельных сегментах сети и установить межсетевой экран между сетью WLAN и внутренней сетью организации.

Наряду с сегментацией сети следует установить в WLAN систему обнаружения вторжений для выявления несанкционированных посетителей. И тогда при осуществлении попытки выполнения какой-либо активной атаки, вы будете уведомлены.

При использовании рабочей станции в сети WLAN необходимо использовать надежный механизм аутентификации. Стандарт 802.1X предусматривает более надежную аутентификацию, нежели SSID или MAC-адрес, однако он не защищен от перехвата сеанса соединения. Использование надежной аутентификации совместно с VPN значительно снизит возможность злоумышленника получить доступ к внутренним системам.

Нелегальные и несанкционированные точки доступа также представляют собой проблему, которую организации должны разрешать с целью предотвращения неприятностей. Выявлять данные точки можно с помощью таких утилит, как NetStumber или средства обнаружения точек доступа во внутренней сети APTools.

Спасибо за внимание!