ЗАЩИТА КОМПЬЮТЕРНЫХ БЕСПРОВОДНЫХ СЕТЕЙ

1.1 Контроль границы сети

Граница сети – радиуса охвата радиосети.Такой контроль производится путем ограничения зоны распространения радиосигнала, что позволяет решить 2 задачи: снизить вероятность обнаружения радиосети и уменьшить расстояние, с которого злоумышленник может осуществлять активные или пассивные атаки.

Ограничить зону распространения радиосигнала границами физического периметра очень сложно. Однако при проектировании и развертывании радиосети стоит учитывать вопросы минимизации уровня сигнала.

Для ограничения радиуса охвата радиосети могут использоваться такие методы и средства как аттенюаторы (устройства, предназначенные для снижения уровня сигналов, обеспечивающие фиксированное или регулируемое затухание), снижение мощности передатчика встроенными средствами точки доступа, использование направленных антенн и просто правильная ориентация антенн в пространстве. Эффективным способом является выбор места размещения точек доступа в отдалении от границ здания.

Для сетей с высокими требованиями к безопасности могут применяться дополнительные методы, такие как покраска стен помещений с помощью специальной краски, обладающей высоким коэффициентом поглощения в частотном диапазоне, используемом радиосетями. Достаточно радикальным методом, применяемым в серверных комнатах, или в других критичных помещениях является установка помехи в частотном диапазоне радиосетей. Для этого используются специализированные генераторы шума.

Однако не стоит чрезмерно увлекаться снижением мощности передатчиков, поскольку это негативно сказывается на пропускной способности сети, а доступность радиосети — один из немаловажных аспектов ее безопасности.

1.2 Скрытие SSID

В служебных фреймах Beacon и ProbeResponse точка доступа отправляет идентификатор сети и другие служебные данные.

Стандартом предусмотрена и в большинстве точек доступа реализована возможность отключать широковещательную рассылку SSID. Этот режим обычно называется disablessidbroadcast или noguestmode. В результате в поле SSID во фреймах Beacon и ProbeResponse будет указываться пустая строка. Такие сети не будут отображаться в утилитах типа Netstumbler и не будут видны в списке доступных сетей стандартного беспроводного клиента.

Все станции в сети, подключенные к точке доступа, знают SSID и при подключении, когда рассылают ProbeRequest запросы, указывают

РЕПОЗИТОРИЙ ГГУ ИМЕНИ ФРАНЦИСКА СКОРИНЫ

Создано демо-версией Универсального Конвертера Документов. Полная версия не добавляет этот штамп.
WWW.PRINT-DRIVER.RU

идентификаторы сетей, имеющиеся в их профилях подключений. Если точка доступа отвечает на такой фрейм, значит, ее SSID совпадает со значением, указанным в запросе, и можно приступать к процедуре подключения.

Однако данный способ не обеспечивает должного уровня защиты, так как злоумышленник, прослушивающий сеть в режиме мониторинга, имеет возможность узнавать идентификатор сети. Существует большое количество утилит, работающих по такому принципу, например, популярный анализатор беспроводных сетей Kismet. Однако, несмотря на свои недостатки, данный механизм защиты безусловно, является полезным для обеспечения защищенности сети.

1.3 Аутентификация IEEE 802.11X

При использовании протокола 802.1X станция, физически подключающаяся к сети, не получает доступа к другим узлам до прохождения аутентификации. За реализацию этой функции отвечает активное сетевое оборудование (коммутатор, точка доступа), отключающее станции от сети до получения положительного вердикта об их аутентичности. Устройство, выполняющее подобные функции, называется аутентификатором (Authenticator). Протокол 802.1X реализован в большинстве точек доступа и беспроводных коммутаторов.

Часть программного обеспечения подключающейся станции, воспринимающее запросы аутентификатора и реализующее клиентскую часть протокола проверки идентичности, носит название инициатора (Supplicant).

Функции аутентификации не выполняются непосредственно на коммутаторе, аутентификатор используется в качестве сервера-посредника между инициатором и третьим компонентом 802.1X, сервером аутентификации (AuthenticationServer). В роли сервера аутентификации может быть использована практически любая реализация сервера RADIUS.

При подключении к сети аутентификатор посылает инициатору по протоколу ExtensibleAuthenticationProtocoloverLAN (EAPOL) запрос на аутентификацию. Если клиент не поддерживает 802.1X, запрос игнорируется, и станция не имеет возможности взаимодействия с сетью. В противном случае клиент инициирует протокол проверки подлинности, в ходе которого происходит взаимная аутентификация сервера RADIUS и подключаемой станции. Аутентификатор преобразует запросы EAPOL в команды протокола RADIUS и обратно. Если клиент успешно прошел аутентификацию и авторизацию, сервер RADIUS дает аутентификатору команду на подключение к сети, после чего станция получает возможность взаимодействия в рамках контролируемого коммутатором или точкой доступа сегмента. Дополнительно сервер RADIUS может генерировать и передавать точке доступа и подключаемой станции ключи шифрования (WEP, PMK для WPA или WPA2).

РЕПОЗИТОРИЙ ГГУ ИМЕНИ Ф. СКОРИНЫ

Создано демо-версией Универсального Конвертера Документов. Полная версия не добавляет этот штамп.
WWW.PRINT-DRIVER.RU

1.4 Аутентификация по MAC — адресам

Большинство точек доступа и беспроводных коммутаторов позволяет указывать черные и белые списки MAC — адресов станций, которым запрещено (или разрешено) подключаться к сети. MAC — адрес — это 48-битный адрес для каждого устройства. Первые 24 бита относятся к производителю и являются общими для всех устройств, сделанных им. Оставшиеся 24 бита являются уникальными для каждого устройства. Обычно каждый сетевой адаптер нумеруется последовательно при помощи этого уникального номера, который является своеобразным идентификатором устройства для всей остальной сети.

Для ограничения доступа с помощью фильтрации MAC – адресов используют 2 метода:

- Точка доступа позволяет получить доступ только станциям, чьи MAC-адреса находятся в доверительном списке;
- Точка доступа запрещает доступ станциям, чьи MAC-адреса находятся в “чёрном списке”;

Наиболее надежным с точки зрения безопасности является первый вариант, хотя он не рассчитан на подмен MAC-адреса, что не так сложно осуществить злоумышленнику.

В результате при попытке установления ассоциации проверяется, разрешено ли станции с таким MAC — адресом подключатся к сети, и если нет, то отсылается фрейм Disassociate.

1.5 Конфигурирование структуры пакетов

В каждой сети структура пакета будет зависеть от множества показателей, а именно: используемой топологией и типом линий связи, используемой в сетях. Но есть общая структура создания пакета, которая и будет рассматриваться здесь. Давайте взглянем на рисунок 2, отображающий стандартную структуру пакета:

Рисунок 2 – Радиус действия беспроводных сетей

РЕПОЗИТОРИЙ ГГУ ИМЕНИ ФРАНЦИСКА СКОРИНЫ

Создано демо-версией Универсального Конвертера Документов. Полная версия не добавляет этот штамп.
WWW.PRINT-DRIVER.RU

Теперь давайте пройдемся по каждой составляющей в структуре пкаета:

- Преамбула - служит настройкой для сетевой карты (обработка пакетов и их прием)
- идентификатор приемника - идентификатор, который есть у каждого абонента в сети (сетевой адрес).
- идентификатор передатчика - тот же сетевой адрес, но принимающей стороны
- данные для управления обработкой - в этом поле содержатся основные ведения, касающиеся передаваемого пакета:
  - размер
  - формат
  - маршрут
  - тип
  - номер

- данные - основная информация, ради которой и используются пакеты, т.е. передаваемые данные
- контрольная сумма - специальное число, служащее проверкой целостности пакета
- стоповая комбинация - фиксирует окончание передачи пакета

Некоторые поля, в рассматриваемой структуре пакета, являются необязательными. Например, в некоторых сетях поле преамбула отсутствует. А некоторые сети сами могут фиксировать окончание приема пакетов (при использовании самосинхронизирующихся кодов), что позволяет еще упростить структуру пакета и отбросить стоповую комбинацию.

Задача для злоумышленника довольно сильно усложнится, если использовать нестандартную структуру пакетов. В рамках применения данного механизма защиты скрывается SSID и настраиваются параметры точки доступа. Благодаря этому злоумышленнику становится трудно анализировать пакеты.

1.6 Криптозащита

Одними из наиболее эффективных методов защиты информации на сегодняшний день являются криптографические методы защиты информации. Если мы говорим о беспроводных сетях, то широкое распространение для защиты БС приобрели два алгоритма:

- WEP, основанный на RC4,
- WPA, основанный на AES.

Первоначально широкое распространение в различных системах обеспечения беспроводного доступа к цифровым сетям получил алгоритм WEP, с помощью которого осуществляется шифрование трафика, затрудняющее анализ последнего сканирующей аппаратурой. Для шифрования данных стандарт предоставляет возможности шифрования с

РЕПОЗИТОРИЙ ГГУ ИМЕНИ ФРАНЦИСКА СКОРИНЫ

Создано демо-версией Универсального Конвертера Документов. Полная версия не добавляет этот штамп.
WWW.PRINT-DRIVER.RU

использованием алгоритма RC4 с 40-битным разделяемым ключом, разработанным РономРайвестом, одним из основателей компании RSA DataSecurity.

Достоинства алгоритма WEP:

- возможность периодической смены ключа и частой смены вектора инициализации;
- самосинхронизация шифра по каждому сообщению, что снижает вероятность потери пакетов;
- эффективность алгоритма и возможность его реализации как программными, так и аппаратными средствами;
- статус дополнительной возможности, что позволяет пользователю самому решать вопрос об использовании этого алгоритма.

Однако эта простая система защиты трафика недостаточно устойчива к некоторым вариантам атак. Система защиты БС, основанная на WEP со статическими ключами, не соответствует условиям безопасной эксплуатации. Это потребовало усовершенствования процедур аутентификации и работы WEP. Версия WEP2 защищена надежнее своей предшественницы благодаря 128-разрядному вектору инициализации IV и 128-разрядным ключам. В то же время в ней применены прежние алгоритм шифрования RC-4 и схема контроля целостности. Усовершенствования версии WEP2 устраняют проблему конфликтов IV, но совместное администрирование WEP-ключей в различных системах и устранение уязвимости контроля целостности так и осталось без изменений.

Стандартом IEEE 802.11 не предусмотрены какие-либо механизмы управления ключами шифрования. По определению, алгоритм WEP поддерживает лишь статические ключи, которые заранее распространяются тем или иным способом между абонентами и точками доступа беспроводной сети. Поскольку IEEE 802.11 аутентифицирует физическое устройство, а не его пользователя, утрата абонентского адаптера, точки доступа или собственно секретного ключа представляют опасность для всей системы безопасности в целом. В результате при каждом подобном инциденте администратор сети будет вынужден вручную произвести смену ключей у всех абонентов и в точках доступа. Эти административные действия приемлемы для небольшой БС, но совершенно неприемлемы для сетей, в которых абоненты исчисляются сотнями и тысячами, и/или распределены территориально. В условиях отсутствия механизмов генерации и распространения ключей администратор вынужден пристально охранять абонентские адаптеры и оборудование инфраструктуры сети, что на практике является весьма трудновыполнимой задачей.

Следующим шагом на пути увеличения безопасности беспроводных сетей является применение нового алгоритма шифрования WPA , основанный на AES.

AES – это симметричный итерационный блочный шифр, оперирующий блоками данных размером 128 и длинной ключа 128, 192 или 256 бит – название стандарта соответственно «AES-128», «AES-192» и «AES-256»

РЕПОЗИТОРИЙ ГГУ ИМЕНИ Ф. СКОРИНЫ

Создано демо-версией Универсального Конвертера Документов. Полная версия не добавляет этот штамп.
WWW.PRINT-DRIVER.RU

Можно отметить следующие преимущества, относящиеся к аспектам реализации данного алгоритма:

- AES может выполняться быстрее, чем обычный блочный алгоритм шифрования за счет выполнения оптимизация между размером таблицы и скоростью выполнения;
- преобразование раунда допускает параллельное выполнение, что является важным преимуществом для будущих процессоров и специализированной аппаратуры;
- алгоритм шифрования не использует арифметические операции, поэтому тип архитектуры процессора не имеет значения;
- алгоритм шифрования полностью «самоподдерживаемый», то есть он не использует других криптографических компонентов;
- длины блоков от 192 до 256 бит позволяют создавать хэш — функции без коллизий, использующие AES в качестве функции сжатия;
- разработка позволяет специфицировать варианты длины блока и длины ключа в диапазоне от 128 до 256 бит с шагом в 32 бита;
- хотя число раундов AES зафиксировано, в случае возникновения проблем с безопасностью оно может модифицироваться и выступать в качестве параметра .

Недостатком же алгоритма можно считать лишь примененную в нем нетрадиционную схему – она содержит некоторые скрытые уязвимости.

1.7 Оптимизация конфигурации беспроводного сегмента сети

Во многих случаях угрозой является неправильно сконфигурированный беспроводной сегмент сети. В этом случае необходимо улучшение конфигурации. Это может быть изменение конфигурации конфигурации всей сети или отдельных её компонентов.

РЕПОЗИТОРИЙ ГГУ ИМЕНИ ФРАНЦИСКА СКОРИНЫ

Создано демо-версией Универсального Конвертера Документов. Полная версия не добавляет этот штамп.
WWW.PRINT-DRIVER.RU

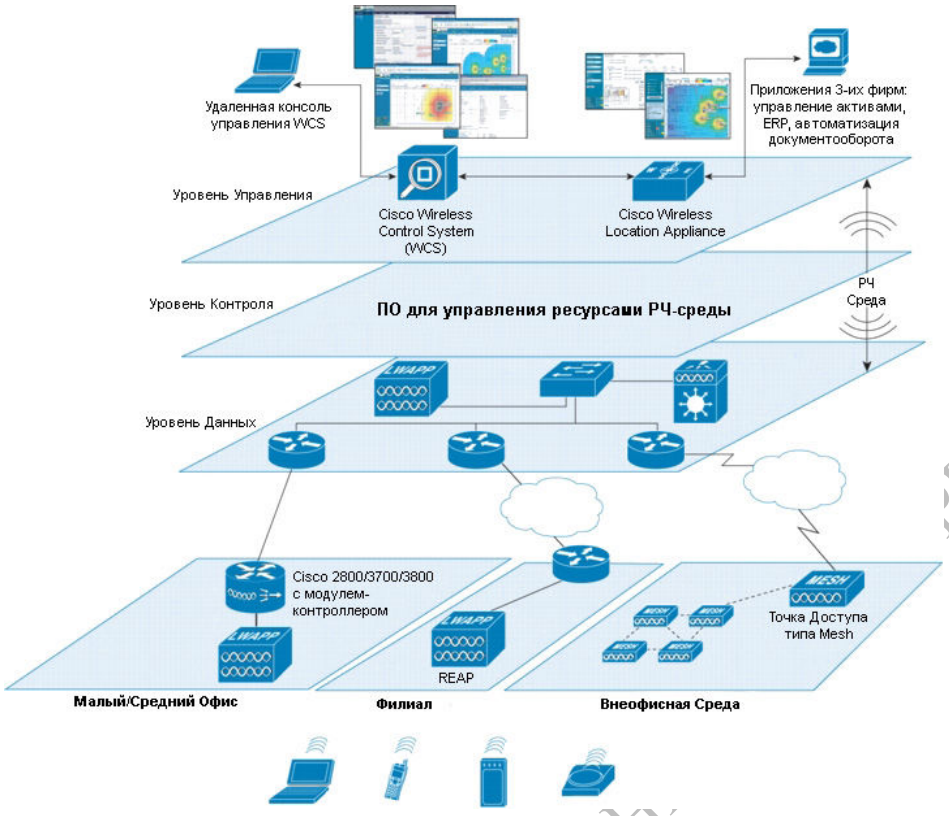

Рисунок 3 – Схема подключения "облегченной" точки доступа

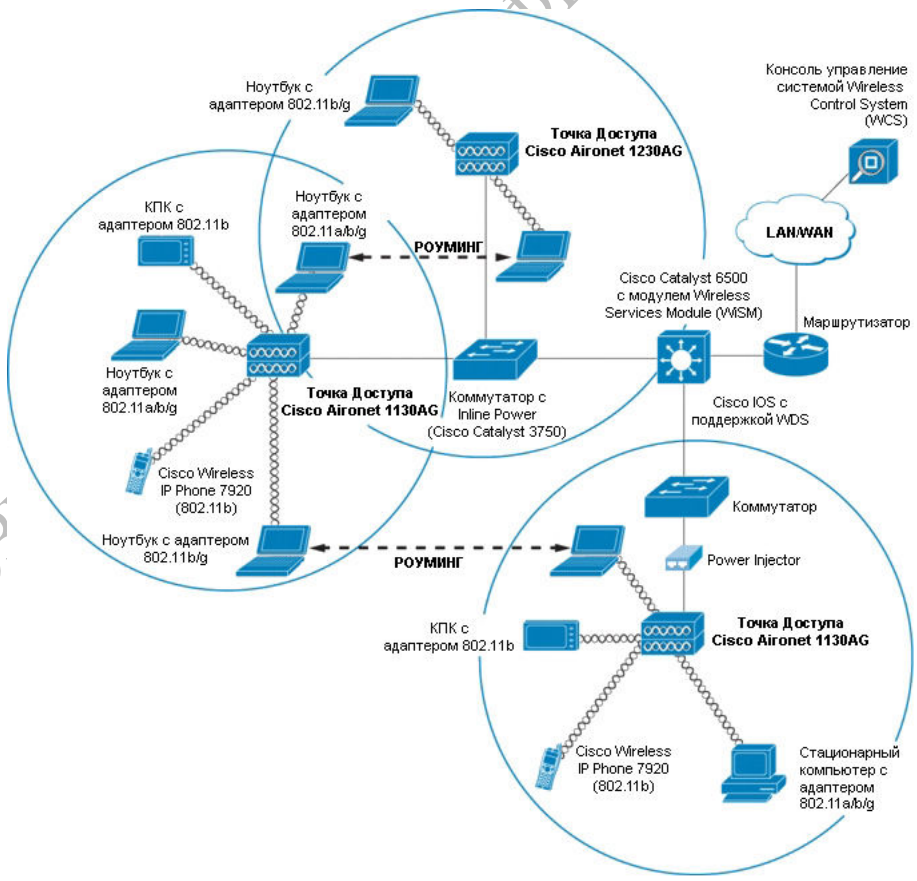

Рисунок 4 – Схема подключения автономной точки доступа

Создано демо-версией Универсального Конвертера Документов. Полная версия не добавляет этот штамп.
WWW.PRINT-DRIVER.RU