1. Основные стандарты Wi-Fi (набор стандартов 802.11).
2. Сравнение стандартов беспроводной передачи данных.
3. Принцип организации Wi-Fi.
4. Классификация беспроводной сети Wi-Fi
5. Преимущества и недостатки сети Wi-Fi
6. Архитектура, компоненты сети Wi-Fi.
7. Типы и разновидности соединений.
8. Безопасность сети Wi-Fi (основные методы и протоколы защиты).
9. Протокол шифрования WEP (принцип шифрования, основные уязви-

мости).

**Принцип шифрования**

Основан на алгоритме RC4, который реализован в виде симметричного потокового шифрования. Генерируется ключевой поток, с помощью специальной функции, и этот ключевой поток суммируется с потоком данных по модулю два. Дешифрация – генерация этого же потока и зашифрованного потока по модулю два, тем самым получая исходные данные.

Существует 2 вида шифрования: потоковое и блочное.

Потоковое – побитовое сложение по модулю 2. Длина ключа равна длине кодируемого сообщения.

Блочное – Исходное сообщение разбивается на блоки, и каждый блок отдельно складывается побитово с ключом

Данные в виды шифрования используют метод электронной книги (ECB). Это значит что одно и то же исходное сообщение – всегда одно и то же зашифрованное сообщение на выходе. Это недостаток, который исправляют с помощью вектора инициализации и обратной связи.

С помощью вектора инициализации изменяют ключевую последовательность при каждой новой отправке сообщения

Обратная связь работает в блочном шифровании: каждый новый блок суммируется по модулю два с зашифрованным предыдущим, а для первого блока генерируется ключ с помощью вектора инициализации.

**Основные уязвимости:**

*Пассивные сетевые атаки:*

Некоторые векторы инициализации дают возможность установить побайтовый состав секретного ключа, применяя статистический анализ.

*Активные сетевые атаки:*

Индуктивное вычисление секретного ключа :

- Повторное использование вектора инициализации: хакер отправляет жертве различные пакеты данных, и прослушивает его сеть, получая зашифрованные пакеты. Далее применяет функцию XOR (сложение по модулю 2), воссоздавая вектор инициализации и ключ шифрования. Такую ключевую последовательность можно будет «вырастить» для любой длины, хакер методом подбора находит нужный новый байт, ведь на правильную ключевую последовательность, точка доступа в атакуемой сети ответит однозначно.

- Манипуляция битами:

Опирается на уязвимость вектора контроля целостности. Хакер манипулирует битами канального уровня с целью икажения пакетов 3 его уровня.

Алгоритм: Какое то время читает трафик жертвы, далее захватывает пакет, произвольно меняет биты протокола третьего уровня. Модифицирует вектор контроля целостности. Передает модифицированный фрейм в локальную сеть. Принимающая сторона проверяет контроль целостности, и анализирует данные протоколоа 3 его уровня, а там моифицированные хакером данные. Тогда обратно в сеть отправляется зашифрованное сообщение об ошибке. Хакер с помощью данного сообщения вычисляет ключевую последовательность (как в предыдущем случае).   
 Вычисления вектора целостности сообщения : Исходный фрейм имеет вектор С1. Содается фрейм F2 такой же длины и делается XOR. Так мы создаем модифицированный фрейм F3. Вычисляется промежуточный вектор C2 для F3. Далее XOR C1 и C2 – получаем C3 – нужный нам вектор целостности.

1. Протокол шифрования WPA (принцип шифрования, основные уяз-

вимости).

**Принцип шифрования**

Усовершенствованный протокол TKIP вместо RC4

-Пофреймовое изменение ключей шифрования:

Базовый WEP ключ смешивается со старшими 32 разрядами вектора инициализациии MAC адресом передатчика. Получаем ключ первой фазы

Ключ 1 фазы + вектор инициализации + MAC-адрес

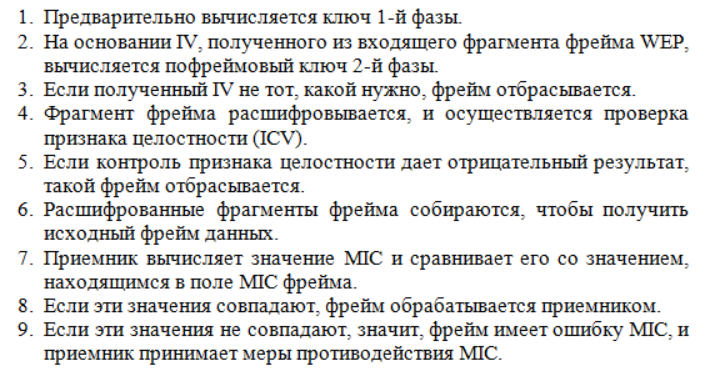
Через пофреймовый ключ вычисляется новая ключевая последовательность, и применяется алгоритм RC4. И так для каждого фрейма.

Для контроля целостности сообщения применяется алгоритм MIC. MIC имеет уникальный ключ, который перемешивается с MAC-адресом источника и MAC-приемника, а также со всей незашифрованной частью фрейма.

Алгоритм TKIP

1. Генерируется пофреймовый ключ как описано выше
2. Генерируется вектор контроля целостности с помощью алгоритма MIC
3. Фрейм шифруется с помощью пофреймового ключа
4. Передача зашифрованного фрейма

Дешифровка сообщения



**Уязвимости**

1. Протоколы аутентификации в сети Wi-Fi (использующей техноло-

гию 802.11X).

**Open system authentication**

В случае если используется аутентификация типа Open System, то клиент отсылает точке доступа запрос с её идентификатором (MAC-адресом). Точка доступа проверяет, проходит ли клиент по списку MAC-адресов (если он включен), затем соответствие WEP-ключей (если включено WEP-шифрование). Поддерживается роуминг между точками доступа.

Используемые шифры: без шифрования, статический WEP, CKIP.

**Open system authentication with eap**

Предыдущий вариант аутентификации может использоваться совместно с аутентификацией через протоколы EAP на RADIUS сервере.

Используемые шифры: без шифрования, динамический WEP, CKIP.

**Shared system authentication**

В этом случае клиент отсылает запрос на соединение к точке доступа. Затем точка доступа отсылает клиенту последовательность, которую он шифрует и отсылает обратно. Если последовательность зашифрована верно, то аутентификация проходит успешно. Внимание! В этом варианте защита слабее, чем в случае Open System!

Используемые шифры: без шифрования, динамический WEP, CKIP.

**WI-FI protected access (wpa)**

После появления первых атак на WEP, стало понятно, что требуется менять системы безопасности в беспроводных сетях. Тогда началась разработка нового стандарта 801.111. Для существующего оборудования было решено выпустить “промежуточный” стандарт WPA, который включал в себя новую систему аутентификации на базе 801.1х и новый метод шифрования TKIP. Существуют два варианта аутентификации: с помощью RADIUS сервера (WPA-Enterprise) и с помощью предустановленного ключа (WPA-PSK).

Используемые шифры: TKIP[стандарт], AES-CCMP [расширение], WEP[в качестве обратной совместимости].

**WI-FI protected access2 (wpa2, 801.111)**

WPA2 или стандарт 801.111- это финальный вариант стандарта безопасности беспроводных сетей. В качестве основного шифра был выбран стойкий блочный шифр AES. Система аутентификации по сравнению с WPA претерпела минимальные изменения. Также как и в WPA, в WPA2 есть два варианта аутентификации WPA2-Enterprise с аутентификацией на RADIUS сервере и WPA2-PSK с предустановленным ключом.

Используемые шифры: AES-CCMP [стандарт], TKIP [в качестве обратной совместимости].

Внимание! Некоторые производители под WPA с AES-CCMP подразумевают WPA2 с AES-CCMP. Далее чтобы не путаться под ШРАмы будем подразумевать WPA-TKIP (т.е. аутентификацию WPA с методом шифрования TKIP), а под WPA2 будем подразумевать WPA2 с AES-CCMP (т.е. аутентификацию WPA2 с методом шифрования AES-CCMP).

**Cisco centralized key management (cckm)**

Вариант аутентификации от фирмы CISCO. Поддерживает роуминг между точками доступа. Клиент один раз проходит аутентификацию на RADIUS-сервере, после чего может переключаться между точками доступа.

Используемые шифры: WEP, CKIP, TKIP, AES-CCMP

1. Коды обнаружения ошибок

Позволяют легко обнаружить ошибку. Используются в протоколах, где есть схема ARQ. В кратце, с каждым пакетом передается его контрольная сумма. Приемник также вычисляет контрольную сумму пакета, и если они не совпали, значит есть ошибка. Алгоритмы: контроль по паритету, вертикальный и горизонтальный контроль по паритету. Циклический избыточный контроль.

1. Коды с коррекцией ошибок

Для коррекции ошибок необходимо знать минимальное расстояние Хэмминга – минимальное число битовых разрядов, в которых отличается любая пара разрешенных кодов. Коды хэмминга, это блочные коды без памяти. Для схем контроля по паритету расстояние хэмминга равно 2, и при таком расстоянии коды хэмминга могут только обнаруживать ошибки.

14. Протоколы с автоматическим запросом повторной передачи

15. Выбор Wi-Fi роутера (основные параметры).

16. Основные угрозы безопасности Wi-Fi.

- нарушение физической целостности сети: …

- подслушивание трафика: …

- вторжение в сеть: …