	WEP (802.11)	WPA	WPA2 (802.11i)
Алгоритм	RC4 (потоковое)	RC4	AES
Размер ключа	40+24, 104+24	40+24, 104+24	128
ключ	статический	пофреймовый (TKIP)	блочный (CCMP)
Уязвимости	1) пассивные: сбор фреймов и стат. анализ (слабые IV) KSA 2)активные: повторное использование IV, манипуляция битами	брутфорс	krack
Особенности	Аутентификация физ. устройства, а не абонента;	1) Контроль целостности для предотвращения манипуляции битами (MIC) – уник. ключ 2) двойное смешивание при выработке ключевой последовательности	1) RSN – концепция повышенной безопасности, иерархия временных ключей 2) CCMP вычисляет MIC CBC-MAC
Аутентификация	1) Открытая (любой абонент) 802.11 2) Общий ключ (SKA) 802.11 3) MAC **not** 802.11 (сравнен. сервер)	1) Enterprise (сервер Radius) 2) PSK – персональн.	1) Enterprise (сервер Radius) 2) PSK – персональн.

<u>WEP</u>

Открытая аутентификация:
1) Фрейм Probe Request ➔
2) ➔ Фрейм Probe Response
3) Auth Request ➔
4) ➔ Auth Response
5) Ассоциирование Request ➔ (согласование SSID, пароля, сетевого режима a/b/g/n.., режим безопас. WEP,
6) ➔ Ассоциирование Response (WPA, WPA2, настройки канала)

Уязвимости WEP:
1. Идентификация SSID (фреймы Beacon, probe response)
2. Открытая auth – легитимность абонента?
3. SKA – xor cipher and open text
4. MAC передается в открытом виде (чел может подставить свой)

802.1x/EAP (Enterprise-режим)
Алгоритм аутентификации Extensible Authentication Protocol или EAP (расширяемый протокол идентификации) поддерживает централизованную аутентификацию элементов инфраструктуры беспроводной сети и ее пользователей с возможностью динамической генерации ключей шифрования

<u>Архитектура 802.1x</u>
1) Клиент (1) ассоциируется с аутентификатором, 3) EAP Response)
2) Аутентификатор (2) EAP Request indentity, 5) авторизован, передача всего трафика)
3) Сервер аутентификации (4) Radius-ACCEPT/REJECT)

Аутентификация по протоколу EAP.

- EAP-MD5 – не поддерживает динамическое распределение ключей, уязвим для атаки человек по середине (фальшивая AP), подслушивание запроса в ходе аутентификации).
- EAP-TLS – взаимная аутентефикация на базе сертификатов (нужен удостоверяющий центр)
- EAP-LEAP – От циско. Основано на паролях. Аутентифицирует пользователя, а не устройство (брутфорс)
- PEAP и EAP-TTLS – сертификат только у сервера. Как eap-tls, но не поддерживает утаревших PAP, CHAP. Вместо них PEAP-MS-CHAPv2, PEAP-EAP-TLS.

VPN

VPN отвечает трем условиям: конфиденциальность, целостность и доступность. Следует отметить, что никакая VPN не является устойчивой к DoS- или DDoS-атакам и не может гарантировать доступность на физическом уровне просто в силу своей виртуальной природы.

- **топология "сеть-сеть".** VPN-туннель между двумя географически разнесенными частными сетями;
- **топология "хост-сеть".** удаленные пользователи подключаются к корпоративной сети через Internet;
- **топология "хост-хост".** 2 хоста, обменивающихся друг с другом шифрованными и нешифрованными данными.

Распространенные туннельные протоколы

- **IPsec.** предоставляет службы аутентификации и шифрования данных на сетевом уровне. Протокол IPSec состоит из трех основных частей:
  • заголовка аутентификации (Authentication Header - AH);
  • безопасно инкапсулированной полезной нагрузки (Encapsulating Security Payload - ESP);
  • схемы обмена ключами через Internet (Internet Key Exchange - IKE).
- **PPTP.**
  Протокол определяет следующие типы коммуникаций:
  • PPTP-соединение, по которому клиент организует PPP-канал с провайдером;
  • Управляющее PPTP-соединение, которое клиент организует с VPN-сервером и по которому согласует
  характеристики туннеля;
  • PPTP-туннель, по которому клиент и сервер обмениваются зашифрованными данными.
- **L2TP.** Канальный уровень. Используется PPP с аутентификацией по протоколу PAP или CHAP, но, в отличие от PPTP, L2TP определяет собственный туннельный протокол. не содержит средств шифрования.

IDS – выявлять и своевременно предотвращать вторжения в вычислительные сети

1) на базе сети
2) на базе хоста

NIDS – анализируют трафик с целью обнаружения известных атак на основании имеющихся у них наборов правил

HIDS – устанавливаются непосредственно на узлах и осуществляют наблюдение за целостностью файловой системы

1) на основе сигнатур (события, происходящие в сети, сравниваются с признаками известных атак, которые и называются сигнатурами.)
2) на основе базы знаний (основанными на поведении или статистическими)

Из коммерческих решений хорошо известны программы AirDefense Guard и Isomair Wireless Sentry. Они основаны на размещении сенсоров на территории

Угрозы в WI-FI сетях

1) Прямые угрозы (человек посередине)
2) Чужаки (возможность неавторизованного доступа к корпоративной сети)
3) Некорректно сконфигурированные точки доступа
4) Некорректно сконфигурированные беспроводные клиенты
5) Взлом шифрования
6) Имперсонация и Identity Theft (кража личности)

Особенности функционирования беспроводных сетей

1) Активность в нерабочее время
2) Интерференция
3) Связь

Методы ограничения доступа

1) Фильтрация MAC-адресов
2) Режим скрытого идентификатора SSID (англ. Service Set IDentifier)

Cisco Centralized Key Managment (CCKM)
Вариант аутентификации от фирмы CISCO. Используемые шифры: WEP, CKIP, TKIP, AES-CCMP.

Атаки на Wi-Fi сети

Наиболее распространённые программы для сбора информации – это Kismet и Aircrack-ng suite. Другие программы: Dwepcrack (улучшенная FMS атака), AirSnot (FMS), WepLab (улучшенная FMS атака, атака Koreka).

1. Атаки на сети с WEP-шифрование

- **FMS-атака (Fluhrer, Martin, Shamir) – самая первая атака на сети с WEP-** шифрованием, появилась в 2001 году. Основана на анализе передаваемых векторов инициализации и требует, чтобы пакеты содержали «слабые» инициализационные вектора (Weak IV).
- **2. Атака KOREK'A (ник хакера, придумавшего атаку).** Количество требуемых уникальных IV – несколько сотен тысяч, для ключа длиной 128 бит. Главное требование – чтобы IV не совпадали между собой. Абсолютно не важно наличие слабых IV.
- **PTW-атака (Pyshkin, Tews, Weinmann).** прослушивание большого количества ARP-пакетов

Достаточно 10000-100000 пакетов. Самая эффективная атака на сеть с WEP-шифрованием.

Манипуляция с ICV

2. Атаки на сети с WPA/WPA2-шифрованием

уязвимости Hole196 в протоколе WPA2. Используя эту уязвимость, авторизовавшийся в сети злонамеренный пользователь может расшифровывать данные других пользователей, используя свой закрытый ключ. Никакого взлома ключей или брут-форса не требуется.
На сегодня основными методами взлома WPA2 PSK являются атака по словарю и метод грубой силы.

Атака по словарю на WPA/WPA2 PSK. PSK не знаем, знаем SSID, Authenticator Nounce (ANounce), Supplicant, Nounce (SNounce), Authenticator MAC-address (MAC-адрес точки доступа) и Suppliant MAC-address (MAC-адрес wifi-клиента). Через проверку MIC будет подбираться PSK.

<u>WPA2</u>

Кардинальными отличиями WPA2 от WPA стало индивидуальное шифрование данных каждого пользователя и более надежный алгоритм шифрования – AES. Долгое время основными методами взлома маршрутизаторов, работавших по WPA2, был взлом PIN-кода при подключении через WPS (Wi-Fi Protected Setup) или перехват рукопожатия и подбор ключа методом подбора «грубой силой». Обезопасить себя можно было, отключив WPS и установив достаточно сильный пароль.
KRACK – способа взлома сетей Wi-Fi, использующих WPA2. С этого момента эксперты стали считать протокол WPA2 ненадежным. Установить ПО.

Свойство	Статический WEP	Динамический WEP	WPA	WPA 2 (Enterprise)
Идентификация	Пользователь, компьютер, карта WLAN	Пользователь, компьютер	Пользователь, компьютер	Пользователь, компьютер
Авторизация	Общий ключ	EAP	EAP или общий ключ	EAP или общий ключ
Целостность	32-bit Integrity Check Value (ICV)	32-bit ICV	64-bit Message Integrity Code (MIC)	CRT/CBC-MAC (Counter mode Cipher Block Chaining Auth Code — CCM) Part of AES
Шифрование	Статический ключ	Сессионный ключ	Попакетный ключ через TKIP	CCMP (AES)
Распределение ключей	Однократное, вручную	Сегмент Pair-wise Master Key (PMK)	Производное от PMK	Производное от PMK
Вектор инициализации	Текст, 24 бита	Текст, 24 бита	Расширенный вектор, 65 бит	48-бит номер пакета (PN)
Алгоритм	RC4	RC4	RC4	AES
Длина ключа, бит	64/128	64/128	128	до 256
Требуемая инфраструктура	Нет	RADIUS	RADIUS	RADIUS

Нововведения WPA3

Для защиты от brute-force введено ограничение на число попыток аутентификации в рамках одного handshake.

Вместо PSK (Pre-Shared Key) ключа в WPA3 реализована технология SAE (Simultaneous Authentication of Equals). Компрометация закрытого ключа одной из сторон не приводит к компрометации сессионного ключа, т.е. даже узнав пароль атакующий не сможет расшифровать ранее перехваченный трафик.

Достоинства WPA3-Personal:

• пользователи могут выбирать легко запоминаемые пароли, не задумываясь о безопасности;

• новые алгоритм SAE обеспечивающий улучшенную защиту за счет изменения алгоритма авторизации;

• шифрование данных Forward Secrecy, защищает трафик данных, даже если пароль был скомпрометирован.

WPA3-Enterprise 192-bit mode

Individualized data encryption в WPA3

Упрощение настройки подключения WPA3 (WPS)

Enhanced Open – протокол, разработанный для защиты пользователя в открытой сети

	WEP	WPA	WPA2	WPA3
Release Year	1999	2003	2004	2018
Encryption Method	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol(TKIP) with RC4	CCMP and Advanced Encryption Standard	Advanced Encryption Standard(AES)
Session Key Size	40-bit	128-bit	128-bit	128-bit(WPA3-Personal) 192-bit(WPA3-Enterprise)
Clipher Type	Stream	Stream	Block	Block
Data Integrity	CRC-32	Message Integrity Code	CBC-MAC	Secure Hash Algorithm
Key Management	Not provided	4-way handshaking mechanism	4-way handshaking mechanism	Simultaneous Authentication of Equals handshark
Authentication	WPE-Open WPE-Shared	Pre-Shared Key(PSK)& 802.1x with EAP variant	Pre-Shared Key(PSK)& 802.1x with EAP variant	Simultaneous Authentication of Equals(SAE)&802.1x with EAP variant