Криптографические протоколы

Протоколы WEP, WPA, WPA2, WPA3

Деркач Максим Юрьевич

December 11, 2019

Ссылки

https://www.cs.jhu.edu/~Eastubble/dss/ae.pdf
http://cseweb.ucsd.edu/~mihir/papers/oem.pdf
https://habr.com/en/post/425637/

Введение

WEP (Wired Equivalent Privacy) - один из старейших протоколов безопасности, который может использовать WiFi-маршрутизатор, и он не очень безопасный. Он был использован в 1990-х годах, но с тех пор были разработаны другие протоколы безопасности.

WPA (Wi-Fi Protected Access) - это протокол, который первоначально заменило WEP как более безопасный способ хранения данных. В то время он был не идеален, но он лучше, чем WEP. Весь смысл разработки этого протокола состоял в том, чтобы преодолеть некоторые из основных недостатков WEP.

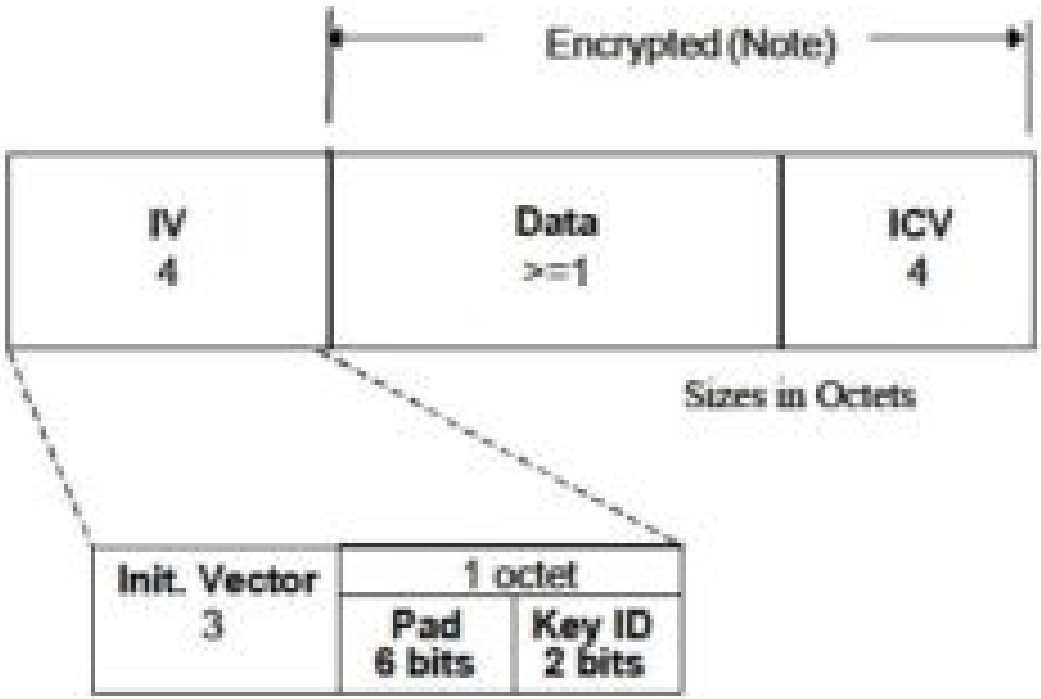
WEP

В основе WEP лежит поточный шифр **RC4**, выбранный из-за своей высокой скорости работы и возможности использования переменной длины ключа. Для подсчета контрольных сумм используется **CRC32**.

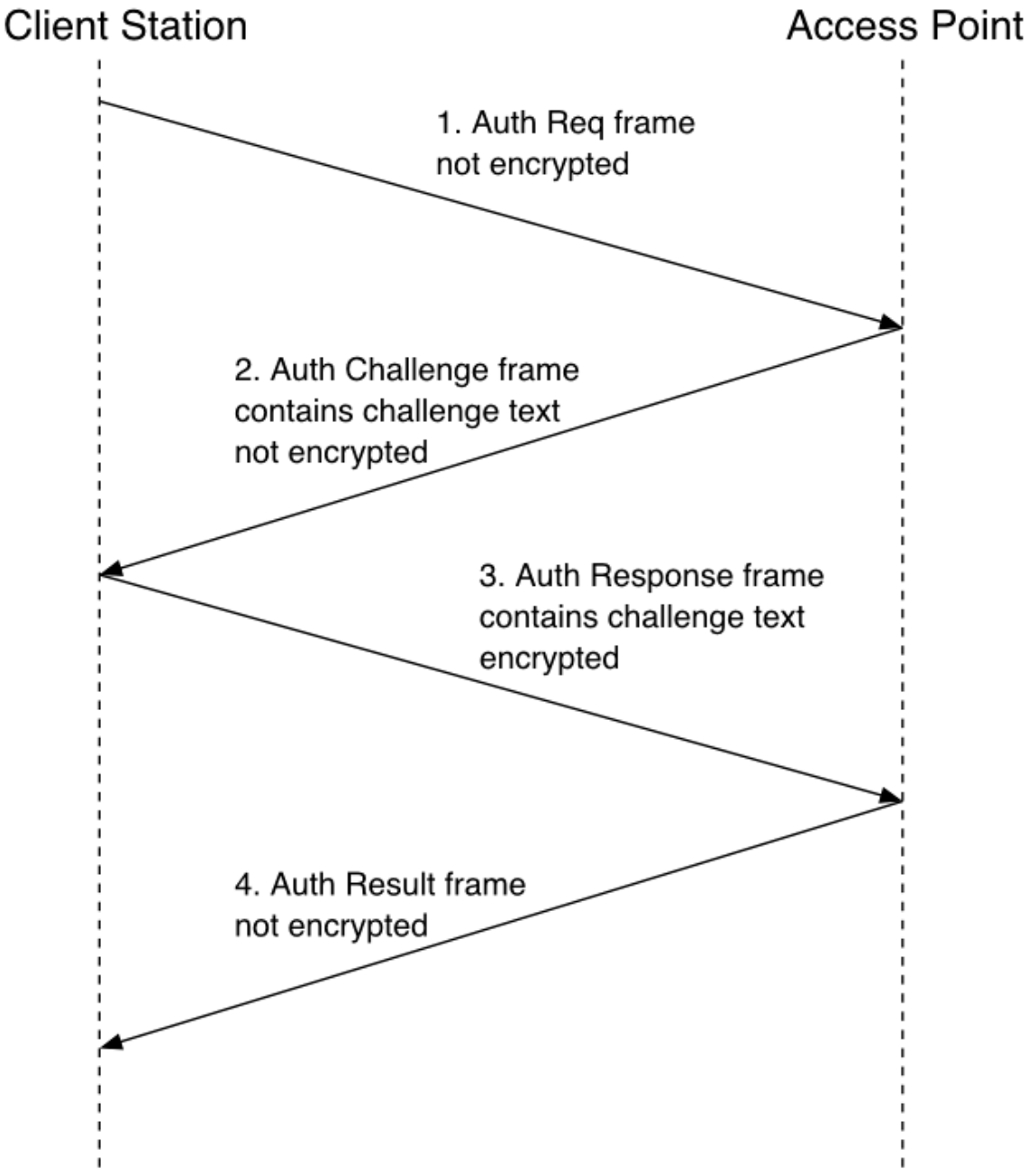
WEP

Пакет WEP протокола состоит из 2 частей:

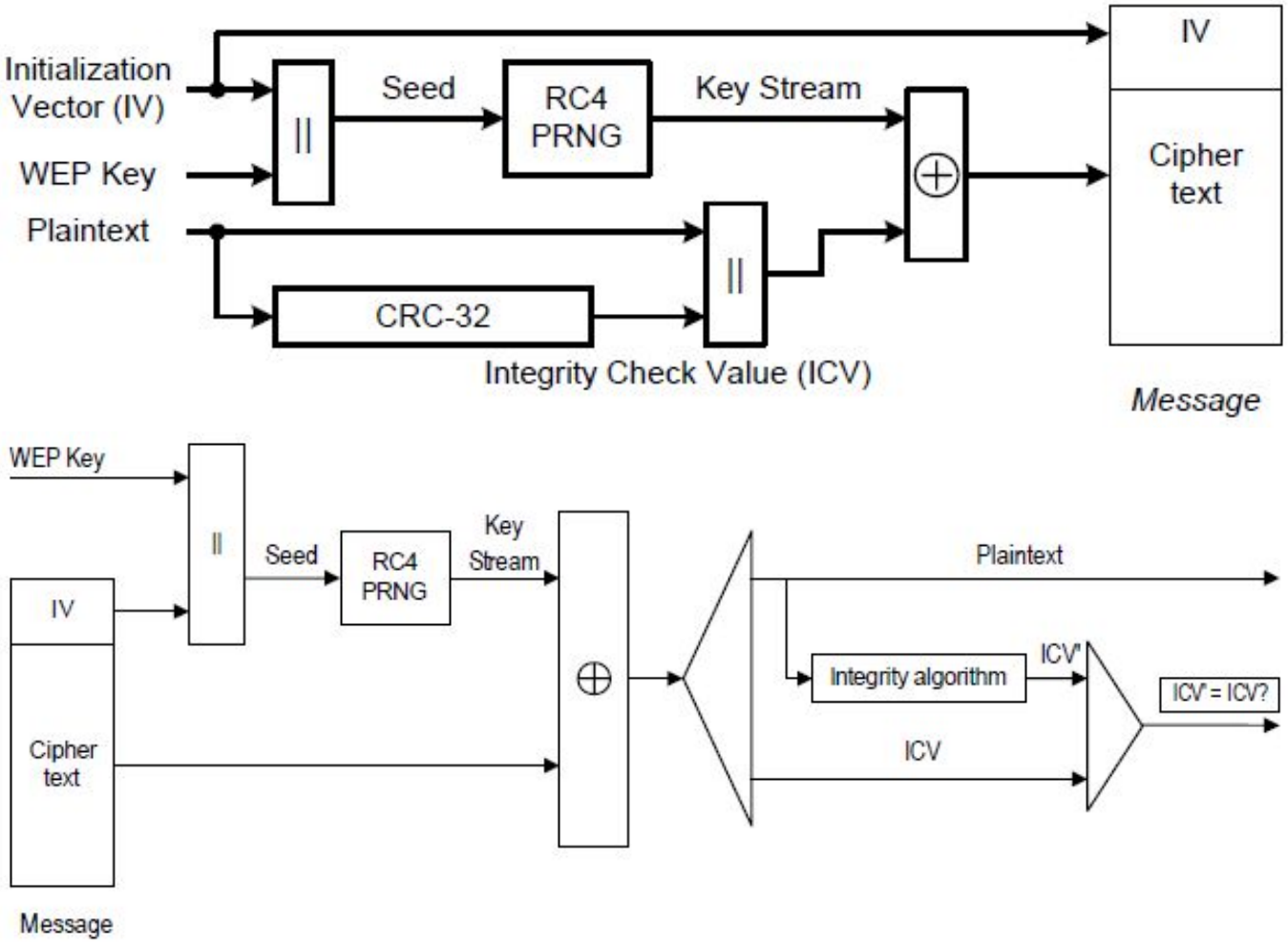
1. Открытые данные:
   - 1.1 Синхропосылка (IV) - 3 байта;
   - 1.2 Пустое место (Padding) - 6 бит;
   - 1.3 Идентификатор ключа (Key ID) - 2 бит;
2. Зашифрованные данные:
   - 2.1 Данные
   - 2.2 Контрольная сумма



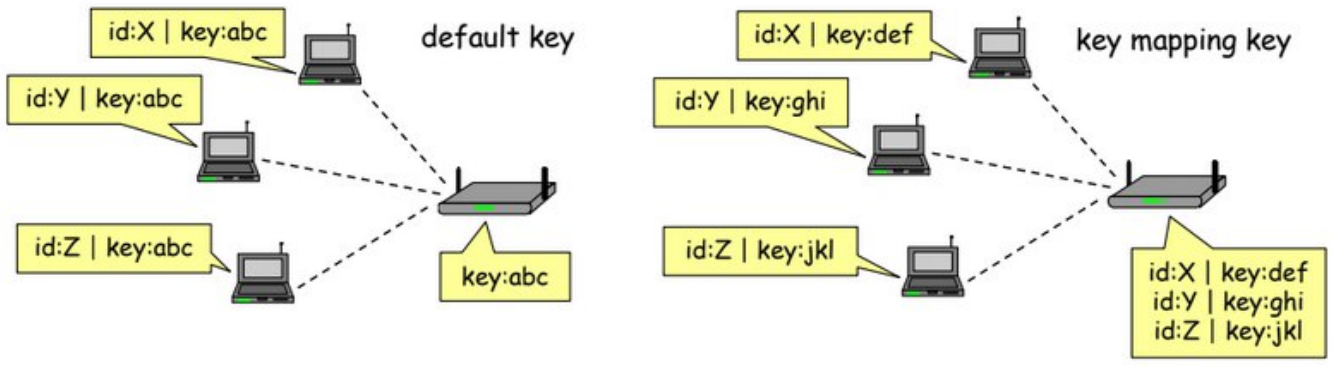
WEP Auth Protocol



WEP Encryption and Decryption



WEP Keys


id:X | key:abc
id:Y | key:abc
id:Z | key:abc
default key
key:abc
id:X | key:def
id:Y | key:ghi
id:Z | key:jkl
key mapping key
id:X | key:def
id:Y | key:ghi
id:Z | key:jkl

WEP Security

В протоколе WEP есть множество слабых мест:

1. Механизмы обмена ключами и проверки целостности данных:
   - В качестве MAC функции в WEP используется некриптографический алгоритм CRC.
2. малая разрядность ключа и вектора инициализации:
   - Повторное использование IV создает идентичные ключевые потоки, и поскольку длина IV мала, это гарантирует, что IV повторится через относительно короткое время (5-7 часов) в загруженной сети.
   - Стандарт 802.11 не описывал ограничения и правила на генерацию IV. Поэтому некоторые производители беспроводных адаптеров генерировали одинаковые последовательности IV, постоянное IV. В результате хакеры могли записывать сетевой трафик, определять поток ключей и использовать его для расшифровки зашифрованного текста.

WEP Security

1. Способ аутентификации:
   - Одностороняя аутентификация, AP - не аутентифициорован.
   - В результате аутентификация не устанавливается сессионный ключ.
2. Алгоритм шифрования.

Authentication

1. ...
2. $AP -> STA : r$
3. $STA -> AP : IV|r \oplus K$
4. ...

Атака

1. ...
2. $AP -> I(STA) : r'$
3. $I(STA) -> AP : IV|r' \oplus K$
4. ...

WEP Security

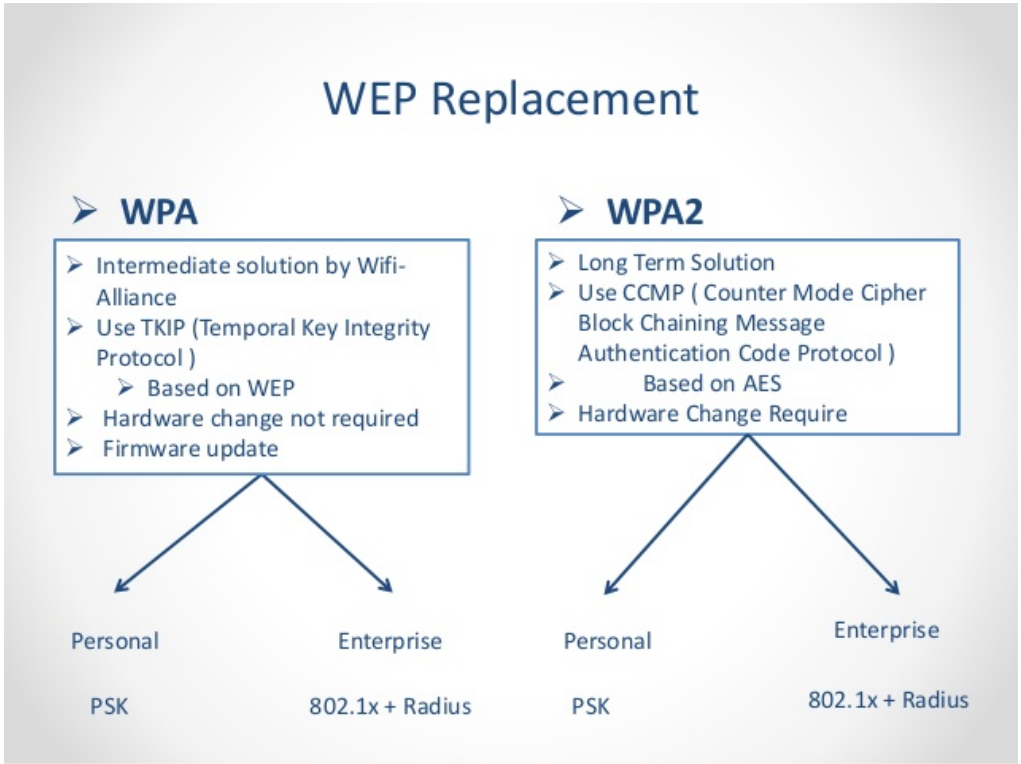
CRC:
$CRC(X \oplus Y) = CRC(X) \oplus CRC(Y)$

Атака
$((M|CRC(M)) \oplus K) \oplus (\hat{M}|CRC(\hat{M}) =$
$((M \oplus \hat{M})|(CRC(M) \oplus CRC(\hat{M})) \oplus K$

WPA | 802.11i

Улучшения в 802.11i:

1. Добавлен фраймворк аутентификации(EAP).
2. Алгоритмы шифрования и целостности испозьуют разные ключи.
3. Улучшенна защита целостности.
4. Улучшенна защита конфиденциальности.



WPA-PSK

PSK and EAP

- As far as authentication 802.11i supports two modes of authentication:
  - **WPA-Personal (PSK)**:
    - Useful for residential and personal use
    - Relies on a shared passphrase between the two entities
    - Does not require a separate authentication server
    - Also named ***PSK*** (Pre-Shared Key)
  - **WPA-Enterprise (EAP)**:
    - Useful for enterprises that require stronger authentication procedures
    - No shared passphrases
    - Uses a central ***RADIUS*** server for authentication
    - Follow ***802.1X*** protocol
    - Authentication protocol is ***EAP*** (Extensible Authentication Protocol)
    - EAP is just a wrapper protocol of other protocols, hence we have ***EAP-TLS***, ***EAP-TTLS***, ***EAP-PEAP***, ...

WPA Структура ключей

Начальный процесс аутентификации выполняется либо с использованием предварительного общего ключа pre-shared key (PSK), либо после обмена EAP через 802.1X.

Этот процесс гарантирует, что клиентская станция (STA) аутентифицирована с точкой доступа (AP).

После аутентификации PSK или 802.1X генерируется общий секретный ключ, называемый **парным главным ключом Pairwise Master Key (PMK)** .

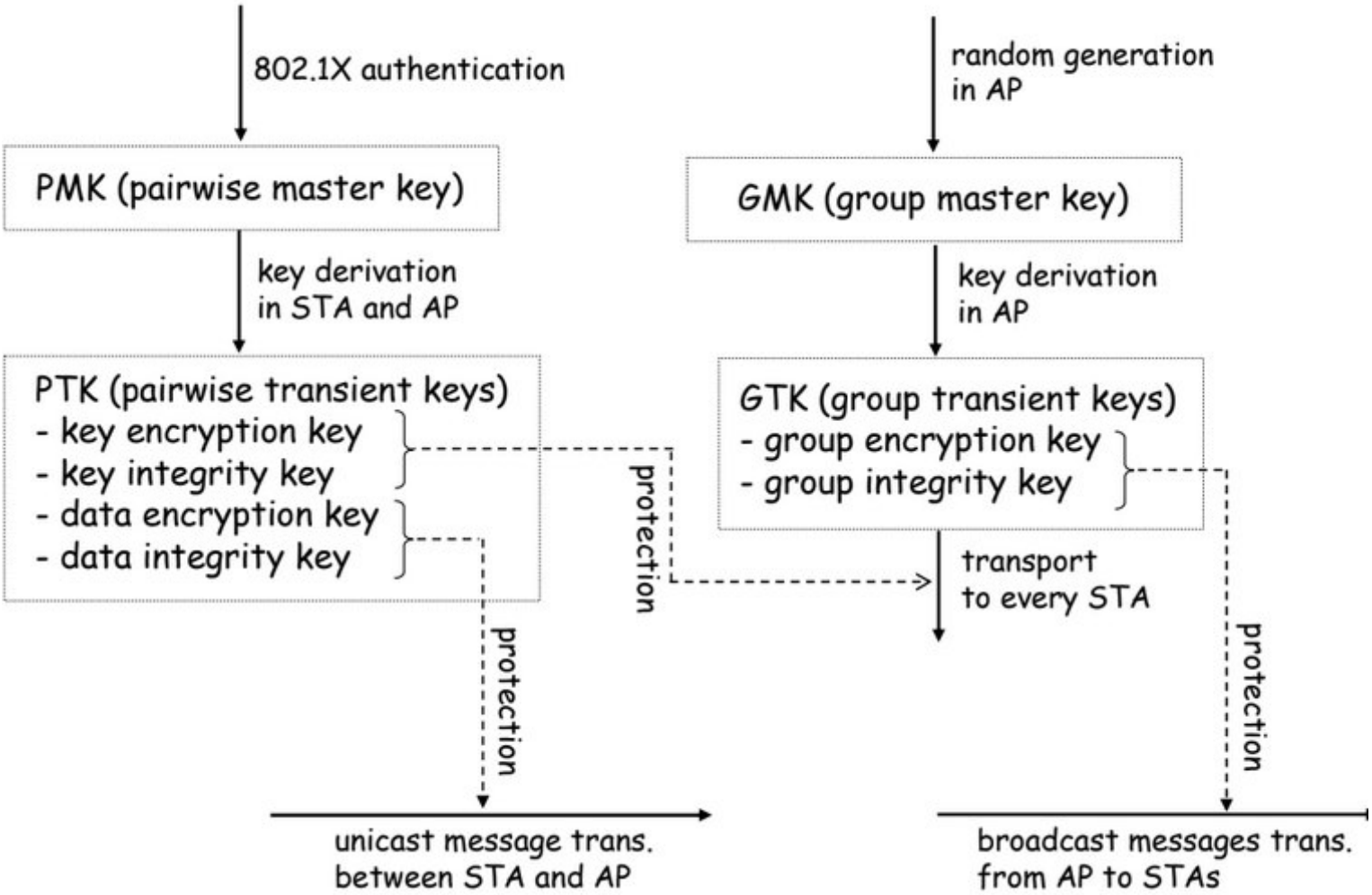
WPA Структура ключей

Групповой временный ключ (GTK), используемый в сети, может нуждаться в обновлении из-за истечения предварительно установленного таймера. Когда устройство покидает сеть, GTK также необходимо обновить. Это сделано для того, чтобы устройство не получало больше многоадресных или широковещательных сообщений от точки доступа.

Для обновления группового ключа, происходит 2-этапное рукопожатие:

1. $AP -> STA : E_{KEK}(G\hat{T}K)|T|MIC_{KIK}$
2. $STA -> AP : T + 1|MIC_{KIK}$

WPA Структура ключей



WPA Структура ключей

- for TKIP

PRF-512(PMK,
"Pairwise key expansion",
MAC1 | MAC2 | Nonce1 | Nonce2) =
= KEK | KIK | DEK | DIK

PRF-256(GMK,
"Group key expansion",
MAC | GNonce) =
= GEK | GIK

- for AES-CCMP

PRF-384(PMK,
"Pairwise key expansion",
MAC1 | MAC2 | Nonce1 | Nonce2) =
= KEK | KIK | DE&IK

PRF-128(GMK,
"Group key expansion",
MAC | GNonce) =
= GE&IK

Протокол аутентификации (Four-way handshake)

Задачи:

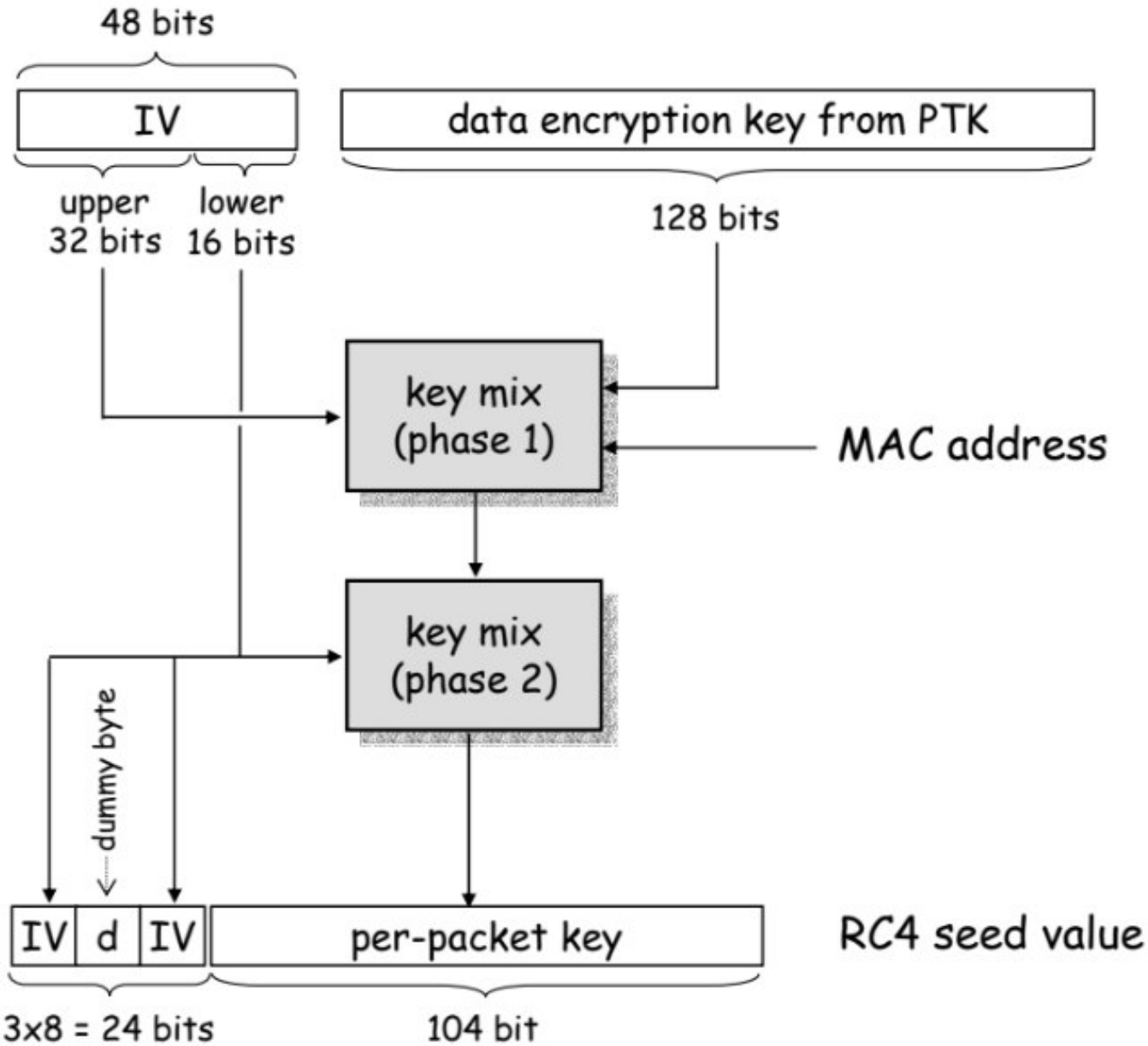
1. Доказательство знания PSK/PMK.
2. Передача случайных чисел между точкой доступа(AP) и клиентом (STA).

1. $*AP$: Генерирует nonce (R_{AP})
2. $AP -> STA : R_{AP}|N$
3. $*STA$: Генерирует nonce (R_{STA}) и высчитывает PTK.
4. $STA -> AP : R_{STA}|N|MIC_{KIK}$
5. $*AP$: Высчитывает PTK, генерирует GTK и проверяет MIC.
6. $AP -> STA : R_{AP}|T+1|E_{KEK}(GTK)|MIC_{KIK}$
7. $*STA$: Проверяет MIC и устанавливает ключи.
8. $STA -> AP : T+1|MIC_{KIK}$
9. $*AP$: Проверяет MIC и устанавливает ключи.

N - счетчик воспроизведения ключей.

MIC - код целостности.

TKIP


48 bits
IV
data encryption key from PTK
upper 32 bits
lower 16 bits
128 bits
key mix (phase 1)
MAC address
key mix (phase 2)
dummy byte
IV
d
IV
per-packet key
RC4 seed value
3x8 = 24 bits
104 bit

AES-CCMP

- CCMP means CTR mode and CBC-MAC
  - integrity protection is based on CBC-MAC (using AES)
  - encryption is based on CTR mode (using AES)
- CBC-MAC
  - CBC-MAC is computed over the MAC header, CCMP header, and the MPDU (fragmented data)
  - mutable fields are set to zero
  - input is padded with zeros if length is not multiple of 128 (bits)
  - CBC-MAC initial block:
    - flag (8)
    - priority (8)
    - source address (48)
    - packet number (48)
    - data length (16)
  - final 128-bit block of CBC encryption is truncated to (upper) 64 bits to get the CBC-MAC value
- CTR mode encryption
  - MPDU and CBC-MAC value is encrypted, MAC and CCMP headers are not
  - format of the counter is similar to the CBC-MAC initial block
    - "data length" is replaced by "counter"
    - counter is initialized with 1 and incremented after each encrypted block

EAP, EAPOL, RADIUS

EAP (Extensible Authentication Protocol, Расширяемый Протокол Аутентификации) — :

1. фреймворк аутентификации, который часто в беспроводных сетях и соединениях точка-точка;
2. 4 типа сообщений:
   - EAP reqiest - сообщение от клинета к серверу аунтефикации.
   - EAP response - сообщение от сервера аунтефикации к клинету.
   - EAP sucess
   - EAP failure

EAPOL (EAP over LAN) — протокол для передачи ESP через LAN протолы.