**Иерархия ключей**

**Концепция RSNA определяет следующие иерархии ключей [10]:**

* **Иерархия парных ключей, использующихся для защиты одноадресного трафика (Рис. 16).**
* **Иерархия групповых ключей для защиты многоадресного и широковещательного трафика**
* **Иерархия целостности GTK (iGTK), состоящая из одного ключа необходимого для защиты целостности многоадресных кадров управления.**

**Поддержка парных ключей в связке с расширенными криптографическими механизмами позволяет принимающей стороне обнаружить атаки типа MAC-spoofingи подделки данных. Архитектура RSNAпривязывает передаваемый и принимаемый парные адреса к парному ключу. Если злоумышленник создаст MPDUс поддельным адресом передатчика, то процедура декапсуляции обнаружит подлог. Иерархия групповых ключей не обладает таким свойством.**



Рис.16. Иерархия парных ключей

Процедуры распределения ключей тесно связаны с механизмами аутентификации. В стандарте 802.11 – 2012 различные ключи используются для различных целей. Эти ключи образуют иерархию как показано на рисунке. На верхнем уровне находится парныймастер-ключ(PMK), который затем используется для выработки других ключей. В случае аутентификации по протоколу 802.1xPMKгенерируется на этапе взаимной аутентификации между клиентом и сервером аутентификации. В случае использования аутентификации предустановленным ключом, **PMK генерируется из предустановленного ключа с помощью функции PBKDF2 (Password-basedKeyDerivationFunction 2) [10]:**

PSK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256), где

passphrase – предустановленныйключ. Представляет собой последовательность ASCII-символов длиной от 8 до 63 бит. Каждый символ в предустановленном ключе должен быть закодирован в таблице ASCIIв диапазоне от 32 до 126 включительно;

ssid (servicesetidentifier) – идентификаторточкидоступа, где используется вышеуказанный предустановленный ключ. Представляет собой строку октетов, которая включается в кадры Beaconи ProbeResponse;

ssidLength – длина SSID в октетах;

4096 – количество раз, которое будет захэширован предустановленный ключ;

256 – длина PSK.

После того, как PMKсгенерирован, он участвует в вычислении парногопередаточного ключа (PTK). Кроме случаев, когда используется предварительная проверка подлинности, в иерархии ключей для вычисления PTKвырабатывается из PMKс помощью псевдослучайных функций PRF-384 и PRF-512.

**PTKвычисляется по следующей формуле [10]:**

PTK ← PRF-X(PMK, “Pairwise key expansion” || Min(AA,SPA) || Max(AA,SPA) ||Min(ANonce,SNonce) || Max(ANonce,SNonce)), где

**PRF-X – псевдослучайная функция, результат которой имеет размер “X” (384 или 512);**

**PMK – парный мастер-ключ;**

*“Pairwisekeyexpansion” –* строка;

**Min() –функция выбора минимального значения из указанных в скобках;**

**Max() –функция выбора максимального значения из указанных в скобках;**

**AA – MAC адресаутентификатора (Authenticator MAC Address);**

**SPA – MAC адресклиента (Supplicant MAC Address);**

**ANonce – случайное число генерируемое аутентфикатором;**

**SNonce – случайное число генерируемое клиентом.**

PTKзатем разбивается на тир ключа [10]:

1. KCK (EAPoL-KeyConfirmationKey) – используется для проверки подлинности данныхв сообщениях четырехстороннего рукопожатия.KCKпредставляет собой последовательность битPTK с 0 до 127.
2. KEK (EAPoL-KeyEncryptionKey) – используется для обеспечения конфиденциальности в сообщениях четырехстороннего рукопожатия. KEKпредставляет собой последовательность битPTK с 128 до 255.
3. Временный ключ (temporalkey) - используются для защиты одноадресного соединения между аутентификатором и конкретным клиентом. Составляет последовательность битPTK с 256 по 511.

С помощью этих ключей можно обеспечить защиту одноадресныхкадров, то есть предназначенных для единственного пользователя. Для широковещательныхкадров предусмотрена своя иерархия- иерархиягрупповых ключей (Рис. 17). На вершине иерархии находится групповой мастер-ключ (GMK–GroupMasterKey).Поскольку групповые ключи используются только для защиты сообщений и не используются для обеспечения аутентификации, нет необходимости связывать конкретный ключ с конкретным устройством. Таким образом, аутентификатор просто генерирует 256-битное криптографически качественное случайное число и использует его для получения GTK по следующей формуле:

### GTKPRF-X(GMK, “Groupkeyexpansion” || AA || GNonce),где

### PRF-X – псевдослучайная функция с результатом “X” бит;

### X = 256 + (количество бит временного ключа);

### “Groupkeyexpansion” – строка;

### AA – MAC адрес аутентификатора;

### GNonce – случайное число.



Рис.17. Иерархия групповых ключей