**Защита на Wi-Fi мрежа  
801.11i  
TKIP и CCMP/AES криптация**Изготвил  
Стефано Огнянски

**Стандарт 801.11i**

Появата му се дължи на уязвимостта на WEP -Wireless Equivalent Privacy. Стандартът 801.11i представлява два криптиращи протокола ТКIP и CCMP. TKIP – Temporal Key e проектиран да повиши сигурността до максимума, позволен от наличния хардуер. CCMP – Mode with CBC-MAC Protocol е създаден по изцяло нов модел за да покрива всички стандарти за сигурност.

**TKIP**

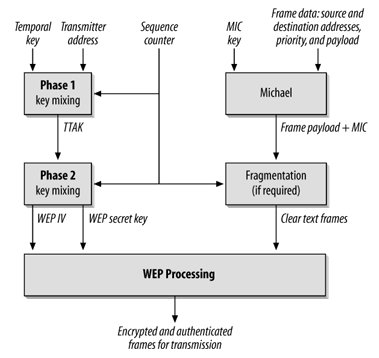
Първоначалното название на TKIP било WEP2, но поради лошото име с което се славило WEP криптирането името било сменено. Има няколко основни основни параметъра по които се различават TKIP и WEP:

* -Йерархия и автоматично управление на ключовете: TKIP използва множество мастър ключове докато WEP използва един;
* -Шифриране на база пакет: TKIP съдържа миксиране на ключове, тоест извежда уникален Р RC4 (лагоритъм за криптиране) ключ за всеки пакет;
* -Последователен брояч: С помощта на номериране на всеки пакет с последователен номер, може да бъде установено наличието на пакети, идващи извън реда. Отбелязването на тези пакети дава възможност да се избягват атаките от типа *replay attacks*, при които атакуващата страна прихваща валиден трафик и го препредава в по-късен момент от време.
* -Нова провррка за интегритета на съобщението – MIC: TKIP заменя линейния hash-метод на WEP с по-надежден криптографски hashing-алгоритъм за проверка на интегритета, наречен *Michael;*

**Обработка на данните и функциониране на TKIP**

Като входни данни TKIP използва следните обекти:

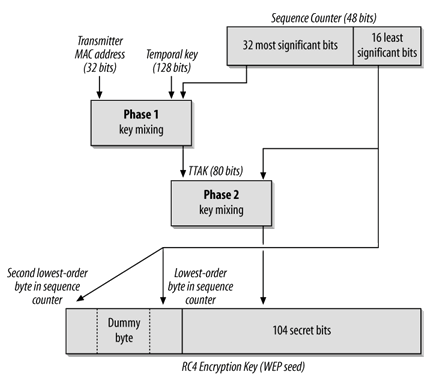
* Пакета, който трябва да бъде обработен;
* Временен ключ, използван за криптиране на пакета;
* MIC-ключ, използван от алгоритама Michael за защита на съдържанието на пакета. TKIP извежда двойка ключове, така че MIC-ключа, използван от станцията към точката за достъп, се различава от ключа, използван в посока от точката за достъп към мобилната станция. Една от разликите между TKIP и WEP е в използването на ключ при проверката за интегритет на съобщението;
* Адреса на предавателя се използва като вход на TKIP, тъй като той е необходим за осъществяване на автентификацията на източника. Адреса на предавателя идва заедно с пакета и не е необходимо да се осигурява от софтуера от по-високите OSI-слоеве;
* Последователен брояч, който се поддържа от драйвера или програмното осигуряване на картата.



**Конструиране и смесване на TKIP ключове**

TKIP разделя изчисляването на смесените ключове на две фази. Първата фаза има за вход адреса на предавателя, старшите 32 бита на последователния брояч и 128-битов временен ключ. Като изход се получава 80-битова стойност. Въпреки че изчислението изглежда малко объркано, то се състои изцяло от “прости” операции, като събиране, преместване, изключващо ИЛИ, което значително намалява изчислителния товар. Изходящата стойност на първата фаза е константна, доколкото старшите 32 бита на последователния брояч са константни, тоест тази стойност трябва да бъде изчислявана само веднъж на 65536 пакета.

Фаза 2 на смесителната функция се изчислява за всеки пакет. Вход за тази фаза представлява резултата от работата на фаза 1, временния ключ и 16-те младши бита от последователния брояч. Единствената входяща стойност, която се изменя от пакет на пакет, е стойността на последователния брояч. Тя се променя по добре дефиниран начин, така че приложенията могат да използват предварително изчисляване на стойността на базата на набор от следващи стойности на брояча, докато пакетите се подготвят за предаване.

****

**TKIP пакет**

**

**CCMP**

CCMP протокола е базират на стандарта за криптиране AES (Advanced Encyprtion Standard). AES може да работи с различни дължини на ключа, но за стандарта 802.11i ипозлва 128-битови ключовек и 128-битови блокове.

**WPA-Personal**

Наричан също като WPA-PSK (предварително споделен ключ) режим. Той е предназначен за домашни и малки офис мрежи и не изисква сървър за удостоверяване. Всяко безжично мрежово устройство криптира мрежовия трафик, като извлича 128-битовия ключ за шифроване от 256 битовия споделен ключ. Този ключ може да бъде въведен или като низ от 64 шестнадесетични цифри, или като парола от 8 до 63 ASCII символа, които могат да се отпечатват. Режимът WPA-Personal е достъпен с WPA и WPA2.

**WPA-Enterprisе**

Наричан също като WPA-802.1X режим, а понякога и само WPA (за разлика от WPA-PSK), е предназначен за корпоративни мрежи и изисква RADIUS сървър за удостоверяване. Това изисква по-сложна настройка, но осигурява допълнителна сигурност (например защита срещу атаки с речници – brute force attack). Режимът WPA-Enterprise се предлага с WPA и WPA2.

**Wi-Fi Protected Setup (WPS)**

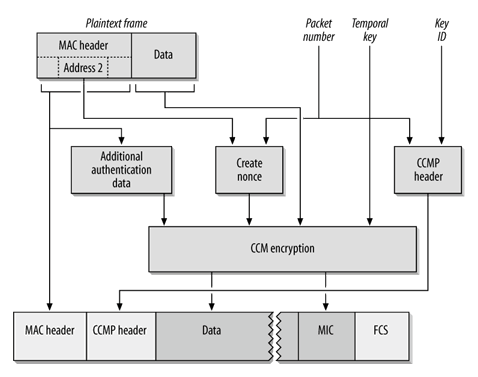
Това е алтернативен метод за разпространение на ключове за удостоверяване. Предназначен е за опростяване и укрепване на процеса, но създава голяма дупка в сигурността чрез възстановяване на WPS PIN.

**Обработка и предаване на данните чрез CCMP**

CCMP осигурява едновременна поддръжка на криптиране и на защита на интегритета на пакетите в рамките на един и същ процес. Използва следните входни данни:

* Самия пакет;
* Временен ключ, използван за автентифициране и криптиране на пакета. Един и същ ключ се използва и за криптирането и за автентифицирането на пакета;
* Идентификатор на ключа, който позволява употребата на много различни ключове. За всеки отделен пакет обаче се използва само един ключ;
* Номер на пакета**,** който уникално идентифицира предавания в момента пакет.

1. Пакета се състои от хедър и полезен товар.
2. На пакета се присвоява 48-битов номер на пакет (*Packet Number, PN*). Подобно на последователните номера при TKIP, номерата на пакетите никога не се употребяват повторно за един и същ временен ключ. За всяко предаване номера на пакета се увеличава с единица, което помага за детектиране на replay-атаки.
3. Конструира се полето *Additional Authentication Data (AAD)*. То се състои от полета в хедъра на пакета, които трябва да бъдат автентифицирани с оглед на сигурността, но в същото време трябва да останат некриптирани, така че да могат да оперират протоколите 802.11.
4. Като следваща стъпка се изгражда *CCMP nonce* полето. Това са допълнителни битове данни, които гарантират, че криптирането се извършва върху уникални данни.
5. Конструира се *CCMP header* полето. То се състои от номера на пакета, разпределен върху 6 байта с идентификатор на ключа в средата.
6. Криптирания пакет се подготвя за предаване, като се взема оригиналния MAC-хедър, към него се прикачва CCMP-хедъра и криптираните данни. Така получения пакет се подава към радио-интерфейса за предаване.

****

Най-ефективна защита на съвременните WiFi мрежи се осъщестява чрез WPA2/3 – AES и излючен WPS. Все още няма популярен ефективен метод за защита от атака от типа Evil Twin (вид man in the middle), чрез която можем да залгушим желаната мрежа като изпращаме „deauthentication packets”, след което създаваме фалшива точка за достъп копие на вече загушената и ако жетвата влезе в нашата мрежа ще получи съобщение да си въведе паролата, поради причини свързани със сигурността на неговата мрежа.

Източници

*Доц. д-р Емил Владков* “*Безжични мрежи и протоколи 802.11i: Robust Security Networks, TKIP и CCMP”*

*https://en.wikipedia.org/wiki/Wi-Fi\_Protected\_Access*