Анализ на информационната сигурност в стандартите за безжична локална мрежа IEEE 802.11

К. Димитров

Analysis of the Information Security in WLAN Standards IEEE 802.11

K. Dimitrov

Key Words: *Wireless LAN (WLAN) security; WEP; RC4; IEEE 802.11; IEEE 802.1X; IEEE 802.11i; WPA; TKIP; WPA2; AES; CCMP; KRACK attack.*

Abstract. *On the basis of extensive research in the specialized literature, a critical analysis of information security protocols in the standards for IEEE 802.11 wireless LAN (WLAN, WiFi) has been carried out. Finally, some conclusions and recommendations are made. The first WLAN security protocol - WEP is extremely insecure and should not be used. Due to the inherited vulnerabilities of WEP and the fact that some parts of TKIP (such as the Michael function) have some security deficiencies, WPA has already exhausted its role as a temporary WEP fix for legacy hardware and is not recommended. Despite the mathematically proven cryptographic security of the AES standard in CBC mode, a weakness in the cryptographic key management process makes it vulnerable and leads to a security breach of WPA2 in October 2017. Although the vulnerability is removable by patch, probably a lot of WiFi-Devices have not been updated, which puts users at risk. In addition, despite updates of the firmware and recommendations from information security professionals to circumvent and/or block the protocol breach, reports emerged in October 2018 that the vulnerability to KRACK was still being exploited.*

1. Увод

Безспорни са предимствата на безжичните локални (WiFi) мрежи пред кабелните: гъвкавост, мобилност, лесно и бързо разгръщане най-вече заради отсъствие на физически връзки между устройствата. В допълнение развитието и усъвършенстването на безжичните технологии подобрява непрекъснато техните характеристики и същевременно снижава цената на WiFi устройствата. Това наложи масовото им приложение във всички области и им отреди роля на съществена част от мрежите за достъп до интернет. Негативната страна на WiFi мрежите произхожда от тяхното основно предимство – радиокомуникацията. Като среда за пренос на данни радиокомуникацията е общодостъпна (broadcast media), поради което удовлетворяването на критериите за *поверителност, управление на достъпа и цялостност на данните е истинско предизвикателство*.

В статията е представен критичен анализ на протоколите за информационна сигурност в стандартите за безжична локална мрежа IEEE 802.11 (Wireless LAN – WLAN, WiFi).

2. Протокол за сигурност: еквивалентна на кабелната мрежа (Local Area Network – LAN) неприкосновеност на личното пространство (Wired Equivalent Privacy – WEP)

Още с излизането на първия стандарт за безжични локални мрежи IEEE 802.11 през 1997 г. в него е интегриран механизъм за сигурност, наречен еквивалентна на кабелната мрежа неприкосновеност на личното пространство (*Wired Equivalent Privacy – WEP*). Основната цел на този механизъм е да гарантира сигурността на потребителските данни, като ги защитава от неоторизиран достъп [1]. Както подсказва наименованието му, идеята тогава е била да се гарантира сигурността на безжичната мрежа до степен, сравнима с тази на кабелната локална мрежа. За постигане на тази цел е необходимо да се удовлетворят и поддържат на определено ниво критериите за *поверителност, управление на достъпа и цялостност на данните*.

Основен подход при осигуряване на поверителността на данните е шифриране/дешифриране (или още криптиране/декриптиране).

2.1. Процес криптиране/декриптиране в WEP

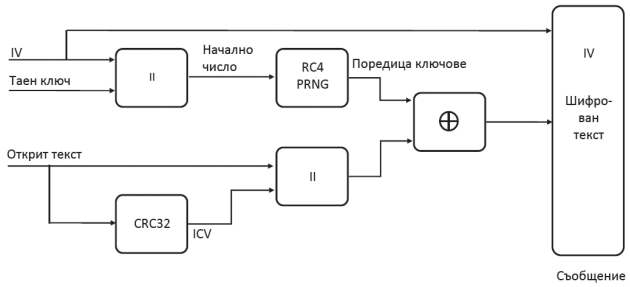
В криптографията почти винаги се използват някакъв вид генератори на псевдослучайни числа (Pseudo Random-Number Generator – PRNG). В протокола WEP тази функция се изпълнява от потоковия шифър RC4 (RC4-PRNG). Инициализиран с някаква начална стойност (начално число), той генерира поток от псевдослучайни числа. И както е при всички поточни шифри, той ще генерира същия поток от случайни числа отново, ако му бъде зададена същата начална стойност [1].

С цел постигане на някакво разнообразие на генерираните случайни числа в RC4 се използва инициализиращ

вектор IV. Той е дълъг 24-бита и се допълва до 40-битов таен ключ посредством конкатенация. С оглед да се предпази генераторът RC4-PRNG от генерирането на едни и същи числа за всеки пакет, този IV трябва да се променя колкото е възможно по-често. При размер от 24 бита за IV съществуват само 22^4 = 16 777*10^3 различни стойности на IV.

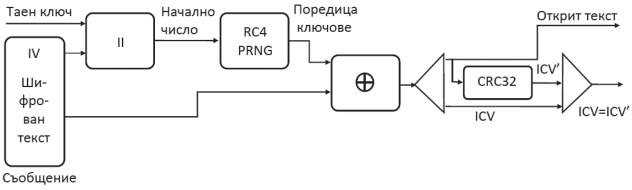
За да се осигури целостността на данните (или още отсъствието на промяна/модификация на данните при пренос), се въвежда стойност за проверка за целостността (Integrity Check Value – ICV). WEP използва алгоритъма CRC32.

Фиг. 1 илюстрира процеса на криптиране на съобщението в протокола WEP. Генераторът RC4-PRNG се инициализира с начално число от таен ключ (парола) и инициализиращ вектор IV и като резултат той генерира последователност (поток/поредица) от ключове. Върху тази поредица от ключове и конкатенацията от обикновените данни (открит текст) и тяхната CRC32 стойност (ICV) се изпълнява операцията изключващо ИЛИ. Накрая криптираното съобщение се конкатенира/слепва с некриптираната стойност на IV (открит текст) и се предава [1].



Фиг. 1. Процес криптиране на съобщението в протокол WEP

Приемащият клиент трябва само да обърне процеса, за да възстанови текстовото съобщение в открит/некриптиран вид, да изчисли отново върху него стойността на CRC32 кода за проверка (ICV') и да извърши проверка на целостността на съобщението чрез сравняване на ICV и ICV'. Методът е илюстриран на *фиг. 2*.



Фиг. 2. Процес декриптиране на съобщението в протокол WEP

2.2. Анализ на сигурността в протокол WEP

Сигурността на протокола WEP разчита единствено на трудността на разкриване на тайния ключ.

Първоначално WEP е бил предназначен за 40-битови ключове, което има за резултат пространство от 2^{40} = 1099*10^9 ключове. При използването на съвременен хардуер не е невъзможно да се открие ключът с обхождане на всички реализации в рамките на приложим на практика интервал от време. Поради това дължината на ключа е увеличена до 128-бита и общото пространство от ключове вече възлиза на 2^{128} = 3402*10^{35}. Това разширение прави атаката от тип изчерпателно търсене на ключа неосъществима в разумен срок, дори и с помощта на най-мощния (към момента на корекцията в стандарта) хардуер [2].

Въпреки това WEP притежава някои много критични недостатъци в проектирането, които правят стандарта практически безполезен.

През 2001 г. Scott Fluhrer, Itsik Mantin и Adi Shamir [3] публикуват първия криптоанализ на WEP. Тримата изследователи фокусират своя анализ върху начина на функциониране на шифъра RC4. Потоковият шифър RC4 е съставен от две части: алгоритъм за планиране на ключове (Key Scheduling Algorithm – KSA) и алгоритъм за генериране на псевдослучайни числа (Pseudo Random Generator Algorithm – PRGA). В цитираната по-горе публикация се описват някои слабости в алгоритъма за планиране на ключове в RC4 и е оценена тяхната криптоаналитична значимост. Идентифицирани са голям брой слаби ключове, при които познаването на малък брой битове от ключа е достатъчно, за да се определят многобройни състояния и изходни битове с непренебрежима вероятност. Тримата учени използват тези слаби ключове, за да структурират нови различители (семантични нерегулярни отличителни признаци –distinguishers) за RC4, както и да предприемат реализуеми на практика атаки със свързани/корелирани ключове с практическа сложност. Накрая те показват, че RC4 е напълно несигурен в популярния режим на работа, който се използва в протокола WEP. При този режим неизменяем таен ключ се конкатенира с известни IV модификатори, за да се шифроват различни съобщения. Тяхната пасивна и насочена само към шифриран текст атака (passive ciphertext-only attack) в този режим може да възстанови произволно дълъг ключ за време, което расте в линейна зависимост от неговия размер както за 24-, така и за 128-битови IV модификатори.

Накратко за RC4

Тук следва да се отбележи, че докато първите публикации за уязвимости на WEP са през 2001 г., то проблемите в RC4 стават известни скоро след анонимното публикуване на неговото описание и последващо разпространение в интернет. Първоначално, след като е бил проектиран от Ron Rivest през 1987 г., RC4 (известен още като Rivest Cipher 4, а също така като Ron's Code) е търговска тайна. Още през 1995 г. една от първите слабости, публикувани за RC4, е открита от Roos [4]. Установена е корелация между (някои) битове от тайния ключ и началното състояние на PRGA, генерирано от KSA. Също така отново Roos [4] и Wagner [25] идентифицират класове слаби ключове, които издават тайния ключ, ако първите байтове на ключа са известни.

В годините след това са публикувани много различни атаки срещу WEP. Повечето от тях се основават на слабостите на използвания потоков шифър RC4. Докато при първите атаки са били необходими голямо количество натрупани данни, при по-новите подходи, като атаката на Andreas Klein [5], са необходими относително малък брой

на предаваните пакети. Използвайки подхода на A. Klein и интензивното инжектиране на пакети, Erik Tews et al. [6] проектират процес за генериране на достатъчно трафик за разбиване на 128-битов WEP[1] ключ за по-малко от 60 секунди. За осъществяване на атаката не е бил необходим мощен хардуер със специално предназначение [2].

Друга слабост на протокола WEP е, че за проверка на целостността на данните използва поле, чиято стойност се генерира от цикличен код с излишък CRC-32 и което поле е част от шифрования полезен товар на пакета. Критичен анализ в [2] показва, че контролната сума CRC32 е недостатъчна, за да се гарантира, че нападател не може да модифицира съобщение: т.е. CRC32 не е криптографски сигурен код за удостоверяване на целостността на данните. CRC32 е предназначен за откриване на случайни грешки в съобщение, но не е устойчив срещу злонамерени атаки. По-нататък авторите демонстрират, че тази уязвимост на CRC32 се усилва от факта, че като част от полезния товар на съобщението неговата стойност е криптирана с потоковия шифър RC4.

В заключение може да се каже, че WEP е много несигурен и не трябва да се използва.

3. Стандарт за безжичен защитен достъп IEEE 802.11i

Скоро след първите публикации за уязвимостите на WEP и очакваните реализации на много ефективни приложения за атака IEEE започва работа по замяна на стандарта. На 24 юни 2004 г. с оглед да се обезпечи по-добра сигурност за безжични локални мрежи е ратифициран IEEE 802.11i. IEEE 802.11i е изменение и допълнение на оригиналния IEEE 802.11. Стандартът определя два класа алгоритми за сигурност [7,8,9, 1]:

1. Алгоритъм за асоцииране към мрежа с робастна/гарантирана сигурност (Robust Security Network Association – RSNA, съответно Robust Security Network – RSN).

2. Алгоритъм за асоцииране към мрежа с до-робастна/негарантирана (предшестваща робастната) сигурност (Pre-Robust Security Network Association – Pre-RSNA, съответно Pre-Robust Security Network – Pre-RSN).

Вторият клас Pre-RSNA включва наследените възможности за сигурност, разработени в оригиналната спецификация на IEEE 802.11: автентификация от тип отворена система/или споделен ключ на идентичността на безжична станция (WiFiустройство) и WEP протокол за защита на поверителността на трафика.

По същество автентификацията от тип отворена система е т. нар. нулев алгоритъм за удостоверяване и означава, че няма верификация на безжичната станция и безжичната мрежа (точката за достъп – AP). По принцип този тип автентификация разрешава достъп на всяко устройство, което подава заявка за удостоверяване до точката за достъп. Ако не е активирано шифроване, всяко WiFi устройство, което знае идентификацията на безжичната мрежа, може да получи достъп до нея. Ако WEP протоколът е активиран за точката за достъп, споделеният ключ става средство за контрол на достъпа. Устройство, което не разполага с правилния WEP ключ, не може да предава данни към точката за достъп, нито да дешифрира изпращани от AP данни [10].

Първият клас алгоритми, посочен по-горе, включва редица механизми за сигурност за създаване на RSN, която да отговори на всички известни недостатъци на WEP и да осигури солидна защита (гарантирана сигурност) на безжичната връзка, включително цялостност и поверителност на данните. IEEE 802.11i дефинира RSN като безжична мрежа, която допуска създаването само на RSN асоциации (RSNA).

На практика някои мрежи могат да имат комбинация от RSNA и Pre-RSNA връзки. Мрежата, която позволява създаването на смесени асоциации от предшестващи RSN (pre-RSNA) и RSNA, се нарича мрежа за сигурност на прехода (или още мрежа с преходна сигурност). Предназначението ѝ е да бъде временно средство за осигуряване на свързаност, докато дадена организация мигрира към мрежи, използващи само RSNA [9].

Специфични особености на RSN и RSNA

Стандартът IEEE 802.11i въвежда концепцията за Robust Security Network (RSN) и съответно RSNA. С оглед по-лесно разбиране на концепцията и основните принципи в стандарта IEEE 802.11i е необходимо кратко въведение в стандарта 802.1X.

Стандартът IEEE 802.1X осигурява методология (и процедура) за управление на достъпа, която използва разширяем протокол (за избор на метод) за автентификация – EAP (Extensible Authentication Protocol) и налага централизирана взаимна автентификация. Първоначално IEEE 802.1X е разработен за кабелни локални мрежи, но е адаптиран от IEEE 802.11i и за WLAN мрежи. Стандартът IEEE 802.1X също така дефинира някои термини и компоненти (обекти/субекти), свързани с удостоверяването.

Фиг. 3 представя изглед на минималния набор компоненти съгласно стандартите IEEE 802.1X и IEEE 802.11i, участващи в създаването на RSN/RSNA и всички взаимодействия между тях.

Съгласно стандарта изобразените на фиг. 3 компоненти се означават като STA – Station (мобилно устройство на потребителя, WiFi-устройство), AP – Access Point (точка за достъп) и AS – Authentication Server (сървър за автентификация). Докато не се извърши успешно удостоверяване между STA и AS, комуникациите на STA се блокират от AP. Техниката, използвана за блокиране на комуникациите, е известна като базирано на порт управление на достъпа. IEEE 802.1X може да управлява потоците от данни, като различава EAP кадри от не-EAP кадри и пропуска EAP кадрите през неуправляем порт, а не-EAP кадрите през управляем порт, с който може да се блокира достъпът. Стандартът IEEE 802.11i допълва този протокол с цел да ограничи комуникацията на AP, докато криптографските ключове не се доставят на съответните им места. По този начин IEEE 802.11i предотвратява възможността измамна/подставена

1 Поради 24-битовия размер и открит текст на IV, конкатениран към ключа, ефективната дължина на ключа е само 104 бита.

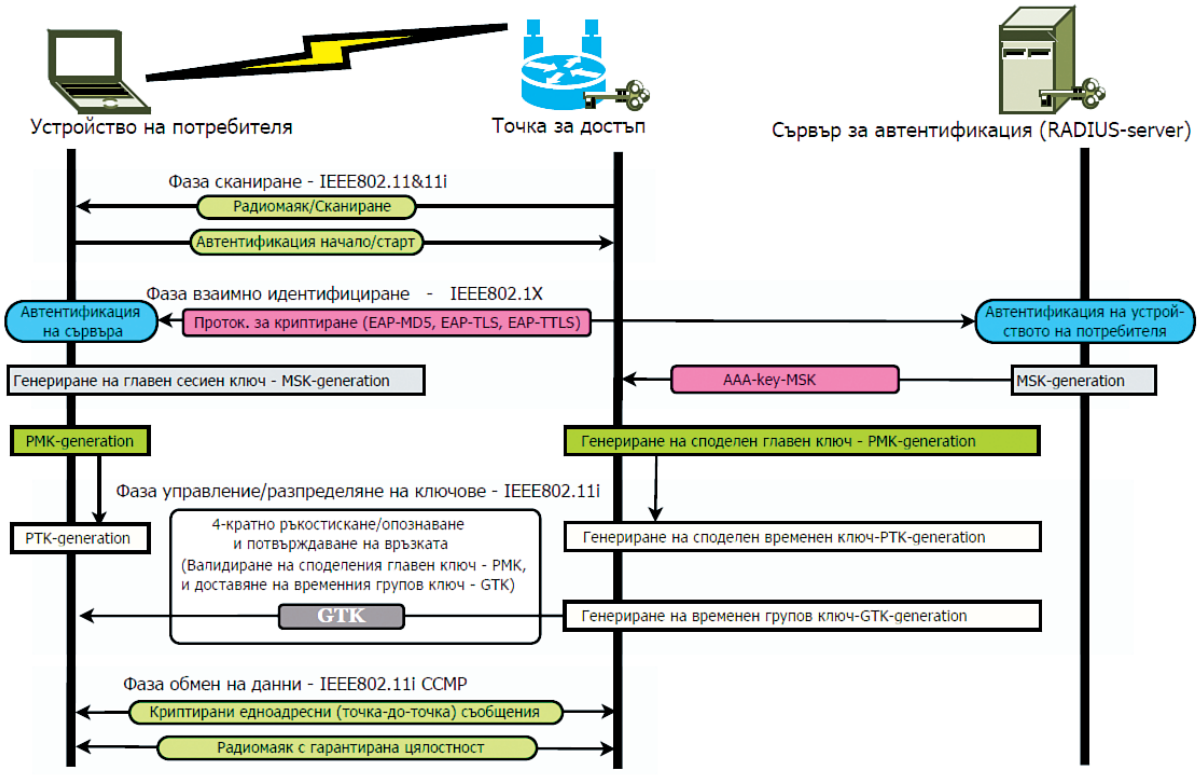
точка за достъп да обменя други данни освен EAP трафик с комуникационната подсистема на STA.

Автентификаторът е обект в единия край на от точка до точка сегмент на локалната мрежа, който съдейства за идентифицирането на обект, прикрепен към другия край на тази връзка. Например AP на *фиг. 3* служи като *автентификатор*. *Заявител* е субектът, който подлежи на автентификация, т.е. STA. *Сървърът за удостоверяване/автентификация (AS)* е система/субект, който предоставя удостоверителни услуги (и съответно обслужване) на *автентификатора*. Това обслужване определя въз основа на пълномощията, предоставени от *заявителя*, дали същият има право (е оторизиран) да получи достъп до услугите, предоставяни от удостоверяващия (*автентификатора*). AS осигурява услуги за удостоверяване и доставя сесийни ключове на всяка AP в безжичната мрежа, а всяка STA или получава сесийни ключове от AS, или сама (автономно) извлича сесийни ключове. Също така AS сам удостоверява STA и AP или предоставя информация на STA и AP, така че те да могат да се автентифицират взаимно. При решение, базирано на стандарта IEEE 802.11i, най-често използваната система за автентификация е сървърът за удостоверяване, оторизация и отчетност (Authentication, Authorization and Accounting – AAA-server/protocol), а за пренос на свързания с удостоверяването трафик – протокола Remote Authentication Dial In User Service (RADIUS) или Diameter. Използваният в протокола WEP модел *кандидат-заявител/автентификатор* по същество е едностранен (еднопосочен), а не модел за взаимно удостоверяване, т.е. кандидатът се удостоверява в мрежата. IEEE 802.11i се противопоставя на този подход, като изисква използваният EAP метод да осигури взаимна автентификация.

След успешното завършване на фазата на удостоверяване STA и AP изпълняват серия от функции с цел доставяне на криптографските ключове в двата обекта. Тази фаза се нарича фаза на генериране и разпределение на ключове (Key Generation and Distribution – KGD). Тя осигурява последната стъпка в удостоверяването и позволява на STA и AP да извличат ключове, които правят възможен сигурния пренос на данните. Фазата на KGD има няколко цели, включително следните: потвърждаване на съществуването на Pairwise Master Key (PMK); осигуряване актуалността на ключовете за сигурност на асоцииране; извличане и синхронизиране на инсталирането на ключове за шифриране на трафика (временните ключове) в AP и STA; доставяне на групов ключ за защита на преноса за многоадресно (multicast) и към всички (broadcast) предаване; потвърждаване на избора на шифриращия пакет (метод).

Фазата на KGD включва два вида взаимодействия (от тип ръкостискания): четирикратно ръкостискане (4-Way Handshake) и групово ръкостискане (Group Handshake). Груповото ръкостискане е необходимо само когато STA участват в трафик за многоадресно или към всички предаване. И двата вида ръкостискане използват следните основни механизми за сигурност: проверка на целостността на съобщенията, потвърждаване/валидиране на източника на трафик; криптиране на съобщенията с цел защита от неразрешено разкриване на данни.

Алгоритъмът RSNA реализира два протокола за осигуряване на поверителност на данните, известни като *Counter-Mode-CBC-MAC Protocol (CCMP) и Temporal Key Integrity Protocol (TKIP)*.



Фиг. 3. Компоненти и процедури за сигурност в WLAN съгласно стандартите IEEE 802.1X и IEEE 802.11i

По идея TKIP е предназначен да обезпечи по-голяма сигурност за наследения (стария) хардуер с помощта на RC4, докато CCMP изисква съвместим с AES (Advanced Encryption Standard) хардуер. Алиансът WiFi-Alliance[2] сертифицира TKIP съвместим хардуер под името Wi-Fi Protected Access (WPA), т.е. безжичен защитен достъп.

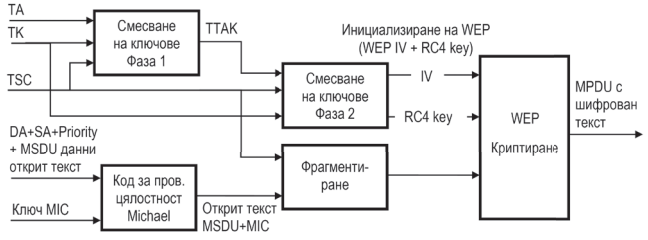
3.1. Безжичен защитен достъп

WPA влиза в ролята на временна корекция с цел да се подобри сигурността на WLAN мрежите, базирани на стар хардуер. TKIP се основава на RC4 и включва хеш-функцията с ключ Michael (keyed hash-function Michael) [3]. TKIP може да бъде разглеждан като обвивка около съществуващите WEP криптиране/декриптиране и служи като щит пред техните най-опасни уязвимости [7].

Фиг. 4 илюстрира процеса криптиране в TKIP, а в *табл. 1* е дадено описание на използваните съкратени означения.

Табл. 1. Описание на използваните съкратени означения в процесите криптиране и декриптиране в TKIP

Описание	Означение
Адрес на предаващата станция/Transmitter Address	TA
Миксиран (смесен) между TA и TK TKIP-ключ/TKIP Mixed Transmitter Address and Key	TTAK
Временен ключ/Temporal Key	TK
Пореден/сериен номер на пакет/Sequence number (TKIP sequence counter – TSC)	TSC
Инициализиращ вектор/Initialisation Vector	IV
Адрес на получателя/Destination Address	DA
Адрес на изпращача/Source Address	SA
Полезен товар от данни в MAC подслоя/MAC Service Data Unit	MSDU
Полезен товар + служебни (управляващи) данни в MAC подслоя/MAC Protocol Data Unit	MPDU

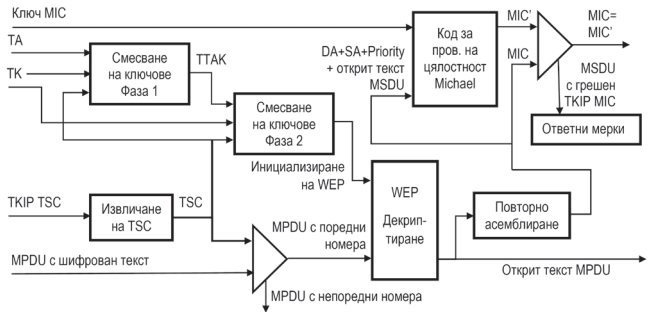


Фиг. 4. Процес криптиране в TKIP (от стандарт IEEE Std 802.11™-2012)

Блокът за WEP криптиране (WEP-Encapsulation) съответства на схемата за WEP криптиране от *фиг. 1*. Разширението с TKIP носи подобрения в сигурността само чрез промяна на входа на процеса на криптиране WEP. Най-важната промяна в класическия протокол WEP е, че се използва нов временен ключ за всеки пакет. Този ключ се създава чрез смесване заедно на главен ключ, на MAC адреса на предавателната станция и 48-битов последователен номер посредством т. нар. процедура за смесване на ключове, която използва специален 8-рундов шифър на Feistel [11]. Главният ключ се създава наново всеки път, когато една станция се свързва с мрежата и операцията по смесването може да се направи с малко изчислителна мощност, но осигурява значително повишаване на криптографската сигурност. Чрез добавяне на последователни номера в ключа се осигурява, че той ще бъде различен за всеки пакет. 48-битовото пространство за последователните номера предотвратява атаки и нападения от тип WEP сблъскване/колизии, както и от тип повторение. С помощта на IEEE 802.1X тайните ключове се разпределят по-надеждно и сигурно между участващите в удостоверяването станции (STAs).

Както беше споменато в предния раздел, втората голяма уязвимост в WEP е използването на линейната функция за проверка на целостността CRC32. Чрез прилагане на хеш-функцията с ключ *Michael* този проблем е отслабен, но не е разрешен, тъй като *Michael* също притежава някои проектни недостатъци (виж по-долу в този раздел).

Фиг. 5 показва процеса на декриптиране в TKIP, който може да се разглежда като обвивка около схемата за WEP декриптиране. Той работи точно по обратния начин на процеса на TKIP криптиране.



Фиг. 5. Процес декриптиране в TKIP (от стандарт IEEE Std 802.11™-2012)

Детайли на Michael кода за проверка на целостността (Michael Message Integrity Code – MIC)

Michael е код за проверка на целостността на съобщението и е проектиран от Niels Ferguson през 2002 г. [13]. Това е хеш функция с ключ, която работи със съобщения с произволна дължина и с 64-битов ключ *Michael*. Ключът се преобразува в две 32-битови думи и изходното съобщение се разделя на блокове с дължина от по 32-бита и допълнени така, че дължината на съобщението да е кратна на четири.

Като всяка хеш функция с ключ и функцията *Michael* трябва да отговаря на основните изисквания [1]:

1. Дайджест кодът на съобщението (Message Digest Code – MDC) $h(m)$ да може да се изчислява много бързо.

2. h трябва да бъде еднопосочна функция. При дадено/известно y трябва да бъде изчислително невъзможно да се намери m' с $h(m') = y$. y е MDC на някое съобщение.

3. Трябва да бъде изчислително невъзможно да се намерят съобщения m_1 и m_2, за които $h(m_1) = h(m_2)$. При удовлетворяване на това изискване функцията се нарича силно устойчива на сблъскване/колизии.

2 Международна асоциация с идеална цел, удостоверяваща оперативната съвместимост на продукти за безжични локални мрежи, базирани на спецификацията IEEE 802.11. http://www.wi-fi.org/.

Анализ на сигурността в TKIP

Една от слабостите в TKIP се дължи на недостатъци в проектирането на кода за проверка на целостността/интегритета Michael. Дори авторът на функцията Michael е знаел за описания по-долу недостатък още от публикуването ѝ [1]:

„Атака с познат открит текст може да разкрие потока от ключове за определен IV и ако вторият пакет, криптиран със същия IV, е по-къс от първия, стойността на MIC се разкрива, което след това може да се използва за извличане на ключа за удостоверяване".

Avishai Wool [12] установява, че *Michael* не е еднопосочна функция, създава алгоритъм, който е в състояние да инвертира функцията *Michael* и предлага атака тип свързано съобщение (related-message attack). В [14] Huang et al. доказват, че *Michael* освен това не е устойчив на сблъскване и показват че не е много трудно да се открие една колизия и по-нататък да се постави началото на атака с фалшифицирани пакети (packet-forgery attack) [1].

Макар че подсказаните по-горе атаки не намират особено масово самостоятелни реализации на практика, установените слабости на хеш функцията с ключ *Michael* я правят несигурна и удобна за комбиниране с други уязвимости.

Една от първите практически атаки над WPA/TKIP е реализирана от Beck и Tews [15]. Съчетавайки някои от посочените по-горе недостатъци на функцията *Michael* и вече известната от WEP уязвимост на използвания и в TKIP CRC32, авторите успяват да възстановят MIC ключа, което им дава възможност да изпращат по няколко фалшиви пакета с малък размер. Vanhoef и Piessens [16] модифицират и подобряват атаката, което им позволява да изпращат произволен брой пакети с определен максимален размер. Освен това атаката на Vanhoef и Piessens може да се използва за декриптиране на произволни пакети.

ALFardan et al. [17], Paterson et al. [18] и Vanhoef et al. [16] отново се фокусират върху известните вече слабости на използвания и тук потоков шифър RC4. Изследователите провеждат сериозни по обем статистически и емпирични тестове за функционирането на RC4. Посредством статистически хипотези от натрупаните данни са установени емпирично нови систематични отклонения от очакваното равномерно разпределение на вероятността (COPB) за генериране на ключове biases, които съответно са класифицирани според някои техни свойства като еднобайтови, двубайтови, многобайтови COPB; кратковременни (short-term), дълговременни/регулярни (long-term) COPB.

Върху данните за тези COPB учените прилагат емпирични оценки, статистически и криптоанализи, в резултат на които установяват нови корелации между определени байтове на използваните входящи ключове и изходящия шифриращ поток от ключове, както и някои емпирични оценки за функциите на разпределение на вероятността на участващите в процеса на шифриране стохастични величини: шифриращ поток от ключове, шифриран и открит текст (и техните значения).

По-нататък учените създават алгоритми, в основата на които стоят математически методи и апарат за обработка на данни от областта на вероятностния и статистическия анализ с цел пробиване на WPA/TKIP. Paterson et al. [18], Vanhoef et al. [16] публикуват резултати за проведени ефективни статистически атаки за възстановяване на открит текст.

Може би няма да е без значение, ако в допълнение тук добавим, че при част от споменатите по-горе задълбочени статистически анализи на RC4 е открита уязвимост и в TLS – Transport Layer Security [17,19]. Широко използваният в интернет протокол TLS става уязвим, тъй като в някои от режимите за шифриране използва RC4. Новооткритите слабости в RC4 правят възможно създаването на алгоритми съответно за атаки тип възстановяване на открит текст само от прихванат шифрован текст (*ciphertext-only plaintext recovery attacks against TLS when RC4 is selected for encryption*) [17], както и възстановяване на открит текст директно от прихванати шифровани бисквитки отново срещу TLS, но използван от протокола HTTPS [19]. Както може да се види от *фиг. 3*, TLS се използва от EAP във фазата взаимна идентификация и установените уязвимости в TLS косвено и потенциално засягат и сигурността в IEEE 802.11i.

Поради наследените уязвимости на WEP и фактът, че някои части от TKIP (като функцията *Michael*) притежават известни недостатъци, свързани със сигурността, към момента WPA постепенно излиза от употреба и не се препоръчва.

3.2. Безжичен защитен достъп 2/Wi-Fi Protected Access 2 (WPA2)

Алиансът Wi-Fi Alliance сертифицира системи за съответствие със стандарта IEEE 802.11i и по-точно алгоритъма R*obust Security Network Association (RSNA)* в комбинация с *CTR with CBC-MAC Protocol (CCMP)* под името Wi-Fi защитен достъп 2 (*Wi-Fi Protected Access 2 – WPA2)*. WPA2 може да се разглежда като първия протокол за безжични локални мрежи, който към момента на неговото въвеждане осигурява реална криптографска сигурност. Единственият му недостатък е бил необходимостта от нов хардуер, защото стандартният шифър RC4 от WEP е заменен от Advanced Encryption Standard (AES) [3,7,9].

CCMP е базиран на шифриращия алгоритъм AES, работещ в режим CCM. Режимът CCM съчетава функциите на CTR (Counter-Mode) за поверителност на данните и CBC-MAC (Cipher Block Chaining – Message Authentication Code) за автентификация и цялостност на данните. Използването на AES носи някои много сериозни подобрения.

С един-единствен 128-битов AES ключ е възможно да се криптират всички пакети, елиминирайки проблемите с алгоритъма за планиране на ключовете във WEP и TKIP. Освен това CCMP предоставя базиран на AES код за проверка на целостността на данните – *Message Integrity Code* (MIC) върху тялото на пакета и почти цялата заглавна част (header) на MAC кадъра. Поверителността и целостността на съобщението са подобрени чрез използването на един и същи 128-битов AES ключ. И тук, както и в TKIP, CCMP използва 48-битов сериен номер (PN), за да се предотвратят атаки от тип повторение и PN колизии.

В обобщение може да се каже, че протоколът CCMP осигурява едновременно поверителност и цялостност на

данните, както и автентификация и защита от атаки тип повторно изпращане. Съгласно стандарта IEEE 802.11i, за да удовлетворява една безжична локална мрежа на критериите на RSN, използването на CCMP е задължително [7].

Фиг. 6 илюстрира процеса на криптиране CCMP, докато табл. 2 обяснява използваните означения и съкращения.

Следващите стъпки обясняват CCMP криптирането на открития текст (полезния товар) на MPDU и капсулирането на шифрирания текст в MAC кадъра [1,7]:

1. С цел да се получи нов PN номер за всеки MPDU и съответно за създаването на временен ключ, този номер се инкрементира след всеки пакет.

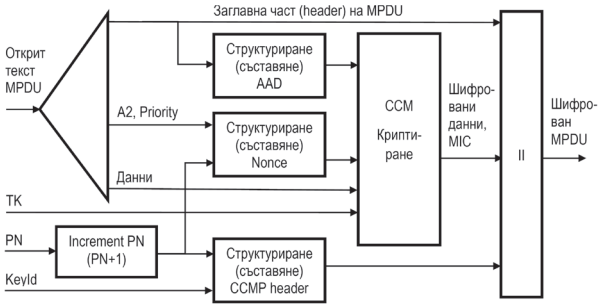
2. Допълнителните данни за автентификация (additional authentication data – AAD) се формират от заглавната част на MAC пакета и се предоставят за криптиране на CCM модула.

3. Едноразовото число (за еднократна употреба) – nonce на CCM в дадения случай се формира от инкрементирания PN, A2 (MPDU Address 2 field) и полето приоритет (Priority).

4. Идентификаторът на ключа (KeyId) и PN се поставят в заглавната част на CCMP пакета.

5. TK, AAD, *nonce* и MPDU данните се подават на модула за CCM криптиране, за да формират шифрирания текст и MIC. Тази стъпка е известна също така като обработка от CCM първоизточника или същинското CCM шифроване (*CCM originator processing*).

6. Последната стъпка е да се комбинират резултатите от предишните стъпки, за да се формира пакет, включващ заглавната част на MPDU, заглавната част на CCMP, шифрованите данни и MIC.



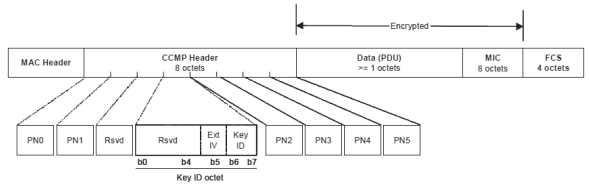
Фиг. 6. Процес криптиране съгласно протокол CCMP (от стандарт IEEE Std 802.11™-2012)

Табл. 2. Означения и съкращения съгласно протокола CCMP

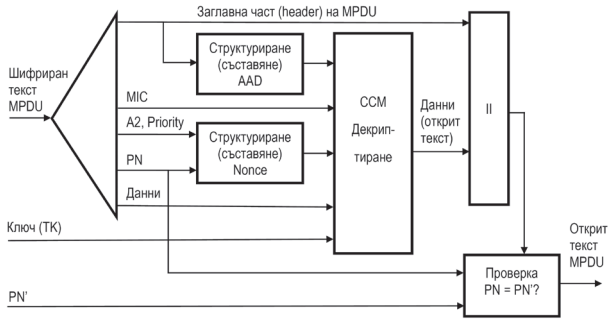
Описание	Означение
Номер на пакет/Packet number	PN
MPDU адрес 2/MPDU Address 2 field	A2
Допълнителни данни за удостоверяване/Additional authentication data	AAD
Временен ключ/Temporal key	TK
Идентификатор на ключ/Key identifier	KeyId
Данни (полезни и служебни) на MAC протокола/ Media access control (MAC) Protocol Data Unit	MPDU

Фиг. 7 показва формат на пакета WPA2 след CCMP криптиране.

Процесът на декриптиране съгласно протокол CCMP, показан на *фиг. 8*, работи точно по обратния начин на процеса на криптиране.



Фиг. 7. Формат на WPA2 пакет след CCMP криптиране (от стандарт IEEE Std 802.11™-2012)



Фиг. 8. Процес декриптиране съгласно протокол CCMP (от стандарт IEEE Std 802.11™-2012)

Използването на AES въвежда математически доказана криптографска сигурност в безжични локални мрежи [20]. Без познаването на ключа злонамерен противник не е в състояние да наруши поверителността или целостността на данните. Дори при атака с познат открит текст не е възможно да се получи информация за ключа [21].

Подобно на всеки приложим на практика криптографски механизъм и CCMP протоколът разчита на неприкосновеността на ключа. Добре известно е обаче, че схемите с предварително споделен ключ са много уязвими. Затова с цел изграждане на RSNA IEEE 802.11i налага процедурите за осигуряване на строго взаимно удостоверяване с помощта на протокола 802.1X и четирикратно ръкостискане (*фиг. 3*).

Анализ на сигурността на CCMP

Към момента на завършване на представеното в статията проучване няма информация за компрометиране на криптографската сигурност на AES в режим CBC. Т.е. без знанието на ключа не е възможен пробив в поверителността и нарушаване на целостността на шифрираните по протокола CCMP данни. Също така правилното използване на IEEE 802.1X и процедурата по четирикратно ръкостискане даваха гаранция, че временните ключове могат да се обменят безопасно между комуникиращите станции и че не е възможно злонамерен атакуващ да получи ключ. До октомври 2017 г. споменатата по-горе процедура остава доказано сигурна и не е атакувана, когато Vanhoef et al. [22] установяват, че тя е уязвима на атака за преинсталиране на ключ – *key reinstallation attack*, добила популярност като KRACK от *Key Reinstallation AttaCK*.

KRACK атаката е сравнително сложна, но най-общо би могла да се опише по следния начин [22][3]. Всеки

3 Като първа стъпка атакуващият заема позиция човек по средата (man-in-the-middle (MitM) position) между STA кандидат/заявител и автентификатора (AP) чрез реализация на базирана на канали атака човек по средата, при която AP е клонирана на различен безжичен канал с MAC адреса на целевата/атакуваната AP. Това гарантира, че клиентът и AP получават един и същи ключ на сесията.

път, когато клиент (*кандидат-заявител*) се асоциира към безжична мрежа, изпълнява процедурата четирикратно ръкостискане, за да бъде постигнато споразумение за нов сесиен ключ. Той инсталира този ключ след получаване на съобщение 3 от ръкостискането. След като ключът бъде инсталиран, той се използва за шифроване на обикновени кадри за данни от съответния протокол за осигуряване на поверителност на данните. Но тъй като е възможно отделни съобщения да бъдат изгубени или отхвърлени, *автентификаторът* препредава съобщение 3, ако не получи подходящ отговор като потвърждение от клиента. В резултат на това клиентът може да получи съобщение 3 няколко пъти. Всеки път, когато получава това съобщение, той преинсталира един и същи ключ на сесия и по този начин нулира постепенно инкрементирания брояч на пакети за предаване (*nonce*) и брояча на приетите пакети реплики, използвани от протокола за поверителност на данните. Авторите показват, че атакуващият може да инициира тези нулирания чрез многократно повторно предаване на съобщение 3. Повторното използване на nonce по този начин създава условия (възможност) да бъде атакуван протоколът за поверителност на данните, например пакетите могат да бъдат повторно изпращани, декриптирани и/или подправени. Същата техника Vanhoef et al. използват за атака над ръкостисканията за: групов ключ, PeerKey (процедура за четирикратно ръкостискане, използвана, когато два клиенти искат да комуникират помежду си по сигурен начин) и бърз BSS преход (Fast BSS Transition (FT) handshake).

Пораженията от успешна KRACK атака зависят от вида на атакуваното ръкостискане и използвания протокол за поверителност на данните. Срещу AES-CCMP противникът може да изпраща повторно пакети и да декриптира (но не може да фалшифицира) пакети. Това обаче прави възможно отвличане/прихващане на TCP потоци и инжектиране на злонамерени данни в тях. Според авторите при атака срещу WPA-TKIP и GCMP (Galios/Counter Mode Protocol – добавка в протокола с цел осигуряване и поддръжка на комуникации с малък обхват на честоти около 60 GHz, които изискват бърз шифър GCM) въздействието е катастрофално: пакетите могат да бъдат препредавани, декриптирани и подправени. Тъй като GCMP използва един и същи ключ за удостоверяване в двете посоки на комуникация, той е особено засегнат. В допълнение освен че потвърждават констатациите си с практически реализации, Vanhoef et al. са убедени, че всяко устройство с Wi-Fi е уязвимо към някакъв вариант на KRACK. Те установяват, че атаката е изключително поразяваща за Android 6.0: KRACK принуждава клиента да използва предсказуемия нулев (*all-zero*) ключ за шифроване.

Въпреки фирмените актуализации и препоръки на специалисти по информационна сигурност за заобикаляне и/или запушване на пробива в протокола и през октомври 2018 г. се появяват съобщения, че уязвимостта към KRACK все още се използва [23].

4. Безжичен защитен достъп 3 (WPA3)

От началото на 2018 г. Wi-Fi Alliance® въвежда Wi-Fi CERTIFIED WPA3™ отново в два варианта в зависимост от областта на използване: за лична/персонална употреба – *WPA3-Personal,* и за корпоративни приложения – *WPA3-Enterprise*. Съвсем накратко тук представяме някои нови характеристики относно информационната сигурност на WPA3 така, както ги лансират от Wi-Fi Alliance® [24].

WPA3-Personal

WPA3-Personal обещава по-добра защита на отделните потребители, като предоставя по-стабилна автентификация на базата на пароли, дори когато потребителите избират пароли, които не отговарят на типичните препоръки за сложност. Тази възможност се осигурява от функцията Simultaneous Authentication of Equals (SAE), която замества предварително споделения ключ (PSK) в WPA2-Personal. Технологията SAE е устойчива на атаки с offline речници, при които противникът се опитва да определи мрежова парола без допълнително взаимодействие в мрежата. В същото време WPA3-Personal предлага улеснения при използване като:

- Избор на естествена парола – позволява на потребителите да избират пароли, които са по-лесни за запомняне.
- Лесна употреба – подобрява защитата без промяна в начина, по който потребителите се свързват към мрежата.
- Поверителност напред/в перспектива (forward secrecy) – защитава трафика на данни, дори ако паролата е компрометирана след предаването на данните.

WPA3-Enterprise

WPA3-Enterprise се основава на WPA2 и осигурява строго и безкомпромисно прилагане на протоколите за сигурност в мрежата. В допълнение WPA3-Enterprise предлага (опционно) избор на усилени протоколи за сигурност и криптографски инструменти за по-добра защита на чувствителните данни, използващи като минимум 192-битови ключове:

- Автентифицирано криптиране (Authenticated encryption): 256-bit Galois/Counter Mode Protocol (GCMP-256).
- Извличане и потвърждаване на ключ (Key derivation and confirmation): 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384).
- Управление и удостоверяване на ключове (Key establishment and authentication): Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve.
- Солидна/гарантирана защита на управляващите кадри (Robust management frame protection): 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256).

Макар да е твърде рано за анализ на сигурността на WPA3, все пак още сега можем да забележим известни прилики в някои характеристики на WPA3 и WPA2. Например изтъква се, че методът на криптиране при WPA3-Enterprise е автентифицирано криптиране, какъвто по принцип е и методът на шифроване, използван във WPA2, но за блокови шифри с дължина на блока 128-бита [20]. Освен това тук отново се използва Galois/Counter Mode Protocol – GCMP (виж в част **Анализ на сигурността на CCMP**), който е доказано уязвим от KRACK. Новото е само в размера на използваните ключове.

5. Заключение

Резултатите от проведените проучване и анализ в специализираната литература на използваните протоколи за сигурност в безжични локални мрежи ни дават възможност да направим някои полезни изводи.

Първият протокол за сигурност в безжични локални мрежи WEP е изключително несигурен и не трябва да се използва. Поради наследените уязвимости от WEP и фактът, че някои части от TKIP (като функцията Michael) притежават известни недостатъци, свързани със сигурността, към момента WPA постепенно изчерпва своята роля на временна корекция на WEP за наследен/стар хардуер и не се препоръчва.

Въпреки че към момента на завършване на представеното в статията проучване няма информация за компрометиране на криптографската сигурност на AES в режим CBC, слабо място в процедурата за управление на криптографските ключове го прави уязвим и довежда до пробив в сигурността на WPA2 през октомври 2017 г. Макар че уязвимостта е отстранима чрез кръпка (patch), вероятно много WiFi-устройства не са актуализирани, което излага на риск потребителите. Освен това въпреки фирмените актуализации и препоръки на специалисти по информационна сигурност за заобикаляне и/или запушване на пробива в протокола и през октомври 2018 г. се появяват съобщения, че уязвимостта към KRACK все още се използва.

Литература

1. Gunther Lackner. A Comparison of Security in Wireless Network Standards with a Focus on Bluetooth, WiFi and WiMAX. – *International Journal of Network Security,* 15, Nov. 2013, No. 6, 420-436.

2. Borisov, N., I. Goldberg and D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. International Conference on Mobile Computing and Networking, 2001, 180.

3. Scott Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the Key Scheduling Algorithm of RC4, S. Vaudenay and A. Youssef (Eds.): SAC 2001, LNCS 2259, 1–24.

4. Andrew Roos. Vironix Software Laboratories. A Class of Weak Keys in the RC4 Stream Cipher, 22 September 1995.

5. Klein, A. Attacks on the rc4 Stream Cipher. – *Designs, Codes and Cryptography*, 48, 2008, No. 3, 269.

6. Tews, E., R. P. Weinmann and A. Pyshkin. Breaking 104 bit WEP in Less than 60 Seconds. Proceedings of the 8th International Conference on Information Security Applications, 2007, 188-202.

7. IEEE Std 802.11™-2012. https://legal.vvv.enseirb-matmeca.fr/download/amichel/%5BStandard%20LDPC%5D%20802.11-2012.pdf.

8. Keun Young Park et al. Security Enhanced IEEE 802.1x Authentication Method for WLAN Mobile Router, 2012 14th International Conference on Advanced Communication Technology (ICACT), 19-22 Feb. 2012.

9. Sheila Frankel et al. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, Recommendations of the National Institute of Standards and Technology, Special Publication 800-97, February 2007.

10. https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/68583-FAQ-Wireless-Security.html.

11. Kenneth G. Paterson, Bertram Poettering and Jacob C. N. Schuldt. Plaintext Recovery Attacks Against WPA/TKIP, Information Security Group Royal Holloway, University of London, 1 March 2014.

12. Avishai Wool. A Note on the Fragility of the "Michael" Message Integrity Code. – *IEEE Transactions on Wireless Communications*, 3, September 2004, No. 5, 1459-1462.

13. Ferguson, N. Michael: An Improved MIC for 802.11 WEP. Tech. Rep. IEEE, Jan 17, 2002.

14. Huang, J., W. Susilo, J. Seberry and M. Bunder. On the Security of the IEEE 802.11i Message Integrity Code Michael. Tech. Rep., 2004.

15. Martin Beck, Erik Tews. Practical Attacks against WEP and WPA. 8 November 2008.

16. Mathy Vanhoef and Frank Piessens. Practical Verification of WPA-TKIP Vulnerabilities. ASIA CCS'13, 8-10 May 2013, Hangzhou, China. Copyright 2013 ACM 978-1-4503-1767-2/13/05.

17. Nadhem AlFardan et al. On the Security of RC4 in TLS. This paper is included in the Proceedings of the 22nd USENIX Security Symposium. 14-16 August 2013, Washington, D.C., USA, ISBN 978-1-931971-03-4.

18. Kenneth G. Paterson, Bertram Poettering and Jacob C. N. Schuldt. Plaintext Recovery Attacks Against WPA/TKIP. Information Security Group Royal Holloway, University of London, 1 March 2014.

19. Mathy Vanhoef and Frank Piessens. All Your Biases Belong to Us:Breaking RC4 in WPA-TKIP and TLS. 24th USENIX Security Symposium, 12-14 August 2015, Washington, D.C. ISBN 978-1-931971-232.

20. RFC3610.

21. C. He and J. C. Mitchell. Security Analysis and Improvements for IEEE 802.11i. Proceedings of the 12th Annual Network and Distributed System Security Symposium, 2005, 90-110.

22. Mathy Vanhoef and Frank Piessens. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, CCS'17, 30 October – 3 November 2017, Dallas, TX, USA.

23. Mathy Vanhoef and Frank Piessens. Release the Kraken: New KRACKs in the 802.11 Standard. In 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18), 15-19 October 2018, Toronto, ON, Canada. ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3243734.3243807.

24. https://www.wi-fi.org/discover-wi-fi/security.

25. Wagner, D. Weak Keys in RC4 (sci.crypt). 1995.

За контакти:

Инж. **Кирил Димитров**

Секция „Комуникационни системи и услуги"

Институт по информационни и комуникационни технологии – БАН

e-mail: kpd@iccs.bas.bg