7. Benchmarking network IDS. [Электронный ресурс] / Режим доступа: http://archives.neohapsis.com/archives/sf/ids/2000-q4/0244.html, свободный. – Загл. с экрана.

Половко Иван Юрьевич
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: ivan.polovko@gmail.com.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 8(8634)371-905.
Кафедра безопасности информационных технологий; аспирант.

Polovko Ivan Yurevich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: ivan.polovko@gmail.com.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: 8(8634) 371-905.
The Department of IT Security; post-graduate student.

УДК 681.324

К.И. Емельянов

РЕАЛИЗАЦИЯ АТАКИ НА ПРОТОКОЛ WPA2

В статье описывается практическая реализация атаки на подсистему обеспечения безопасности беспроводных протоколов TKIP (Temporal Key Integrity Protocol), использующуюся в WPA/WPA2.

Безопасность беспроводных протоколов; WPA; WPA2; TKIP; атака; точка доступа.

K.I. Emelianov

IMPLEMENTATION OF THE ATTACK ON THE PROTOCOL WPA2

The article describes the practical realization of the attack on the subsystem wireless security protocols, TKIP (Temporal Key Integrity Protocol), used in WPA/WPA2.

Wireless security protocols; WPA; WPA2; TKIP; attack; access point.

Анализ безопасности протокола WPA

Протокол WPA, хоть и является более защищённым, чем WEP, но имеет уязвимости, обусловленные используемым алгоритмом шифрования RC4 и использованием алгоритма CRC32, который не дотягивает по требованиям до криптографической хеш-функции.

На рис. 1 блок Network Data идет после MAC Header (чек-сумма FCS здесь не показана, так как ее обработка ведется на нижележащем уровне модели OSI). IV – это тот же 24-битовый WEP Initialization Vector, только смысл его несколько иной, структура данных же пакета значительно усложнилась.

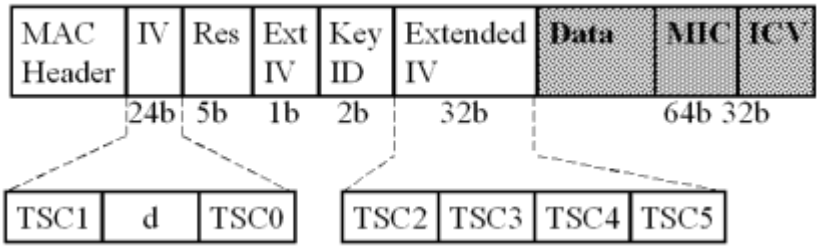

Рис. 1. Формат TKIP пакета

Чтобы понять, что означают представленные поля, рассмотрим протокол TKIP (рис. 2).

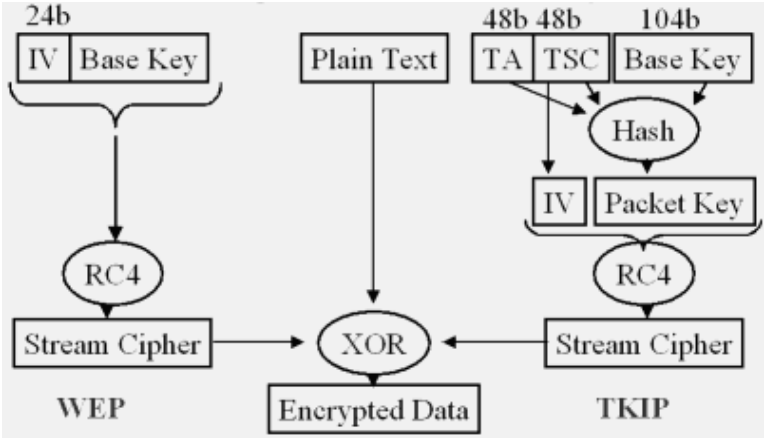

Рис. 2. Алгоритм TKIP

TKIP (Temporal Key Integrity Protocol) реализует три подхода к улучшению безопасности радиопротоколов семейства IEEE 802.11. Во-первых, это функция смешения ключей, которая комбинирует секретный основной ключ PTK (см. ниже) с вектором инициализации перед тем, как передать его в качестве ключа алгоритму RC4. Во-вторых, это последовательный счетчик (TSC – TKIP Sequence Counter) 48-битной длины, значение которого растет с каждым переданным пакетом. Пакеты, полученные в неверном порядке, будут отвергнуты (а именно, будут отвергнуты пакеты с более ранним TSC), что позволяет защищаться от так называемых replay-атак. Наконец, это 64-битный код защиты сообщения MIC (Message Integrity Code).

TKIP реализует также механизм rekeying'а – смены сессионных ключей и гарантирует, что каждый пакет будет передан с уникальным RC4 ключом.

Основной сессионный ключ PTK (Pairwise Transient Key) – это набор из 4-х 128-битных ключей, используемый для TKIP для шифрования отдельных пакетов в периоды между сменами ключей. Заметим, что PTK – это не пароль WEP и ни он, ни механизм его генерации частью TKIP не являются.

В PTK входят 4 ключа: один – для шифрования данных в TKIP (назовем его TK), другой – для вычисления MIC (а его MTK) и еще два так называемых EAPOL

ключа, которых я касаться не буду. Ключи генерируются с использованием пароля WPA, известного обеим сторонам, в процессе четырехэтапного «рукопожатия».

На рис. 2 видим, что все, что между MAC Header и Data по сути – счетчик TSC плюс некоторые служебные поля, служащие для защиты от слабых ключей и говорящие о том, что используется Extended IV. TSC устанавливается в нуль при начале сессии и монотонно увеличивается с каждым переданным данным устройством пакетом, емкости в 48 бит хватит на ~250 триллионов пакетов, что можно считать достаточным с учетом периодической реинициализации сессионных ключей (в отличие от 24-битного IV в WEP). Уникальный ключ для шифрования пакета вычисляется из TK, TA (Transmittor Address – MAC адрес передатчика) и TSC путем определенного двухфазного механизма хеширования, который дает на выходе 104-битовую строку, к которой добавляется WEP IV для получения 128-битового ключа.

MIC создан, в основном, для борьбы с подделкой (forgery) пакетов. Код вычисляется от данных всего сообщения (плюс адреса передатчика и приемника) еще до фрагментации и возможной смены порядка пакетов с помощью алгоритма под названием MICHAEL, генерирующего подпись длины 64 бит. Алгоритм, кроме данных, использует ключ, а именно, вышеупомянутый MTK. Что немаловажно, алгоритм в некотором смысле обратим, то есть зная данные и MIC-подпись, можно вычислить ключ MTK.

Борьба с подделкой со стороны Access Point происходит так: если пришел пакет с неверным MIC (при этом он валиден по остальным признакам, то есть имеет допустимое значение TSC и ICV сумма прошла проверку), то отправителю посылается уведомление и, если есть возможность, данное событие фиксируется в журнале как попытка взлома. Если в течение 60 секунд приходит еще один пакет с неверным MIC, точка доступа инициализирует rekeying с данным отправителем. Таким образом, поддельные пакеты относительно безнаказанно можно слать не чаще, чем раз в минуту.

Практическая атака на WPA

Из внушительного списка атак, к которым уязвим WEP, рассмотрим так называемую Chop-Chop-атаку (от англ. chop, вольный перевод — «отрезать ломтик»). Эта атака позволяет узнать plaintext сообщения (то есть данные сообщения до шифрования), а значит и RC4 keystream пакета (plaintext + keystream = ciphertext => keystream = ciphertext + plaintext). Атака использует тот факт, что CRC32 чек-сумма отнюдь не проходит по требованиям в криптографическую хеш-функцию [3].

CRC есть остаток от деления исходной строки S, представленной в виде многочлена (от X) с коэффициентами, равными соответствующим разрядам в ее двоичной записи, на предопределенный многочлен PCRC(X), причем арифметические операции выполняются в поле GF(2) (подробнее, например, в википедии). Однако в такой форме CRC нечувствителен к нулям в начале и в конце исходной строки, поэтому на практике в начало и конец дописываются специальные строки (длины, равной количеству разрядов CRC), которые обозначим как Li (начало) и Lf (конец). Обычно обе они состоят из 32-х двоичных единиц. Таким образом, для CRC32:

$$CRC = (X32 * S + Li * Xn+32 + Lf) \bmod PCRC, \quad (1)$$

где n – длина S в битах.

Примечательно, что если к исходной строке S приписать справа ее CRC, то CRC от полученной строки будет постоянна и равна CRC пустой строки, которую обозначим за Pzero (доказывается очень просто, достаточно помнить, что в GF(2) сложение и вычитание суть одна и та же операция — XOR), или в виде формулы

$$(X32 * (X32 * S + CRC) + Li * Xn+64 + Lf) \bmod PCRC = Pzero. \quad (2)$$

В WEP-пакете последние байты данных (Network Data) – это зашифрованный ICV, то есть CRC от сообщения. Забудем на время о шифровании и рассмотрим, что будет, если убрать последний байт, который обозначим как R, из пакета. Пусть Q – пакет без последнего байта, тогда Q уже навряд ли будет иметь нужный остаток (то есть CRC). Но оказывается, что к Q можно прибавить некий многочлен M так, чтобы исправить CRC. Подставив сначала SO = Q * X8 + R, а затем S1 = Q + M в (2), легко найти, что M = (X32)-1 * (1 + (X8)-1) * (Pzero + Lf) + (X8)-1 * R.

Возвести многочлен P в -1ю степень означает найти такой многочлен P', что P * P' = 1 mod PCRC, что всегда возможно, так как PCRC неприводим и многочлены с операциями по модулю PCRC образуют поле. Кстати, степень M не превышает 32, так как M достаточно взять по модулю PCRC.

Если перебирать все байты R от 0 до 255 и отправлять их в сеть точке доступа, то, в конце концов, можно наткнуться на правильный. Понять, что попали в байт в реальности также несложно: пакеты с неверным ICV отбрасываются как переданные с ошибкой; если же CRC верна, мы вправе ожидать ответный пакет, например, в случае WPA, это обычно будет пакет, информирующий о неверном MIC.

Тот факт, что пакет шифрован, значения не имеет, так как шифрование RC4 алгоритмом сводится к XOR-иванию данных с keystream'ом, но прибавление M это тот же XOR, а так как операция XOR коммутативна и ассоциативна, то и неважно, прибавлять M к исходным данным, а потом шифровать, или к уже зашифрованным.

Описанный процесс можно повторять дальше, беря по байту от сообщения, и теоретически можно расшифровать WEP пакет произвольной длины.

Рассмотрим на практике Chop-Chop атаку на сеть с WPA защитой. TKIP имеет, в основном, 2 средства для защиты от подобных атак:

1. Пакеты с неверной ICV отбрасываются. Если ICV угадана, но неверен MIC-код, атакующий должен выдержать минуту, чтобы не спровоцировать смену ключей.

2. Если пакет принят, TSC-счетчик для этого канала (TSC-счетчики существуют отдельно для каждого канала, в которые данное устройство может слать пакеты) увеличивается на 1. Пакеты с меньшим, либо равным TSC с этого момента отбрасываются.

Первый пункт частично на руку атакующему, так как позволяет понять, когда он угадал очередной байт. Со вторым сложнее: действительно, пусть перехвачен ARP пакет, посланный одним из устройств в сети, его же получила и Access Point, пересылать этот пакет ей еще раз бессмысленно, ведь TSC уже инкрементирован, плюс то первое устройство, возможно, наслало еще пакетов, увеличив счетчик еще больше. Авторы рассматриваемой атаки нашли выход в спецификации IEEE 802.11e, определяющей улучшения в QoS для сетей Wi-Fi [4]. Устройства Wi-Fi поддерживают несколько очередей пакетов, по словам одного из авторов, Эрика Тьюза, предполагалось использовать 4 канала, в стандарте их 8, в реальности авторы обнаруживали до 16. Каналы обыкновенно не используются одновременно,

экономя пропускную способность для важных пакетов. В ненагруженной сети часто весь трафик идет в один канал, таким образом пакет мы скорее всего поймаем на канале с высоким значением счетчика TSC, перепосылать же его можно, переключившись на менее нагруженный канал. Важно, что при отсылке сообщения о неправильном MIC счетчик канала не увеличивается, таким образом дальше каналы можно не переключать.

Если в сети не поддерживаются QoS-расширения, атака, в принципе, также осуществима, если удастся предотвратить попадание выбранного для дешифровки пакета на AP и отключить пославшее его устройство от сети.

Понятно, что пытаться расшифровать сколько-нибудь длинные пакеты по байту в минуту бессмысленно – стандартный Wi-Fi-пакет имеет размер ~2300 байт, то есть на него уйдет порядка полутора суток, а за это время или TSC-счетчик увеличится, или ключи сменятся, или перезагрузится точка доступа. Причем, имея одно устройство, взломать можно только один пакет.

Поэтому имеет смысл направлять усилия на расшифровку коротких пакетов, например, ARP, которые легко идентифицировать по их длине (14 байт). Собственно, атакующий знает большую часть содержимого APR-пакета, а именно, заголовки и MAC-адреса. Если можно также сделать и некоторые предположения об IP-структуре взламываемой сети (в сети созданной из под Windows, например, можно ожидать, что IP-адреса будут иметь вид 192.168.0.x), то угадать останется совсем немного. То есть, угадав 12 байт ICV + MIC, остальное можно просто подобрать, используя ICV-сумму.

Расшифровав один пакет, атакующий узнает RC4-keystream пакета (использовать его, правда, можно только, пока TSC не изменился) и, что более важно, сессионный MTK – а MIC обратим, и по данным и подписи можно установить ключ. Последнее означает, что до следующей смены ключей нет необходимости больше угадывать MIC, и, например, чтобы взломать следующий ARP-пакет (с теми же предположениями о структуре сети), уйдет 4-5 минут. Использовать дешифрованные данные для посылки forged пакетов можно, в зависимости от количества QoS каналов, от 7 до 15 раз (меньше, если трафик идет по более, чем одному каналу), дальше придется анализировать другой пакет.

Заключение

Атака позволяет расшифровать отдельные короткие пакеты, с которыми ведется работа, затрачивая в самом лучшем случае по 4-5 минут на пакет, и, используя результаты дешифровки, инжектировать очень ограниченное число столь же коротких пакетов обратно в сеть.

Атака не может быть использована ни для подключения к домашней или корпоративной сети, ни для того, чтобы отслеживать в них трафик.

Тем не менее, с её помощью можно «отравить» ARP и DNS-кеш, и прочитать некоторый объем приватного трафика, обмануть некоторые фаерволы.

Хотя шифры и не взламываются окончательно, администраторы беспроводных сетей должны переосмыслить использование WPA и TKIP. Многие компании уже столкнулись с необходимостью модернизации беспроводных сетей для обеспечения их соответствия требованиям стандарта PCI DSS 1.2, который недавно появился для замены WEP в качестве меры защиты в беспроводных сетях, работающих с конфиденциальной информацией.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin*. Breaking 104 bit WEP in less than 60 seconds [Электронный ресурс] / Режим доступа: http://eprint.iacr.org/2007/120.pdf, свободный. – Загл. с экрана.

2. Aircrack manual [Электронный ресурс] / Режим доступа: http://www.aircrack-ng.org/doku.php, свободный. – Загл. с экрана.

3. *Adam Stubble_eld, John Ioannidis, and Aviel D. Rubin.* A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). ACM Transactions on Information and System Security, 7(2):319{332, May 2004.

4. *Erik Tews.* Attacks on the wep protocol. Cryptology ePrint Archive, Report 2007/471, 2007. [Электронный ресурс] / Режим доступа: http://eprint.iacr.org/. - свободный. – Загл. с экрана.

Емельянов Константин Игоревич
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: kostaemrlyanov@gmail.com.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; аспирант.

Emelianov Konstantin Igorevich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: kostaemrlyanov@gmail.com.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
The Department of IT Security; post-graduate student.

УДК 007.51:004.822

М.И. Тенетко, О.Ю. Пескова

АНАЛИЗ И ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ С ИСПОЛЬЗОВАНИЕМ НЕЧЁТКОЙ СЕМАНТИЧЕСКОЙ СЕТИ

В данной статье предложен новый подход к описанию информационного риска, основанный на нечётких множествах и нечётких семантических сетях. Проведено теоретико-множественное исследование структуры риска. Построена нечёткая семантическая сеть, описывающая структуру риска. Сделаны выводы относительно практического применения рассмотренного подхода.

Анализ рисков; нечеткие множества; нечеткие семантические сети.

M.I. Tenetko, O.U. Peskova

ANALYSIS AND RISK ASSESSMENT INFORMATION USING FUZZY SEMANTIC WEB

In the given article a new fuzzy sets and fuzzy semantic networks based approach to description of informational risk is proposed. A set-theoretical analysis of a risk struc-