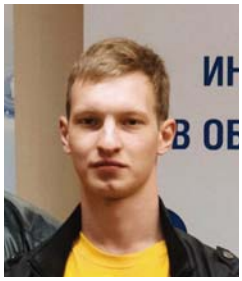
АНАЛИЗ БЕЗОПАСНОСТИ БЕСПРОВОДНОЙ СЕТИ



Закревский Александр Сергеевич
Студент 4 курса, направление: «Информационная безопасность автоматизированных си-стем» Московского политехнического университета

Будылина Евгения Александровна
Кандидат физико-математических наук, доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета.

Аннотация: *В статье рассматриваются протоколы безопасности беспроводной сети, их ограничения и недостатки. Также рассмотрена атака с использованием ключа восстановления, и продемонстрирована его эффективность в уменьшении среднего числа пакетов перехвата на основе выбора векторов инициализации. Было проведено ряд сравнительных экспериментов по атакам только зашифрованным текстом, чтобы изучить эффективность такой техники и подчеркнуть возникшие трудности.*

Ключевые слова: *информационная безопасность, цифровые технологии, Wi-Fi, : WEP, WPA, WPA2, FMS, протоколы передачи данных.*

Abstract: *the article discusses wireless network security protocols, their limitations and disadvantages. An attack using a recovery key is also considered, and its effectiveness in reducing the average number of intercept packets based on the selection of initialization vectors is demonstrated. A number of comparative experiments on ciphertext-only attacks were conducted to examine the effectiveness of such a technique and highlight the difficulties encountered*

Keywords: *information security, digital technologies, Wi-Fi,: WEP, WPA, WPA2, FMS, data transfer protocols.*

Введение. В последние время наблюдается значительное увеличение развития беспроводных сетей; они становятся неотъемлемой частью Интернета и демонстрируют эффективность в управлении связью для ограниченных общедоступных локальных сетей и военных приложений. В основном это связано с их мобильностью и дешевыми решениями; тем не менее, они также подвержены нескольким атакам, связанным с целостностью данных, отказом в обслуживании и прослушиванием. На самом деле, беспроводные сети становятся важным инструментом связи благодаря своей гибкости, эффективности и низкой стоимости. С другой стороны, беспроводные сети имеют много ограничений в отношении традиционных сетей, таких как уменьшение объема данных и низкое энергопотребление [1,2]. Кроме того, беспроводные сети передают данные с помощью радиоволн, которые обычно чувствительны к прослушиванию; хотя необходимо сохранять данные, передаваемые через сетевые узлы, постоянно зашифрованными, чтобы предотвратить несанкционированный доступ к своему контенту. В беспроводных сетях управление связью осуществляется протоколами WEP, WPA и WPA2, разработанными для защиты связи. Однако и с учетом их ограничений решения для безопасности, предназначенные для таких сетей, становятся недостаточными для защиты от атак на секретные ключи. Целью данного исследования является описание вопросов, связанных с безопасностью в беспроводных сетях; Мы сосредоточены на протоколах WEP и WPA, которые все еще широко используются, но также не способны обеспечить защиту от различных угроз и уязвимостей, таких как атака FMS, которая основана на слабости вектора инициализации и требует около 4 миллионов пакетов для восстановления секретного ключа [3]. , Наш вклад заключается в том, чтобы найти лучший способ выбора, чтобы уменьшить среднее количество пакетов перехвата, необходимых для восстановления секретного ключа. Этот факт уменьшает время прослушивания при использовании пассивных атак. Итак, после введения в статье представлен краткий обзор существующих беспроводных протоколов, их особенностей и недостатков в разделах 2; Раздел 3 представляет справочную информа-

цию о предыдущих работах, связанных с угрозами и атаками [4]. Мы фокусируемся на производительности атаки FMS в разделе 4, затем следуют некоторые сравнительные эксперименты, основанные на статистическом анализе объема перехваченного трафика с целью выявления секретных ключей, после чего обсуждаются результаты и выводы.

Wi-Fi Протоколы: проводные соединения на основе стандарта IEEE 802.11 позволяют подключать ноутбуки, настольные компьютеры, КПК или любое устройство с широкополосным соединением на расстоянии нескольких сотен метров в открытой среде. Wired Equivalent Privacy (WEP), часть стандарта IEEE 802.11, создана в 1999 году и широко применяется на устройствах WLAN; он разработан для обеспечения конфиденциальности, аутентификации и целостности, аналогичных проводным сетям [5]. WEP основан на схеме шифрования RC4 и CRC-32 для обеспечения целостности данных и использует секретный ключ сегмента k длиной от 5 до 13 байтов. Чтобы создать зашифрованный текст C и его контрольную сумму ICV из открытого текста M, ключ k объединяется с вектором инициализации из 3 байтов в соответствии со следующей формулой (1):

$$C=M||ICV(M) \oplus RC4(K)||IV$$

где || обозначает оператор конкатенации, а $\oplus$ - побитовый исключающий оператор ИЛИ.

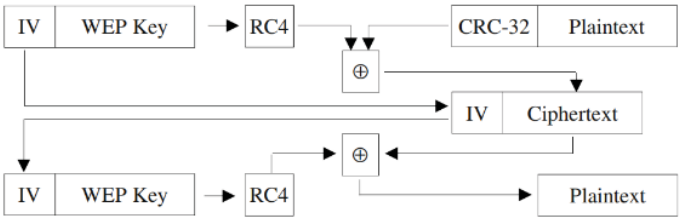


Рисунок 1. WEP процесс инкапсуляции

Вектор является краеугольным камнем безопасности WEP; он увеличивается для каждого испускаемого пакета, чтобы два последующих пакета не могли быть зашифрованы одним и тем же ключом. Это предполагает поддержание достойного уровня безопасности и предотвращение утечки информации [6]. WEP был задуман как первый инструмент безопасности сетей Wi-Fi. WEP призван быть относительно эффективным и реализуемым как в аппаратном, так и в программном обеспечении. Кроме того, испускаемые пакеты шифруются отдельно независимо друг от друга, что позволяет избежать повторной синхронизации при потере пакетов. Защищенный доступ Wi-Fi (WPA) является улучшенной версией стандарта 802.11i, разработанной Wi-Fi-Aliance в 2001 году [7]. Он основан на протоколе целостности временного ключа (TKIP), надежном алгоритме шифрования, построенном на основе WEP; это позволяет генерировать случайные ключи, которые отключают атаки на основе статистического анализа. WPA включает некоторые улучшенные свойства, такие как код целостности сообщения (MIC) и хэш-функция ключа, чтобы избежать атак. Рисунок 2 иллюстрирует процесс WPA-TKIP, где TK, DA, SA обозначает соотв. временный ключ, адреса отправителя и получателя и ||, оператор конкатенации.

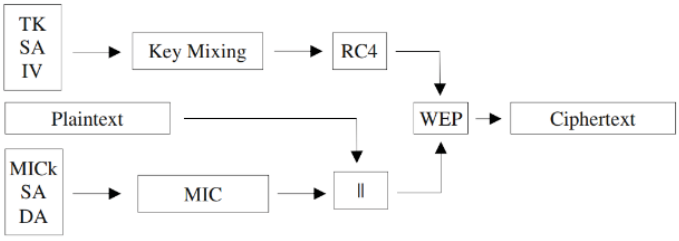


Рисунок 2. WPA процесс инкапсуляции

Обзор безопасности протоколов Wi-Fi: конфиденциальность и целостность данных являются наиболее важной проблемой в безопасности беспроводных сетей, особенно при обмене конфиденциальной информацией о промышленных, военных приложениях или распределении ключей. Защита WEP основана на структуре Rivest Cipher 4 (RC4), алгоритме потокового шифра, где открытый текст X-ored с последовательностью случайных байтов, сгенерированных алгоритмом планирования ключей (KSA) и алгоритмом псевдослучайной генерации (PRGA), части RC4, однако, доказано, что эти байты на самом деле не случайные, как они должны быть; они построены на длине ключа 64 бита, но на самом деле 40 бит фиксированы. Оставшиеся 24 бита предлагают всего 16 миллионов возможностей и, статистически, дают 50% шанс повторного использования IV после менее чем 5000 пакетов; однако, это может быть уязвимым для парадоксальной атаки на день рождения. Кроме того, в WEP используется один ключ, общий для всех узлов и точек доступа, и он не часто меняется. Основываясь на этих недостатках, WEP уязвим для нескольких ключевых типов атак, таких как DoS-атаки, захваты узлов, анализ трафика и т. д. Borison et al. представили некоторые недостатки в WEP, связанные со структурой RC4, которая состоит из инициализации и увеличения их на единицу для каждого использования [8]. А поскольку пространство клавиш сокращено, что дает высокую вероятность повторного использования потоков ключей; Слабость также была обнаружена Fluhrer et al. с использованием атаки FMS; идея заключалась в том, чтобы идентифицировать слабые клавиши, которые можно использовать для определения набора выходных битов; Результаты показали, что для восстановления секретного ключа достаточно 4 миллионов пакетов. Та же атака требует более 5 миллионов пакетов для восстановления секретного ключа в другой реализации, реализованной в. Подобно атаке FMS, атака Korek пытается выявить начальные биты ключей из блоков данных, сгенерированных алгоритмом PRGA; Результаты были получены методом грубой силы на наборе 1 миллион ключей. Несколько других атак, таких как атака Клейна , атака PTW , позволили раскрыть секретный ключ с 30–60 тысячами пакетов. VV атака использует случайные пакеты; Результаты показали, что для восстановления секретного ключа достаточно 32 тысяч

пакетов. Эти результаты были уменьшены до 24 тысяч Beck et al. Используя разные ключи для каждого зашифрованного пакета, успешные атаки на протоколы WPA и WPA2 кажутся редкими и сложными на практике. DoS, основанные на атаках, где они часто используются, пытаются насыщать целевой компьютер внешним трафиком, чтобы замедлить его; атаки заставляют систему перезагружаться; следовательно, он становится не в состоянии идентифицировать законные запросы [9]. Также является популярной атакой, она нацелена, в частности, на GTK, общий ключ для всех сетевых устройств, используемых для широковещательного трафика, который не может обнаружить подделку адресов и подделку данных. Этот ключ позволяет пользователю в сети осуществлять атаку, такую как DoS или спуфинг DNS, путем внедрения трафика из одной точки доступа в другие машины, связанные с той же самой точкой доступа. Этот акт продвигает машины-жертвы для пересылки трафика, предназначенного для точки доступа. Злоумышленник способен перехватывать все незашифрованные пакеты, не будучи обнаруженным точкой доступа. Аналогично, другие атаки были также выполнены на TKIP, BT-атака состоит в том, чтобы выполнить незначительные изменения в коротких пакетах ARP и DNS для восстановления открытого текста и потока ключей и, в свою очередь, перейти к атакам отравления DoS и ARP. Атака BT была улучшена атакой Ohigashi-Morii , которая сочеталась с атакой «человек посередине», чтобы сократить время выполнения. Таблица 1 иллюстрирует наиболее популярные атаки на протоколы WEP и WPA, где секретный ключ раскрывается по количеству упомянутых пакетов.

Обзор атаки FMS: секретный ключ k и вектор инициализации представляют собой основной недостаток протокола WEP; только 3 байта изменяются для каждого передаваемого пакета, в то время как 13 байтов k все еще статичны. Эти недостатки используются большинством атак против ключевых потоков. FMS, известная атака открытого текста, требует знания первого байта ключевого потока и большого количества векторов инициализации, чтобы иметь достаточно слабого, необходимого для успеха атаки. FMS основана на двух условиях:

а. На итерации i KSA, если мы достигли стадии, где x = Si , y = Si [x], x + y = Si [x] + Si [Si [y]] с 1<i<x<x+y; тогда вероятность 5% того, что ни один из элементов x, y и x + z не будет использоваться в последующих итерациях, и S [x] + S [S] может быть первым байтом, сгенерированным PRGA. Эта ситуация называется разрешенным состоянием.

б. В разрешенном состоянии показывает, что значение следующего байта ключа ключа k с вероятностью 5% будет равно $S(b)=S_{b+2}^{-1}[Out]-J_{b+2}-S_{b+2}[b+3]$, если S [1] <I и S [x] + S [S [1]] = I + b, где Out - первый выход PRGA; I, S, S-1 являются векторами состояния KSA для первых b итераций. При применении WEP мы предполагаем, что мы знаем первые байты секретного ключа k , .., k [a + 2]. Изначально мы имеем a = 0, поэтому известны только 3 байта. Исходя из этих соображений, FMS пытается смоделировать первые x итераций KSA, что позволяет определить перестановку Sx-1 и связанные с ней индексы ix-1 и jx-1. Следующее значение i также известно (ix = x), но следующее значение j зависит от следующего выбранного байта ключа. Байт случайного ключа имеет только 5% шансов быть верным; таким образом, можно определить следующий байт ключа среди нескольких байтов-кандидатов при их появлении, извлеченных из большого количества пакетов. Этот принцип может быть выбран при выборе всех следующих байтов ключа. Как это указывает, успех такой идеи зависит

Таблица 1. Сводка самых популярных атак восстановления секретных ключей

Protocol	Attack	Type	IV-search	Year	Packets (million)
WEP	FMS [10]	Statistical	Random	2001	4-6
	Korek [13]		Random	2004	0.1
			Brute-force		0.001-1
	PTW [15]		Random	2007	0.04
			Brute-force		1
	VV [16]		Random	2007	0.32
	Klein [14]	Key-recovery	Random	2008	0.25-0.6
	BT [17]		Aircraft-ng	2009	0.24
WPA	Dictionary attack	Key-recovery			
	Beck and Tews [19]	QoS		2009	
	Ohigashi-Morii [20]	Inject packets		2009	
	Hole196 [18]	Man-in-the-middle		2010	

от слабого пакета. Слабый пакет позволяет раскрыть информацию о ключевых байтах, он имеет особую форму (a + 3, 255, x), где a обозначает k-байт, который должен быть найден, а x не имеет значения. Эта форма обозначена высокой корреляцией между пакетом и выходом PRGA. Поскольку IV просты, слабые IV легко обнаружить. Другой вариант Weak-IV, называемый независимыми от ключа слабыми пакетами, предложенный с приведением к t = S3 [1] + S3 [S3 [1]] и используемый для угадывания k [t], где 3t. Также Fluhrer & al. [предложил другой способ выбора: зависимые от ключа слабые приводят к SI [1] <I и SI [x] + SI [SI [1]] = I + b, где I, размер IV (= 3) и a, угаданный a-тый байт ключа.

Экспериментальное исследование: обзор реализации FMS-атаки на протоколы WEP. Цель эксперимента - проанализировать эффективность такой атаки в реальной среде Wi-Fi, ее стоимость и, если возможно, внести свой вклад в ее улучшение. Эксперименты проводились на 3,2 ГГц процессоре; среда включает пакет aircrack-ng в системе Linux; нам также необходимо установить беспроводную карту в режиме монитора. Для сбора данных мы используем инструмент airdump-ng, переключаемый на определенные пакеты AP из одного канала. Мы использовали совместимый сетевой интерфейс, который позволяет генерировать и вводить пакеты для увеличения трафика. Захваченные пакеты были разделены на три файла в соответствии с их особенностями: специфическая форма, зависимость от ключа слабая и независимая от ключа слабая. Кроме того, все захваченные пакеты были сохранены в другом файле, который использовался для исчерпывающего поискового теста [10]. Наконец, мы приступаем к атаке, которая выглядит типовой: для каждого байта ключа мы выбираем файл, каждый пакет соединяется с секретным ключом и переходим к первым трем итерациям алгоритма KSA. Затем мы можем искать каждый байт ключа, который проверял разрешенное условие, используя aircrack-ng. Гистограмма на следующем рисунке показывает изменение времени процессора для каждой категории.

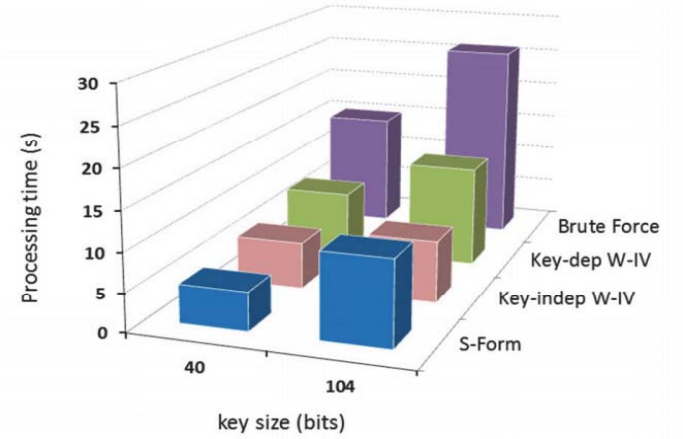


Рисунок 4. Изменение времени процессора с формой выбора

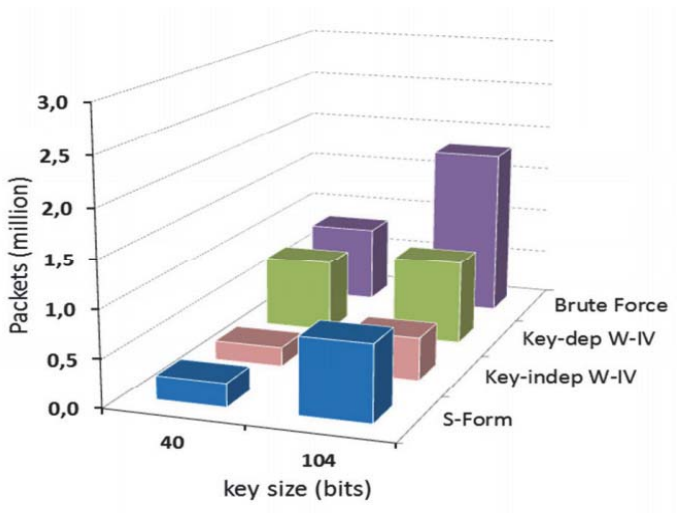


Рисунок 5. Вариация трафика, используемая с IV формой выбора

Примечательно, что независимый от ключа слабые пакеты превосходит другие формы. Кроме того, грубой силе требуется гораздо больше времени, чтобы улучшить свою производительность, особенно для ключа длиной 104 бита. Кроме того, оказывается, что и в той же среде независимый от ключа слабый IV в большинстве случаев значительно лучше. В целом, атака FMS доказала свою эффективность для атаки WEP. В целом, наш вклад с менее чем 0,2 миллионами пакетов и по сравнению с результатами, представленными в Таблице 2, представляется улучшенным способом значительного уменьшения размера данных, необходимых для успеха атаки FMS. Однако текущие исследования в области беспроводного криптоанализа направлены на атаки WPA и WPA2, которые остаются неэффективными до сегодняшнего дня.

Table 2. Summary of most popular alternatives of FMS attack

FMS attack	Amount of packets (million)	Success prob.
Fluhrer et al. [10]	4-6	100
Stubblefield et al. [11]	1-2	
Hilton [27]	1	
Tews et al [15]	0.7	50

Рисунок 6. Размеры данных, необходимых для успеха атаки FMS

Вывод: Протоколы Wi-Fi заявляют о предоставлении решения безопасности, такого как проводные сети; они по-прежнему представляют интерес до сегодняшнего дня. Однако такие протоколы не являются полностью безопасными и могут стать целью атак восстановления ключей в реальном мире. В этой статье мы пролили некоторый свет на поведение протокольных атак и продемонстрировали, что на практике они кажутся сложнее, чем в теории, и вероятность их успеха часто просчитывается и зависит от среды тестирования, которая различается в зависи-

мости от каждого вклада. Результаты в литературе не могут быть воспроизведены из-за отсутствия деталей среды, таких как особенности пакетов и настройки реализации, которые, кажется, воспринимаются эвристически. Наши эксперименты показывают, что FMS не является полной атакой восстановления ключа, но может быть улучшена путем хорошего сбора пакетов; Таким образом, независимая от ключа стратегия слабого кажется лучшим способом выбора слабых ключей и позволяет выявлять секретные ключи менее чем за 10 секунд в среднем с полмиллиона пакетов. На основании предыдущих результатов можно сделать вывод, что ключевая безопасность протоколов на основе алгоритма RC4 просто предотвращает произвольные уязвимости, но не против злоумышленников; Векторы инициализации кажутся самым слабым звеном в процессе безопасности. Алгоритм AES, основанный на протоколах, является более устойчивым к атакам, но его развертывание в активных сетях кажется слишком дорогим из-за их схемы шифрования (CCMP), которая требует изменений в аппаратном оборудовании.

Список литературы

1. Akyildiz I. F, Su W, Sankarasubramaniam Y and Cayirci E. Wireless sensor networks: a survey. Computer Networks 2002; 38:393-422.
2. IEEE Std 802.11a. Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. LAN/MAN Standards Committee of the IEEE Computer Society. 1999.
3. Rivest R. The RC4 encryption algorithm. RSA Data Security. 1992.
4. IEEE Std 802.11.Information Technology-Telecommunication and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11-Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.1997.
5. Edney J, William A. Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Boston: Addison-Wesley Longman Publishing Co. 2003.
6. Ferguson N. Michael: an improved MIC for 802.11 WEP. IEEE doc. 802.11-2/020r0. 2002.
7. Housley R, Whiting D, Ferguson N. Alternate Temporal Key Hash. IEEE doc. 802.11-02/282r2. 2002.
8. Moen V, Raddum H and Hole K J. Weaknesses in the Temporal Key Hash of WPA. Mobile Computing and Communications Review, 2001. 76-83.
9. Borisov N, Goldberg I and Wagner, D. Intercepting mobile communications: The insecurity of 802.11. Chez MOBICOM, Rome, Italy, 2001.
10. Fluhrer S, Mantin I, Shamir A. Weaknesses in the key scheduling algorithm of RC4. Chez Annual Workshop on Selected Areas in Cryptography, Toronto, CA, 2001.