3. Интернет-адрес: http://developer.android.com/guide/index.html.
4. Интернет-адрес: http://extapi.wialon.com/hw/cfg/Wialon%20IPS.pdf.
5. *Брайн Харди.* Программирование под Android (Для профессионалов). – СПб: Питер, 2014. – С. 592.

ИССЛЕДОВАНИЕ ЭЛЕМЕНТОВ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ СТАНДАРТА 802.11

Ю. Ю. Литвинович, П. И. Горбанов

ВВЕДЕНИЕ

Появление стандарта 802.11 послужило толчком для быстрого развития и широкого распространения беспроводных сетей. Однако пользователи этих сетей не всегда осведомлены о существующих угрозах безопасности, которые приносит с собой данная технология [1].

В работе анализируется безопасность элементов защиты сетей стандарта IEEE 802.11 и методом проведения атак исследуется надежность каждого из них.

ЭЛЕМЕНТЫ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ СТАНДАРТА 802.11

Беспроводные сети стандарта 802.11 для приема и передачи информации используют 2.4ГГц и 5ГГц диапазоны радиочастот. Как следствие этого, любая станция, настроенная на данные частоты, имеет возможность принимать и передавать сигналы. Поэтому безопасный обмен информацией в беспроводных сетях возможен только при наличии двух составляющих - контроля доступа и шифрования.

В качестве средств контроля доступа в стандарте 802.11 предусмотрены аутентификация (открытая и с совместно используемым ключом), скрытие SSID-имени сети и фильтрация по MAC-адресам. Сюда также можно отнести изменение мощности сигнала, которое настраивается на большинстве современных точек доступа. К механизмам обеспечения шифрования стандарта 802.11 относятся технологии WEP и WPA/WPA2 [2].

Однако все перечисленные выше элементы имеют уязвимости, которые при их грамотном использовании приводят к нарушению безопасности беспроводных сетей. Исследуем каждый из них.

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ АУТЕНТИФИКАЦИИ

Анализ механизмов аутентификации позволяет выявить в них некоторые уязвимости.

В случае аутентификации с совместно используемым ключом точка доступа аутентифицирует клиента путем расшифровки зашифрованного с ключа ответа на вызов и дальнейшей проверки того, что полученный текст вызова полностью соответствует отправленному. При захвате и открытого текста вызова, и зашифрованного ответа можно установить первоначальный ключ. Эта уязвимость обусловлена математическими методами, лежащими в основе данной технологии, а именно использованием операции XOR. Механизм же открытой аутентификации, в принципе, не предоставляет средств для определения того, кто получает доступ к сети.

Уязвимость сокрытия SSID-имени сети основана на передаче SSID в незашифрованном виде во фреймах **Probe Request**. Таким образом, даже после отключения широковещательной рассылки с целью изменить на пустую строку значение имени сети во фреймах **Beacon** и **Probe Response** SSID может быть установлен через сканирование эфира и захвата кадров **Probe Request** [3].

Анализ принципов работы механизма MAC-фильтрации и канальных протоколов передачи в беспроводных сетях показывает, что уникальный MAC-номер сетевого интерфейса передается в открытом виде даже при применении шифрования данных. Поэтому для получения дозволенного точкой доступа адреса необходимо просканировать эфир и извлечь оттуда интересующий адрес, проанализировав нужные пакеты [4].

Обнаруженные в ходе проделанного исследования уязвимости с успехом были использованы для проникновения в беспроводную сеть. Атака производилась в среде **Kali Linux** с помощью адаптера **Alfa Networks AWUS036H**, который на уровне прошивки поддерживает вход в режим мониторинга. В результате за время порядка 15 минут удалось взломать каждый из выше рассмотренных элементов, чем был получен доступ в защищенную беспроводную сеть.

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ШИФРОВАНИЯ

Уязвимость механизма шифрования WEP обусловлена тем, как применяется алгоритм составления ключа на основе поточного шифра RC4. Часть векторов инициализации (их называют слабые IV) могут раскрыть биты ключа в результате проведения статистического анализа. Заполучить WEP-ключи длиной как 40, так и 104 бит можно после обработки достаточного количества перехваченных фреймов [5].

С WPA и WPA2 дела обстоят сложнее. Единственным способом подобрать ключ является перехват фреймов первоначального рукопожатия и их декодирование прямым перебором или по словарю. Специально со-

ставленные словари для подбора основаны на том факте, что многие пользователи используют в качестве паролей типичные символьные комбинации (qwerty123, 12345678 и др.) [6]. В исследовании установлено, что это значительно облегчает злоумышленнику задачу взлома.

Для обхода защиты использовалась среда **Kali Linux** и беспроводной адаптер **Alfa Networks AWUS036H**. Сравнительный анализ надежности механизмов шифрования при различных алгоритмах и времени, необходимого на взлом каждого из них при различной степени сложности ключей, приведен в таблице 1.

Табл. 1

Сравнение результатов взлома ключа

Тип ключа	Алгоритм шифрования	Ключ	Пакеты	Время подбора, мин:сек
WEP 64 bit	RC4	E5EE22CB76	135000	0:05
WEP 64 bit	RC4	6CA05BD750	200000	0:05
WEP 128 bit	RC4	61EB31676F8798074C0FC6479B	100000	0:05
WEP 128 bit	RC4	1A956C11D63175974A5941A5F3	205000	0:05
WPA	AES	yfxfkmybr(= начальник)	800	0:21
WPA	TKIP	yfxfkmybr(= начальник)	940	0:21
WPA2	AES	yfxfkmybr(= начальник)	1200	0:21
WPA2	TKIP+AES	yfxfkmybr(= начальник)	1000	0:21
WPA	AES	goodyear	800	3:21
WPA	TKIP	goodyear	500	3:23
WPA2	AES	goodyear	800	3:26
WPA2	TKIP+AES	goodyear	400	3:25
WPA	AES	belarussian	700	29:23
WPA	TKIP	belarussian	1000	29:20
WPA2	AES	belarussian	900	29:25
WPA2	TKIP+AES	belarussian	1200	29:29
WPA2	AES	qwerty123	1000	263:40
WPA2	AES	aveAlmaMaterBSU	800	не подобран

Как видно из результатов, представленных в таблице 1, использование WEP ключа совершенно небезопасно. Его взлом не составляет труда и не требует привлечения больших вычислительных ресурсов. Длина ключа и

количество набранных пакетов никак не влияют на скорость взлома, которая оказалась равной нескольким секундам.

Интереснее обстоят дела с WPA/WPA2 шифрованием. Количество собранных пакетов не влияет на скорость подбора, т.к. для такой операции достаточно перехватить только пакеты с первоначальным рукопожатием.

Из таблицы 1 также несложно увидеть, что время взлома WPA ключа не зависит от используемого алгоритма шифрования(AES, TKIP, AES+TKIP). Оно также не зависит от версии WPA (WPA или WPA2). Полученные результаты можно объяснить методикой взлома, согласно которой из всех пакетов необходимы только пакеты рукопожатия для проведения дальнейшей атаки прямым перебором, скорость которой напрямую зависит от вычислительной мощности системы.

ЗАКЛЮЧЕНИЕ

Исследованы уязвимости беспроводных сетей стандарта IEEE 802.11. Методом организации атак проведено тестирование механизмов аутентификации, скрытия SSID сети, фильтрации по MAC-адресам, WEP и WPA/WPA2 шифрования. Результаты тестирования позволяют заключить, что для обеспечения безопасности беспроводных сетей стандарта 802.11 необходимо применение комбинированного подхода. Следует по возможности использовать все доступные механизмы защиты, но с обязательным применением WPA/WPA2 шифрования. Пароль должен иметь достаточную длину и состоять из комбинации цифр, строчных и заглавных символов. Чем выше случайность пароля, тем более он надежен. Простых и типичных паролей, которые могут быть подобраны по словарю, нужно избегать. При соблюдении всех этих условий высокая безопасность беспроводной сети обеспечена.

Литература

1. *Lemstra, W.* The Innovation Journey of Wi-Fi: The Road To Global Success / *W. Lemstra, V. Hayes, J. Groenewegen*. - Cambridge University Press, 2010.
2. *Earle, Aaron E.* Wireless Security Handbook / *Aaron E Earle*. - Auerbach Publications, 2006.
3. *Гордейчик, С.В*. Безопасность беспроводных сетей / *С.В Гордейчик, В.В Дубровин*. - Горячая Линия – Телеком, 2008.
4. *Roshan, P*. 802.11 Wireless LAN Fundamentals / *Perjman Roshan, Jonathan Leary*. – Cisco Press, 2009.
5. *Fleishman, G*. Take Control of Your Wi-Fi Security / *Glenn Fleishman, Adam C Engst*. - Ithaca, NY: TidBITS Publishing, 2009.
6. *Росс, Д*. Wi-Fi. Беспроводная сеть / *Д. Росс*. - Москва: НТ Пресс, 2007.