УДК 004.732

Неустроев Н.С.

студент

Северо-Восточный федеральный университет им. М.К.Аммосова

Российская Федерация, г.Якутск

Научный руководитель: Леонтьев Н.А., к.т.н.

доцент

АНАЛИЗ БЕЗОПАСНОСТИ WI-FI ПО WPS В ЖИЛЫХ ЗДАНИЯХ

А**ннотация:** *В статье изложен анализ уязвимости беспроводных сетей в жилых зданиях. Исследуется качество безопасности роутеров от различных производителей и взлом по WPS.*

Ключевые слова: *Wi-Fi, беспроводные сети, защита Wi-Fi, WPS.*

Neustroev Nikita Sergeevich

M. K. Ammosov North-Eastern Federal University

Yakutsk, Russia

ANALYSIS OF THE SECURITY OF WI-FI ON WPS IN RESIDENTIAL BUILDINGS

Abstract: *In this article is set out the vulnerability of wireless networks in residential buildings. The congestion of security of routers from various manufacturers and hacking by WPS are investigated.*

Keywords: *Wi-Fi, wireless networks, Protection of WiFi, WPS.*

Возраст Интернета насчитывает всего несколько десятков лет, ведь он появился на рубеже 60-70 годов прошлого века. Однако его вторжение в жизнь человека нельзя назвать иначе, чем ошеломляющим. Треть населения Земли использовали Всемирную Паутину хотя бы раз, причем большинство делает это регулярно.

Главная причина уязвимости пользовательских данных, когда эти данные передаются через сети WiFi, заключается в том, что обмен происходит по радиоволне. А это дает возможность перехвата сообщений в любой точке, где физически доступен сигнал WiFi.

WEP (WIRED EQUIVALENT PRIVACY). Использует генератор псевдослучайных чисел (алгоритм RC4) для получения ключа, а также векторы инициализации. Так как последний компонент не зашифрован, возможно вмешательство третьих лиц и воссоздание WEP-ключа.

WPA (WI-FI PROTECTED ACCESS) Основывается на механизме WEP, но для расширенной защиты предлагает динамический ключ. Ключи, сгенерированные с помощью алгоритма TKIP, могут быть взломаны посредством атаки Бека-Тевса или Охигаши-Мории. Для этого отдельные пакеты расшифровываются, подвергаются манипуляциям и снова отсылаются в сеть.

WPA2 (WI-FI PROTECTED ACCESS 2) Задействует для шифрования надежный алгоритм AES (Advanced Encryption Standard). Наряду с TKIP добавился протокол CCMP (Counter-Mode/CBC-MAC Protocol), который также базируется на алгоритме AES. Защищенную по этой технологии сеть до настоящего момента взломать не удавалось. Единственной возможностью для хакеров является атака по словарю или «метод грубой силы», когда ключ угадывается путем подбора, но при сложном пароле подобрать его невозможно.

Стандарт WPS был разработан производителями оборудования Wi-Fi для того, чтобы автоматизировать процесс настраивания беспроводной сети и облегчить этим настройку для неопытного пользователя. С помощью этой технологии стало возможным очень быстро и просто настроить работу беспроводной сети и основные параметры безопасности, не настраивая эти параметры вручную.

В Wi-Fi роутерах с поддержкой технологии WPS есть уязвимость относительно безопасности сети. Используя эту уязвимость можно подобрать пароли к протоколам шифрования WPA и WPA2. Эта уязвимость заключается в том, что можно методом подбора узнать используемый ключ сети. Сам PIN-код содержит восемь цифр и поэтому возможно 10^8 вариантов подбора кода. Но в реальности вариантов подбора намного меньше. Это происходит из-за того, что в последней цифре кода заключена контрольная сумма, подсчитанная по первым семи цифрам. Это уже сокращает варианты к 10^7. Сам протокол аутентификации WPS тоже содержит уязвимости. В итоге получается, что для подбора кода нужно примерно 11000 вариантов перебора. Это сравнительно не много.

В качестве примера, рассмотрим беспроводную сеть жилых зданий. Для сканирования эфира будет использовано приложение WiFiAnalyzer, а для взлома по WPS приложение WiFi Warden для Android.

Петровского 34 подъезд 2 имеет 9 этажей, в каждом этаже 4 квартиры. Взломаны: ASUS, DiEgo-PC Shut, SOROKOVA, sway.

Таблица 1 – Список точек доступа и их данные в Петровского 34

№	Точка доступа	MAC-адрес	Производитель роутера	Безопасность
1	Honor 10	b8:94:36:ae:09:f7	HUAWEI TECHN	[WPA2-PSK-CCMP][ESS]
2	TP-LINK_POCKET_3020_546C08	e8:de:27:54:6c:08	TP-LINK TECHN	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]
3	RTK-4	44:e9:dd:27:60:3b	Sagemcom	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]
4	ana	e0:a3:ac:bd:4f:88	HUAWEI TECHN	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][WPS][ESS]
5	Keenetic-6439	28:28:5d:87:56:68	Zyxel Commun	[WPA2-PSK-CCMP][WPS][ESS]
6	Ushkanov	2c:ab:25:fe:e3:6b	SHENZHEN GONG	[WPA-PSK-CCMP][WPA2-PSK-CCMP][ESS]
7	Bubyakini	a0:f3:c1:84:a8:52	TP-LINK TECHN	[WPA2-PSK-CCMP+TKIP][ESS]
8	Oktyarum	e8:94:f6:58:93:e8	TP-LINK TECHN	[WPA2-PSK-CCMP][WPS][ESS]
9	ROSTELECOM_1951	f0:82:61:61:19:52	Sagemcom	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][WPS][ESS]
10	DiEgo-PC	38:2c:4a:e1:74:c0	ASUSTek COMP	[WPA2-PSK-CCMP][WPS][ESS]
11	chaika	b0:4e:26:37:99:f6	TP-LINK TECHN	[WPA2-PSK-CCMP][WPS][ESS]
12	ROSTELECOM_XXXX	f0:82:61:61:2d:b0	Sagemcom	[WPA-PSK-CCMP][WPA2-PSK-CCMP][ESS]
13	Shut	28:28:5d:8d:b3:a8	Zyxel Commun	[WPA2-PSK-CCMP][WPS][ESS]
14	sway	38:2c:4a:ad:28:ac	ASUSTek COMP	[WPA2-PSK-CCMP][WPS][ESS]
15	ASUS	bc:ee:7b:ee:df:98	ASUSTek COMP	[WPA2-PSK-CCMP][WPS][ESS]
16	SOROKOVA	9c:5c:8e:49:b0:68	ASUSTek COMP	[WPA2-PSK-CCMP][WPS][ESS]

Ойунского 16 подъезд 3 имеет 9 этажей, в каждом этаже 4 квартиры. Взломаны: ASUS_38, ASUS_30_2G, Horde, wifi_enduro, wakaflocka, ZyXEL_KEENETIC_4G_FEC2E6, Aiaal

Таблица 2 – Список точек доступа и их данные в Ойунского 16

№	Точка доступа	MAC-адрес	Производитель роутера	Безопасность
1	Kalininskiy	1c:5f:2b:59:62:ab	D LINK INTER	[WPA2-PSK-CCMP][ESS]
2	start	4c:60:de:e6:de:d5	NETGEAR	[WPA2-PSK-CCMP][WPS][ESS]
3	ASUS_30_2G	70:4d:7b:5d:18:30	ASUSTEK COMP	[WPA2-PSK-CCMP][WPS][ESS]
4	Home Wlant	90:f6:52:b9:27:fc	TP-LINK TECHN	[WPA-PSK-TKIP][WPS][ESS]
5	ZyXEL_KEENETIC_4G_FEC2E6	cc:5d:4e:fe:c2:e6	Zyxel Commun	[WPA2-PSK-CCMP][WPS][ESS]
6	SULUS	e8:94:f6:b4:00:70	TP-LINK TECHN	[WPA2-PSK-CCMP][WPS][ESS]
7	ASUS	30:85:a9:6a:b0:28	ASUSTek COMP	[WPA2-PSK-CCMP][ESS]
8	RT-WiFi_3A18	70:2e:22:6f:3a:18	zte corporat	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]
9	wifi_enduro	d8:eb:97:1c:93:5a	TRENDnet	[WPA-PSK-CCMP][WPS][ESS]
10	ROSTELECOM_9C89	f0:82:61:2d:9c:8a	Sagemcom	[WPA2-PSK-CCMP][ESS]
11	*	30:85:a9:69:88:78	ASUSTek COMP	[WPA2-PSK-CCMP][ESS]
12	ASUS_38	70:4d:7b:d2:58:38	ASUSTek COMP	[WPA2-PSK-CCMP][WPS][ESS]
13	flower	28:28:5d:69:9e:04	Zyxel Commun	[WPA2-PSK-CCMP][WPS][ESS]
14	Keenetic-8724	e4:18:6b:53:3c:b6	Zyxel Commun	[WPA2-PSK-CCMP][WPS][ESS]
15	Aiaal	10:7b:44:40	ASUSTek COMP	[WPA2-PSK-

		:09:18		CCMP][WPS][ESS]

Петровского 14 подъезд 2 имеет 9 этажей, в каждом этаже 4 квартиры.

Взломаны: ASUS, ASUS_69, ВЕТЕРАН’s Wi-Fi, RT-WiFi_F9F4

Таблица 3 – Список точек доступа и их данные в Петровского 14

№	Точка доступа	MAC-адрес	Производитель роутера	Безопасность
1	HUAWEI-3FUH	9c:71:3a:db:6f:28	HUAWEI TECHN	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]
2	TP-LINK_985408	c0:4a:00:98:54:08	TP LINK TECHN	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][WPS][ESS]
3	Berezin	d4:bf:7f:07:95:a5	UPVEL	[WPA2-PSK-CCMP][WPS][ESS]
4	Severina	f8:1a:67:aa:e5:5a	TP LINK TECHN	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]
5	HUAWEI-4cBJ	10:c1:72:da:bf:18	HUAWEI TECHN	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]
6	Andrey	c4:e9:84:28:4e:4e	TP LINK TECHN	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]
7	Aiastaan	f8:f0:82:55:c8:62	NAG LLC	[WPA2-PSK-CCMP][ESS]
8	ASUS_69	70:4d:7b:d2:47:00	ASUSTEK COMP	[WPA2-PSK-CCMP][WPS][ESS]
9	Visenka	1c:5f:2b:4e:98:4a	D LINK INTER	[WPA2-PSK-CCMP][WPS][ESS]
10	daniil	20:f1:7c:19:1b:10	HUAWEI TECHN	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]
11	ASUS	4c:60:de:e3:7a:10	NETGEAR	[WPA2-PSK-CCMP][WPS][ESS]
12	Tanya	a4:dc:be:aa:93:9c	HUAWEI TECHN	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]
13	Huawei4283888	24:7f:3c:c3:7b:8c	HUAWEI TECHN	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][WPS][ESS]
14	osa-ttk	f4:6d:04:f1:03:52	ASUSTEK COMP	[WPA2-PSK-CCMP][ESS]
15	ZyXEL Keenetic-0425 4G III	04:bf:6d:06:0b:68	ZYXEL COMMUN	[WPA2-PSK-CCMP][WPS][ESS]
16	RT-WiFi_F9F4	d4:76:ea:23:f9:f4	ZTE CORPORAT	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]
17	Lillian	f8:d1:11:8	TP LINK TECHN	[WPA-PSK-CCMP][WPA2-

		2:83:f2		PSK-CCMP][WPS][ESS]
18	ВЕТЕРАН's Wi-Fi	38:d5:47:81:85:98	ASUSTEK COMP	[WPA2-PSK-CCMP][WPS][ESS]

Из 69 роутеров у 46 (66% от общего числа) включены WPS. Из этих 46 роутеров взломаны 16 (23% от общего числа) роутеров.

Таблица 4 – Список статистики взломанных роутеров и роутеров с включенными WPS

Производители роутеров	Количество	WPS	Взломано
Всего	69	46	16
TP-LINK TECHNOLOGIES	19	18	0
ASUSTek COMPUTER INC	12	9	9
Zyxel Communications Corporation	7	7	3
HUAWEI TECHNOLOGIES	7	2	0
Sagemcom Broadband SAS	5	1	0
D-Link International	5	2	1
SHENZHEN GONGJIN ELECTRONICS	3	0	0
NAG LLC	2	0	0
NETGEAR	2	2	1
zte corporation	2	2	1
QTECH LLC	2	0	0
Apple	1	0	0
UPVEL	1	1	0
TRENDnet	1	1	1
неизвестный	1	1	0

Исследование показало, что не все точки доступа с поддержкой WPS уязвимы. Причина «непробиваемости» роутеров может заключаться в том, что они поставили: 1) блокировку WPS, 2) фильтрацию MAC-адресов.

Самые уязвимые роутеры – это роутеры от ASUSTek COMPUTER INC (все подключенные к WPS точки доступа были взломаны). У Zyxel Communications Corporation малая половина взломана. TP-LINK TECHNOLOGIES показала свое качество: не было взломано ни одного роутера, хоть почти все (кроме одного) подключены к WPS.

Список литературы:

1. Леонтьев Н.А., Протопопова В.Ф. Проблема доступа к широкополосному интернету в условиях Якутии // Форум молодых ученых. 2017. №1 (5). С. 329-331.

2.Неустроев Н.С. Анализ загруженности каналов частотной области стандарта Wi-Fi в университетских кампусах СВФУ // Современные подходы к исследованию закономерностей государственно-правовой жизни общества. эффективные технологии современных научных исследований. 2017. С. 94-99.

3. Скафенко О.Н. WI-FI как система беспроводной передачи информации // Педагогическое образование на Алтае. 2015. № 2. С. 49-52.

4. Стрельников А.Ю., Страмоусова С.А. Технология беспроводной передачи данных WI-FI // Молодой ученый. 2016. № 9-4 (113). С. 67-69. ©