ПРОБЛЕМЫ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ ДОМАШНИХ WI-FI СЕТЕЙ

Вечирко К.О.
Научный руководитель – ст. препод. Медведев Е.А.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. КРиСТЗИ, тел. (057)702-14-30)
e-mail: eugene.medvedev@nure.ua

Nowadays, wireless Wi-Fi networks are an essential attribute of the majority of private apartments and houses. The technology of wireless data transmission has firmly entered our lives and settled in many devices, from mobile phones to refrigerators.

The report reviews the security features of home wireless Wi-Fi networks and provides their statistical security analysis. It also suggests basic recommendations for setting up home budget routers.

На сегодняшний день беспроводные сети Wi-Fi, являются неотъемлемым атрибутом большинства приватных квартир и домов. Технология беспроводной передачи данных прочно вошла нашу жизнь и поселилась во многих устройствах, начиная с мобильных телефонов и заканчивая холодильниками. Так же все больше находят внедрения системы «умного дома», которые отвечают за различные узлы жизнеобеспечения дома (отопление, системы кондиционирования, подача питания, контроль утечки газа, сигнал и др.) и для удаленного управления так же требуют подключения к сети интернет.

Как правило при создании домашней беспроводной сети среднестатистический пользователь покупает недорогой Wi-Fi маршрутизатор или точку доступа и настраивает его при помощи опциональной настройки предложенной заводом изготовителем, такой вариант настройки является не надежный и может привести к возможному проникновению в сеть и фатальным последствиям. Так как покрытие беспроводной сети зачастую больше квартиры, а значит потенциальный злоумышленник может произвести атаку на точку доступа за пределами помещения то необходимо уделять особое внимание настройке безопасности таких сетей.

Предположим ситуацию, что в жилой квартире развернута система умного дома, которая подключена к беспроводной сети, которую раздает бюджетный роутер, настроенный при помощи «быстрой заводской настройки». Вероятность проникновения в такую сеть будет достаточно высокая и как следствие злоумышленник сможет влиять на работу умного дома, например, отключить автономную сигнализацию, отключать различные датчики, иметь данные есть ли в данный момент кто то дома и т.д. Так же злоумышленник может перехватывать данные из домашней сети, внедрять вредоносное ПО и совершать другие действия, которые

могут нанести вред их обладателю.

При оценке безопасности домашних беспроводных сетей был проведен статистический сбор данных с жилых домов. Для анализа применялся мобильный телефон Samsung Galaxy A3 с бесплатным ПО Wi- Fi Analyzer, а так же ноутбук Dell Inspiron с ОС Kali Linux. При анализе беспроводных точек получили данные со 100 устройств установленных в жилых квартирах. Нас интересовали следующие параметры: модель роутера, тип используемого шифрования, наличие клоченного WPS.

Для определения модели роутера использовалась программа-анализатор трафика Wireshark, для анализа самой точки и определения наличия включенного WPS использовалось встроенное ПО в ОС Kali Linux. Анализ показал, что подавляющее число беспроводных точек доступа относятся к бюджетному сегменту, и не имеют дополнительных защит от различных атак. У 70% используется шифрование WPA2-PSK, 25% -WPA, 3%-WEP, 2% – не имеют шифрования. Так же у 46% беспроводных точек была включена функция WPS. Так же был проведен опрос 40 квартир о том, как они настраивали свои беспроводные точки доступа, 33 были настроены при помощи быстрой настройки, что по нашему наблюдению является неправильным. Опрашивали только те квартиры, у которых на беспроводной точке доступа была включена функция WPS, так как вероятность взлома в таком случае равна 99,9%.

В докладе рассмотрены особенности безопасности домашних беспроводных Wi-Fi сетей. Как показал статистический анализ преобладающая часть роутеров являются бюджетными и не имеют встроенных систем препятствующих взлому. Так же наблюдение показало, что у 46% беспроводных точек включена функция WPS, и, следовательно такие точки легко поддаются взлому. Предложены базовые рекомендации по настройке бюджетных роутеров, которые значительно усложняют взлом беспроводной точки доступа.

Список литературы

1. Виды атак на Wi-Fi, портал «Hackware.ru», [Электронный ресурс] Режим доступа: https://hackware.ru/?p=158 – Загл. с экрана.

2. Как взломать Wi-Fi, портал «Codeby», [Электронный ресурс] Режим доступа: https://codeby.net/tags/kak-vzlomat-wi-fi/ – Загл. с экрана.

3. Хабракен Д., Домашние беспроводные сети [Текст] / Д.Хабракен - М: НТ- Пресс, 2009, 250 с.

4. Флѐнов, М.Е. Linux глазами хакера. 4-е изд / М.Е. Флѐнов. – СПб.:БХВ-Петербург, 2016. – 432 с.

5. Как взломать Wi-Fi, портал «codeby.net» [Электронный ресурс] Режим доступа: https://codeby.net/tags/kak-vzlomat-wi-fi/ – Загл. с экрана.