DOI: 10.17117/na.2016.10.03.210

<http://ucom.ru/doc/na.2016.10.03.210.pdf>

Поступила (Received): 23.10.2016

Мельникова А.С. Состояние и перспективы анализа защищенности Wi-Fi сетей

Melnikova A.S.
State and prospects of security analysis of Wi-Fi networks

Состояние и перспективы анализа защищенности Wi-Fi сетей являются важными составляющими для максимально безопасной организации сетей Wi-Fi. Но для большинства действующих сетей беспроводной связи, все равно остаются угрозы несанкционированного доступа, которые необходимо учитывать

Ключевые слова: безопасность, беспроводные сети, угроза, уязвимость

Status and prospects of security analysis of Wi-Fi networks are important components for the safest possible organization of Wi-Fi networks. But for most of current wireless networks still remain the threat of unauthorized access that must be considered

Key words: security, threat, wireless networks, vulnerability

Мельникова Анастасия Сергеевна

Студент

Омский государственный технический университет

г. Омск, пр. Мира, 11

Melnikova Anastasiya Sergeevna

Student

Omsk state technical university

Omsk, Mira ave., 11

На сегодняшний день, имеется два главных способа организации рабочих Wi-Fi сетей:

- Ad-hoc;
- Hot-spot.

Система организации беспроводной сети организованной по типу Ad-hoc. Эта система подразумевает прямую передачу информационных данных между устройствами.

Система организации беспроводной сети Hot-spot. В современных Hot-spot сетях имеется точка доступа (от англ. слова Access point), при помощи которой осуществляется взаимодействие внутри рабочей сети и практически полный доступ к имеющимся внешним сетям. При этом, взломав данную точку для осуществления доступа, несанкционированный пользователь получит данные со станций, которые работают в этой сети.

Основные угрозы. Эти угрозы информационной защищенности сетей, появляющиеся при применении Wi-Fi сетей, имеется возможность разделить на 2 основных класса, таких как:

- прямые угрозы;

– косвенные классы угроз.

Прямые угрозы. Канал, по которому происходит передача информационных данных, используемый в большинстве Wi-Fi сетей, подвержен вмешательству злоумышленников для того, чтобы получить несанкционированный доступ к имеющейся информации закрытого характера. В современных рабочих сетях Wi-Fi имеются как аутентификация, так же и шифрование, но все подобные элементы для осуществления защиты имеют свои недостатки. Эти недостатки могут оказывать существенное влияние на анализ состояния защищенности действующих беспроводных сетей Wi-Fi, поэтому их необходимо максимально полно учитывать.

Практически любое шифрование в достаточно высокой степени уменьшает скорость передачи информационных данных между устройствами. Поэтому, многие администраторы производят отключение шифрования для того, чтобы максимально повысить трафик.

Чужаки. Чужаками называют специальные устройства, которые позволяют несанкционированно подключиться к локальным сетям и получить необходимую информацию в требуемом объеме. Отказ от беспроводных систем для осуществления связи не снимает угроз беспроводных атак, когда в действующей системе имеется чужак.

Нефиксированная связь. Многие устройства беспроводной связи могут изменять тип подключения во время своей работы.

К примеру, могут осуществляться «случайные комбинации», когда ПК, с установленным Windows CE 6.0 (относящийся к действующим беспроводным сетям), или не правильно настроенный клиент сети ассоциируется в автоматическом режиме и подключается к рабочей сети Wi-Fi. При этом злоумышленник переключает определенного пользователя для осуществления процесса сканирования существующих уязвимостей, фишинга или атак. А когда пользователь уже имеет подключение и к сети Wi-Fi, тогда он становится точкой для осуществления входа, то есть чужаком. Большое число пользователей, которые подключены к сети и имеющие определенного типа интерфейс, а также невысокие скоростью или работой данной сети, достаточно часто переключаются на другую точку доступа (или ОС выполняет это в автоматическом режиме при некорректной работе). При этом имеющаяся защита Wi-Fi сети перестает выполнять требуемый уровень защиты.

Список используемых источников:

1. Белорусов Д.И., Корешков М.С. Специальная техника // Wi-Fi-сети и угрозы информационной безопасности. 2009. № 6. С. 2-6.
2. Бандурян А. Анализ угроз для беспроводных сетей, 2010.
3. Борисов В.И., Щербakov В.Б., Ермаков С.А. Спектр уязвимостей беспроводных сетей стандарта IEEE 802.11 // Информация и безопасность. Компьютерное обозрение. № 12 (723). 2010. Т. 11. № 3. С. 431–434.