3. Reeves, Colin R. Genetic algorithms principles and perspectives. A Guide to GA Theory [Text] / Colin R. Reeves, Jonathan E. Rowe. – New York, Boston, Dordrecht, London, Moscow : Kluwer Academic Publishers, 2002. – 332p.
4. Sivanandam, S.N. Introduction to Genetic Algorithms [Text] / S.N. Sivanandam, S.N. Deepa. – Berlin: Springer-Verlag Berlin Heidelberg, 2008. – 442p.
5. Панченко, Т.В. Генетические алгоритмы [Текст] / Т.В. Панченко. – Астрахань: Издательский дом «Астраханский университет», 2007. – 87с.
6. Лю, Б. Теория и практика неопределенного программирования [Текст] / Б. Лю ; перевод с англ. – М. : БИНОМ. Лаборатория знаний, 2005. – 416с.
7. Рутковская, Д. Нейронные сети, генетические алгоритмы и нечеткие системы [Текст] / Д. Рутковская, М. Пилиньский, Л. Рутковский ; перевод с польск. И.Д. Рудинского. – М. : Горячая линия – Телеком, 2006. – 452с.

Проведено практичне дослідження продуктивності бездротових мереж, побудованих на базі технологій і стандартів IEEE 802.11g, IEEE 802.11n. Дана загальна характеристика мережевих аналізаторів, на прикладі програм inSSIDer і Vistumbler

Ключові слова: бездротові мережі, мережеві аналізатори, безпека

Проведено практическое исследование производительности беспроводных сетей, построенных на базе технологий и стандартов IEEE 802.11g, IEEE 802.11n. Дана общая характеристика сетевых анализаторов, на примере программ inSSIDer и Vistumbler

Ключевые слова: беспроводные сети, сетевые анализаторы, безопасность

A practical study of the performance of wireless networks basedon technologies and standards-based IEEE 802.11g, IEEE 802.11-1n is conducted. General characteristic of the network analyzer, in terms of programs inSSIDer and Vistumbler

Keywords: wireless networking, network analyzers, security

УДК 004.725.5

СЕТЕВЫЕ АНАЛИЗАТОРЫ БЕСПРОВОДНЫХ СЕТЕЙ. БЕЗОПАСНОСТЬ ДОСТУПА К ЛИЧНОЙ ИНФОРМАЦИИ ЧЕРЕЗ СЕТИ WI-FI

М.В. Лойко*
Контактный тел.: 095-632-67-41
E-mail: Maxim.BDB@gmail.com

А.Л. Овчинников
Ассистент*
Контактный тел.: 097-825-35-65
E-mail: ovchinnikov.alexseder@fcs.snu.edu.ua
*Кафедра автоматизации и компьютерно-интегрированных технологий
Восточноукраинский национальный университет имени Владимира Даля
кв. Молодёжный, 20а, г. Луганск, 91034

1. Введение

Развитие рынка портативных устройств идет очень высокими темпами. Так, по данным компании Strategy Analytics количество продаваемых планшетных ПК, за 2011 год выросло в два с половиной раза и достигло отметки в 10,5 млн устройств за квартал. Продажи смартфонов так же растут с каждым месяцем, практически каждый квартал различные компании презентуют новых флагманов в этой сфере. Поэтому проблема объединения многих устройств в одну локальную сеть есть естественной и с каждым годом становится все более актуальной.

Таким образом, сейчас широкое распространение получила технология беспроводного соединения, имеющая название Wi-fi. Такое соединение производится на частоте 2,4- 2,5 ГГц или 5 ГГц и регламентируется стандартом IEEE 802.11 [1], для которого существует ряд расширений. Сейчас, в основном, распространены устройства, работающие со стандартами 802.11g/n/. Разница между этими стандартами заключается в скорости передачи данных обусловленных используемом беспроводном активном оборудовании. Так, для расширения 802.11 g – максимальная скорость передачи данных составляет до 54 Мбит/с. Что касается, 802.11n то теоретически скорость передачи данных может достигать 600 Мбит/с, применяя передачу данных сразу по четырем антеннам. По одной антенне, до 150 Мбит/с. Также оборудование, рассчитанное для работы в беспроводных сетях, со спецификацией

802.11n, может бесконфликтно работать с оборудованием, использующем для своей работы предыдущие версии стандарта, но максимальной скоростью такой сети будет скорость, регламентированная спецификацией более раннего стандарта. Достоинства данной технологии очевидны – быстрое и простое создание сетей на ее базе, мобильность. Что касается недостатков, то к ним можно отнести – потери скорости из-за невысокого уровня сигнала сети, или же большого количества пользователей подключенных на одном канале к одной точке, сравнительно невысокая надежность. Для решения таких проблем предназначены программы - сетевые анализаторы.

2. Постановка задачи исследований

Анализаторы — это программы, предназначенные для просмотра низкоуровневых данных передаваемых в сети. Они используются двумя группами людей: сетевыми отладчиками и хакерами. Хакеры с их помощью собирают информацию (имена пользователей и пароли), которая помогает им получать несанкционированный доступ к системам. Сетевые отладчики благодаря анализаторам выявляют проблемы, существующие в сети.

InSSIDer – бесплатное программное обеспечение, с открытым исходным кодом, позволяющие сканировать и анализировать беспроводные сети Wi-Fi. Данная программа позволяет проверить сеть пользователя и сети, находящиеся в зоне действия Wi-Fi на предмет устранения неполадок и точек доступа, к которым возможно подключение. Также на сайте производителя данного ПО регламентированы следующие полезные свойства: анализ силы сигнала точек доступа, относительно временной шкалы; фильтр, позволяющий отсортировать точки доступа по принципу «простота доступа»; устойчивая работа в зонах с большим количеством беспроводных сетей, перекрывающих друг-друга; работа с модулями GPS, через использование сервиса Google Earth.

Вторым, популярным сетевым анализатором является программа Xirrus Wi-Fi Inspector. Можно выделить следующие особенности данного программного обеспечения, а именно: предоставляет информацию о ближайших Wi-Fi сетях на удобном графике, стилизованном под радиолокационный радар, подробную информацию о Wi-Fi сетях в виде таблицы, предлагает пользователю различные тесты для беспроводных сетей

Рис. 1. Окно InSSIDer

Рис. 2. Окно Xirrus Wi-Fi Inspector

Таким образом: сетевые анализаторы являются удобным инструментом, позволяющим проанализировать состояние беспроводных сетей. Рассмотренные выше анализаторы позволяют проверить уровень и мощность сигнала, узнать информацию о точках доступа и используемых каналах. С их помощью можно определить корректность настройки и проблемы безопасности WiFi сети, такие как отсутствие шифрования, открытое вещание SSID, и своевременно их решить. Сложно спорить об актуальности этого вопроса.

3. Wardriving

Сравнительно недавно в обиход IT-специалистов, вошло слово wardriving, дословный перевод – «война на колесах». Суть этого явления заключается в следующем, злоумышленник, имея в своем распоряжении ноутбук с внешней антенной и определенным программным обеспечением – пытается проникнуть в беспроводную сеть с различными целями, начиная от бесплатного использования интернет соединения – до промышленного шпионажа[2]. Важным моментом является то – что такой взлом может производиться на очень большом расстоянии и человек, совершающий данный взлом – может скрыться.

Такое явление уже достаточно популярно. Основные моменты вардрайвинга следующие: поиск нужной точки доступа, перехват необходимого количества пакетов, поиск ключа доступа, беспрепятственное подключение к сети.

Поиск точек доступа осуществляется следующим образом: злоумышленник устанавливает на свой ноутбук любой сетевой анализатор – например, InSSIDer – садится в какой либо транспорт и перемещается по городу, в свою очередь InSSIDer связан с GPS модулем. Итог – хакер получает точки доступа с их примерным расположением, дальше – уже руководствуясь личностными интересами, выбирает нужную точку доступа для атаки.

Принцип работы сетевых анализаторов необходимо рассмотреть подробней, для полного понимания алгоритма взлома.

Началом служит то, что сетевой анализатор переводит wi-fi устройство в специфическое состояние. Стоит сказать что, штатными режимами любого беспроводного адаптера считаются Infrastructure и ad-hoc. В первом режиме каждый пользователь под-

ключен к сети через точку доступа, а в режиме ad-hoc беспроводные адаптеры могут общаться друг с другом напрямую, без использования точки доступа. Однако оба эти режима не позволяют беспроводному адаптеру прослушивать эфир и перехватывать пакеты. Так как для этого, устройство должно обязательно состоять в какой-либо сети. Для перехвата пакетов существует специальный режим мониторинга (Monitor mode).

В некоторых случаях, для перевода устройства в такой режим, необходимо установить в систему специальные драйверы, которые пишутся под чип конкретного производителя. В основном, они пишутся под операционные системы семейства Linux. Для Windows найти нужные драйверы будет намного сложнее. В остальных – адаптер в такой режим переводит сама программа анализатор. В данном режиме адаптер, поймав сигнал, в первую очередь принимает беспроводные фреймы (аутентификационные, информационные) сканер, проведя анализ которых, получает информацию о типе сети, наличии в ней WEP, WPA или WPA2 шифрования, SSID, производителя беспроводного активного оборудования и т.д., а также фреймы данных – по которым сканер судит об адресации в сети и ее пользователях.

Сканирование, в свою очередь может быть активным и пассивным. Второе представляет меньший интерес, так как не предоставляет в нужном объеме информацию, необходимую для взлома. Что касается активного сканирования – оно достаточно популярно, так как позволяет выявить большее количество беспроводных сетей, да и информации о сети оно предоставляет больше. Метод активного сканирования используют множество программ, одна из самых популярных это NetStumbler. Данное П.О. позволяло получать избыточную информацию о беспроводных сетях и являлось абсолютно бесплатным – эти аспекты стали причинами его популярности.

На данный момент, поддержка программы прекращена и проект свернут. Поэтому Netstumbler не работает на новых операционных системах, таких как Windows Vista, Seven. Сейчас его место занимают InSSIDer и Kismet под Linux.

Что же касается других программных продуктов, подобных Netstumbler они также оставляют нежелательный для взломщика, след – по которому он может быть вычислен. Режим пассивного сканирования также не является панацеей, так например программа Wellenreiter позволяющая проводить пассивное сканирование после опознавания беспроводной карточки ESSID заменяет следующим: «This is used for wellenreiter», а MAC-адрес конфигурирует на произвольный.

Из вышесказанного следует: любую подозрительную активность сети, необходимо фиксировать и всячески пресекать. Для этого – существует огромное количество программного обеспечения, позволяющего даже вычислить физические координаты устройства – с которого проводится атака. В любом случае, времени, чтобы сорвать атаку на беспроводную сеть – предостаточно. Мгновенный взлом, попросту невозможен. Это объясняется тем, что, даже получив информацию о сети, злоумышленнику необходимо получить ключ доступа для проникновения в сеть. Это следующий этап для злоумышленника, он может отличаться по сложности и времени, затраченному на взлом, многое зависит от шифрования, установленного в сети, мощности оборудования злоумышленника, но принцип один и тот же.

На этом этапе, хакеру необходимо заполучить определенное количество пакетов, передаваемых в этой сети, а когда это будет выполнено – уже в спокойной обстановке – с помощью программы-взломщика получить нужный ключ. Для этих целей чаще всего используется Aircrack-ng.

Aircrack-ng — набор программ, предназначенных для обнаружения беспроводных сетей, перехвата передаваемого через беспроводные сети трафика, аудита WEP и WPA/WPA2-PSK ключей шифрования проверки их стойкости. [3] Таким образом, для сбора пакетов используется программа airodump-ng. Она собирает все пакеты и пишет дамп в файл. Следующим шагом является, работа с данным файлом самой программы взломщика aircrack-ng. По некоторым данным необходимо 500 тыс. пакетов для взлома 128-битного ключа. [4]. Что касается более продвинутого шифрования, такого как WPA2-PSK – то и такие ключи возможно найти данной программой. Например, поиск по словарям или же с помощью брутфорса – данный способ гарантирует нахождение ключа, но сам процесс может быть очень длительным.

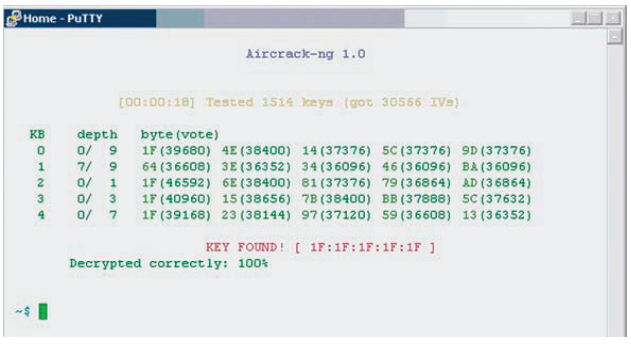

Рис. 3. Рабочее окно программы Aircrack-ng

Все вышеописанные анализаторы применимы для устройств на базе Windows, есть аналоги для Linux, но в последнее время, очень популярными становятся устройства на базе операционной системы Android. Приложение, о котором дальше пойдет речь, не распространялось по средствам маркета, доступ к нему можно получить лишь через сайт разработчика, и при условии что приложение будет использовано лишь для изучения протоколов. Это приложение droidsheep.

4. Попытки несанкционированного доступа к страницам в социальных сетях

Данная программа, по сути, является сетевым анализатором или же снифером, просто ее функционал немного доработан в некоторых аспектах. Как и остальные анализаторы, данное приложение переводит wi-fi адаптер вашего устройства в Monitor mode, о котором было написано ранее. Из-за этого, существует нюанс использования данной программы, ее

работа возможна только на устройствах с root доступом, так как без него операционная система Android блокирует различные аппаратные функции.

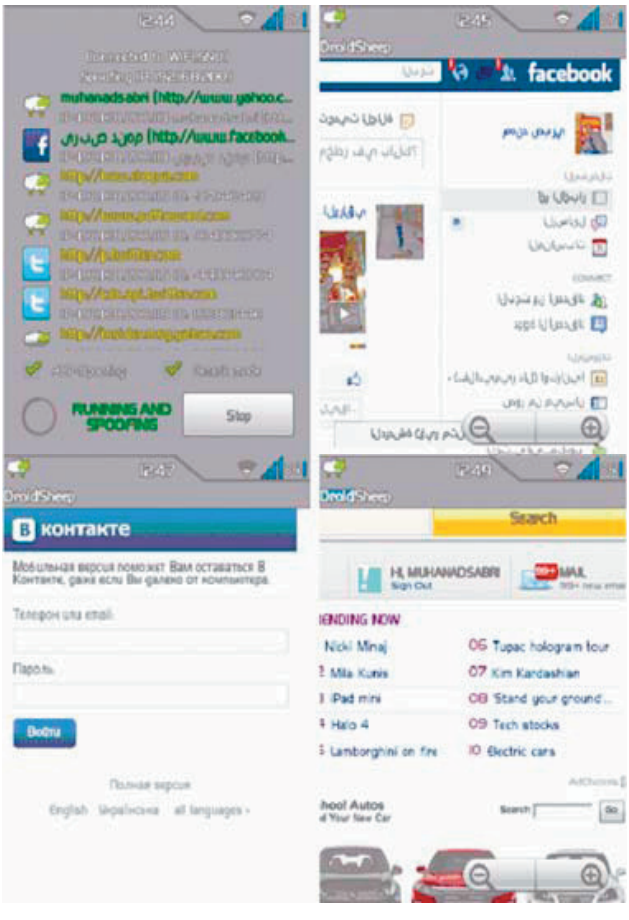

Рис. 4. Работа программы DroidSheep

После перевода устройства в Monitor mode сама программа уже внутри сети перехватывает идентификаторы сессии с различных сайтов и пользователю приложения остается лишь выбрать – к какому именно аккаунту ему необходим доступ. Идентификатор сессии это уникальный идентификационный номер, добавляемый к URL при посещении пользователем веб-страниц, используемый для идентификации посетителей в целях сбора информации об их поведении, просмотренных документах или загружаемых файлах. Таким образом после получения данного уникального идентификатора, пользователь droidsheep получает доступ к чужой сессии и может полноценно использовать ее, например, если это социальная сеть, рассылать всевозможный спам, друзьям человека, чью сессию он перехватил. В возможностях данной программы указано о перехвате идентификаторов следующих популярных социальных сетей: Facebook, Twitter, Vkontakte, Yahoo. При работе с программой был получен доступ к страницам Facebook и Yahoo, сервис Vkontakte выдал страницу с запросом авторизации, Twitter – просто ошибку.

5. Выводы

Беспроводные сети являются неотъемлемой частью IT-инфраструктуры, они предоставляют большие возможности и функционал, обладают приемлемой ценой. Стандарт Wi-Fi динамично развивается, с каждым новым стандартом предоставляя пользователям соединение с более высокими скоростью и безопасностью. Из-за высокой популярности, появилось много П.О., призванного облегчить работу с беспроводными сетями. В статье рассмотрено несколько программных продуктов, которые позволяют оптимально настроить сеть, и предоставляют полную информацию о сети. Так же показаны продукты и описан механизм для несанкционированного доступа к беспроводным сетям и личной информации внутри последних.

Литература

1. Краткое описание стандартов Wi-Fi [Электронный ресурс]. - Режим доступа : \www/ URL: www.nklondike.ru/articles.php?lng=ru&pg=324 - Загл. с экрана.
2. Война на колесах [Электронный ресурс]. - Режим доступа : \www/ URL: http://www.xakep.ru//magazine/xs/059/008/1.asp - Загл. с экрана.
3. Aircrack-ng — набор программ, предназначенных для обнаружения беспроводных сетей [Электронный ресурс]. - Режим доступа : \www/ URL http://ru.wikipedia.org/wiki/Aircrack-ng — Загл. с экрана.
4. В поисках Wi-Fi [Электронный ресурс]. - Режим доступа : \www/ URL: http://www.xakep.ru//magazine/xs/059/012/1.asp - Загл. с экрана.
5. DroidSheep. [Электронный ресурс]. - Режим доступа : \www/ URL: http://droidsheep.de/ - Загл. с экрана.