УДК 004.056.2

К проблеме безопасности открытых Wi-Fi сетей

Альбовский А.В.[10], Егоров Н.А.[11], Заминалов Н.М.[12], Бонч-Бруевич А.М.[13]

Настоящее исследование посвящено проблеме безопасности данных при использовании общественных сетей беспроводной передачи информации. Исследованы известные модели угроз. Была произведена оценка возможности их модернизации. В настоящей работе был получен опытный образец устройства для перехвата трафика. Произведен анализ последствий при реализации построенной модели угроз.

Ключевые слова: информационная безопасность, персональные данные, мобильные сети, перехват данных, поддельные базовые станции

Введение

В больших городах стали набирать популярность и т.н. открытые точки доступа Wi-Fi, через которые различные предприятия раздают интернет. Сейчас почти во всех ресторанах, общественном транспорте, остановках и прочих местах скопления людей есть точка доступа, к которой любой желающий может подключиться и использовать для выхода в Интернет. Данная статья посвящена безопасности данных при пользовании такими сетями. Рассматривается возможность незаметного перехвата данных пользователей. Исследование основано на анализе известных угроз для сетей предыдущего технологического поколения, т.е. мобильных сетей. Результатом работы стало устройство, которое возможно получить за короткий промежуток времени, используя доступное программное и аппаратное обеспечение для выполнения поставленных целей, а именно перехват и последующий анализ трафика.

1. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

1.1. Анализ угроз для пользователя в общественной сети

С развитием технологий для упрощения жизни люди порой забывают о необходимости защищать свои данные. Одной из таких технологий являются беспроводные сети Wi-Fi. Подключаясь к открытым точкам доступа, пользователи не задумываются о том, что подвержены некоторым опасностям [1]. Среди них хотелось бы выделить следующие:

- Перехват сеанса пользователя
- Перехват и просмотр всех данных, выводимых пользователю
- Подмена содержимого страниц, просматриваемых пользователем

1.2. Ситуация с открытыми точками доступа Wi-Fi

Для удобства жителей Москвы в транспорте и на остановках была развернута единая сеть Wi-Fi под названием MT_FREE. За счет единого названия сети, устройства пользователей могут автоматически подключаться к сети. Для стабильного сигнала точек доступа было установлено огромное количество и из-за этого пользователи даже не смотрят, к какой именно точке доступа они подключены.

[10] Альбовский Александр Владимирович, МГТУ им. Н.Э. Баумана, Москва, alex@fayst.su
[11] Егоров Никита Андреевич, МГТУ им. Н.Э. Баумана, Москва, kuzya@kuzya.su
[12] Заминалов Никита Максимович, МГТУ им. Н.Э. Баумана, Москва, sugarbastard@yandex.ru
[13] Бонч-Бруевич Андрей Михайлович, кандидат технических наук, доцент, МГТУ им. Н.Э. Баумана, Москва, 123andryb@mail.ru

2. УСТРОЙСТВО ДЛЯ ПЕРЕХВАТА

2.1. Описание устройства

Устройство представляет из себя портативный компьютер с внешним источником питания, работающий под управлением ОС Linux и имеющем в своем составе СПО для управления двумя Wi-Fi адаптерами. ОС настроена так, что при загрузке автоматически выполняются скрипты, запускающие широковещательную сеть на одном сетевом адаптере и выполняющие подключение другого адаптера к другой известной сети [2, 3].

Разработанное устройство работает в качестве повторителя сигнала. Оно принимает сигнал от сети MT_FREE и передает с тем же именем точки доступа (SSID). Потенциальная жертва в большинстве случаев не замечает подмены сети за счет одинакового SSID и автоматического подключения к открытым известным сетям. Устройство перенаправляет трафик в настоящую сеть MT_FREE, что означает, что пользователь проходит привычную для него процедуру аутентификации, однако весь его трафик доступен для анализа.

2.2. Тестирование

На рис. 1 изображен веб-интерфейс устройства-перехватчика, позволяющий загрузить на компьютер злоумышленника файл с перехваченными данными [4].

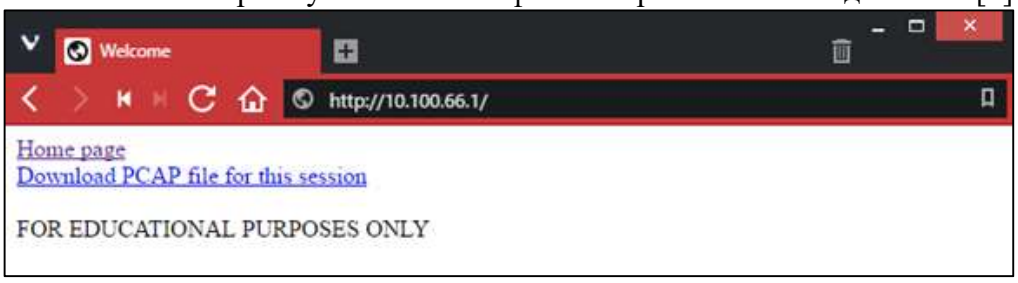

Рисунок 1. Интерфейс устройства

В качестве тестирования произведем подключение к точке доступа и выполним переход на страницу по протоколу http, после этого скачаем файл с сетевыми пакетами и попробуем найти пакет, в котором содержатся данные о переходе на страницу [5, 6].

Вторым тестом будет перехват сессии пользователя.

Тестовая страница в сети Интернет находится по адресу http://kuzya.su/ и представляет собой обычное перенаправление на страницу https://kuzya.su/. После выполнения вышеописанных действий, скачаем файл с помощью веб-страницы и откроем его в сетевом анализаторе Wireshark.

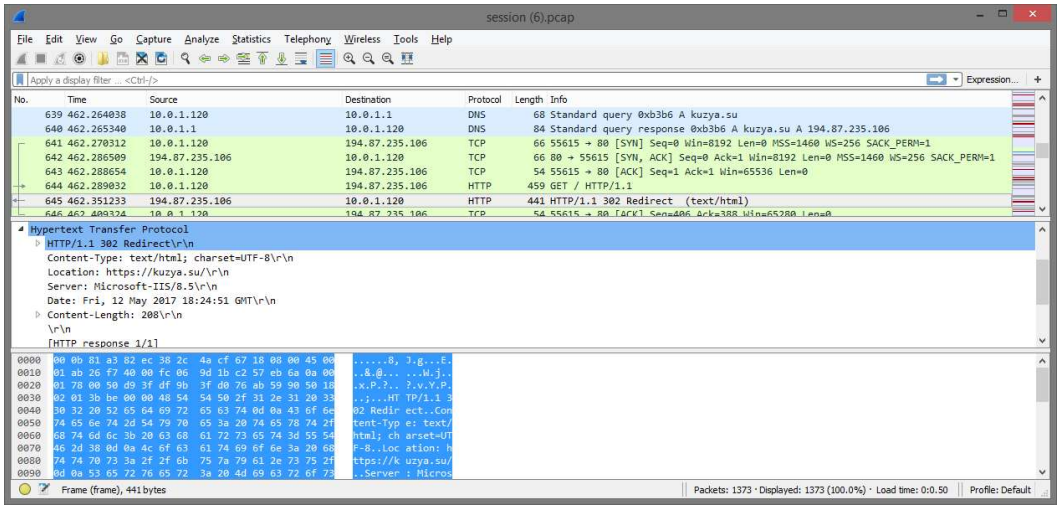

Рисунок 2. Исходный сетевой трафик в Wireshark

Как видно на рис. 2, все вышеописанные действия успешно записались в файл. В программе видно, что пользователь отправил запрос на сервер kuzya.su, а сервер перенаправил его на страницу с защищенным соединением. При этом трафик, переданный по незащищенному соединению, совершенно спокойно может быть прочитан лицом, перехватившим его. Разбор трафика, переданного по защищенному соединению, не представляется возможным из-за особенностей реализации перехватчика, но это не значит, что перехват защищенного соединения не представляется возможным.

Сутью второго эксперимента будет перехват сессии пользователя (рис. 3). Пользователь осуществляет авторизацию на сайте, а злоумышленник перехватывает авторизационные данные (cookies).

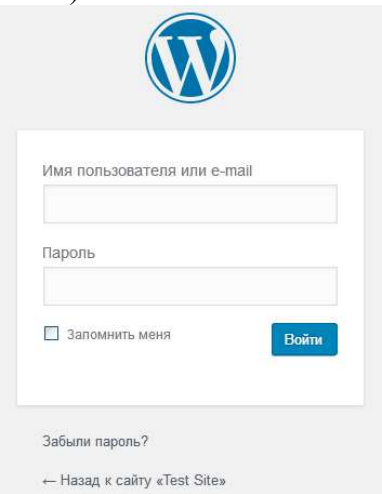

Рисунок 3. Страница входа на сайт

Перехватывающее устройство записывает всю активность пользователя. После авторизации с устройства можно загрузить файл с перехваченными пакетами и анализировать его.

После удачной авторизации жертвы, злоумышленник производит фильтрацию перехваченных пакетов по шаблону «http.cookie» и обнаруживает cookies, переданные сервером жертве (рис. 4).

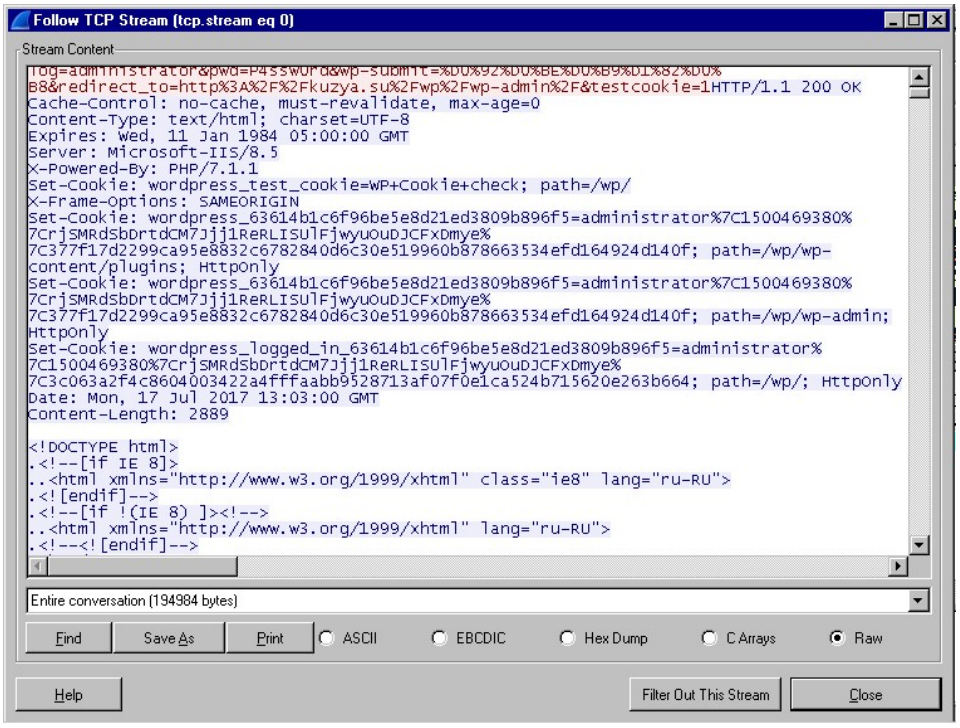

Рисунок 4. Анализ перехваченного трафика

После обнаружения необходимых данных, злоумышленник внедряет их в свой браузер (рис. 5).

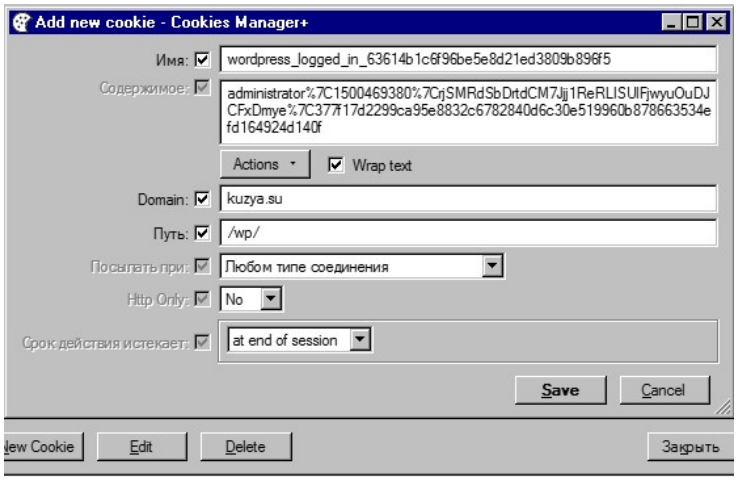

Рисунок 5. Импорт перехваченных данных (cookies) в браузер злоумышленника

После внедрения данных, злоумышленник автоматически оказывается авторизованным от имени пользователя (рис. 6).

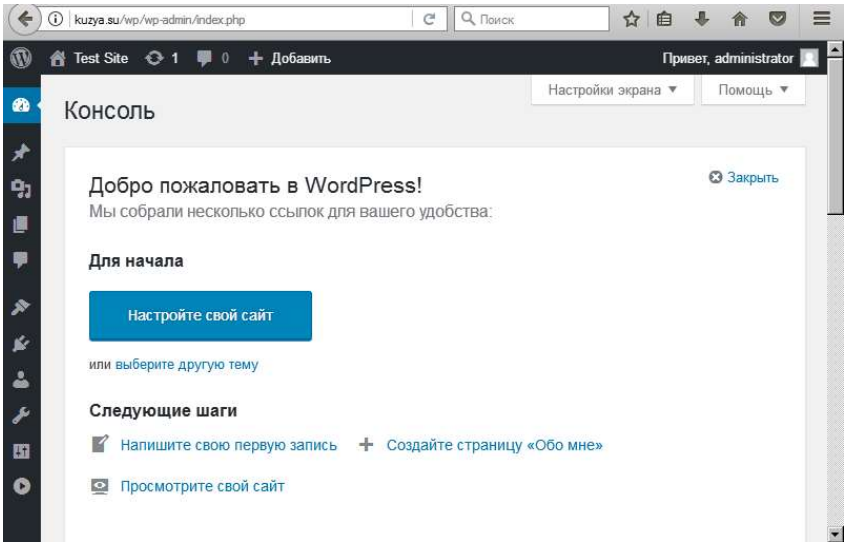

Рисунок 6. Успешная авторизация на сайте

Испытания прибора в вагоне метро показаны на рис. 7.

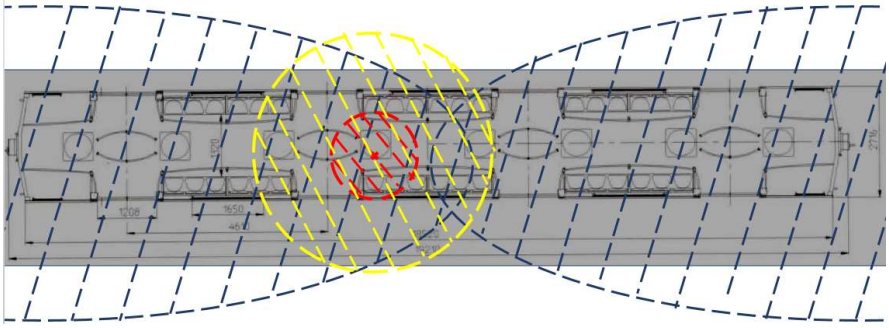

Рисунок 7. Испытания прибора в вагоне метро

Синим на рисунке выделена зона действия настоящих точек доступа MT_FREE. Крестом обозначено место поддельной точки доступа. Красная зона – зона, где у пользователей происходит переподключение на поддельную точку доступа. Желтая зона – зона действия поддельной точки доступа.

3. Последствия перехвата трафика

При подобном способе атаки происходит перехват трафика всех пользователей, подключенной к поддельной точке доступа. Это позволяет злоумышленнику незаметно для пользователя не только перехватить все его данные, но и подменить их для своих целей. Например, можно подменить страницу входа в интернет-банк с целью перехвата идентификационных данных пользователя с последующей кражей средств с банковской карты. Или, как дополнительный пример, можно встроить в страницы «рекламные блоки», содержащие эксплоиты для эксплуатации различных уязвимостей устройства пользователя с последующей кражей личных данных.

4. Ограничения

У устройства существуют следующие ограничения в плане перехвата данных:

- Зашифрованные данные (в т.ч. переданные по протоколу HTTPS [7, 8]) расшифровать не представляется возможным
- Исходя из первого пункта: при использовании шифрованных туннелей перехватить трафик так же не представляется возможным

Однако устройство, рассмотренное в статье, имеет возможность модификации рабочей прошивки, что позволяет внедрять новый функционал.

Например, имеется возможность расширить область применения устройства в плане перехвата зашифрованного трафика. В данном случае устройство будет подменять сертификаты шифрования на собственные и тем самым представлять любой трафик как незашифрованный.

Выводы

Несмотря на всю опасность «наткнуться» на данное устройство где-либо, у пользователя есть несколько возможностей защититься от перехвата данных.

Во-первых, нужно отключить автоматическое подключение к незащищенным Wi-Fi сетям. Это позволит предотвратить утечку данных в случае, если пользователь не пользуется сетью.

Во-вторых, пользователю не стоит игнорировать сообщения о недействительных сертификатах. В большинстве случаев это атака, а не проблема на стороне сервера.

В-третьих, пользователю стоит использовать шифрование. HTTPS, VPN и прочие средства усложнят процесс перехвата, сделав его бесполезным. Вычислительные мощности злоумышленников на данный момент времени не позволяют расшифровывать защищенный трафик пользователей.

Литература

1. Старцев С.С. К вопросу защиты беспроводных сетей на базе технологии WI-FI. ISSN 1818-7900. Вестник НГУ. Серия: Информационные технологии. 2012. Том 10, выпуск 1
2. Рудниченко А. К. Аспекты безопасности использования общественной Wi-Fi сети // Молодой ученый. — 2016. — №6. — С. 44-45.
3. Э.Таненбаум, Д.Уэзеролл «Компьютерные сети» 5-е издание, 2012 г — 960 с.
4. Wi-fi sniffing // Русскоязычная документация по Ubuntu — URL: http://help.ubuntu.ru/wiki/wi-fi_sniffing
5. S. Spero, “Analysis of HTTP Performance Problems,” URL: http://sunsite.unc.edu/mdma-release/http-prob.html
6. R. Fielding, J. Gettys, J. C. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee. Hypertext Transfer Protocol -- HTTP/1.1. June, 1999. URL: https://tools.ietf.org/pdf/rfc2616.pdf
7. Walls Colin. Embedded software. — Newnes, 2005. — P. 344. — ISBN 0-7506-7954-9.
8. Описание протоколов SSL/TLS // 3. — ООО "КРИПТО-ПРО"., 2002. — P. 49.

To the Problem of the Security of Open Wi-Fi Networks

Albovsky A.[14], Egorov N.[15], Zaminov N.[16], Bonch-Bruevich A.[17]

Abstract: As the title implies the article describes the data security problem when people using public networks for wireless transmission of information. The threat model is investigated. The threat modernization possibility is evaluated. Much attention is given to the creation of a prototype device operating on the described threat model. As a result the constructed model threats implementation consequences are analyzed.

Keywords: information security, personal data, mobile networks, data interception, counterfeit base stations

[14] Alexander Albovskiy, Bauman Moscow State Technical University, Moscow, alex@fayst.su

[15] Nikita Egorov, Bauman Moscow State Technical University, Moscow, kuzya@kuzya.su

[16] Nikita Zaminalov, Bauman Moscow State Technical University, Moscow, sugarbastard@yandex.ru

[17] Andrey Bonch-Bryevich, candidate of engineering science, associate professor, Bauman Moscow State Technical University, Moscow, 123andryb@mail.ru