УДК. 004.056.53

АНАЛИЗ РЕАЛИЗАЦИИ ОБЩЕСТВЕННЫХ БЕСПРОВОДНЫХ СЕТЕЙ И МОДЕЛИРОВАНИЕ АТАК НА НИХ

Попов Андрей Александрович[1], Минзов Анатолий Степанович[2]

[1]Студент;
ГБОУ ВО МО «Университет «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: popov.a.a@uni-dubna.ru.

[2]Доктор технических наук, профессор;
ГБОУ ВО МО «Университет «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: 926-565-0570@mail.ru.

В статье дан обзор существующей системы реализации доступа пользователей к общественным беспроводным сетям. В статье рассмотрены уязвимости такой системы и типовые атаки, применяемые к беспроводным сетям. По результатам моделирования атак представлена классификация атак в контексте эффективности использования.

Ключевые слова: общественная беспроводная сеть, беспроводная сеть, сниффинг, sniffing, спуфинг, spoofing, bruteforce, evil twin, злой двойник, man in the middle, человек посередине, защита информации, безопасность беспроводных сетей.

ANALYSIS OF REALIZATION OF PUBLIC WIRELESS NETWORKS AND SIMULATION OF ATTACKS ON THEM

Popov Andrey[1], Minzov Anatoly[2]

[1]Student;
Dubna State University,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: popov.a.a@uni-dubna.ru.

[2]Doctor of Computer Science, professor;
Dubna State University,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: 926-565-0570@mail.ru.

The article provides an overview of the existing system of implementing user access to public wireless networks. The article discusses the vulnerabilities of such a system and the type attacks that are applied to wireless networks. According to the results of attack modeling, a classification of attacks in the context of effectiveness of use is presented.

Keywords: public wireless network, wireless network, sniffing, spoofing, bruteforce, evil twin, man in the middle, information security, wireless security.

Введение

На сегодняшний день в большинстве общественных мест обычно устанавливается точка беспроводного доступа в интернет. Через одну беспроводную общественную сеть проходят сотни пользователей в день. В связи с чем возникают некоторые вопросы безопасности, связанные в первую очередь с пользователями данных сетей и во вторую очередь связанные с владельцами данных сетей. Обще-

ственные точки доступа привлекают злоумышленников, так как это то место, где можно найти большое количество клиентов и, соответственно, уязвимых машин, а из-за особенностей строения беспроводной сети обнаружить злоумышленника очень сложно, так как отсутствует физическая точка входа в сеть. В беспроводной сети злоумышленник может использовать те же методы атаки что и в проводной сети: сниффинг, спуфинг, атаку типа человек посередине. Результатами таких атак становится кража пользовательских данных и другие последствия.

Помимо безопасности данных пользователей, существуют и проблемы безопасности другого уровня. Общественные точки доступа могут использоваться для анонимного распространения незаконной, неправомерной информации. Для предотвращения и отслеживания подобных инцидентов существуют механизмы авторизации и аутентификации пользователей в общественных сетях, описанные в нормативных правовых актах, регулирующих отношения в области связи. Которые, в свою очередь, обязывают владельцев беспроводных точек доступа применять механизмы авторизации и аутентификации.

Самый простой и распространенный способ реализации предписанных механизмов – использование *captive*-порталов. С помощью *captive*-портала доступ в интернет через общественную сеть осуществляется через регистрацию телефонного номера пользователя. Таким образом, осуществляется идентификация пользователя в сети. При этом существуют методы, позволяющие не только обойти меры защиты, но и использовать их во вред.

Совокупность методов защиты и условий предоставления доступа в интернет в общественных сетях всё еще не создаёт безопасную среду для пользователей и информации. Данная статья описывает уязвимые места текущей системы защиты, методы противодействия и рекомендации по улучшению безопасности.

Анализ существующих типовых имитационных средств НСКИ

К беспроводным сетям применимы те же типы атак что и к проводным, но имеются также и уникальные атаки. Рассмотрим наиболее популярные. Сниффинг – технология, использующаяся для «прослушивания» трафика. С помощью сниффинга можно перехватывать все пакеты, которые передаются по сети. Содержимое этих пакетов может отличаться, это могут быть логины и пароли, также это могут быть различные медиафайлы (изображения, видео). Но сниффинг можно так же использовать в целях защиты. Например, при анализе траффика можно обнаружить вирусное ПО или сетевые сканеры.

Рассмотрим области применения, особенности и детали атаки типа сниффинг. Исторически, сниффинг применялся для прослушивания в проводных сетях Ethernet. Во времена отсутствия повсеместного шифрования и использования в сетях вместо коммутаторов – хабов, сниффинг являлся высокоэффективным средством для выявления важной информации из сети. Достаточно находится в такой незащищенной сети и сниффер сможет прослушивать весь сетевой трафик, т.к в сети без коммутаторов сетевая карта компьютера может принимать любой трафик, а не только предназначенный для этого компьютера.

С увеличением сложности архитектуры сети и внедрением протоколов шифрования, эффективность снифферов снижается, но стоит добавить в процесс атаки спуфинг, как эффективность вновь восстанавливается. Вследствие чего, можно говорить о том, что высокая эффективность достигается комбинированием различных типов атак, в чем мы убедимся далее.

Таблица 1. Эффективность атаки Sniffing

Sniffing	Сложность исполнения	Эффективность в незащищенных сетях	Эффективность в защищенных сетях	Вероятность обнаружения	Вес получаемой информации	Итого
standalone	9	10	3	5	5	6,4
inTotal	9	10	8	7	8	8,4

С помощью спуфинга можно усовершенствовать практически любую атаку. Используя инструменты для спуфинга можно подобраться к ранее недоступным узлам сети. Если незащищенную или слабо защищенную сеть можно атаковать с использованием лишь сниффинга, то спуфинг пригодится для атак на сети, где используется шифрование.

Рассмотрим распространенный случай. Используется сеть с настройками по умолчанию. Допустим мы уже имеем доступ к этой сети и нам не нужно взламывать её на предмет получения ключей. Следующим пунктом в планах атакующего является получение каких-либо данных которые передаются через эту беспроводную сеть. Если использовать уже знакомый нам метод сниффинг там и скорее всего получим достаточно мало информации так как большинство сайтов работают через *https* протокол что не позволяет увидеть данные в открытом виде. В этом случае целесообразно использовать *arp-spoofing*. Проанализировав пакеты любым анализатором трафика, например, *wireshark*, можно определить корневой узел сети, например, роутер, который обычно находится на адресе 192.168.0.1 или 192.168.1.1. Используя программное обеспечение для проведения *ARP*-спуфинга злоумышленник может предоставлять свою машину в качестве корневого узла и тогда все остальные пользователи сети будут ошибочно полагать что шлюз – это машина атакующего, а не оригинальный роутер. Результатом данных действий будет то, что все пакеты, которые уходят из этой сети в сеть Интернет будут пропускаться через машину атакующего, таким образом злоумышленник получит доступ ко всем абсолютно пакетом которые отправляют пользователи и сможет производить манипуляции с ними. Что в свою очередь открывает возможность для использования, например, фишинга. Так как являюсь корневым узлом можно изменять маршрутизацию пакетов. Теперь после того, как произведенного вмешательства в сеть можно применять метод сниффинга но перед этим стоит понизить уровни протоколов если мы хотим получать данные сайтов которым пользователи имеют доступ. Сейчас большинство сайтов использует протокол *https*, что не разрешает увидеть данные в открытом виде, но также сайты могут использовать и *http*-протокол для более старых версий браузеров пользователей. Этой уязвимостью и может воспользоваться злоумышленник. Настроив на своей машине dns-сервер, злоумышленник может предоставлять фиктивные имена адресов пользователям. В результате чего пользователи могут не заметить, как защищенный протокол сменится на незащищенный либо же название сайта будет иметь орфографические ошибки. Теперь же, когда данные передаются в открытом доступе до машины злоумышленника сниффинг имеет место быть, и он показывает свою максимальную эффективность.

Итак, добавив еще один метод злоумышленник может наиболее глубоко проводить атаки. Таким образом убирая недостатки метода сниффинга.

Таблица 2. Эффективность атаки Spoofing

Spoofing	Сложность исполнения	Эффективность в незащищенных сетях	Эффективность в защищенных сетях	Вероятность обнаружения	Вес получаемой информации	Итого
standalone	8	5	5	5	0	4,6
inTotal	8	10	8	8	8	8,4

Первое что приходит в голову при упоминании словосочетания «взломать Wi-Fi» это – *bruteforce*. Когда вы пытаетесь подобрать пароль к соседскому *Wi-Fi* используя такие варианты как: «12345678», «*qwerty*12345», «*password*», вы уже совершаете атаку типа *bruteforce* на точку доступа. Минимальный набор инструментов для использования атаки *bruteforce* – это наличие словаря паролей(логинов). Для подключения к беспроводной точке доступа с шифрованием *WPA* или *WPA*2 требуется пароль, который можно попытаться подобрать. Задача простая, но чем сложнее пароль, чем он длиннее, тем меньше целесообразность такого подхода. Ведь на подбор особо сложного пароля могут уйти годы.

Рассмотрим две разные ситуации применения атаки *bruteforce*:

1) Частная точка доступа на территории многоэтажного жилого дома.

2) Корпоративная точка доступа на территории предприятия.

Наша задача – провести анализ двух разных ситуаций и определить целесообразность применения атаки bruteforce.

Представим себя в роли атакующего. Во-первых, определим возможный уровень безопасности:

1) По статистике большинство точек незащищены или имеют часто встречающийся пароль.

2) У крупных предприятий обычно существует IT-отдел и служба безопасности.

Во-вторых, определим полезность информации, которую можно получить со взломанной сети..

1) Различные персональные данные, логины/пароли от интернет-сервисов, возможность использования сети в своих интересах.

2) Персональные данные сотрудников, логины/пароли от внутренних и внешних сервисов, информация, представляющая коммерческую(промышленную) тайну, дестабилизация работы предприятия.

Между уровнем защиты сети и ценностью данных передаваемых через эту сеть есть прямая зависимость, чем ценнее данные, тем выше уровень безопасности. Чем выше уровень безопасности, тем эффективность атаки *bruteforce* ниже, т.к. сложность пароля тоже возрастает.

Атаку типа *bruteforce* стоит использовать в следующих ситуациях:

1) Когда сеть защищена слабым паролем.

2) Когда имеется достаточное количество мощностей чтобы кратно уменьшить время *bruteforce*.

3) Когда ценность информации, полученной в результате атаки, превышает ресурсы, затраченные на её получение.

Таблица 3. Эффективность атаки Bruteforce

Bruteforce	Сложность исполнения	Эффективность в незащищенных сетях	Эффективность в защищенных сетях	Вероятность обнаружения	Вес получаемой информации	Итого
standalone	10	10	1	3	8	6,4
inTotal	10	10	1	3	8	6,4

Атака типа «злой двойник» используется в том случае, когда целевая точка доступа серьёзно защищена.

Смысл атаки заключается в создании клона уже существующей (оригинальной) точки доступа. Таким образом можно украсть данные пользователей для авторизации.

Поднимается точка доступа на компьютере с характеристиками оригинальной точки доступа. На компьютере запускается веб–сервер, база данных и производится настройка перенаправления пакетов. В результате чего, подключившийся клиент будет попадать на страницу авторизации, проходить авторизацию и попадать в интернет, ничего не заметив. Атака «человек посередине» – сложная и эффективная атака на информационную сеть. В беспроводной сети имеет тот же эффект, что и в обычной проводной сети. При проведении атаки «человек посередине» используются вышеописанные методы «*sniffing*» и «*spoofing*». Используя *Arp-spoofing,* атакующий становится посредником, между клиентами сети и маршрутизатором, что позволяет ему осуществлять вмешательство в передаваемый трафик.

С помощью снифферов атакующий проводит анализ трафика и выявляет наиболее полезные узлы сети, с точки зрения ценности и фактора защищенности передаваемой информации.

Большинство сайтов используют протокол *HTTPS* для передачи данных. *HTTPS* трафик также можно перехватить, но, т.к. он зашифрован, информацию достать не получится. Решением этой проблемы является перенаправление пользователя на похожие *HTTP* ссылки путем понижения протокола.

Атака «человек посередине» в принципе состоит из атак *spoofing* и *sniffing*. Эффективность можно посчитать исходя из известных данных: 8.4.

Таблица 4. Эффективность атаки Evil Twin

EvilTwin	Сложность исполнения	Эффективность в незащищенных сетях	Эффективность в защищенных сетях	Вероятность обнаружения	Вес получаемой информации	Итого
standalone	3	2	10	5	10	6
inTotal						

Уязвимости и недостатки текущей реализации системы предоставления общественного Wi-Fi

К общественной беспроводной сети (рис. 1) принадлежат не только устройства, она также включает в себя следующие субъекты:

- владелец общественной сети,
- пользователи общественной сети,
- надзорные органы государства,
- хакеры, злоумышленники.

В контексте безопасности общественной беспроводной сети следует думать не только о контроле доступа в такую сеть, но и об удобстве использования, а также о соблюдении правовых актов. Общественная беспроводная сеть должна быть безопасной и удобной для всех: для владельца, для пользователя и для надзорных органов.

Взаимодействия в сети можно разделить горизонтально и вертикально. Горизонтальные отношения – это отношения между владельцем и государством, причем владелец является объектом наблюдения и надзора со стороны государства, именно на владельце лежит ответственность за использование и безопасность сети.

Вертикальные отношения – это отношения между пользователями и хакерами, где объектом являются пользователи, т.к. цель хакеров – получение данных пользователей.

Существуют и угловые отношения:

- владелец – пользователи,
- пользователь – государство,
- государство – хакер,
- хакер – владелец.

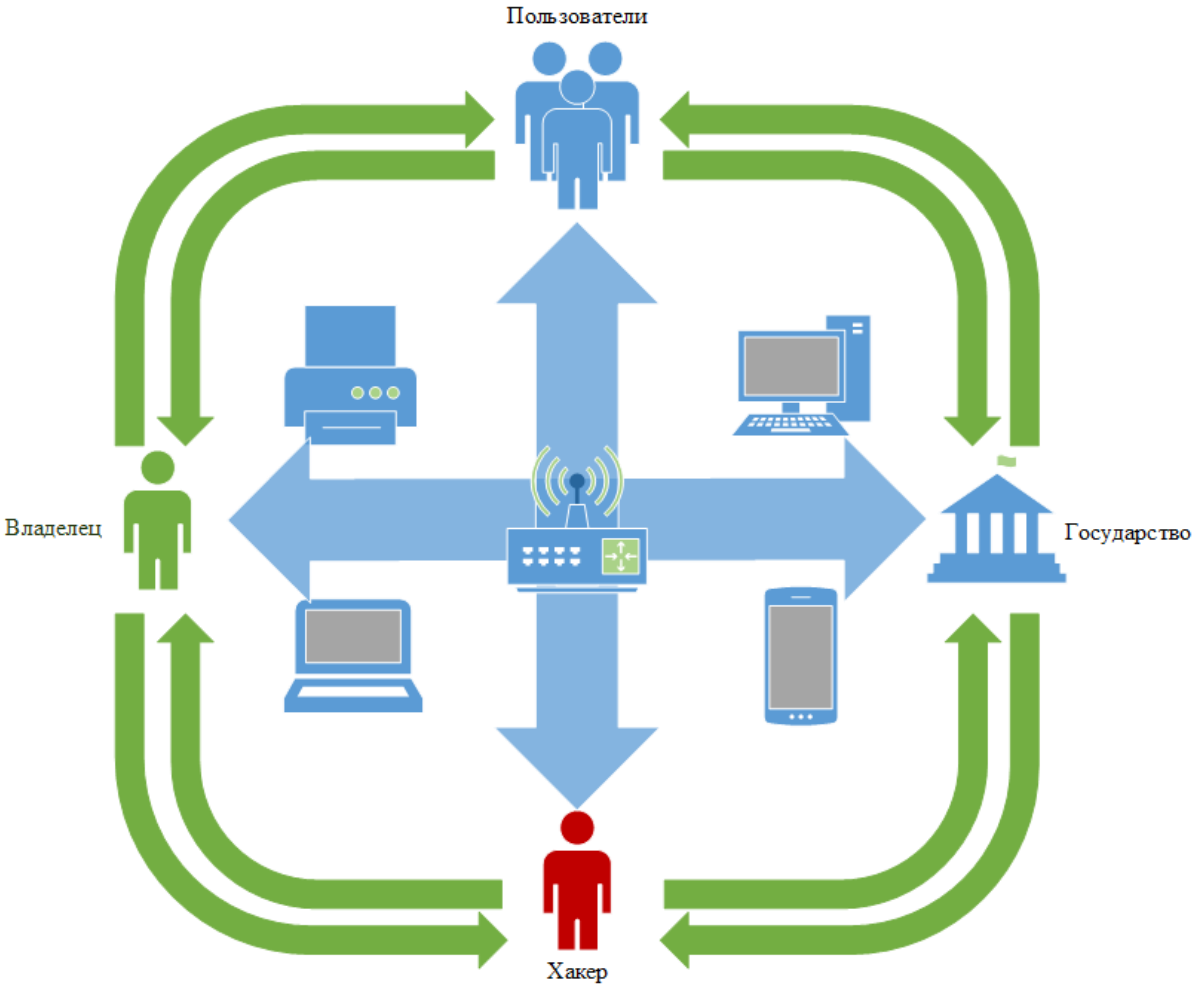

Рис 1. Представление общественной беспроводной сети как информационной системы

В большинстве своём угловые отношения проявляются косвенно на длительном промежутке времени и только при возникновении инцидентов взаимодействие внутри групп производится явным образом.

Популярным методом реализации требований законодательства в общественной беспроводной сети является использование *captive portal*.

Captive portal – это открытая точка доступа, к которой может подключиться кто-угодно.

Сетевое оборудование настроено так, чтобы всех подключившихся перенаправлять на одну и туже веб-страницу, на которой размещены условия доступа к сети. На этой странице пользователь вводит PIN из SMS или логин и пароль. Обычно для доступа к веб-странице перехватывающего портала используется протокол HTTP (а не HTTPS). Это связано с особенностями локальной сети – для локальных адресов невозможно получить валидные SSL сертификаты, а использование невалидных ничего не добавляет к безопасности, но при этом создаёт дополнительные проблемы.

Если вы подключились к Порталу и пытаетесь открыть что-то в веб-браузере, но у вас не происходит переадресация на веб-страницу *Captive Portal*, то вероятнее всего дело в том, что вы пытаетесь зайти на сайт с *HTTPS* протоколом – попробуйте открыть любой сайт на *HTTP* и вас всё-таки перебросит на страницу «входа».

Чтобы пользователи не догадались использовать нестандартные порты (например, для подключения к VPN, использовать браузер Tor или прокси), то весь трафик на всех портах блокируется. Кроме трафика UDP на 53 порту – это необходимо чтобы пропускать запросы к *DNS*-серверу.

После того, как пользователь ввёл верные учётные данные, для его *MAC*-адреса и *IP* адреса открывается неограниченный доступ. Привязка идёт именно к *MAC*-адресу (либо к паре *MAC*-адрес и IP адрес), поскольку по-другому проблематично реализовать доступ для всего устройства. Современ-

ным компьютерам, а особенно мобильным устройствам, недостаточно браузера: телефоны используют разнообразные мессенджеры, многие программы пользуются сетью: онлайн игры, антивирусы для обновления баз, почтовый клиенты и т.д. Т.е. невозможно ограничится *cookie* в веб-браузере или чем-то подобным: необходимо открывать полный доступ для сетевого интерфейса клиента, какой бы трафик и на каком бы порту ему не понадобился. Сетевые интерфейсы обладают уникальным идентификатором – *MAC*-адресом. Именно на основе него и «запоминается» устройство, которому разрешён доступ. *Captive portal* может оставлять *cookie* в веб-браузере, но они носят вспомогательный характер: например, для ускорения повторной аутентификации.

Здесь описана «сильная» конфигурация перехватывающего портала – с максимальной защитой. Конкретные реализации могут быть ещё слабее: например, для перенаправления на страницу Портала может использоваться *DNS* сервер, который на все запросы будет отвечать *IP* адресом *Captive Portal,* и при этом не будет должной фильтрации трафика. Как результат, такой Портал можно обойти просто использованием обычного *VPN* соединения, либо установкой в настройках *DNS* сервера в паре с браузером *Tor* и т.п.

Из описания *captive portal* следует, что уязвимыми точками являются *MAC*-адрес и *UDP* 53 порт.

Заключение

На текущий момент ясно, что способы предоставления доступа к общественным беспроводным сетям имеют серьёзные уязвимости. Но кроме проблем технического характера, в организации безопасности общественных беспроводных сетей существуют проблемы со стороны законодательства Российской Федерации.

Несмотря на то, что рассмотрение вопроса безопасности общественных беспроводных сетей с точки зрения исполнения и соблюдения нормативных актов – это тема отдельно статьи, при анализе и, тем более, при разработке методов защиты стоит учитывать и эту составляющую.

Подобный анализ также необходим для составления требований доверия к таким сетям в последствии.

Список литературы

1. Digital activities internet users worldwide have conducted on a public Wi-Fi network as of June 2017. — [Электронный ресурс]. URL: https://www.statista.com/statistics/731525/unsecured-wifi-risky-behavior-of-adults-global/ – Public Wi-Fi usage of adults worldwide 2017 | Statistic. – (Дата обращения: 18.05.2019).
2. Блиялкин П. А., Смоленков А. В. Выявление электронных устройств перехвата акустической речевой информации, построенных на базе средств беспроводной связи // Молодой ученый. — 2016. — №14. — С. 124-128. — [Электронный ресурс]. URL https://moluch.ru/archive/118/32820/.
3. Most Common Wireless Network Attacks. — [Электронный ресурс]. URL: https://www.webtitan.com/blog/most-common-wireless-network-attacks/ – Most Common Wireless Network Attacks - WebTitan. — (Дата обращения: 18.05.2019).
4. Ethical Hacking – Sniffing — [Электронный ресурс]. URL: https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing.htm – Ethical Hacking Sniffing. — (Дата обращения: 18.05.2019).
5. Kali Linux - Sniffing & Spoofing. — — [Электронный ресурс]. URL: https://www.tutorialspoint.com/kali_linux/kali_linux_sniffing_and_spoofing.htm – Kali Linux Sniffing and Spoofing. — (Дата обращения: 18.05.2019).
6. Russian Wi-Fi Hacking – Evil Twin attacks EXPLAINED. — [Электронный ресурс]. URL: https://www.secplicity.org/2018/10/07/russian-wi-fi-hacking-evil-twin-attacks-explained/ – Russian Wi-Fi Hacking – Evil Twin attacks EXPLAINED | Secplicity - Security Simplified. — (Дата обращения: 18.05.2019).

7. Monitor traffic using MITM (Man in the middle attack). — [Электронный ресурс]. URL: https://www.securitynewspaper.com/2018/12/14/monitor-traffic-using-mitm-man-in-the-middle-attack/ – Monitor traffic using MITM (Man in the middle attack).— (Дата обращения: 18.05.2019).
8. SPOOFING ATTACK: IP, DNS & ARP. — [Электронный ресурс]. URL: https://www.veracode.com/security/spoofing-attack – Protection Against Spoofing Attack : IP, DNS & ARP | Veracode. — (Дата обращения: 18.05.2019).