УДК 004.49

ЗАЩИТА ДАННЫХ В МОБИЛЬНЫХ УСТРОЙСТВАХ

Пользователи мобильных телефонов должны знать о тех угрозах, которые несут мобильные технологии.

Андрей Иванович Касьян, к.т.н., МФПУ "Синергия"
Игорь Александрович Нестеров, к.т.н., МУ МВД РФ

Народная мудрость

Рассматриваются угрозы, связанные с перехватом трафика и несанкционированным доступом.
Threats related to traffic interception and unauthorized access are considered.

Ключевые слова: *анализ трафика, защита, спуфинг, виртуальная частная сеть.*
Keywords: *traffic analysis, defense, spoofing, VPN.*

В современном мире мобильное устройство стало основным средством коммуникации. Этому способствовало широкое распространение Wi-Fi сетей с облегченным или открытым доступом.

Наличие сетей, конечно, благо. Однако широкое использование сети как основного канала коммуникации, например, во время вынужденного бездействия (транспорт, аэропорт, вокзал и т.д.) становятся головной болью при обеспечении безопасности онлайн-сервисов и аккаунтов. Основной причиной неудовлетворительной безопасности является человеческий фактор.

Работа в сетях становится как бы подобием выхода из дома на улицу. Перед выходом Вам необходимо защитить себя (одеться, обуться, взять зонт), после прогулки обязательно вымыть руки, а если одежда испачкана, то почиститься. Причем соблюдение правил личной гигиены для людей очевидно, а вот цифровой "гигиены" - нет. Не стоит упоминать о том, что устанавливать приложения на смартфон нужно только из надежных источников. Минимизируйте количество данных, которые храните на устройстве и не забывайте периодически удалять важные данные. Не афишируйте свой номер. Многие операционные системы позволяют шифровать данные. Например, Android позволяет шифровать данные на картах памяти (Micro SD). Некоторые приложения шифруют собственные данные, а например, OpenKeychain позволяет шифровать сторонние файлы. Используя это приложение вместе с программой K-9 Mail можно шифровать письма (на iOS такой возможности нет).

Пароли можно хранить в единственном файле, если использовать приложение KeePassDroid. Тогда единственный, но очень надежный мастер-пароль защитит все остальные пароли. В операционной системе iOS аналогичное приложение называется MiniKeePass. Для блокировки экрана очень рекомендуем использовать надежный код. Следует также регулярно обновлять операционную систему, что влияет на безопасность. Заметим, что операционные системы обладают документированным API-интерфейсом (API - Application programming interface), позволяющим писать приложения, работающие с основными возможностями смартфона. Но даже и такого рода очевидные требования часто не выполняются.

Далее, если Вы заметили слежку, то можно вынуть батарею и держать все время смартфон при себе. Не следует держать важную информацию на SIM-карте, потому что её трудно зашифровать. Никому не передавайте SIM-карту. Не принимайте сообщения от неизвестных абонентов. Запишите свой IMEI (идентификатор), что поможет Вам доказать, при случае, права собственника. Если отдаете телефон в ремонт, то обращайтесь в надежные мастерские и извлеките SIM-карту и карту памяти. При смене SIM-карты рекомендуется замена и самого смартфона, что делает невозможным слежку, когда мошенник успел выкрасть информацию (например, IMEI или MAC). Заметим, теоретически можно определить новые телефонные номера старых мобильников. Пренебрежение подобного рода советами приводит с большой вероятностью к потере денег и времени. Мы не рассматриваем далее чрезвычайно маловероятный вариант, когда мошенник путем атаки на оператора выкрадывает секретный ключ или подобные случаи.

Для некоторых хакерство - интересное и полезное времяпрепровождение. Беспроводная сеть для них представляет особенный интерес, т.к. нет сервис-провайдера (если не считать жертвы) и следы преступления прямо-таки "растворяются" в воздухе. Заметим, что эти "забавы" преследуются по Закону.

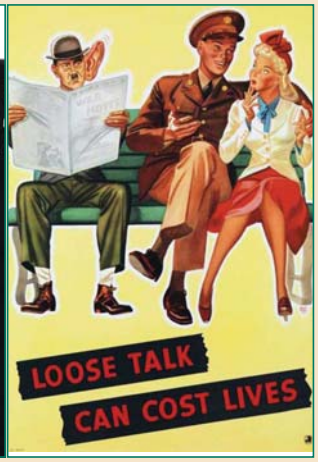
Попытаемся сформулировать некоторые рекомендации по сохранению Ваших денег и времени при работе на мобильном устройстве в открытых сетях Wi-Fi. Прежде всего, давайте рассмотрим, чем практически могут навредить злоумышленники Вашему мобильному устройству. Подключаясь без защиты к открытой сети, Вы фактически выкладываете свои данные в открытый доступ. Перехватить Ваши данные способен даже студент-двоечник. Для этого нужно скачать из интернета "хакерскую" программу, а далее - следовать инструкции по использованию данной программы.

Существует большое количество способов атак, которые злоумышленник может предпринять против Вас при использовании общедоступных сетей. Однако **эксперты выделяют три основных способа:**

- использование программ-снифферов. Сниффер - программа или устройство для перехвата и анализа сетевого трафика. Программ-снифферов существует много, они используются часто и достаточно "успешно". Основная причина "успешности" связана с тем, что около 70 % пользователей не предпринимают никаких действий для защиты своего мобильника и трафика. Перехват пароля, передаваемого в незашифрованном виде, путем подслушивания называется password sniffing. Пользователи очень часто применяют один и тот же логин и пароль для множества приложений. Это создает большую опасность. В результате взлома прослеживается вся история работы в сети, появляется доступ к корпоративным ресурсам, возможно даже копирование кредитных карт и т.д.

Выделяют win-снифферы, предназначенные для перехвата по сетям, в том числе беспроводным (Wi-Fi), и http-снифферы, предназначенные для перехвата в Internet. Прослушивание проводится пассивное и активное. Пассивное принимает весь проходящий трафик. Активное прослушивание подразумевает принятие специальных мер для того, что бы принудительно переводить трафик на злоумышленника, даже из другого сегмента сети. Для парирования угроз необходимо применять для аутентификации однократные пароли;

- использования ARP-спуфинга (подмены) - злоумышленник или программа успешно маскируется под другую, путем фальсификации данных. ARP (Address Resolution Protocol - протокол определения адреса) - протокол в компьютерных сетях, предназначенный для опре-



деления MAC-адреса по IP-адресу другого компьютера (MAC-адрес - это уникальный идентификатор, присваиваемый каждой единице активного оборудования). Суть подмены: так как в ARP-протоколе не предусмотрена проверка подлинности пакетов, злоумышленник отправляет подменные MAC-адреса на атакуемое мобильное устройство и роутер. В результате мобильное устройство станет посылать запросы на MAC-адрес злоумышленника, а роутер отвечать через этот же адрес. Весь трафик на виду. Результат аналогичен предыдущему. Такая атака относится к типу MITM ("человек в середине"). Признаком атаки может стать факт появления сигнала в тех местах, где обычно "не ловится";

- фальшивые, подменные точки доступа. Существование компактных и автономных точек доступа позволяет даже при их незначительной мощности получать более сильный сигнал для окружающих устройств. Особенно это удобно в транспорте. В последнее время участились случаи создания поддельных точек доступа в метро и на поездах. Ваш мобильник начинает работать с этой точкой и злоумышленники пытаются заполучить секретный ключ.

Хотелось бы сказать, что обычный пользователь едва ли заметит или сможет обнаружить перехват трафика. Кроме того, хакеры не стоят на месте и совершенствуют способы взлома Ваших устройств. Что же делать? По нашему мнению, в первую очередь необходимо о своей безопасности позаботиться заранее. Соблюдайте "цифровую гигиену"! Этому будет способствовать следование трем указанным ниже принципам.

1. Вся информация, передаваемая по сети, должна быть зашифрована. Это очень важное правило, которое необходимо выполнять неукоснительно.

Очень важно осуществлять шифрованный обмен данными в социальных сетях, с различными сайтами и сервисами. Существует достаточно много сайтов, вовсе не предлагающих или предлагающих ограниченную поддержку шифрованию по HTTPS (шифрование по протоколу SSL/TLS). Каким способом увидеть, что Вы осуществляете зашифрованный обмен данных? В адресной строке современных браузеров соединения по HTTPS, как правило, обозначаются значком замка и подсвечиваются зеленым цветом. Проблемы, возникающие при шифровании, заключаются в том, что в вопросах безопасности приходится полагаться на администраторов сайта, т.к. только от них зависит, какой именно будет использоваться протокол.

2. Использование безопасного протокола значительно усложняет жизнь взломщикам. Однако для безопасной аутентификации мы рекомендуем использовать двухфакторную аутентификацию (аутентификация подтверждает подлинность и предотвращает несанкционированный доступ). При таком подходе Вы значительно повысите защищённость аккаунта. Двухфакторную аутентификацию поддерживает большинство сетей.

3. Считается, что самым надежным способом защиты в публичных сетях Wi-Fi является использование VPN. VPN - это Virtual Private Network, технология, предназначенная для защиты Ваших данных в сети. Слово "частная" означает признание того факта, что весь обмен данными понятен лишь концевым точкам канала, и никому больше. Заметим, что для обеспечения конфиденциальности не следует полагаться на какой-то один механизм или на защиту лишь одного уровня сети. Технология VPN позволяет воспользоваться, например, сетью Internet для предоставления пользователям безопасного доступа. VPN и беспроводные технологии не конкурируют, а дополняют друг друга. VPN работает поверх сетей, обеспечивая конфиденциальность за счет специальных мер безопасности и применения туннельных протоколов. Смысл заключается в том, что в "туннель" не могут проникнуть данные, не зашифрованные соответствующим образом. VPN отвечает трем условиям: конфиденциальность, целостность и доступность. Для использования этой технологии Вы должны подключиться к серверу поставщика услуг. Именно там у Вас меняется IP-адрес (!). По-другому не получится из-за специфики технологии. Вот этот "побочный" эффект и используется при доступе к заблокированным Интернет-ресурсам. Российские законодательство не запрещает VPN. Просто провайдеры должны уважать российские блокировки. Причем, если даже Вы зашли "не туда", Вам как пользователю ничего не грозит. Вся ответственность лежит на провайдерах. То есть VPN - эта не просто законная, а обязательно требуемая технология при работе в публичных сетях. Конечно, никакая VPN не является устойчивой к DoS-атакам в силу зависимости от протоколов нижележащих уровней.

Правда, в рассматриваемом случае существуют некоторые нюансы. Например, не все публичные сети допускают использование VPN. Нужно очень хорошо подумать перед подключением к таким сетям. **И даже если подключились, то не вводите никаких паролей, а тем более не работайте в онлайн банкинге.** Это крайне опасно.

Услуги по VPN-подключению могут быть платными и бесплатными. Бесплатное подключение обладает рядом недостатков. По мнению экспертов, подтвержденных исследованиями, Вы сильно рискуете, подключаясь по бесплатному VPN. В интернете очень много псевдо-VPN-решений, которые, собственно, не являются ими. Они не шифруют трафик, содержат вредоносный код и т.д. Поэтому если Вы твердо решили использовать бесплатное решение, то исследуйте вопрос. Найдите проверенного поставщика услуг.

Платные поставщики VPN-услуг тоже неоднородны. Однако они не ведут логов, обеспечивают более высокую скорость, не ограничивают IP, предлагают дополнительные опции. Если Вы часто используете публичные сети ("42 минуты под землей, туда - сюда"), наверное, это Ваш вариант.

Можно настроить и свой VPN. Но и здесь есть свои нюансы. Например, нужно озаботиться собственным IP. И это тоже, как правило, деньги.

Выводы:

1. Аккуратно используйте публичные сети. Проверяйте их подлинность, старайтесь посещать сайты, не требующие авторизации.

2. Старайтесь использовать защищенное подключение HTTPS.

3. Используйте двухфакторную аутентификации.

4. Используйте VPN-подключение везде, где это возможно, в первую очередь в публичных сетях.

Литература

1. Михайлов Д.М., Жуков К.Ю. Защита мобильных телефонов от атак.- М.: Файлис, 2011, 192 с.

Связь с автором: **a.kasyan1@yandex.ru**