В. А. Артамонов

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ, СИСТЕМ И ПРИЛОЖЕНИЙ

Общие положения

Развитие высоких технологий и тренд мобильности привели к тому, что современное мобильное устройство – смартфон/планшет или иной «гаджет» (слово по себе неприятное – *прим. Авт.*) зачастую используется в качестве мобильного офиса, центра развлечений и инструмента для потребления Интернет-контента. Сам аппарат многое может рассказать о своем владельце, ведь в его памяти хранятся: контакты коллег, друзей и близких с их персональными данными; журнал звонков; корпоративная переписка; параметры точек доступа Wi-Fi, которые расположены в пределах ареала обитания владельца; приложения социальных сетей (зачастую с сохраненными паролями); банковские реквизиты или мобильный/СМС банкинг, снимки, видеозаписи, заметки и пр.

Такая концентрация деловых и персональных данных приводит к тому, что абстрактная стоимость информации перевешивает цену самого устройства. Именно поэтому задача защиты телефона/планшета или иного мобильного устройства как от киберугроз так и от банальной утери/выхода из строя является критически важной. К сожалению, часть пользователей осознает важность этих задач лишь постфактум.

Итак, прежде чем перейти к содержательной части проблем безопасности объектов обозначенных в заголовке данной статьи, давайте конкретизируем основные понятия и определения интересующих нас именованных сущностей:

Мобильное устройство (*гаджет* – англ.) – это продукт (иногда система) информационно – коммуникационных технологий.

Согласно определению Национального института стандартов и технологий США (NIST), размещенному в отчете Guidelines for Managing and Securing Mobile Devices in the Enterprise (NIST Special Publication 800-124 Revision 1), мобильными считаются устройства, обладающие малыми габаритами и весом, как минимумом одним беспроводным интерфейсом доступа к Сети (мобильной связи или Интернет), встроенной (несъемной) памятью, операционной системой, не являющейся полноценной ОС настольных компьютеров и ноутбуков, возможностью установки приложений различными способами, имеющие встроенные средства синхронизации локально хранимых данных с удаленным источником. Кроме этого, устройство может обладать другими, необязательными свойствами, в частности, иметь не менее одного беспроводного персонального сетевого интерфейса типа Bluetooth или NFC, а также не менее одного беспроводного сетевого интерфейса для голосовой связи, например сотовый модуль;
оснащаться системой глобального позиционирования;

иметь одну или несколько цифровых камер, а также средства хранения данных (поддержка съемных носителей, поддержка использования самого устройства в качестве съемного носителя информации);

Мобильная телекоммуникационная система – это система информационно – коммуникационных технологий в виде совокупности аппаратно и программно совместимого оборудования, соединенного в единую систему (сеть) с целью передачи, хранения и обработки данных мобильных и иных устройств в пределах заранее определённой территории (зоны покрытия). Мобильная телекоммуникационная система/сеть (далее мобильная телесистема) способна передавать текстовую, графическую, голосовую или видеоинформацию. Чтобы передать информацию из одного пункта и получить ее в другом, телесистеме нужно выполнить некоторые операции, которые главным образом скрыты от пользователей. Прежде, чем мобильная система передаст информацию, ей необходимо установить соединение между передающей (*sende*r) и принимающей (*receive*r) сторонами, рассчитать оптимальный маршрут передачи данных, выполнить первичную обработку передаваемой информации (например, необходимо проверить, что ваше сообщение передается именно тому, кому вы его отослали) и преобразовать скорость передачи компьютера в скорость, поддерживаемую линией связи.

Наконец, мобильная телесистема управляет потоком передаваемой информации (трафиком). Телесистема/сеть обычно содержит разнообразные аппаратные и программные компоненты, которым необходимо работать совместно, чтобы передавать информацию. Различные компоненты сети "общаются" друг с другом, придерживаясь ряда правил, что и позволяет им работать всем вместе. Такой набор правил, регулирующий процесс передачи данных между двумя точками сети, называется протоколом (*protoco*l). Каждое устройство в сети должно правильно "понимать" протокол другого устройства. Главные функции сетевых протоколов следующие: идентифицировать каждое устройство, участвующее в передаче данных, проверить, не нуждаются ли данные в повторной передаче, выполнить повторную передачу, если произошла ошибка;

Мобильное приложение – это компонент, устанавливаемый на мобильное устройство, подключающийся к серверу мобильной телесистемы и управляющий пользовательским интерфейсом и бизнес-логикой мобильного устройства. Мобильные приложения могут быть развернуты с использованием архитектуры *толстый клиент* (приложение, обеспечивающее расширенную функциональность независимо от центрального сервера), или *тонкий клиент* (программа-клиент в сетях с клиент-серверной или терминальной архитектурой, который переносит все или большую часть задач по обработке информации на сервер). Выбор типа приложения («*толстого*» или «*тонкого*»), зависит от его сложности, используемого устройства, сферы применения, а также наличия или отсутствия сетевого подключения.

Аппаратно – программная платформа для корпоративных мобильных приложений (англ. *Mobile Enterprise Application Platform*, сокр. MEAP) обеспечивает клиент-серверную среду исполнения и инструменты для разработки корпоративных мобильных приложений, обладающих высокой адаптивностью к различным типам устройств и имеющимся на них операционным системам, поддерживающих автономный режим работы.

Давайте разберемся от чего именно и каким образом можно (и нужно) защищать наши мобильные устройства, системы и приложения.

Угрозы и уязвимости мобильных устройств

Как правило, мобильные устройства должны обеспечивать решение нескольких задач информационной безопасности (триаду ИБ):

конфиденциальность – возможность доступа к хранимым и передаваемым данным только со стороны авторизованных сотрудников;

целостность данных – определение всех умышленных и неумышленных изменений в хранимых и передаваемых данных;

доступность – обеспечение своевременной доступности корпоративных данных с мобильных устройств.

Прежде чем развертывать мобильные решения, компаниям и организациям стоит разработать модель рисков информационной безопасности, определив возможные уязвимые ресурсы, угрозы и средства обеспечения безопасности, вычислив вероятности успешных атак и их последствий, и т. п.

Мобильные устройства сотрудника обычно используются в местах, не контролируемых компанией, и даже если устройства используются внутри офиса, они переносятся с места на место, что создает угрозу утечки конфиденциальных данных. Смартфоны и планшеты могут быть потеряны или украдены, и данные, хранимые на них, подвергаются риску быть скомпрометированными. При формировании политик и регламентов использования мобильных устройств необходимо учитывать, что такие устройства могут попасть в руки злоумышленников, которые попытаются получить конфиденциальные данные либо напрямую с устройства, либо используя их для удаленного доступа к ресурсам организации. Стратегия по смягчению последствий этого состоит из нескольких уровней [1].

Первый включает защиту конфиденциальных данных либо путем шифрования локального хранилища самого мобильного устройства, либо путем запрета локального хранения конфиденциальных данных. Даже если мобильное устройство всегда находится при владельце, существуют другие угрозы безопасности – например, возможность подглядеть важные данные или процесс ввода пароля.

Второй уровень включает обязательную аутентификацию пользователя. Как правило, у устройства имеется единственный идентификатор, поскольку предполагается только один владелец – следовательно, имя пользователя отсутствует, а есть только пароль, зачастую в виде простого PIN, что снижает

защищенность. Поэтому нужны более надежные методы аутентификации, такие как аутентификация в домене, используемые вместо или в дополнение к встроенным возможностям устройства.

Многим мобильным устройствам, принадлежащим сотрудникам, которые они используют в своей производственной деятельности (концепция DYOD), не хватает, так называемых, «корней доверия», криптопроцессоров (криптопровайдеров), которые давно уже встраиваются, например, в ноутбуки. Также применительно к мобильным устройствам распространен пользовательский взлом устройств (например, так называемый «джейлбрейк») – нарушение встроенных ограничений безопасности.

Организации должны придерживаться *презумпции ненадежности мобильных устройств* и предоставлять доступ с них к корпоративным данным и приложениями только после обеспечения безопасности, постоянно отслеживая состояние устройств в процессе их работы.

Есть несколько стратегий устранения рисков использования *недоверенных* мобильных устройств. Можно ограничить или запретить использование личных устройств и обеспечивать безопасность каждого корпоративного устройства, перед тем как выдавать его пользователю – это приводит устройство в наиболее безопасное состояние, и все отклонения от него могут быть отслеживаемы и контролируемы. Также есть технические решения, обеспечивающие определенный уровень доверия, – например, запуск корпоративных приложений в изолированных контейнерах или использование приложений, отслеживающих состояние устройства. Как правило, у организаций, а тем более пользователей нет возможности контролировать безопасность сетей, используемых мобильными устройствами. Системы связи поддаются прослушиванию, что может привести к компрометации передаваемых данных. Атаки типа «человек посередине» также могут использоваться для перехвата и изменения соединения. Организации должны придерживаться презумпции небезопасности соединения между мобильными устройствами и корпоративными ресурсами, если нет полной уверенности в том, что устройства будут использоваться только в контролируемых организацией сетях. Риски использования небезопасных сетей могут быть сокращены путем применения сложных алгоритмов шифрования для защиты конфиденциальности и целостности передаваемых данных, а также за счет взаимной аутентификации для проверки обоих узлов перед передачей данных. Мобильные устройства разрабатывались с целью упрощения поиска, получения, установки и использования приложений, что сразу создает очевидные риски безопасности, особенно на платформах, которые не ставят ограничений безопасности на публикацию сторонних приложений. Организации должны планировать защиту своих мобильных устройств исходя из предположения, что загружаемые пользователями сторонние приложения изначально опасны.

Есть несколько способов сократить риски, вызванные подобными приложениями, – например, запретить установку всех внешних приложений,

составить списки разрешенных или запрещенных приложений, использовать безопасный контейнер изоляции корпоративных данных и приложений от всех прочих, имеющихся на устройстве. Еще одна общая рекомендация – оценивать риски, создаваемые тем или иным сторонним приложением, перед разрешением его использования на мобильных устройствах организации. Важно отметить, что даже если эти стратегии устранения рисков безопасности применяются, пользователи все равно через встроенный браузер будут иметь доступ к небезопасным веб-приложениям. Связанные с этим риски можно сократить, ограничивая или запрещая использование браузера либо применяя специальный браузер внутри безопасного контейнера для всех рабочих нужд, оставляя встроенный браузер для всего остального.

Мобильные устройства могут взаимодействовать с другими системами для хранения и синхронизации данных. Локальное взаимодействие обычно включает в себя подключение мобильного устройства к настольному компьютеру или ноутбуку. Удаленное взаимодействие чаще всего включает автоматическое архивирование данных в облачном хранилище. Если все компоненты находятся под контролем организации, то риски в целом приемлемы, но обычно как минимум один компонент оказывается внешним для организации: возможно подключение личного мобильного устройства к корпоративному ноутбуку; подключение корпоративного мобильного устройства к удаленному хранилищу; перенос вредоносного программного кода с одного устройства на другое. Стратегии сокращения рисков в этом случае зависят от типа соединения. Предотвращение синхронизации корпоративного устройства с личным компьютером требует наличия на мобильном аппарате средств выбора устройств, с которыми разрешено синхронизироваться. Предотвращение синхронизации личных мобильных устройств с корпоративным компьютером требует аналогичных средств управления и на нем. Предотвращения доступа к удаленным хранилищам можно достигнуть путем блокирования сервисов, не позволяя, например, соединиться с доменными службами или конфигурируя мобильные устройства с целью исключения использования этих сервисов. На мобильных устройствах присутствует ненадежный контент, не встречающийся на других типах устройств, – например, QR-коды, специально созданные для обработки камерами мобильных устройств. Каждый такой код переводится в URL, и злоумышленники могут направлять пользователей на опасные веб-страницы, проводя целенаправленные атаки и размещая опасные QR-коды в местах физического присутствия целевых пользователей мобильных устройств, например на конференциях или в транспорте. Ключевой стратегией сокращения рисков, связанных с ненадежным контентом, является информирование пользователей о соответствующих рисках и запрет доступа к подобному контенту с любых мобильных устройств, применяемых в служебных целях. Также можно запретить использование определенных функций мобильных устройств – например, отключить камеру устройства во избежание обработки QR-кодов. С точки зрения корпоративной безопасности

мобильные устройства с работающими службами геолокации подвергаются повышенному риску целенаправленной атаки: злоумышленникам становится легче определить местоположение устройства и его пользователя, соотнести эту информацию со сведениями о том, с кем он работает, чем занимается в данном месте, – и заранее организовать на него атаку на базе, например, QR-кодов. Эти риски можно сократить, если отключить геолокационные сервисы или запретить их использование конкретными приложениями, такими как социальные сети или приложения для фото.

Если говорить о программном обеспечении (ПО), то существующие угрозы можно разделить на две группы:

Различное вредоносное ПО (вирусы, трояны) – обычно предназначено для хищения персональных данных, получения контроля над устройством или вывода его из строя;

Уязвимости (потенциальные ошибки) в прошивке или приложении, как правило, приводят к потенциальной практической возможности обхода аутентификации, искажения процессов обработки информации на устройстве.

На сегодняшний день мобильные устройства, в зависимости от типов использования встроенных операционных систем, можно разделить на:

1. устройства Android;
2. устройства Apple (IOS);
3. устройства Blackberry;
4. устройства Windows Mobile (снята с поддержки и заменена несовместимой с ней Windows Phone). Анонсированы Windows 8 и Windows 10.

Приведём несколько бытовых способов защитить свой телефон, планшет или иной гаджет:

Блокировка экрана и защита паролем.

Это самая важная защита, которую вы можете обеспечить своему устройству. Причем настроить ее можно за считанные минуты. Хотя такая зашита и не спасет от самых квалифицированных нарушителей (хакеров), но все же поможет избежать нежелательного просмотра информации в вашем телефоне. Рекомендуем также применить ее к программам, которые взимают плату за дополнительный контент, чтобы дети случайно не израсходовали ваш бюджет.

Устройства Android:

Для настройки блокировки экрана устройств Android нажмите Настройки> Безопасность> Блокировка экрана. Здесь можно выбрать способ блокировки/разблокирования экрана.

Нет (экран не блокируется).

Face Unlock (для разблокирования используется функция распознавания вашего лица через переднюю камеру).

Графический ключ (используется сетка 3x3, на которой вы можете создать графический ключ для разблокирования экрана).

PIN-код (4-значный PIN-код).

Пароль (вы сами выбираете пароль).

Выбирая один из способов защиты, учтите, что пароль целесообразно использовать только в том случае, если его тяжело угадать. Графический ключ также может быть ненадежным, если у вас грязные пальцы, ведь угол проведения четко будет видно на экране.

Разблокирование экрана на устройствах Android

Защиту паролем можно также использовать для отдельных программ с помощью функции App Lock (доступно тут). Она будет полезна, если платежные реквизиты сохраняются во время осуществления покупки через программу. Это обеспечит вам дополнительную защиту, поэтому вы спокойно можете давать детям поиграть с телефоном.

Устройства Apple:

Для устройств Apple доступна только одна функция защиты – 4-значный PIN-код. Чтобы настроить его, нажмите Настройки > Основные > Защита паролем.

Устройства Blackberry:

Пользователи телефонов и планшетов Blackberry могут выбрать для блокировки экрана функцию защиты паролем. Для этого нажмите Настройки > Безопасность и конфиденциальность > Пароль устройства или Настройки > Персонализация > Пароль. Просто включите функцию и выберите пароль.

Устройства Windows Mobile:

Как и для устройств Blackberry, для устройств Windows Mobile также можно активировать блокировку экрана с помощью пароля. Для этого нажмите Настройки > Блокировка экрана > Пароль.

Программы защиты.

Для устройств Android, Blackberry и Apple можно загрузить специальные программы защиты:

Android :

Самая популярная программа защиты для устройств Android – это TrustGo Antivirus & Mobile Security: она включает средство сканирования вирусов, проверку программы и даже антикражевые инструменты, позволяющие в случае похищения заблокировать устройство и определить его местонахождение (см. сайт TrustGo.com);

Apple:

Существует множество программ защиты для устройств iOS, однако самый популярный бесплатный вариант – это Lookout Antivirus, программа, которой пользуется более 20 млн. человек. Недавно вышла ее обновленная версия, содержащая новую опцию для пользователей iPhone и iPad – антикражевое ПО. Такая же версия также доступна для устройств Android и Kindle (см. сайт Lookout.com);

Windows Mobile:

Windows Mobile – это операционная система, содержащая программное обеспечение системы безопасности для устройств семейства Windows. Предлагают решение безопасности Windows Mobile, включающее Symantec, AVG (также и для устройств Android и Apple) и Kaspersky (также для устройств Android и Blackberry). В настоящее время снята с поддержки

Microsoft и заменена на Windows Phone, к стати тоже не получившей широкого распространения. Большие надежды возлагаются на анонсированные универсальные ОС – Windows 8 (2013 г.) и Windows 10 (2015 г.);

Blackberry:

Компания Blackberry выпустила полезную программу под названием Blackberry Protect, которая копирует ваши данные и помогает найти устройство в случае утери. Есть также предложения и от известных разработчиков, таких как Kaspersky и McAfee.

Подозрительные ссылки.

Согласно результатам исследования, пользователи мобильных устройств втрое чаще переходят по подозрительным ссылкам, чем пользователи компьютеров и ноутбуков. А причина довольно проста: небольшой размер экрана не позволяет должным образом распознать источник ссылки. Поэтому будьте бдительны, когда переходите на сайты, и проверяйте, надежен ли источник. А во время загрузки файлов необходима предельная осторожность. Проверенное правило такое: если не уверены в источнике, не переходите по ссылке.

Проверка программ.

Сначала трудно устоять перед искушением, чтобы не загрузить первые попавшиеся бесплатные программы. Однако всегда обращайте внимание, на какой сайт вы переходите. Загружайте файлы только из проверенных интернет-магазинов, таких как Google Play, Amazon или iTunes. Рекомендуем также сначала просмотреть отзывы других пользователей о необходимом продукте, чтобы убедится, что он не только широко используется, но и достаточно безопасен.

Важным аспектом безопасности является и тот факт, разрешает ли система устанавливать программы из неизвестных источников. Если да, веб-сайт может автоматически начать установку программы на ваш телефон. Если вы не уверенны в надежности источников, настройте телефон так, чтобы система запрещала установку таких программ.

На устройствах Android это можно сделать, нажав Настройки > Безопасность > Неизвестные источники. Флажка быть не должно.

Устройства Apple, Blackberry и Windows разрешают загрузку только с дочерних магазинов. Поэтому можете не волноваться, если вы пользуетесь одним из этих мобильных устройств.

Общие советы:

- Просматривая сайты на ноутбуке, планшете или телефоне, помните о правилах политики безопасности, принятые в вашей организации, которые нужно соблюдать;
- Будьте осторожны, открывая беспроводные точки доступа Wi-Fi;
- Когда вы пользуетесь общим интернет-соединением (в том числе и через мобильное соединение через GSM или Wi-Fi), история вашего просмотра передается через сеть, к которой могут получить доступ находящиеся рядом люди. Хотя это и нелегко, но все же возможно

через это соединение получить доступ к вашему компьютеру. Поэтому не просматривайте важную информацию и не осуществляйте онлайн-платежи, если эта сеть ненадежная;

- Желательно используйте устройство только по назначению;
- Устройства иногда используются не только по назначению, но и в других целях, непредусмотренных их программированием. В этом случае помните, что таким образом вы рискуете снизить степень защиты, что может повлечь за собой множество проблем и лишение гарантии;
- Не включайте функцию сохранения и автозаполнения для пароля. Защита паролем очень важна. Настроить ее можно за считанные минуты. Однако она теряет всякую силу при автоматическом запоминании пароля на переносных устройствах. Не желая каждый раз вводить пароль вручную, вы применяете эту функцию для просмотра страниц, соцсетей, онлайн-платежей и оплаты, которая производится через программу. Однако делать этого не рекомендуется;
- Все эти советы позволят относительно безопасно пользоваться мобильными устройствами в быту.

Ну а как быть на предприятии, когда в бизнес-процессы вовлечены сотни сотрудников, вооружённых мобильными устройствами? Первое что сразу приходит на ум – это *управление мобильными устройствами* с целью достижения приемлемого уровня ИБ, в соответствии с принятой на предприятии политикой безопасности.

Управление мобильными устройствами

Есть два базовых подхода к управлению мобильными устройствами: использование возможностей сервера обмена сообщениями (часто от того же производителя, что и устройства) или использование стороннего продукта, который разработан для управления несколькими марками устройств. У типичного решения достаточно простая клиент-серверная архитектура. В организации установлен один или несколько серверов, обеспечивающих централизованное управление, а на все мобильные устройства устанавливаются клиенты, которые настраиваются для постоянной работы в фоновом режиме. Если устройство выдано организацией, клиентское приложение обычно управляет конфигурацией и безопасностью всего устройства (режим управления мобильными устройствами, MDM). Если устройство принадлежит сотруднику, то клиентское приложение управляет только конфигурацией и безопасностью самого приложения и корпоративных данных (режим управления мобильными приложениями, MAM). Клиентское приложение и корпоративные данные изолированы от прочих приложений и данных устройства, помогая сохранить конфиденциальность как корпоративных данных, так и личного контента пользователя. Централизованное

управление мобильными устройствами может задействовать другие корпоративные службы, такие как доменные службы аутентификации и VPN.

Если в организации отсутствует централизованное решение или некоторые мобильные устройства несовместимы с ним, тогда устройствами приходится управлять вручную. Мобильные устройства часто не предоставляют возможности строго настроить средства безопасности, как это делают клиентские приложения централизованных устройств. Например, мобильные устройства часто поддерживают только простой пароль для аутентификации и не поддерживают надежного шифрования хранилища. Это потребует приобретения, установки, настройки и поддержки целого перечня сторонних приложений, чтобы компенсировать недостающий функционал. Управление устройством, физически не находящимся в стенах организации, может оказаться невозможным. Можно установить утилиты для удаленного управления устройствами, но это потребует значительно больше сил для ручного обновления ПО и прочей технической поддержки мобильных устройств, находящихся вне офиса.

Организации, намеревающиеся использовать мобильные устройства, должны обдумать достоинства каждого сервиса безопасности и определить, какие именно необходимы для их среды.

Общие политики.

Централизованная технология, позволяющая применять корпоративные политики безопасности, вводящие ограничения на работу с мобильным устройством:

- запрет пользователю и приложениям доступа к отдельным модулям устройства, таким как цифровая камера, GPS, Bluetooth, USB или съемная карта памяти;
- запрет доступа к встроенному веб-браузеру, почтовому клиенту, службам установки приложений и т. д.;
- управление беспроводными интерфейсами (Wi-Fi, Bluetooth и т. д.);
- автоматическое отслеживание устройства, определение и оповещение о нарушениях политик.

Передача и хранение данных.

Надежное шифрование передачи данных между мобильным устройством и организацией, что, как правило, происходит в форме VPN, хотя можно использовать и другие типы шифрования. Надежное шифрование локально хранимых данных, как во встроенном хранилище, так и на съемной карте памяти. Съемные карты памяти также могут «привязываться» к конкретным устройствам, чтобы зашифрованные данные можно было считать только тогда, когда карта подключена к данному устройству, тем самым уменьшая риск атаки на носитель в автономном режиме. Удаленное очищение устройства в случае подозрения на то, что оно потеряно, украдено или иным способом попало в руки третьих лиц. Часто автоматическая очистка устройства запускается после определенного количества неудачных попыток аутентификации.

Аутентификация пользователей и устройств.

Должна быть предусмотрена реализация требования аутентификации по паролю и/или другой (например, доменной) перед получением доступа к корпоративным ресурсам. Это включает базовые параметры сложности пароля и количества попыток ввода пароля до наступления негативных последствий (блокировки учетной записи, очистки устройства). Если включена блокировка учетной записи или забыт пароль, то администратор может удаленно сбросить пользователю пароль для восстановления доступа к устройству. Кроме этого, надо требовать повторной аутентификации по истечении определенного периода бездействия и удаленно блокировать устройство, если есть подозрение, что оно могло быть оставлено в незаблокированном состоянии в небезопасном месте.

Приложения.

Сервисы работы с приложениями должны уметь устанавливать определенные программы (вести черный и белый списки), управлять установкой обновлений и удалением приложений, отключать использование служб синхронизации. Необходимо также работать с цифровой подписью приложений с целью убедиться, что на устройстве установлены только доверенные приложения и их код не изменялся. Важной функцией является организация и мониторинг распространения необходимых для работы программ через корпоративный магазин приложений. Кроме того, следует ограничивать или предотвращать доступ к корпоративным ресурсам в случае несовпадения версии операционной системы мобильного устройства или версии клиентского приложения.

Безопасность мобильных данных.

Основные угрозы, которые несет предприятию мобильность, лежат в плоскости информационной безопасности, и сегодня, чем более мобильны и удобны технологии в обращении, тем потенциально они менее защищены.

Мобильные устройства часто теряют, либо их целенаправленно крадут — согласно глобальному исследованию компании InfoWatch, 18,2% всех инцидентов, связанных с утечкой конфиденциальной информации, приходится на долю забытых или украденных мобильных устройств [2]. При этом их владельцы редко по собственной инициативе пользуются какими-либо средствами защиты – например, шифрованием: этой работой занимаются системные администраторы/офицеры безопасности компании, допускающей применение персональных мобильных устройств для обработки корпоративных данных. В помощь администраторам безопасности компании – вендоры сервисов средств защиты зачастую предлагают программные продукты, позволяющие обеспечить шифрование данных на различных мобильных устройствах.

Часто в мобильных устройствах нет четкой границы между приватной и корпоративной информацией, хотя эти данные должны использоваться и храниться отдельно, поэтому компаниям необходимо разработать соответствующие политики работы с конфиденциальными данными.

Корпоративная информация должна храниться и обрабатываться в защищенном режиме – это может быть особая виртуальная среда с контролем за движениями данных, допускающая запуск только конкретных приложений. Переход от контроля информации на уровне инфраструктуры к контролю на уровне приложений и самих данных представляется очень перспективным, это использование DLP – систем.

Для эффективной защиты всех видов конфиденциальной информации на мобильных устройствах, требуются технологии, позволяющие контролировать все перемещения данных как внутри корпоративного периметра, так и вне его. В первую очередь это системы защиты данных от утечки (DLP), осуществляющие мониторинг конфиденциальных данных при различных сценариях использования мобильных устройств. Если компания допускает использование личных мобильных устройств в корпоративной сети, то логична установка мониторинговых агентов на каждое устройство для организации контроля трафика с этих устройств на серверном уровне. Кроме этого, политики информационной безопасности должны включать обязательное разделение личной и рабочей переписки, ограничение доступа к сетевым ресурсам и обязательное шифрование. Решения по контролю за трафиком в виде выше упомянутых DLP – систем позволяют осуществлять мониторинг и анализ данных, отправляемых за пределы организации через почтовые системы, интернет-ресурсы, системы обмена мгновенными сообщениями, предотвращая утечку конфиденциальной информации и позволяя расследовать инциденты, связанные с неправомерными действиями сотрудников.

Жизненный цикл решений по безопасности мобильных устройств

Рассмотрим весь жизненный цикл решений для определения актуальности тех или иных рекомендаций пои безопасности мобильных устройств.

Инициация.

Данный этап включает решение ряда подготовительных задач, таких как определение текущих и будущих потребностей, уточнение требований по производительности, функциональности и безопасности. Разработка корпоративных политик безопасности при использовании мобильных устройств — важнейшая часть этапа инициации. Политики безопасности должны определять, каким типам мобильных устройств разрешен доступ к корпоративным ресурсам, степень доступа различных классов мобильных устройств (например, личных или корпоративных) и как должна производиться подготовка к работе. Также здесь рассматриваются принципы администрирования серверов централизованного управления мобильными устройствами и способы обновления политик. Политики безопасности для мобильных устройств должны быть отражены в плане обеспечения информационной безопасности всей корпоративной системы. Корпоративные политики часто ограничивают типы мобильных устройств, которые можно использовать для доступа к ресурсам, — например,

организация может разрешать доступ только с корпоративных мобильных устройств. В некоторых организациях используется многоуровневая система доступа: корпоративные устройства имеют доступ ко всем ресурсам; личные устройства с установленным клиентом системы управления мобильными устройствами имеют доступ к ограниченному набору ресурсов; все прочие мобильные устройства имеют доступ только к избранным веб-ресурсам, например к почте. Таким образом, организация может сокращать риски, определяя уровень доступа с учетом оценки безопасности при работе с мобильных устройств.

Конфиденциальность работы.

Организации могут иметь более строгие ограничивающие требования к работе с конфиденциальной информацией — например, давать разрешение доступа к такой информации только с корпоративных устройств, однако при этом следует учитывать правовые аспекты удаленного стирания данных с личных мобильных устройств.

Уровень доверия в соблюдении политик безопасности.

Соблюдение многих требований корпоративной безопасности зачастую может быть обеспечено только при условии, что организация контролирует процесс настройки мобильных устройств. Если такие устройства не используют корпоративную систему управления мобильными устройствами, то некоторые требования могут быть проверены автоматическим сканированием, осуществляемым системой управления мобильными устройствами при попытке подключения, но прочие требования проверке не поддаются.

Издержки.

Издержки, связанные с использованием мобильных устройств будут различаться в зависимости от принятых политик. Главными прямыми издержками являются стоимость выдаваемых сотрудникам корпоративных устройств и стоимость клиентского ПО. Кроме того, есть косвенные издержки, связанные с поддержкой мобильных устройств и предоставлением технической помощи пользователям.

Расположение рабочего места.

Риски устройств, используемых только в корпоративной среде, как правило, ниже, чем у устройств, используемых в разных местах присутствия сотрудника.

Технические ограничения.

Для запуска конкретных приложений могут потребоваться определенные типы мобильных устройств. Кроме того, корпоративная система управления мобильными устройствами может поддерживать только определенные типы мобильных устройств.

Соответствие регламентам.

Некоторым организациям при работе с мобильных устройств необходимо соблюдать требования, которые являются внешними для организации, например требования регулирующих органов. Многие организации принимают более строгие меры обеспечения безопасности для ситуаций,

связанных с высокими рисками — например, вводят требование о работе только с безопасных корпоративных устройств или требование многофакторной аутентификации для доступа к мобильному устройству и корпоративным ресурсам.

Другим способом является перенос ресурсов с высоким риском на корпоративные серверы. Кроме того, организация может сократить риски, запрещая доступ с мобильных устройств к определенным типам информации, таким как персональные данные. Ежегодно происходит множество изменений в функционале мобильных устройств, способах управления их безопасностью и типах угроз, следовательно, организации должны периодически пересматривать политики и порядок применения мобильных устройств при работе на конкретном уровне доступа. Организации должны быть в курсе появления новых типов решений для мобильных устройств и изменений в существующих системах управления такими аппаратами для своевременного обновления корпоративных политик.

У организаций часто есть дополнительные соображения по безопасности мобильных устройств, которые позволяют сократить риски, однако их исполнение не всегда возможно, поэтому важно донести до сотрудников необходимость соблюдения мер безопасности и закрепить это в политиках и регламентах. Первое возможное соображение относится к так называемым личным беспроводным сетям, не требующим дополнительного оборудования: беспроводные мыши, клавиатуры, принтеры, беспроводные гарнитуры смартфонов, Bluetooth и NFC домашние радиотелефоны стандарта DECT. На устройствах, находящихся поблизости от потенциальных источников угроз, пользователи не должны включать данные технологии без необходимости.

Разработка.

На этом этапе определяется, какие технологии управления мобильными устройствами стоит использовать, и разрабатываются решения для их развертывания.

Архитектура.

Проектирование архитектуры включает выбор системы управления мобильными устройствами, расположение сервера управления этими устройствами и других централизованных элементов.

Аутентификация.

Включает в себя выбор средств аутентификации мобильных устройств и пользователей, в том числе определение порядка выдачи и возврата аутентификаторов.

Криптография.

Включает выбор алгоритма шифрования и защиты целостности передаваемых на мобильные устройства данных, выбор сложности ключа для алгоритмов, поддерживающих различную длину ключа.

Конфигурация.

Определение минимальных стандартов безопасности для мобильных устройств (например, обязательные средства по усилению безопасности

серверов и степень обновленности), а также указание дополнительных мер обеспечения безопасности, которые должны быть использованы на мобильных устройствах, таких как VPN-клиент.

Сертификация.

Установка требований к безопасности и производительности, которым должны отвечать приложения, а также определение того, как контролируется соответствие данным требованиям. Организация должна также определить порядок обработки инцидентов, связанных с мобильными устройствами, и его задокументировать.

Внедрение.

На этой стадии для каждого типа мобильных устройств следует оценить степень надежности подключения устройства и защиты его данных. Пользователи могут подключаться ко всем или только к части корпоративных ресурсов, а информация, хранимая на мобильных устройствах, и данные, передаваемые между устройством и корпоративными ресурсами, должны быть защищены в соответствии с предъявляемыми требованиями. Особое внимание необходимо уделить аутентификации, которая не может быть легко скомпрометирована или обойдена, а также должно быть обеспечено исполнение всех политик аутентификации устройств, пользователей и аутентификации в домене.

Все приложения должны поддерживаться соответствующими функциями мобильного решения при выполнении всех ограничений по их установке. Администраторы могут эффективно и безопасно конфигурировать и управлять всеми компонентами мобильного решения. Поводом для беспокойства может быть возможность изменения настроек мобильного устройства и клиентского ПО пользователем с целью ослабления безопасности решения. Ведение логов мобильного решения должно производиться в соответствии с регламентами организации. При развертывании решения нужно удостовериться, что все его компоненты обеспечивают адекватную производительность как при нормальных, так и при пиковых нагрузках. Также важно учитывать производительность промежуточного оборудования, такого как маршрутизаторы и межсетевые экраны. В процессе внедрения решения могут возникнуть уязвимости, поэтому рекомендуется произвести дополнительную проверку компонентов – как минимум все они должны быть обновлены до последней версии и настроены в соответствии с практиками обеспечения безопасности. Кроме того, должен автоматически определяться факт взлома пользователем устройства, чтобы запретить работу с ним. Специалисты, внедряющие решение, должны внимательно ознакомиться с настройками мобильных устройств и изменить их для соответствия требованиям безопасности. Организация должна полностью убедиться в безопасности каждого корпоративного мобильного устройства перед его выдачей пользователю — любое выданное устройство с неизвестным профилем безопасности должно быть изъято и возвращено к безопасному состоянию.

Эксплуатация и обслуживание.

На стадии эксплуатации нужно регулярно выполнять проверку наличия обновлений для компонентов решения, отслеживать их получение, тестирование и разворачивание на устройстве сотрудника. Важно также проводить постоянную синхронизацию часов каждого из компонентов решения с единым источником времени – временные метки должны соответствовать меткам, создаваемым другими системами. Регулярно должна проводиться перенастройка системы контроля доступа с учетом изменения политик, технологий, требований аудита и новых задач, возникающих перед предприятием. Администратор должен выявлять и документировать аномалии в инфраструктуре мобильных устройств, которые могут указывать на вредоносную активность или отклонения от политик безопасности. Кроме того, должно проводиться регулярное обследование, например путем анализа логов или путем проведения сканирования, в поисках уязвимостей или следов проникновения. Пользователи мобильных устройств должны проходить тренинги (обучение) для повышения осведомленности об угрозах и рекомендованных практиках.

Удаление.

Прежде чем компонент мобильного решения будет списан, организация должна убедиться в удалении с него всей конфиденциальной информации. Задача удаления данных с носителей, таких как жесткие диски или карты памяти, зачастую оказывается неожиданно сложной из-за большого количества мест, в которых хранятся данные, и активного использования флэш-носителей.

Перечисленные рекомендации могут оказаться полезными для предприятий, которые планируют переходить на мобильные «рельсы» вне зависимости от уже используемых у них ИТ-компонентов и доступных технологий MDM и MAM. Выбор конкретных решений будет обусловлен многими факторами, но основные угрозы безопасности и способы их устранения неизменны – главное, чтобы организации изначально придерживались презумпции ненадежности мобильных устройств и планировали предоставлять доступ к своим корпоративным данным и приложениями только при соблюдении всех необходимых мер обеспечения безопасности.

Почему смартфоны/планшеты или иные мобильные устройства являются объектом столь пристального внимания со стороны злоумышленников? К примеру, поищите свой смартфон (мобильный телефон, планшет или иной гаджет) – скорее всего он всегда пребывает на расстоянии вытянутой руки, в отличии от вашего компьютера, смартфон почти постоянно включен и скорее всего постоянно подключен к сети Интернет. Это создает весьма благоприятные условия для быстрой монетизации кибератак.

Как показывают исследования, проведенные аналитической компанией **CSA Mobile**, 81% респондентов считают, что на сегодняшний день одной из основных угроз безопасности мобильных устройств (кроме кражи и потери)

являются небезопасные Wi-Fi – соединения и незащищенные точки доступа к сети Интернет через мобильные телекоммуникационные системы связи типа GSM.

Лидирует в списке угроз и потеря данных. Специалисты отмечают различные способы и механизмы потери информации, включая кражу или потерю гаджета, а также распространение различных вредоносных программ, нацеленных на конфиденциальные данные владельцев мобильных устройств.

Вместе с этим, исследователи отмечают распространение и других угроз, таких как небезопасные сторонние приложения, уязвимости в системе безопасности операционной системы, возможность подключиться к чужому устройству с помощью технологии бесконтактной передачи данных и мобильных платежей **NFC**, небезопасные Wi-Fi – соединения, а также мошеннические онлайн-магазины и каталоги приложений.

Смартфоны или планшеты сегодня часто используются для интернет-банкинга, мобильных платежей и передачи конфиденциальных бизнес-данных, в связи с чем эти устройства привлекают к себе все больше злоумышленников. Мобильные приложения часто загружают, не думая об их безопасности, поэтому у хакеров есть практически карт-бланш на совершение атак. Взломщики могут получить очень ценную добычу: финансовую и личную информацию. Смартфоны могут подключаться к Интернету для обновления программного обеспечения или синхронизации файлов. Данный способ соединения крайне уязвим для атак. Вместе с тем производители устройств и операторы беспроводных сетей развивают по преимуществу коммуникационные возможности и другие сервисы, а безопасности уделяется незначительное внимание.

Угрозы и уязвимости мобильных телекоммуникационных систем

Сети сотовой связи стандарта GSM

В Европе принят единый стандарт для систем мобильной связи GSM (groupe special mobile, второе поколение мобильных средств связи). GSM использует диапазоны 900 и 1800 МГц. Это довольно сложный стандарт, его описание занимает около 5000 страниц. Идеологически система имеет много общего с ISDN (например, переадресацию вызовов). GSM имеет 200 полнодуплексных каналов на ячейку, с полосой частот 200 кГц, что позволяет ей обеспечить пропускную способность 270,833 бит/с на канал. Каждый из 124 частотных каналов делится в GSM между восемью пользователями (мультиплексирование по времени). Теоретически в каждой ячейке может существовать 992 канала, на практике многие из них недоступны из-за интерференции с соседними ячейками.

Система мультиплексирования по времени имеет специфическую структуру. Отдельные временные домены объединяются в мультифреймы. Каждый временной домен (TDM) содержит 148-битовый кадр данных, начинающийся и завершающийся последовательностью из трех нулей. Кадр имеет два 57-битовых поля данных, каждое из которых имеет специальный

бит, который указывает на то, что лежит в кадре: голос или данные. Между информационными полями размещается поле синхронизации (Sync). Хотя информационный кадр имеет длительность 547 мксек, передатчику позволено передавать его лишь раз в 4615 мксек, так остальное время зарезервировано для передачи другими станциями. Если исключить накладные расходы каждому соединению выделена полоса (без учета сжатия данных) 9600 кбит/с.

Восемь информационных кадров образуют TDM-кадр, а 26 TDM-кадров объединяются в 128-микросекундный мультифрейм. Как видно из рисунка 4.1.8.1.2 позиция 12 в мультифрейме занята для целей управления, а 25-я зарезервирована для будущих применений. Существует также стандарт на 51-позиционный мультифрейм, содержащий больше управляющих вставок. Управляющий канал используется для регистрации, актуализации положения и формирования соединения. Каждая стационарная станция поддерживает базу данных, где хранится информация обо всех обслуживаемых в данный момент клиентах. Общий управляющий канал делится на три субканала. Первый служит для обслуживания вызовов (paging channel), второй (random access channel) реализует произвольный доступ в рамках системы ALOHA (устанавливаются параметры вызова). Третий субканал служит для предоставления доступа (access grant channel).

Упрощенная схема структуры кадров показана на рис. 1.

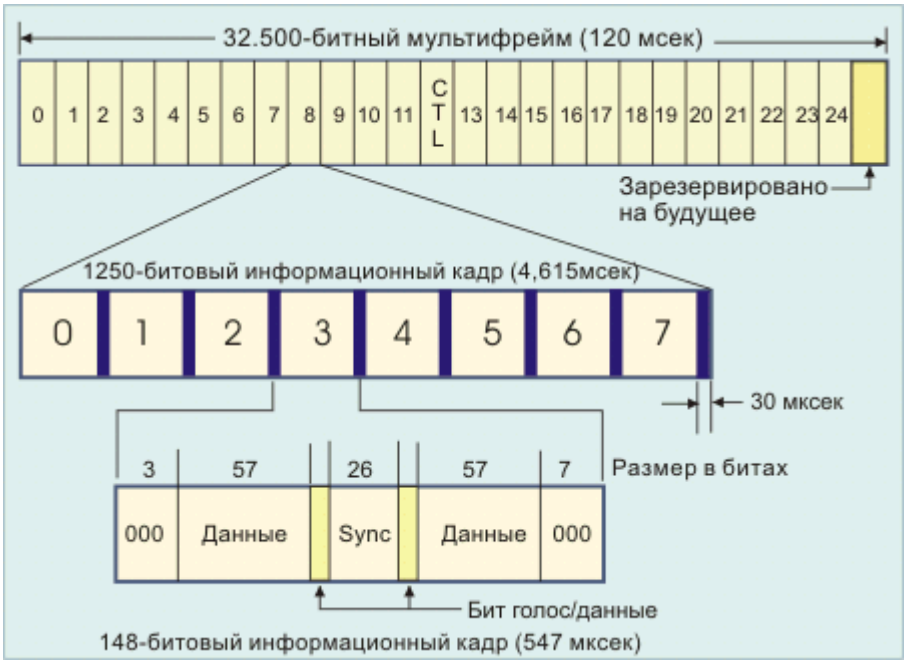

Рис.1. Структура кадров в GSM

Стоит отметить, что на сегодня стандарт GSM официально считается защищенным от несанкционированного прослушивания. Согласно официальным данным, прослушать разговор в GSM-канале можно только с санкции одной из сторон - оператора или абонента. Однако на протяжении 21 года существования данной технологии полуофициально все же ходили

слухи о наличии возможностей по обходу алгоритмов шифрования. Официально они так и не получили подтверждения.

Немецкий компьютерный криптоаналитик Керстин Нол сообщил (29.12.2009) о создании метода взлома системы шифрования самого популярного в мире стандарта сотовой связи GSM [3]. По его словам, система шифрования разговоров в сетях GSM имеет фундаментальные уязвимости и программный код, созданный им, использует эти уязвимости. При этом, сам инженер говорит, что его целью было не предоставить всем желающим возможность прослушивать мобильные разговоры людей, а указать телекоммуникационным компаниям на фундаментальные недочеты, чтобы те могли их исправить.

Сам разработчик алгоритма взлома говорит, что его технология является первой с 1988 года реально обходящей систему и ставящей под угрозу приватность разговоров до 80% пользователей сотовой связи в мире. "Этот пример показывает, что существующие техники защиты GSM не соответствуют современным нормам", - говорит разработчик.

Демонстрацию своей разработки инженер провел в рамках конференции Chaos Communication Congress в Берлине. "Мы уже давно пытались призвать операторов связи реализовать более надежные системы защиты", - говорит Нол.

В Ассоциации GSM сообщили, что им уже удалось изучить код представленный разработчиком и передать его образцы представителям сотовых операторов. Представители называют разработки инженера с одной стороны незаконными, а с другой отмечают, что разработчик значительно преувеличивает опасность своих разработок. "Это (взлом) теоретически возможно, но практически вряд ли. Можно сказать, что пока еще никому не удавалось полностью обойти систему шифрования GSM. Также можно отметить, что в ряде стран, в частности в США или Великобритании, такие разработки вообще незаконны", – говорит представительница Ассоциации Клэр Крентон.

Впрочем, с позицией Ассоциации не согласны многие эксперты, утверждающие, что представленный код вполне можно усовершенствовать и при запуске на современных многоядерных многопроцессорных системах он может быть вполне эффективен. К примеру, в исследовательской компании ABI Research, занимающейся мобильными и телекоммуникационными исследованиями, говорят, что всем заинтересованным сторонам следовало бы отнестись к данной угрозе серьезно, так как примерно через полгода уже может появиться более продвинутая версия программы, тем более, что ее код свободно доступен в интернете.

Сам немецкий инженер рассказывает, что код создавал он не один. Ему помогали энтузиасты, которых он нашел на одном из хакерских форумов в Амстердаме. Всего над созданием системы взлома работали почти 25 человек из разных европейских стран. Говоря о законности или незаконности своих разработок Керстин Нол заявил, что его интерес при разработке программы был исключительно академическим и в реальности ни одного звонка он не

прослушал и не нарушил ни одного закона. Проверяли работоспособность программы они на специальных программных симуляторах, воспроизводящих режимы работы сети. "Сейчас образцы кода уже доступны на многих сайтах, на Torrent, на форумах", – говорит он.

Напомним, что система защиты GSM базируется на так называемом алгоритме A5/1, представляющем собой 64- битный двоичный код. Отметим, что на сегодня большинство современных компьютерных систем работает с ключами длиной 128-512 бит, что считается более надежным. В 2007 году Ассоциация GSM разработала стандарт A5/3, обладающий длиной ключа в 128 бит, однако лишь незначительное число операторов развернуло поддержку этой технологии.

Впрочем, эксперты говорят, что смена алгоритма – это дело не только технически сложное, но и невыгодное с точки зрения финансов. Компаниям придется менять до 60 несущих частот на всех своих станциях, а учитывая, что большинство операторов сотовой связи почти на 100% задействуют свой радиочастотный ресурс, то и емкость сети значительно снизится.

GSM использует довольно сложную комбинацию методик ALOHA, TDM и FDM. CDPD для передачи одиночных кадров не вполне согласуется с алгоритмом CSMA. Впрочем, существует еще один метод формирования радио каналов, – CDMA (Code Division Multiple Access), основанный на кодовом разделении каналов.

Впрочем, не останавливаясь на технологии CDMA как на мало распространённой, перейдём к перспективной технологии будущих 4G-сетей мобильной связи, поглощающей GSM и CDMA – LTE (Long-Term Evolution), как технологии четвёртого поколения мобильных телесистем [4].

Технология нового поколения сотовой связи – LTE

LTE-технология (акроним Long-Term Evolution), обычно позиционируется как сеть 4G LTE, является стандартом для беспроводной высокоскоростной передачи данных для мобильных телефонов, устройств и терминалов сбора и обработки данных (гаджетов).

Технология нового поколения сотовой связи LTE постепенно внедряется во многих странах мира. Уже выдаются лицензии на частоты LTE основным игрокам мобильного рынка, однако непонятно, насколько ее использование безопасно для абонентов в плане ИБ. Поскольку технология LTE полностью основана на протоколе IP, не превратятся ли мобильные сети этой технологии в Интернет с присущими ему угрозами и уязвимостями? Чтобы ответить на этот вопрос, рассмотрим сначала, чем LTE-сети отличается от предыдущего поколения мобильной связи.

Мобильная связь четвертого поколения предусматривает использование целого спектра технологий, которые раньше развивались параллельно. Это технология кодового разделения сигнала CDMA, технология цифровой мобильной связи GSM/GPRS, основанная на временном разделении сигнала, и стандарт радио-Ethernet под названием WiMAX, который подразумевает динамическое разделение ресурса базовой станции между абонентами. Все они внесли свой вклад в спецификацию LTE, также реализованной в двух

основных вариантах: технология с дуплексным частотным разделением FDD (Frequency Division Duplex) и временным разделением TDD (Time Division Duplex). Опора на множество различных технологий затрудняет поиск уязвимостей в LTE, что хорошо с точки зрения безопасности – взлом радиоканала для одних методов может сработать, а для других – нет. Алексей Лукацкий, менеджер по развитию бизнеса компании Cisco, считает, что, поскольку стандарты LTE и LTE Advanced – это всего лишь усовершенствованные стандарты мобильной связи 3G, то никаких принципиально новых угроз безопасности для данного вида коммуникаций не появилось. Однако акценты в моделировании угроз технологии LTE чуть сместились. Теперь все угрозы связаны с протоколом IP. Если в 3G голосовой трафик и данные передавались по двум разным сетям – по сети с коммутацией каналов (через MSC – Mobile Switching Centre) и по сети данных (через узлы маршрутизации данных и обслуживания абонентов GGSN/SGSN), то в сетях 4G весь трафик проходит через единую архитектуру EPC (Evolved Packet Core) по протоколу IP.

Нельзя забывать и об ограничениях LTE. Например, увеличение скорости подключения оборачивается обычно уменьшением радиуса действия базовой станции – в среднем для LTE он составляет около 5 км, хотя зависит от используемого частотного диапазона. Из-за этого базовых станций в сети становится больше и расположены они должны быть ближе друг к другу. В результате метод определения местоположения абонента по сигналам базовых станций (триангуляция) будет работать точнее. С одной стороны, это хорошо – оператор точнее будет знать местонахождение абонента. С другой стороны, сервисы геопозиционирования (Location-based service, LBS) можно использовать и для слежки за абонентом, что создает опасность новых угроз. Поэтому сервисы на основе LBS можно назвать сервисами двойного назначения.

Увеличенная плотность размещаемого сетевого оборудования может выразиться и в появлении на сети фемто- и даже пикосот, которые сам пользователь или предприятие может установить у себя для улучшения покрытия LTE-сети. Однако появление новых сетевых элементов может быть чревато атаками на них и каналы их связи с остальной сетью. И пока не совсем понятно, кто именно будет конфигурировать и обеспечивать безопасность этих фемтосот – пользователь, который их приобретает, или оператор, к чьей сети они подключаются.

Также нужно учесть, что базовые станции в LTE стали более интеллектуальными и самостоятельными – они получили возможность маршрутизировать трафик. «Особенность сети 4G в том, что из ее архитектуры исчезло понятие контроллера радиосети (RNC), который в 3G выполнял основную функцию по управлению коммуникационными ресурсами, – пояснил Лукацкий. – Трафик от базовых станций шел к RNC, а затем через ядро сети к другим контроллерам и базовым станциям».

Для того чтобы осуществить атаку на инфраструктуру 3G целиком, необходимо было получить доступ к контроллеру (контроллерам), а это

сопряжено с трудностями по физическому доступу к RNC. В сетях LTE картина поменялась: звено RNC полностью исчезло, а управляющие функции перешли к базовым станциям, получившим название eNodeB (eNB), которые и стали принимать решение о маршрутизации всего трафика. Это позволило организовывать соединения между абонентами напрямую, минуя ядро сети. В результате у злоумышленников появилась возможность атаковать сами базовые станции eNB. Они работают только по протоколу IP, поэтому облегчается несанкционированный доступ к сети – могут быть использованы классические атаки на канальном уровне, широковещательные штормы, создание фальшивого eNB и другие варианты нападений.

Еще одна особенность LTE в том, что эта технология ориентирована на подключение интеллектуальных пользовательских устройств: компьютеров с LTE-модемами, планшетов, смартфонов или иных гаджетов. Простым телефонам, которые умеют только звонить и отправлять SMS, технология LTE не особенно нужна. Это означает, что по мере распространения в сети LTE интеллектуальных устройств, в том числе мобильных, количество нападений на них будет только возрастать. Ведь смартфоны, ПК и планшеты подвержены более широкому кругу угроз, нежели простые телефоны. Вирусы на компьютерах стали делом обычным, троянцев для Android становится все больше, продукция Apple и Microsoft тоже уязвима для вредоносных программ. Сергей Голованов, ведущий антивирусный эксперт «Лаборатории Касперского» по мобильным технологиям, считает, что внедрение высокоскоростного стандарта LTE принесет в мобильные средства связи все те угрозы, которые мы сейчас видим в ситуации с обычными компьютерами: атаки DDoS, рассылку спама, перехват видео и звука с камеры устройства и др.

Угрозы LTE

Первая очевидная угроза – атаки DoS (Denial of Service) на сеть. Емкость радиоканала в LTE предполагается большая, но все же она имеет ограничения. Сетевые ресурсы базовой станции делятся между абонентами, и хотя есть ограничения для монополизации полосы отдельным пользователем, тем не менее атака на отказ в обслуживании сети вполне возможна. По мнению Алексея Лукацкого, исчезновение RNC привело к тому, что доступ к ядру сети LTE возможен непосредственно с базовой станции. Например, атаку, провоцирующую отказ мобильной сети, можно выполнить с помощью специального троянца, который активируется в определенной соте или географических координатах, либо хакер может перехватить контроль над отдельной базовой станцией и вывести ее из строя. «Угрозы начинаются не на канальном уровне LTE, а на более высоком уровне протокола TCP/IP со всеми его известными особенностями и применением злоумышленниками, – пояснил Голованов. – Тот же самый пресловутый вариант SYN Flood как форма проведения DoS-атаки будет работать и в сетях LTE».

Вторая угроза – вирусные атаки. Хотя таким атакам подвержены устройства, а не сеть, технология LTE увеличивает скорость распространения вредоносных программ, поскольку сам этот стандарт является

высокоскоростным. «Проблемы начинаются при установке пользователями дополнительных прошивок или при получении полного доступа к мобильному устройству, когда при неверной конфигурации злоумышленникам становятся доступны все ресурсы телефона через тот же протокол SSH (Secure SHell), – предупредил Голованов. – Сейчас ограничения скорости при сканировании в сетях 3G не позволяют злоумышленникам находить потенциально уязвимые устройства. Ситуация изменится с повсеместным распространением LTE». К тому же плата за пользование услугами четвертого поколения вряд ли будет зависеть от объема трафика – тарифы будут либо безлимитными, либо с ограничением по полосе пропускания. Поэтому пользователи не смогут быстро заметить трафик, порождаемый вредоносными программами и встроенными в них сканерами уязвимостей. А значит, у разработчиков вирусов будет больше возможностей для монетизации своих мобильных разработок: от слежки за конкретным человеком до воровства одноразовых паролей в системах дистанционного банковского обслуживания.

Третья угроза – атаки на дополнительные сервисы. Собственно, LTE разрабатывалось не только для обеспечения доступа к Интернету мобильных пользователей, а скорее как платформа для внедрения новых услуг: видео, игровых и многих других. Эти сервисы также могут быть уязвимы для самых разнообразных атак – как из Интернета, так и из мобильной сети. Вполне возможно, что, атаковав один из сервисов, злоумышленники смогут внедрить в клиентские устройства опасные программы.

Угроза пользователям LTE может исходить и от сервисов двойного назначения. Мобильные операторы имеют так много ценной информации об абонентах, что рано или поздно захотят ее монетизировать. Типичным примером являются LBS-сервисы. С одной стороны, их можно использовать, например, для контроля за перемещением грузов, для определения местонахождения детей и для оповещения о чрезвычайных ситуациях, но с другой – их же можно использовать для незаконной слежки. С распространением интеллектуальных устройств число потенциально опасных сервисов будет только возрастать. Взлом такого сервиса позволит злоумышленникам получить доступ к ценной информации провайдера и построить новые схемы преступлений и незаконного получения денег.

Мы привели далеко не полный список новых угроз, связанных с появлением LTE. Есть также проблемы и с самим стандартом. Вот что говорит видный российский эксперт по ИБ Алексей Лукацкий: «Очень остро стоит задача взаимодействия с *недоверенными* (не LTE) сетями. Если трафик между пользовательским оборудованием и eNB шифруется (это требование стандарта) и угроза нарушения конфиденциальности становится неактуальной, то, например, взаимодействие eNB с радиоконтроллером сети 3G по умолчанию никак не защищено, а следовательно, это брешь для возможных атак со стороны злоумышленников. Как и отсутствие обязательной аутентификации между ядром сети и eNB, эту опцию оператор

связи может как использовать, так и не задействовать в принципе, чтобы снизить свои издержки по развертыванию сети LTE».

Защита LTE

Разработчики мобильной технологии LTE все же позаботились о ее защите несколько больше, чем разработчики Интернета. Поэтому можно надеяться, что мобильная сеть будет более надежна и безопасна, чем Всемирная паутина. В LTE используется почти такая же модель безопасности, как и в ранних версиях мобильной связи. Хотя архитектура сети несколько изменилась, общие принципы защиты остались прежними. Если в предыдущих версиях мобильной сети за безопасность отвечал RNC, то теперь его нет, а защита возложена на базовые станции, которые стали более интеллектуальными. По сообщениям экспертов МТС (МТС – *Мобильные телесистемы* – оператор сотовой связи России), все функции защиты в LTE объединены стандартом и подразумевают защиту на нескольких уровнях. Предусмотрена защита на уровне доступа к сети, на уровнях сетевого и пользовательского доменов, на уровне приложений и уровне отображения и конфигураций.

Каждый из этих уровней предполагает аутентификацию и авторизацию всех устройств, чего нет в Интернете. Хотя каждое устройство в IP-сети имеет свой адрес, а часто еще и уникальный идентификатор MAC, его достаточно легко изменить и подделать. Однако технология LTE предусматривает использование не только IP-адреса, но и системы распространения ключей шифрования для всех устройств, подключенных к сети. В результате для всех взаимодействий в мобильной сети есть возможность безопасного обмена ключевой информацией и установления шифрованного канала связи между ними.

В LTE сохраняются и методы аутентификации пользователей по привязке к карте USIM, как в традиционной мобильной связи: пользователь может заблокировать доступ к телефону по PIN-коду. Василий Сахаров, руководитель отдела информационной безопасности компании «Демос», отмечает, что в LTE от GSM и UMTS наследуются схемы протокола аутентификаиции EAP, в которые добавлены новые алгоритмы, более длинные ключи и расширенная иерархия PKI. Предусмотрены и новые функциональные возможности для новых сценариев, включающих межмашинное взаимодействие (M2M) и однократную аутентификацию (SSO). Кроме того, предусмотрена защита от несанкционированных соединений поверх мультимедийной IP-сети IMS. Вполне возможно, что используемая в мобильной связи более жесткая система аутентификации позволит навести порядок и в Интернете.

Угрозы и уязвимости Wi-Fi – сетей

Стандарт/технология Wi-Fi для для широкополосных беспроводных сетей связи разработан на основе телекоммуникационного стандарта IEEE 802.11 (англ. *Institute of Electrical and Electronics Engineers*) [5]. Изначально

технология Wi-Fi была ориентирована на организацию точек быстрого доступа в Интернет (hotspot) для мобильных пользователей. Преимущества беспроводного доступа очевидны, а технология Wi-Fi изначально стала стандартом, которого придерживаются производители мобильных устройств. Постепенно сети Wi-Fi стали использовать малые и крупные офисы для организации внутренних сетей и подсетей, а операторы создавать собственную инфраструктуру предоставления беспроводного доступа в Интернет на основе технологии Wi-Fi. Таким образом, в настоящее время сети Wi-Fi распространены повсеместно и зачастую имеют зоны покрытия целых районов города.

С точки зрения безопасности, следует учитывать не только угрозы, свойственные проводным сетям, но также и среду передачи сигнала. В беспроводных сетях получить доступ к передаваемой информации намного проще, чем в проводных сетях, равно как и повлиять на канал передачи данных. Достаточно поместить соответствующее устройство в зоне действия сети [6]. Обобщённая картина угроз и уязвимостей представлена на рис. 2.

Существует два основных варианта устройства беспроводной сети:

- Ad-hoc – передача напрямую между устройствами;
- Hot-spot – передача осуществляется через точку доступа.

В Hot-spot сетях присутствует точка доступа (англ. Access point), посредством которой происходит не только взаимодействие внутри сети, но и доступ к внешним сетям. Hot-spot представляет наибольший интерес с точки зрения защиты информации, т.к., взломав точку доступа, злоумышленник может получить информацию не только со станций, размещенных в данной беспроводной сети.

Угрозы информационной безопасности, возникающие при использовании Wi-Fi сетей, можно условно разделить на два класса:

– *прямые* – угрозы информационной безопасности, возникающие при передаче информации по беспроводному интерфейсу IEEE 802.11;

– *косвенные* – угрозы, связанные с наличием на объекте и рядом с объектом большого количества Wi-Fi-сетей.

Прямые угрозы.

Радиоканал передачи данных, используемый в Wi-Fi потенциально подвержен вмешательству с целью нарушения конфиденциальности, целостности и доступности информации. В Wi-Fi предусмотрены как аутентификация, так и шифрование, но эти элементы защиты имеют свои уязвимости.

Шифрование значительно снижает скорость передачи данных, и, зачастую, оно осознанно отключается администратором для оптимизации трафика. Первоначальный стандарт шифрования WEP (Wired Equivalent Privacy) был дискредитирован за счёт уязвимостей в алгоритме распределения ключей RC4. Это несколько притормозило развитие Wi-Fi рынка и вызвало создание институтом IEEE рабочей группы 802.11i для разработки нового стандарта, учитывающего уязвимости WEP, обеспечивающего 128-битное AES шифрование и аутентификацию для защиты данных. Wi-Fi Alliance в 2003

представил свой собственный промежуточный вариант этого стандарта - WPA (Wi-Fi Protected Access). WPA использует протокол целостности временных ключей TKIP (Temporal Key Integrity Protocol). Также в нём используется метод контрольной суммы MIC (Message Integrity Code), которая позволяет проверять целостность пакетов . В 2004 Wi-Fi Alliance выпустили стандарт WPA2, который представляет собой улучшенный WPA. Основное различие между WPA и WPA2 заключается в технологии шифрования: TKIP и AES.

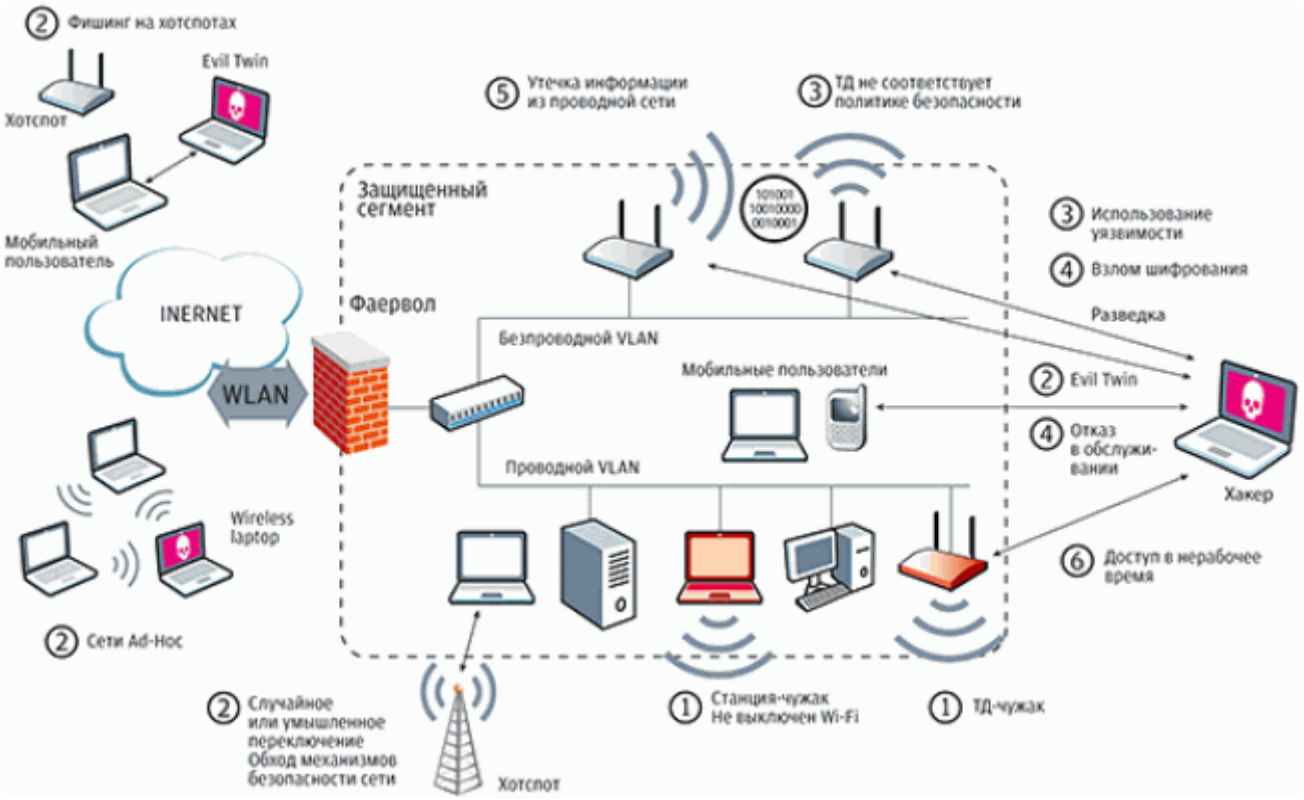

Рис.2. Угрозы и уязвимости Wi-Fi – сетей

WPA2 обеспечивает более высокий уровень защиты сети, так как TKIP позволяет создавать ключи длиной до 128 бит, а AES – до 256 бит.

При разработке самой технологии угроза блокирования информации в канале Wi-Fi практически оставлена без внимания. Само по себе блокирование канала не является опасным, так как обычно Wi-Fi сети являются вспомогательными, однако блокирование может представлять собой лишь подготовительный этап для атаки типа Man-in-the-Middle – "человек посередине", когда между клиентом и точкой доступа появляется третье устройство, которое перенаправляет трафик между ними через себя. Такое вмешательство позволяет удалять, искажать или навязывать ложную информацию.

Чужаки.

Чужаками (Rogue Devices, Rogues) называются устройства, предоставляющие возможность неавторизованного доступа к корпоративной сети, обычно в обход механизмов защиты, определенных политикой безопасности. Запрет на использование устройств беспроводной связи не защитит от беспроводных атак, если в сети, умышленно или нет, появится чужак. В роли чужака может выступать всё, у чего есть проводной и беспроводной интерфейсы: точки доступа (включая программные), сканеры, проекторы, ноутбуки с обоими включёнными интерфейсами и т.д.

Нефиксированная природа связи.

Беспроводные устройства могут менять точки подключения к сети прямо в процессе работы. Например, могут происходить «случайные ассоциации», когда ноутбук с Windows XP (доверительно относящейся ко всем беспроводным сетям) или просто некорректно сконфигурированный беспроводной клиент автоматически ассоциируется и подключает пользователя к ближайшей беспроводной сети. Таким образом, нарушитель переключает на себя пользователя для последующего сканирования уязвимостей, фишинга или атак "человек посередине". А если пользователь при этом подключен и к проводной сети, то он становится точкой входа - чужаком. К тому же многие пользователи, подключённые к внутренней сети и имеющие Wi-Fi – интерфейс, недовольные качеством и политикой работы сети, переключаются на ближайшую доступную точку доступа (или операционная система делает это автоматически при отказе проводной сети). При этом вся защита сети терпит крах.

Сети Ad-Hoc.

С помощью этих сетей удобно передавать файлы коллегам или печатать на принтере с Wi-Fi. Но такая организация сетей не поддерживает многие методы обеспечения безопасности, что делает их лёгкой добычей для нарушителя. Новые технологии Virtual Wi-Fi и Wi-Fi Direct только ухудшили ситуацию.

Уязвимости сетей и устройств

Некорректно сконфигурированные устройства, устройства со слабыми и недостаточно длинными ключами шифрования, использующие уязвимые методы аутентификации – именно такие устройства подвергаются атакам в первую очередь. Согласно отчётам аналитиков, большая часть успешных взломов происходит как раз из-за неправильных настроек точек доступа и программного обеспечения клиента. Достаточно подключить неправильно настроенную точку доступа к сети для взлома последней. Настройки "по умолчанию" не включают шифрование и аутентификацию, или используют ключи, прописанные в руководстве и поэтому всем известные. Маловероятно, что пользователи достаточно серьёзно озаботятся безопасной конфигурацией устройств. Именно такие привнесённые точки доступа и создают основные угрозы защищённым сетям. Некорректно настроенные устройства пользователей – угроза опаснее, чем некорректно сконфигурированные точки доступа. Это устройства пользователей и они не

конфигурируются специально в целях безопасности внутренней сети предприятия. К тому же они находятся за периметром контролируемой зоны, так и внутри него, позволяя злоумышленнику проводить всевозможные атаки, как то распространять вредоносное программное обеспечение или просто обеспечивая удобную точку входа.

Взлом шифрования.

О защищённости WEP и речи уже нет. Интернет полон специального и удобного в использовании ПО для взлома этого стандарта, которое собирает статистику трафика до тех пор, пока её не станет достаточно для восстановления ключа шифрования. Стандарты WPA и WPA2 также имеют ряд уязвимостей разной степени опасности, позволяющих их взлом. Пока что нет информации об успешных атаках на WPA2-Enterprise (802.1x).

Имперсонация и Identity Theft.

Имперсонация авторизованного пользователя – серьезная угроза любой сети, не только беспроводной. Однако в беспроводной сети определить подлинность пользователя сложнее. Конечно, существуют SSID и можно пытаться фильтровать по MAC-адресам, но и то, и другое передается в эфире в открытом виде, и их несложно подделать, а подделав – как минимум снизить пропускную способность сети, вставляя неправильные кадры, а разобравшись в алгоритмах шифрования – устраивать атаки на структуру сети (например, ARP-spoofing). Имперсонация пользователя возможна не только в случае MAC-аутентификации или использования статических ключей. Схемы на основе 802.1x не являются абсолютно безопасными. Некоторые механизмы (LEAP) имеют сложность взлома схожую со взломом WEP. Другие механизмы, EAP-FAST или PEAP-MSCHAPv2 хотя и надёжнее, но не гарантируют устойчивость к комплексной атаке.

Отказы в обслуживании.

DoS и DDoS-атаки – это атаки направленные на нарушение качества функционирования сети или на абсолютное прекращение доступа пользователей. В случае Wi-Fi сети отследить источник, заваливающий сеть "мусорными" пакетами, крайне сложно – его местоположение ограничивается лишь зоной покрытия. К тому же есть аппаратный вариант этой атаки – установка достаточно сильного источника помех в нужном частотном диапазоне.

Косвенные угрозы.

Сигналы Wi-Fi – устройств имеют достаточно сложную структуру и широкий спектр, поэтому эти сигналы, а тем более, окружающие устройства Wi-Fi невозможно идентифицировать обычными средствами радиомониторинга. Уверенное обнаружение сигнала Wi-Fi современными комплексами радиомониторинга в широкой полосе частот возможно только по энергетическому признаку при наличии полос параллельного анализа шириной несколько десятков МГц на скорости не менее 400 МГц/с и лишь в ближней зоне. Сигналы точек доступа, находящихся в дальней зоне, оказываются ниже уровня шумов приёмника. Обнаружение Wi-Fi –

передатчиков при последовательном сканировании узкополосными приёмниками вообще невозможно.

Исходя из того, что практически каждый объект окружает множество "чужих" Wi-Fi сетей, отличить легальных клиентов своей сети и соседних сетей от нарушителей крайне сложно, что позволяет успешно маскировать несанкционированную передачу информации среди легальных Wi-Fi – каналов. Wi-Fi – передатчик излучает так называемый «OFDM сигнал». Это означает, что в один момент времени устройство передаёт в одном сигнале, занимающем широкую полосу частот (около 20 МГц) несколько несущих информацию – поднесущих информационных каналов, которые расположены так близко друг от друга, что при приёме их на обычном приёмном устройстве, сигнал выглядит как единый «купол». Выделить в таком «куполе» поднесущие и идентифицировать передающие устройства можно только специальным приёмником.

В крупных городах Wi-Fi – сети общего пользования имеют достаточно обширную зону покрытия, что отпадает в необходимости использовать точку доступа мобильных телесистем сотовой связи рядом с объектом информационных отношений, при этом несанкционированное устройство доступа может подключиться к доступной Wi-Fi – сети.

Пропускная способность Wi-Fi сетей позволяет передавать звук и видео в реальном времени. Это упрощает злоумышленнику использовать акустические и оптические каналы утечки информации – достаточно легально купить Wi-Fi – видеокамеру и установить её в качестве устройства негласного получения информации.

Примеры:

- С Wi-Fi видеокамеры с микрофоном информация передаётся на точку доступа, работающую в режиме ретранслятора. Точка расположена на крыше и имеет направленную антенну – таким образом можно значительно увеличить дальность сигнала – до нескольких километров. Сам сигнал принимается на контрольном пункте.
- Смартфон сотрудника с помощью вируса записывает окружающий звук и передаёт его злоумышленнику с помощью Wi-Fi. В качестве контрольного пункта используется точка доступа со скрытым именем, чтобы обнаружить её было труднее.
- Если на объекте ограничен вынос носителей информации и выход в Интернет ограничен, то одним из вариантов скрытой передачи большого объёма информации является Wi-Fi. Нужно подключиться к соседним Wi-Fi сетям, оставаясь незамеченным среди легальных пользователей.

Утечки информации из проводной сети.

Как правило, беспроводные сети соединяются с проводными. Значит через точку доступа можно атаковать проводную сеть. А если наличествуют ошибки в настройке как проводной, так и беспроводной сети, то открывается целый плацдарм для атак.

Пример – точки доступа, работающие в режиме моста (Layer 2 Bridge), подключённые в сеть без маршрутизаторов или в сеть с нарушением сегментации и передающие в радиоэфир широковещательные пакеты из проводной части сети (ARP-запросы, DHCP, кадры STP и д.р.). Эти данные в целом полезны для разведки, и на их основе можно проводить такие атаки, как "человек посередине", атаки отказа в обслуживании, отравление кеша DNS и др.

Другой пример – при наличии нескольких ESSID (Extended Service Set Identifier) на одной точке доступа. Если на такой точке настроена как защищённая сеть, так и публичная, при неправильной конфигурации широковещательные пакеты будут отправляться в обе сети. Это позволит злоумышленнику, например, нарушить работу DHCP или ARP в защищённом сегменте сети. Это можно запретить, организовав привязку ESS к BSS, что поддерживается практически всеми производителями оборудования класса Enterprise (и мало кем из класса Consumer).

Особенности функционирования беспроводных сетей.

У беспроводных сетей наличествуют некоторые особенности, отсутствующие в проводных сетях. Эти особенности в целом влияют на производительность, безопасность, доступность и стоимость эксплуатации беспроводной сети. Их приходится учитывать, хотя они и не относятся напрямую к шифрованию или аутентификации. Для решения этих вопросов требуется специальный инструментарий и механизмы администрирования и мониторинга.

Активность в нерабочее время.

Исходя из того, что политикой безопасности логично ограничить доступ к сети вне рабочего времени (вплоть до физического отключения), беспроводная активность сети в нерабочее время должна отслеживаться, считаться подозрительной и подлежать расследованию.

Скорости.

Скорость подключения зависит от соотношения сигнал/шум (SNR). Если, скажем, 54 Мбит/с требует SNR в 25 dB, а 2 Мбит/с требует 6 dB, то кадры, отправленные на скорости 2 Мбит/с «пролетят» дальше, т.е. их можно декодировать с большего расстояния, чем более скоростные кадры. Также все служебные кадры , а также бродкасты, отправляются на самой нижней скорости. Это означает, что сеть будет видно на значительном расстоянии. Если в сети, где все работают на определённой скорости (офис территориально ограничен и скорости подключения у пользователей примерно одинаковые) появляется подключение на 1-2 Мбит/с - скорее всего это нарушитель. Также можно отключить низкие скорости, тем самым повысив скорость передачи информации в сети.

Интерференция.

Качество работы Wi-Fi сети как радиоэфира зависит от многих факторов. Один из них - интерференция радиосигналов, которая может значительно снизить пропускную способность сети и количество пользователей, вплоть до полной невозможности использования сети. В качестве источника может

выступать любое устройство, излучающее на той же частоте сигнал достаточной мощности. Это могут быть как соседние точки доступа, так и микроволновки. Эту особенность могут также использовать злоумышленники в качестве атаки отказа в обслуживании, или для подготовки атаки "человек посередине", заглушая легитимные точки доступа и оставляя свою с таким же SSID.

Связь.

Существуют и другие особенности беспроводных сетей помимо интерференции. Неправильно настроенный клиент или сбоящая антенна могут ухудшить качество обслуживания всех остальных пользователей. Или вопрос стабильности связи. Не только сигнал точки доступа должен достичь клиента, но и сигнал клиента должен достичь точки. Обычно точки мощнее, и чтобы добиться симметрии, возможно придётся снизить мощность сигнала. Для 5 ГГц следует помнить, что надежно работают только 4 канала: 36/40/44/48 (для Европы, для США есть еще 5). На остальных включен режим сосуществования с радарами (DFS). В итоге, связь может периодически пропадать.

Методы ограничения доступа.

Фильтрация MAC-адресов:

Данный метод не входит в стандарт IEEE 802.11. Фильтрацию можно осуществлять тремя способами:

Точка доступа позволяет получить доступ станциям с любым MAC-адресом;

Точка доступа позволяет получить доступ только станциям, чьи MAC-адреса находятся в доверительном списке;

Точка доступа запрещает доступ станциям, чьи MAC-адреса находятся в “чёрном списке”;

Наиболее надежным с точки зрения безопасности является второй вариант, хотя он не рассчитан на подмену MAC-адреса, что легко осуществить злоумышленнику.

Режим скрытого идентификатора SSID (англ. Service Set IDentifier):

Для своего обнаружения точка доступа периодически рассылает кадры-маячки (англ. beacon frames). Каждый такой кадр содержит служебную информацию для подключения и, в частности, присутствует SSID (идентификатор беспроводной сети). В случае скрытого SSID это поле пустое, т.е. невозможно обнаружение вашей беспроводной сети и нельзя к ней подключиться, не зная значение SSID . Но все станции в сети, подключенные к точке доступа, знают SSID и при подключении, когда рассылают Probe Request запросы, указывают идентификаторы сетей, имеющиеся в их профилях подключений. Прослушивая рабочий трафик, с легкостью можно получить значение SSID, необходимое для подключения к желаемой точке доступа.

Методы аутентификации.

Аутентификация - выдача определённых прав доступа абоненту на основе имеющегося у него идентификатора.

1. Открытая аутентификация (англ. Open Authentication):

Рабочая станция делает запрос аутентификации, в котором присутствует только MAC-адрес клиента. Точка доступа отвечает либо отказом, либо подтверждением аутентификации. Решение принимается на основе MAC-фильтрации, т.е. по сути это защита беспроводной Wi-Fi сети на основе ограничения доступа, что не безопасно.
Используемые шифры: без шифрования, статический WEP, CKIP.
2. Аутентификация с общим ключом (англ. Shared Key Authentication):
Необходимо настроить статический ключ шифрования алгоритма WEP (англ. Wired Equivalent Privacy). Клиент делает запрос у точки доступа на аутентификацию, на что получает подтверждение, которое содержит 128 байт случайной информации. Станция шифрует полученные данные алгоритмом WEP (проводится побитовое сложение по модулю 2 данных сообщения с последовательностью ключа) и отправляет зашифрованный текст вместе с запросом на ассоциацию. Точка доступа расшифровывает текст и сравнивает с исходными данными. В случае совпадения отсылается подтверждение ассоциации, и клиент считается подключенным к сети.
Схема аутентификации с общим ключом уязвима к атакам «Man- in- the-middle». Алгоритм шифрования WEP – это простой XOR ключевой последовательности с полезной информацией, следовательно, прослушав трафик между станцией и точкой доступа, можно восстановить часть ключа.
Используемые шифры: без шифрования, динамический WEP, CKIP.
3. Аутентификация по MAC-адресу:
Данный метод не предусмотрен в IEEE 802.11, но поддерживается большинством производителей оборудования, например D-Link и Cisco. Происходит сравнение MAC-адреса клиента с таблицей разрешённых MAC-адресов, хранящейся на точке доступа, либо используется внешний сервер аутентификации. Используется как дополнительная мера защиты.

IEEE начал разработки нового стандарта IEEE 802.11i, но из-за трудностей утверждения, организация WECA (англ. Wi-Fi Alliance) совместно с IEEE анонсировали стандарт WPA (англ. Wi-Fi Protected Access). В WPA используется TKIP (англ. Temporal Key Integrity Protocol, протокол проверки целостности ключа), который использует усовершенствованный способ управления ключами и покадровое изменение ключа.
4. Wi-Fi Protected Access (WPA).

После первых успешных атак на WEP было принято разработать новый стандарт 801.11i. Но до него был выпущен “промежуточный” стандарт WPA, который включал в себя новую систему аутентификации на базе 801.1x и новый метод шифрования TKIP. Существуют два варианта аутентификации: с помощью RADIUS сервера (WPA-Enterprise) и с помощью предустановленного ключа (WPA-PSK). Используемые шифры: TKIP (стандарт), AES-CCMP (расширение), WEP (в качестве обратной совместимости).
5. WI-FI Protected Access2 (WPA2, 801.11I).

WPA2 или стандарт 801.11i – это финальный вариант стандарта безопасности беспроводных сетей. В качестве основного шифра был выбран

стойкий блочный шифр AES. Система аутентификации по сравнению с WPA претерпела минимальные изменения. Также как и в WPA, в WPA2 есть два варианта аутентификации WPA2-Enterprise с аутентификацией на RADIUS сервере и WPA2-PSK с предустановленным ключом. Используемые шифры: AES-CCMP (стандарт), TKIP (в качестве обратной совместимости).

6. Cisco Centralized Key Managment (CCKM).

Вариант аутентификации от фирмы CISCO. Поддерживает роуминг между точками доступа. Клиент один раз проходит аутентификацию на RADIUS-сервере, после чего может переключаться между точками доступа. Используемые шифры: WEP, CKIP, TKIP, AES-CCMP.

Методы шифрования.

WEP-шифрование (Wired Equivalent Privacy).

Аналог шифрования трафика в проводных сетях. Используется симметричный потоковый шифр RC4 (англ. Rivest Cipher 4), который достаточно быстро функционирует. На сегодняшний день WEP и RC4 не считаются криптостойкими. Есть два основных протокола WEP:

40-битный WEP (длина ключа 64 бита, 24 из которых – это вектор инициализации, который передается открытым текстом);

104-битный WEP (длина ключа 128 бит, 24 из которых – это тоже вектор инициализации); Вектор инициализации используется алгоритмом RC4. Увеличение длины ключа не приводит к увеличению надежности алгоритма.

Основные недостатки:

– использование для шифрования непосредственно пароля, введенного пользователем;

– недостаточная длина ключа шифрования;

– использование функции CRC32 для контроля целостности пакетов;

– повторное использование векторов инициализации и др.

TKIP-шифрование (англ. Temporal Key Integrity Protocol)

Используется тот же симметричный потоковый шифр RC4, но является более криптостойким. Вектор инициализации составляет 48 бит. Учтены основные атаки на WEP. Используется протокол Message Integrity Check для проверки целостности сообщений, который блокирует станцию на 60 секунд, если были посланы в течение 60 секунд два сообщения не прошедших проверку целостности. С учетом всех доработок и усовершенствований TKIP все равно не считается криптостойким.

CKIP-шифрование (англ. Cisco Key Integrity Protocol).

Имеет сходства с протоколом TKIP. Создан компанией Cisco. Используется протокол CMIC (англ. Cisco Message Integrity Check) для проверки целостности сообщений.

WPA-шифрование.

Вместо уязвимого RC4, используется криптостойкий алгоритм шифрования AES (англ. Advanced Encryption Standard). Возможно использование EAP (англ. Extensible Authentication Protocol, расширяемый протокол аутентификации). Есть два режима:

Pre-Shared Key (WPA-PSK) – каждый узел вводит пароль для доступа к сети;

Enterprise - проверка осуществляется серверами RADIUS;

WPA2-шифрование (IEEE 802.11i).

Принят в 2004 году, с 2006 года WPA2 должно поддерживать все выпускаемое Wi-Fi оборудование. В данном протоколе применяется RSN (англ. Robust Security Network, сеть с повышенной безопасностью). Изначально в WPA2 используется протокол CCMP (англ. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, протокол блочного шифрования с кодом аутентичности сообщения и режимом сцепления блоков и счетчика). Основой является алгоритм AES. Для совместимости со старым оборудованием имеется поддержка TKIP и EAP (англ. Extensible Authentication Protocol) с некоторыми его дополнениями. Как и в WPA есть два режима работы: Pre-Shared Key и Enterprise.

WPA и WPA2 имеют следующие преимущества:

– Ключи шифрования генерируются во время соединения, а не распределяются статически;

– Для контроля целостности передаваемых сообщений используется алгоритм Michael;

– Используется вектор инициализации существенно большей длины.

Атаки на Wi-Fi сети.

Разведка.

Большинство атак начинаются с разведки, в ходе которой производится сканирование сети (NetStumbler, Wellenreiter), сбор и анализ пакетов - многие служебные пакеты в сети Wi-Fi передаются в открытом виде. При этом крайне проблематично выяснить, кто легальный пользователь, пытающийся подключиться к сети, а кто собирает информацию. После разведки принимаются решения о дальнейших шагах атаки.

Защита сети с помощью отключения ответа на широковещательный запрос ESSID и скрытия название сети в служебных пакетах Beacon frame является недостаточной, так как сеть всё равно видна на определённом радиоканале и атакующий просто ждёт авторизованного подключения к сети, так как при этом в незашифрованном виде передаётся ESSID. На этом защитная мера теряет смысл. Хуже того, некоторые системы (например WinXp Sp2) непрерывно рассылают имея сети в эфир, пытаясь подключиться. Это также является интересной атакой, так как в таком случае можно пересадить пользователя на свою точку доступа и получать всю информацию, что он передаёт по сети.

Можно уменьшить подверженность разведке, разместив точку доступа так, чтобы она обеспечивала необходимое покрытие, и это покрытие минимально выходило за контролируемую территорию. Нужно регулировать мощность точки доступа и использовать специальные инструменты для контроля распространения сигнала. Также можно полностью экранировать помещение с точкой доступа для полной невидимости сети извне.

Hardware

В случае анализа небольшой территории подойдёт встроенный Wi-Fi адаптер ноутбука, но на большее не хватит. Нужен более мощный адаптер с

разъёмом для внешней антенны. Многие используют такие, как Alfa networks AWUS036H, Ubiquiti SRC, Linksys WUSB54GC.

Антенна.

Существуют антенны направленные и всенаправленные. Первые имеют большую дальность при таком же коэффициенте усиления, но меньший угол работы и больше подходят для изучения ограниченной территории. Вторые имеют худшие характеристики, но больше подходят для сбора информации с обширной территории. Для целей сбора информации подойдут антенны с коэффициентом усиления 7-9 dbi.

Навигационные спутниковые системы GPS.

При сборе информации будет нелишним наносить на карту координаты найденных и изучаемых точках доступа. Для этого потребуется GPS, неважно, подключаемые ли к компьютеру внешние GPS-приёмники или смартфон с встроенным GPS. Важно лишь чтобы такой девайс мог передавать данные по протоколу nmea или garmin.

Программное обеспечение.

В Linux–подобных системах настроить работу адаптера на приём всех пакетов, а не только тех, которые предназначены именно ему проще, чем на Windows. В некоторых драйверах такой режим поддерживается изначально, другие нужно изменять. Наиболее распространённые программы для сбора информации – это Kismet и Aircrack-ng suite.

Kismet может не только перехватывать пакеты и обнаруживать скрытые сети, это также и инструмент для мониторинга и отладки сети, причём не только Wi-Fi, программа может работать с телефонными и Bluetooth сетями.

Aircrack-NG представляет собой набор инструментов для аудита беспроводных сетей. А ещё эта программа реализует стандартную атаку FMS наряду с некоторыми оптимизациями KoreK'a, также новую PTW-атаку, которая ещё сильнее уменьшает время на взлом WEP.

Другие программы: Dwepcrack (улучшенная FMS атака), AirSnot (FMS), WepLab (улучшенная FMS атака, атака Koreka).

Атаки на сети с WEP-шифрованием.

Объясняются уязвимостью RC4, в любой из такого рода атак, при этом необходимо получить какое-то количество пакетов из сети:

1. FMS-атака (Fluhrer, Martin, Shamir) – самая первая атака на сети с WEP-шифрованием, появилась в 2001 году. Основана на анализе передаваемых векторов инициализации и требует, чтобы пакеты содержали «слабые» инициализационные вектора (Weak IV). Для проведения атаки нужно как минимум полмиллиона пакетов. После обновления протокола эта атака неуспешна.

2. Атака KOREK’A (ник хакера, придумавшего атаку). Количество требуемых уникальных Weak IV – несколько сотен тысяч, для ключа длиной 128 бит. Главное требование – чтобы Weak IV не совпадали между собой. Абсолютно не важно наличие слабых Weak IV. Атака была предложена в 2004 году.

3. PTW-атака (Pyshkin, Tews, Weinmann). В основе лежит прослушивание большого количества ARP-пакетов (англ. Address Resolution Protocol). Достаточно 10000–100000 пакетов. Самая эффективная атака на сеть с WEP-шифрованием. Данную атаку можно вычислить по большому количеству ARP-пакетов, которые генерируются в сеть. Единственный минус – почти всегда требуется проводить активную атаку на беспроводную сеть, так как ARP-запросы при нормальном функционировании сети никогда не сыпятся как из «рога изобилия».

Атаки на протокол WEP условно можно разделить на активные и пассивные.

Пассивные сетевые атаки.

В 2001 году криптоаналитики Флурер (Fluhrer), Мантин (Mantin) и Шамир (Shamir) показали, что можно вычислить секретный ключ на основе определённых кадров, собранных в сети. Причина – уязвимость метода планирования ключей (Key Scheduling Algorithm – KSA) алгоритма шифрования RC4. Слабые векторы инициализации позволяют с помощью статистического анализа восстановить секретный ключ. Требуется собрать около 4 миллионов кадров, это около 4 часов работы сети. Взломаны как 40-битные, так и 104-битные ключи, причём защищённость ключа не возросла.

Активные сетевые атаки.

Нарушитель воздействует на сеть для получения определенной информации для индуктивного вычисления секретного ключа. В основе активной атаки WEP лежит то, что при потоковом шифровании происходит XOR первоначального сообщения и ключа для вычисления зашифрованного сообщения.

Индуктивное вычисление ключа эффективно в силу отсутствия хорошего метода контроля целостности сообщений. Значение идентификатора ключа (ICV), завершающего кадр WEP, вычисляется с помощью функции CRC32 (циклический избыточный 32-битный код), подверженной атакам с манипуляцией битами. В итоге существуют атаки, основанные на повторном использовании вектора инициализации (IV Replay) и манипуляции битами (Bit-Flipping).

Повторное использование вектора инициализации (Initialization Vector Replay Attacks).

Злоумышленник многократно посылает клиенту Wi-Fi сети по проводной сети сообщение известного содержания (IP-пакет, письмо по электронной почте и т. п.).

Злоумышленник пассивно прослушивает радиоканал связи абонента с точкой доступа и собирает кадры, вероятно содержащие шифрованное сообщение.

Злоумышленник вычисляет ключевую последовательность, применяя XOR к предполагаемому шифрованному и известному нешифрованному сообщениям.

Далее злоумышленник «выращивает» ключевую последовательность для пары вектора инициализации и секретного ключа, породившей ключевую последовательность, вычисленную на предыдущем шаге.

Пара вектора инициализации и секретного ключа, а, следовательно, и порождаемая ими ключевая последовательность может использоваться повторно.

После того, как ключевая последовательность вычислена для кадров некоторой длины, ее можно «вырастить» до любого размера:

Злоумышленник генерирует кадр на один байт длиннее, чем длина уже известной ключевой последовательности. Пакеты ICMP (Internet Control Message Protocol), посылаемые командой ping, отлично подходят для этого, так как точка доступа вынуждена на них отвечать.

Злоумышленник увеличивает длину ключевой последовательности на один байт. Значение дополнительного байта выбирается случайным образом из 256 возможных ASCII-символов. Если предполагаемое значение дополнительного байта ключевой последовательности верно, то будет получен ожидаемый ответ от точки доступа (ICMP в случае ping'а). Процесс повторяется до тех пор, пока не будет подобрана ключевая последовательность нужной длины.

Манипуляция битами (Bit-Flipping Attacks).

Преследуется та же цель, что и при использовании вектора инициализации. Идея в том, что многое служебные поля и их положение в кадре не меняются. Злоумышленник меняет биты пользовательских данных в кадре на канальном уровне (модель OSI), тем самым изменяя пакеты на сетевом уровне.

Злоумышленник пассивно собирает кадры Wi-Fi-сети анализаторами трафика.

Злоумышленник захватывает кадр и произвольно изменяет биты в поле данных протокола 3-го уровня.

Злоумышленник модифицирует значение вектора контроля целостности кадра ICV (описано ниже).

Злоумышленник передает модифицированный кадр в Wi-Fi-сеть.

Принимающая сторона (абонент либо точка доступа) вычисляет значение вектора контроля целостности кадра ICV для полученного модифицированного кадра.

Принимающая сторона сравнивает вычисленное значение вектора ICV с имеющимся в полученном модифицированном кадре.

Если значения ICV совпадают, кадр считается неискаженным и не отбрасывается.

Принимающая сторона деинкапсулирует содержимое кадра и обрабатывает заголовки сетевого уровня.

Поскольку манипуляция битами происходила на канальном уровне, контрольная сумма пакета сетевого уровня оказывается неверной.

Стек протокола сетевого уровня на принимающей стороне генерирует предсказуемое сообщение об ошибке.

Злоумышленник наблюдает за сетью в ожидании зашифрованного кадра с сообщением об ошибке.

Злоумышленник захватывает кадр, содержащий зашифрованное сообщение об ошибке, и вычисляет ключевую последовательность, как же как в случае атаки с повторным использованием вектора инициализации.

Манипуляция с ICV.

Процедура манипуляции с ICV, расположенного в зашифрованной части кадра, для обеспечения его корректности для модифицированного кадра.

Исходный кадр F1 имеет вектор C1. Создается кадр F2 такой же длины, что и F1, служащий маской для модификации битов кадра F1.

Создается кадр F3 путем выполнения двоичной функции XOR над кадрами F1 и F2.

Вычисляется промежуточный вектор C2 для кадра F3.

Вектор C3 для кадра F3 вычисляется путем выполнения двоичной функции XOR над C1 и C2.

Проблемы управления статическими WEP-ключами.

Ещё один недостаток — нельзя управлять ключами шифрования. В WEP поддерживаются только статические ключи, и их нужно заранее распространять между клиентами и точками доступа. Протокол 802.11 аутентифицирует не пользователя, а его устройство, и потеря последнего, или разглашение ключа приводит к тому, что нужно менять ключи у всех абонентов и на всех точках доступа в сети. Вручную. В небольшой локальной сети это ещё реально, но не более. Требуется тщательно следить за оборудованием сети и не допускать утечек ключей.

Атаки на сети с WPA/WPA2-шифрованием.

WPA обычно использует алгоритм шифрования TKIP. WPA2 в обязательном порядке использует алгоритм шифрования AES-CCMP, который более мощный и надежный по сравнению с TKIP. Считается, что взлом WPA2 практически неосуществим.

WPA и WPA2 позволяют использовать либо EAS-bases аутентификацию (RADIUS Server «Enterprise») или Pre-Shared Key (PSK) «Personal»-based аутентификацию. Были проведены атаки только на аутентификацию обеих методов шифрования, после чего методом грубой силы можно подобрать PSK-ключ. Скорость перебора можно увеличить, если заранее вычислить необходимые данные и составить таблицы для перебора. Однако, если для аутентификации используется технология WPS, использующая PIN-код, то атака сводится к перебору всех возможных кодов.

6 ноября 2008 года на конференции PacSec было показано, как взломать ключ TKIP, используемый в WPA, за 12-15 минут. Этот метод позволяет прочитать данные, передаваемые от точки доступа клиентской машине, а также передавать поддельную информацию на клиентскую машину. Ещё одним условием успешной атаки было включение QoS на маршрутизаторе.

В 2009 году сотрудниками Университета Хиросимы и Университета Кобе, Тосихиру Оигаси и Масакату Мории был разработан и успешно реализован на практике новый метод атаки, который позволяет взломать любое WPA

соединение без ограничений, причём, в лучшем случае, время взлома составляет 1 минуту.

WPA с включённым AES и WPA2 не подвержены этим атакам.

23 июля 2010 года была опубликована информация об уязвимости Hole196 в протоколе WPA2. Используя эту уязвимость, авторизовавшийся в сети злонамеренный пользователь может расшифровывать данные других пользователей, используя свой закрытый ключ. Никакого взлома ключей или метода грубой силы не требуется.

На сегодня основными методами взлома WPA2 PSK являются атака по словарю и метод грубой силы.

Атака по словарю на WPA/WPA2 PSK.

WPA/WPA2 PSK работает следующим образом: он вытекает из ключа предварительной сессии, которая называется Pairwise Transient Key (PTK). PTK, в свою очередь использует Pre-Shared Key и пять других параметров — SSID, Authenticator Nounce (ANounce), Supplicant Nounce (SNounce), Authenticator MAC-address (MAC-адрес точки доступа) и Suppliant MAC-address (MAC-адрес Wi-Fi–клиента). Этот ключ в дальнейшем использует шифрование между точкой доступа (AP) и Wi-Fi–клиентом.

Злоумышленник, который в этот момент времени прослушивает эфир, может перехватить все пять параметров. Единственной вещью, которой не владеет злодей это – Pre-Shared key. Pre-Shared key получается благодаря использованию парольной фразы WPA-PSK, которую отправляет пользователь, вместе с SSID. Комбинация этих двух параметров пересылается через Password Based Key Derivation Function (PBKDF2), которая выводит 256-bit'овый общий ключ. В обычной WPA/WPA2 PSK атаке по словарю, злоумышленник будет использовать ПО, которое выводит 256-битный Pre-Shared Key для каждой парольной фразы и будет использует ее с другими параметрами, которые были описаны в создании PTK. PTK будет использоваться для проверки Message Integrity Check (MIC) в одном из пакетов handshake. Если они совпадут, то парольная фраза в словаре будет верной. При этом используются уязвимости протокола аутентификации пользователей – открытая передача ANounce, SNounce, MAC-адреса точки доступа и MAC-адреса Wi-Fi – клиента. Если при воспроизведении алгоритма аутентификации произойдет «успешная авторизация пользователя», значит выбранный из словаря пароль является истинным и атака привела к успешному взлому сети.

Сообщения 4-х стороннего рукопожатия (4 кадра канального уровня) содержат в себе информационные поля следующего содержимого:

– MAC-адрес точки доступа;

– MAC-адрес клиента;

– Случайное 32-байтное число, генерируемое точкой доступа при установлении соединения (Anonce) – кадр I;

– Случайное 32-байтное число, генерируемое клиентом (Snonce) – кадр II;

– Размер текущего кадра аутентификации (без канального заголовка) – кадр II или III или IV;

– Содержимое кадра аутентификации (без канального заголовка) – обязательно тот же, кадр, что выбран в предыдущем пункте;
– Ключ целостности сообщения (MIC) – обязательно тот же, кадр, что выбран в предыдущем пункте;
– Версию протокола защиты данных (WPA или WPA2) – фрейм II или III или IV.

Примеры взлома Wi-Fi – сетей.

Статей о взломе Wi-Fi в Интернете достаточно много, но большинство из них касаются режима работы WEP/WPA(2) – Personal, в котором необходимо перехватить процедуру «рукопожатия» клиента и Wi-Fi-точки. Во многих корпоративных Wi-Fi-сетях используется режим безопасности WPA2-Enterprise, с аутентификацией по логину и паролю – как наименее затратный способ. При этом аутентификация осуществляется с помощью RADIUS-сервера. Один из сценариев такого взлома изображён на рис.3 [7].

ОС клиента устанавливает соединение с RADIUS-сервером, используя шифрование при помощи TLS, а проверка подлинности в основном происходит при помощи протокола MS-CHAPv2. Для тестирования на проникновение в такой сети можно создать поддельную Wi-Fi-точку с RADIUS-сервером – и получить логин, запрос и ответ, которые использует MS-CHAPv2. Этого достаточно для дальнейшего проникновения. Необходимы Kali Linux и карточка, поддерживающая работу в режиме Access Point, что можно проверить при помощи команды iw list, где нарушителя интересует строка: * *#{ AP, mesh point } <= 8*, Еще год назад нужно было проделать множество манипуляций для того, чтобы подделать такую точку доступа с возможностью получения учетных данных. Необходимо было обновить, собрать и правильно настроить определенные версии hostapd и FreeRADIUS.

В августе 2014 года появился набор инструментов Mana Toolkit, позволяющий автоматизировать множество векторов атак на беспроводные клиенты. Поскольку использовать ноутбук не всегда удобно, можно использовать более компактный вариант –телефон. Кроме того, можно использовать Raspberry Pi + FruityWifi. Wi-Fi Pineapple, к сожалению, не поддерживает Mana Toolkit.

Как оказалось, перехватить хеши пользователей можно не всегда. Настольные ОС (Windows, MacOS, Linux), а также пользователи iOS защищены лучше всего. При первичном подключении ОС спрашивает, доверяете ли вы сертификату, который используется RADIUS-сервером в данной Wi-Fi-сети. При подмене легитимной точки доступа ОС спросит про доверие к новому сертификату, который использует RADIUS-сервер. Это произойдет даже при использовании сертификата, выданного доверенным центром сертификации (Thawte, Verisign).

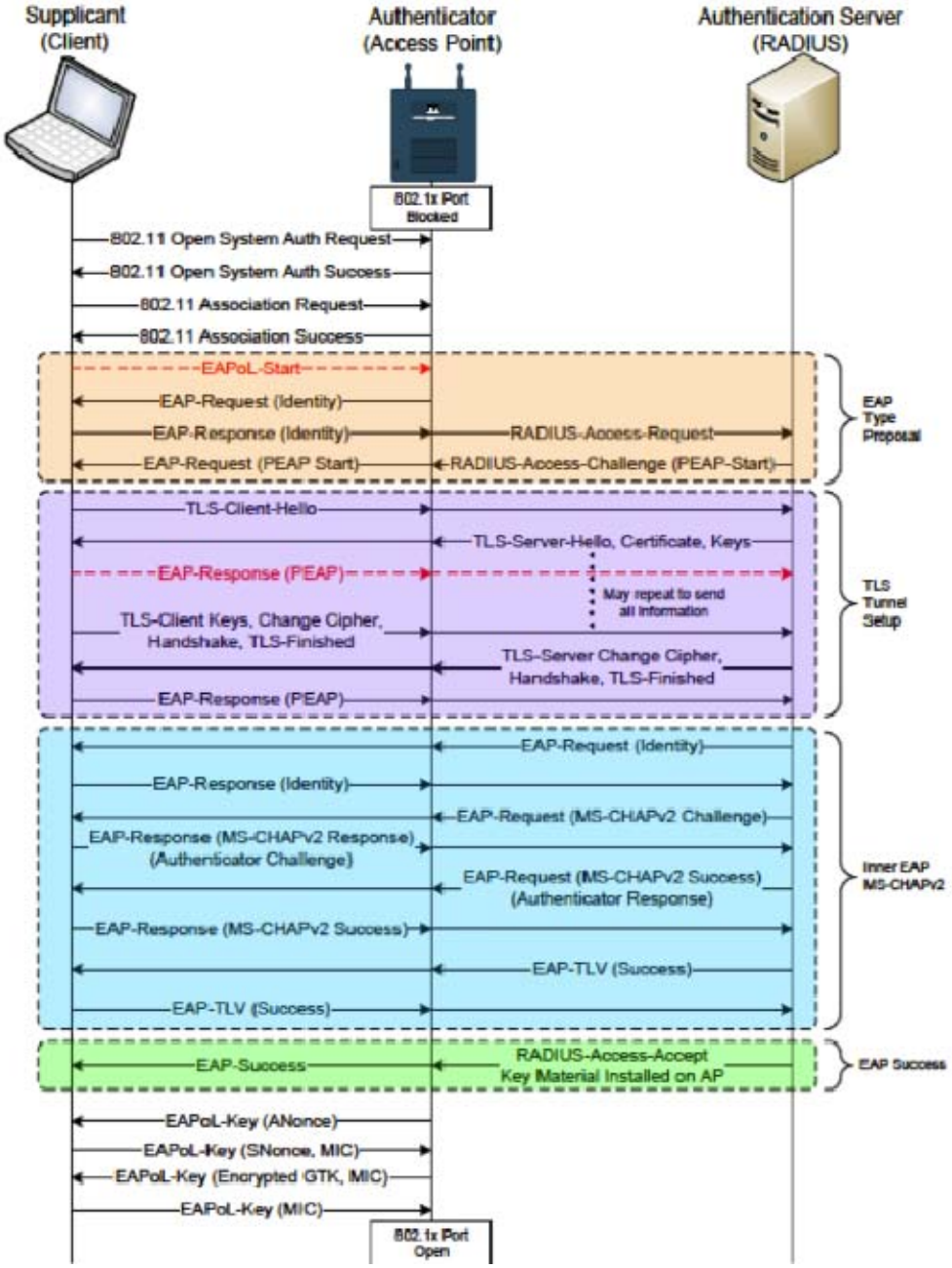

Рис.3. Сценарий взлома Wi-Fi-сети через систему аутентификации.

Угрозы и уязвимости мобильных приложений

В современном мире организации и физические лица все больше полагаются на мобильные программные приложения для поддержки своих критически важных деловых инициатив. Это означает, что защищенность мобильных приложений должна быть главным приоритетом стратегии безопасности бизнес – процессов организаций и частных лиц, использующих технологию мобильных транзакций, включая банковскую.

С ростом популярности разработки мобильных приложений, повышается их капиталоёмкость, а вместе с этим и желание злоумышленников перевести эти капиталы на свои счета. Многие современные мобильные программы

предполагают внутренние покупки, а также отправку SMS на платные номера, именно эти лазейки могут использовать хакеры. Одно дело, сколько стоит создание мобильного приложения, а другое – сколько будет стоить сделать его безопасным. Механизмов взлома и вытаскивания денег из мобильных устройств чрезвычайно много, каждый год появляются новые алгоритмы, но вместе с тем растёт и сила противодействия, способная своевременно бороться с угрозами. В наименьшей степени этим тенденциям подвержены закрытые системы, в частности IOS, поскольку архитектура её выполнена так, что в ней практически невозможно появление вирусов.

Помимо всего прочего, разработка приложений для iPhon – затея, в целом, не из дешёвых, куда проще прописать вредоносный код для других систем. Проще и уязвимее разработка приложений для Android, цены на неё, впрочем, также ниже. Особенно остро встаёт проблема эффективной защиты при работе с закрытой почтой или банковскими приложениями, где любое хищение данных может повлечь за собой колоссальные риски и финансовые потери. Разработчики усложняют процедуру авторизации в таких программах, вводя дополнительные проверки подлинности, однако, здесь важно не перейти ту хрупкую грань, когда процедура входа в аккаунт окажется слишком трудоёмкой и неудобной.

Исследования, проведенные IBM X-Force, наглядно демонстрируют значительный процент уязвимостей, относящийся к мобильным и WEB–приложениям [8]. Для эффективной защиты своих мобильных приложений организациям необходимо проводить широкомасштабное тестирование поддерживающего ПО и самих приложений. Тестирование и проверка на ранних этапах внедрения мобильной технологии помогут уменьшить затраты на обеспечение безопасности.

Решения в области обеспечения безопасности приложений должны быть направлены на решения следующих задач:

– Повышения эффективности управления программами обеспечения безопасности приложений;

– Анализа исходного кода, WEB – и мобильных приложений на наличие уязвимостей;

– Автоматизации результатов статического и динамического тестирования приложений;

–Управления тестированием приложений, отчетами и политиками с помощью одной консоли, в том числе тестированием методом "прозрачного ящика" (разновидность интерактивного тестирования безопасности приложений (IAST).

Классификация приложений для мобильных устройств.

Приложения для мобильных устройств можно классифицировать по множеству критериев, но в контексте безопасности приложений нас интересуют следующие: по месту расположения приложения и по типу используемой технологии передачи данных.

По месту расположения приложения:

- SIM-приложения – приложение на SIM-карте, написанное в соответствии со стандартом SIM Application Toolkit (STK);
- Web-приложения – специальная версия Web-сайта;
- мобильные приложения – приложения, разработанные для определенной мобильной ОС с использованием специализированного API, устанавливаемого в смартфон.

По типу используемой технологии взаимодействия с сервером:

- Сетевые приложения – используют собственный протокол общения поверх TCP/IP, например HTTP;
- SMS-приложения – приложения на основе SMS (Short Messaging Service);
- Приложение обменивается с сервером информацией с помощью коротких текстовых сообщений;
- USSD-приложения – приложения на основе USSD (Unstructured Supplementary Service Data). Сервис основывается на передаче коротких сообщений, схожих с SMS, но имеет ряд отличий;
- IVR-приложения – приложения, базирующиеся на технологии IVR (Interactive Voice Response). Система основана на заранее записанных голосовых сообщениях и тональном наборе.

Именно приложения, разработанные для определенной мобильной ОС с использованием специализированного API, устанавливаемые в смартфон или иной гаджет для взаимодействия с соответствующим сервисом, сейчас наиболее распространены, так как полностью используют возможности мобильного устройства и имеют наиболее дружественный пользовательский интерфейс.

Оценка уровня защищённости некоторых приложений.

Компания Viaforensics провела уникальное исследование в сфере оценки защищённости мобильных приложений, которое дало в итоге достаточно интересные данные. Исследователи этой компании отобрали случайным образом 30 популярных программ мобильных приложений и подвергли их серьёзной проверке на надёжность. В результате порядка четверти заявленных решений вскрыты путём взлома и были названы небезопасными. Специалисты смогли с помощью внешних воздействий вытащить из памяти устройств сохранённые Pin-коды и номера кредитных карт. Также в ряде случаев удалось обеспечить несанкционированный доступ к истории платежей. Безусловно, подобная ситуация выглядит довольно плачевной, по понятным причинам Viaforensics не сообщает, о каких именно приложениях идёт речь.

Эксперты аналитической компании Digital Security также отмечают существование множества способов прорыва через системы безопасности мобильных приложений [9]. Среди них манипуляции с каналами данных, возможности скрытого внедрения SQL-операторов, некорректные права доступа и многое другое. Сегодня разработка приложения для мобильных

телефонов делается под заказчика в сжатые сроки, поэтому исполнители не успевают уделять достаточное внимание вопросам безопасности.

Зная типовые подходы нарушителей к взлому, можно быть несколько более уверенным в защите своего устройства, поскольку на данный момент эти приёмы более или менее фиксированы, большинство схем ожидаемы. Если вы ищете, где заказать разработку IOS-приложений, в частности для финансовых операций, обращайте внимание лишь на проверенных программистов, готовых взяться за создание мощной системы безопасного доступа. Желательно, чтобы решение было изначально прописано так, чтобы типовые алгоритмы обмана на нём просто не работали. При работе приложения данные могут передаваться по каналам связи в открытом виде, хорошим антидотом в этом случае будет постоянное шифрование данных, что нередко используется в продвинутых программах. Также полноценная система безопасности должна всё время обновляться.

Приложения на каждой платформе имеют как свою специфику написания, так и свои специфичные угрозы, реализация которых может привести как к краже личных данных, в том числе банковских, так и к проникновению в корпоративную сеть.

Digital Security провела аудит безопасности клиентской части приложений на следующих мобильных платформах [9]:

- Google Android;
- Apple iOS (iPhone/iPad);
- Java (J2ME/Java ME);
- Windows Phone.

Типовые угрозы.

Были выявлены типовые угрозы для мобильных приложений включающие в себя:

– Секретные данные в открытом виде;
– Небезопасные каналы передачи информации;
– Наличие отладочного кода;
– Внедрение SQL-операторов;
– Межсайтовый скриптинг (XSS);
– Отсутствие проверок входящих данных;
– Неправильная расстановка прав доступа;
– Слабая криптография.

Методика аудита и содержание работ.

Методика аудита безопасности клиентской части мобильного приложения, разработанная исследовательским центром Digital Security, основана на опыте анализа защищенности различных по функциональности и сложности приложений, таких как ERP-системы, автоматизированные банковские системы, банк-клиенты, веб-приложения, системы управления базами данных и др. Подход к анализу основан на общепризнанных методах исследования приложений, описанных в таких документах, как PCI DSS Requirements and Security Assessment Procedures, OWASP Testing Guide, PA-

DSS Requirement and Security Assessment Procedures, и доработан с учетом практического исследовательского опыта DSecRG.

Этапы работы.

Процесс анализа приложения состоит из нескольких базовых этапов:

– Анализ архитектуры клиентской части приложения;

– Составление модели угроз;

– Аудит безопасности кода;

– Стресс-тестирование (fuzzing);

– Реализация угроз в соответствии с логикой приложения.

Экспертный анализ уязвимости мобильных банковских приложений.

Компания «Инфосистемы Джет» обнародовала аналитический отчет по уязвимостям мобильных банковских приложений, функционирующих под управлением iOS, Android и Windows Phone [10]. Результаты исследования показали, что 98% программ имеют уязвимости и 40% из них обладают уязвимостями критического характера.

Отчет основан на данных, полученных экспертами компании в ходе обследования 58 банковских приложений. Был проведен статический и динамический анализ исходного кода продуктов. Эксперты «Инфосистемы Джет» оценили уровень безопасности межсетевого взаимодействия между мобильным приложением и WEB-сервисом, а также настройки защищенного соединения.

«При обследовании мы ориентировались на самые злободневные уязвимости, которым подвержены мобильные банковские приложения. В их числе атаки класса Man-In-The-Middle («человек посередине») и целый ряд брешей, позволяющих злоумышленникам совершать кражи конфиденциальных данных пользователей банковских систем различными способами», – пояснил Георгий Гарбузов, руководитель отдела консалтинга Центра информационной безопасности компании «Инфосистемы Джет».

Выяснилось, что в каждом пятом (22%) из протестированных мобильных банковских приложений используются незащищенные протоколы передач информации, а в каждом четвертом (25%) производится небезопасная аутентификация WEB-сервера. В 87% продуктов специалистами была выявлена недостаточная защита пакета приложения и его компонентов, в 78% – отсутствие проверок наличия несанкционированного привилегированного доступа к мобильному устройству. Больше всего критичных «дыр» было обнаружено в Android-приложениях, меньше всего – в программных решениях, работающих в среде iOS.

Подтвердилась тенденция, отмеченная экспертами в традиционных ежегодных отчетах в области безопасности систем дистанционного банковского обслуживания (ДБО) [11]. Разработчики мобильных банк-клиентов не уделяют достаточного внимания вопросам безопасности приложений, не следуют руководствам по безопасной разработке. Зачастую отсутствуют процессы разработки безопасного кода и архитектуры. Оказалось, что все рассмотренные приложения содержат хотя бы одну уязвимость, позволяющую либо перехватить данные, передающиеся между

клиентом и сервером, либо напрямую эксплуатировать уязвимости устройства и самого мобильного приложения. Так, 35% мобильных банков для iOS и 15% мобильных банков для Android содержат уязвимости, связанные с некорректной работой SSL, а это означает возможность перехвата критичных платежных данных с помощью атаки "человек посередине". 22% приложений для iOS потенциально уязвимы к SQL-инъекции, что создает риск кражи всей информации о платежах с помощью нескольких несложных запросов. 70% приложений для iOS и 20% приложений для Android потенциально уязвимы к XSS - одной из самых популярных атак, позволяющей ввести в заблуждение пользователя мобильного банк-клиента и таким образом, например, украсть его аутентификационные данные. 45% приложений для iOS потенциально уязвимы к XXE-атакам, особенно опасным для устройств, подвергнутым столь популярной в России операции jailbreak. Около 22% приложений для Android неправильно используют механизмы межпроцессного взаимодействия, тем самым фактически позволяя сторонним приложениям обращаться к критичным банковским данным [11].

Защита.

Необходимо использовать криптографические возможности устройства, шифрование критичных данных и при необходимости возможность удаленной очистки данных, а также проводить анализ защищенности приложения, который поможет выявить возможные утечки критичных данных и некорректное использование шифрования.

Атака.

Для атаки через вредоносное приложение нарушителю необходимо установить вредоносное приложение, используя методы социальной инженерии или атаку Drive-by-Download.

После установки вредоносного приложения злоумышленник может поднять свои привилегии в системе, используя эксплойт для уязвимости в ОС смартфона, и получить удаленный доступ к устройству с полными правами доступа, что приведет к полной компрометации устройства: злоумышленник сможет украсть критичные данные пользователя мобильного банкинга или подменять данные платежных операций.

Защита.

Необходимо обновлять ПО на устройстве, использовать программные средства защиты и повышать осведомленность пользователей в вопросах ИБ.

Атаки на канал связи.

В ходе классической атаки "человек посередине" перехватываются данные между устройством клиента и сервером. Для этого необходимо находиться в одной сети с жертвой, например в публичной сети Wi-Fi, или использовать поддельные беспроводные точки доступа и поддельные базовые станции. Предпосылки – уязвимость в мобильном приложении, некорректная работа с шифрованием передаваемых данных или полное отсутствие шифрования данных. Самый распространенный пример – неправильная работа с SSL. В результате злоумышленник может прослушивать и подменять передаваемые

данные, что может в итоге привести к краже денежных средств со счета клиента.

Защита.

Правильная реализация работы с SSL. Также рекомендуется в мобильном приложении при подключении к серверу доверять только SSL-сертификату банка. Это поможет в случае компрометации корневого центра сертификации.

Стоит также отметить, что jailbreak устройства (iOS) или наличие root-доступа на устройстве (Android) пользователя значительно снижает уровень защищенности устройства и упрощает атаку для злоумышленника.

Выводы:

Приложения для мобильных платформ подвержены как старым общеизвестным угрозам, так и новым, еще не изученным до конца. Растет уровень распространения вредоносных приложений для Android.

Угрозы безопасности мобильных банков создают риски компрометации критичных данных пользователей, хищения денежных средств и нанесения ущерба репутации банка.

Разработчики мобильных банк-клиентов не уделяют достаточного внимания вопросам безопасности приложения, не следуют руководствам по безопасной разработке. У разработчиков зачастую отсутствуют процессы разработки безопасного кода и архитектуры.

Рекомендации.

- Осведомлять программистов о вопросах безопасности;
- Закладывать безопасность в архитектуру;
- Проводить аудит кода;
- Проводить анализ защищенности приложения;
- Применять параметры компилятора, связанные с безопасностью;
- Контролировать распространение приложения в сети Интернет;
- Быстро закрывать уязвимости и выпускать обновления.

Приведенное выше показывает, что мобильные банки содержат уязвимости и недостатки, которые могут привести к хищению денежных средств. Уровень защищенности мобильных банков в большинстве случаев не превосходит уровня защищенности обычных мобильных приложений, в то время как связанные с ними риски подразумевают повышенные требования по безопасности.

Современные средства защиты для мобильных устройств – антивирусы, MDM-решения и т.д. – могут сократить риск, но не решить весь спектр проблем. Безопасность должна внедряться еще на этапе проектирования системы и присутствовать на всех этапах жизненного цикла программы, включая этап разработки и внедрения. Необходимо осуществлять аудит кода, анализ защищенности приложения, тестирование на проникновение.

Риски при использовании мобильного банкинга обратно пропорциональны защищенности приложения. Поэтому необходим комплексный аудит защищенности мобильных банковских приложений.

Рекомендации.

1. Осведомлять программистов о вопросах безопасности.
2. Закладывать безопасность в архитектуру.
3. Проводить аудит кода.
4. Проводить анализ защищенности приложения.
5. Применять параметры компилятора, связанные с безопасностью.
6. Контролировать распространение приложения в сети Интернет.
7. Быстро закрывать уязвимости и выпускать обновления.

Литература

1. Якушин Петр. Безопасность мобильного предприятия// Открытые системы № 01, 2013.
2. Аналитический Центр InfoWatch. Глобальное исследование утечек корпоративной информации и конфиденциальных данных, 2014.
3. Шетько Николай. Взлом сотовых сетей GSM: расставляем точки над «i»// ET CETERA – серия цифровых журналов, распространяемых по подписке № 32, 2013.
4. Коржов Валерий. Скорость и безопасность в LTE// «Сети/network world» №6, 2012.
5. 802.11i-2004 – IEEE Standard for Local and Metropolitan Area Networks– Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.
6. Белорусов Д.И. Wi-Fi – сети и угрозы информационной безопасности/ Д.И. Белорусов, М.С. Корешков // СПЕЦИАЛЬНАЯ ТЕХНИКА № 6, 2009; с. 2-6.
7. Трифонов Дмитрий. Как взламывают корпоративный Wi-Fi: новые возможности. [Электр. рес.]// Исследовательский центр Positive Technologies. URL: http://www.securitylab.ru/analytics/471816.php.
8. Безопасность приложений. Аналитический отчёт IBM X-Force.[Электронный ресурс]//Постоянный URL: http://www.ibm.com/software/products/ru/category/application-security.
9. Анализ защищенности мобильных приложений (клиентская часть). Аналитический отчёт компании Digital Security. [Электронный ресурс]//Постоянный URL: http://www.dsec.ru/services/security-analysis/mobile-applications/.
10. 40% мобильных банковских приложений обладают критичными уязвимостям. Аналитический отчёт компании «Инфосистемы Джет»/ [Электронный ресурс]// Постоянный URL: http://servernews.ru/910462
11. Миноженко Александр. Безопасность мобильных банковских приложений/ [Электронный ресурс]// Постоянный URL: http://www.itsec.ru/articles2/25kadr/bezopasnost-mobilnyh-bankovskih-prilozheniy.