

Средства защиты информации для мобильных платформ

Руслан Нигматулин, директор департамента по работе с корпоративными клиентами ЗАО "С-Терра СиЭсПи"



Сегодня все мобильные платформы — это практически стандартизированные устройства для слежения за пользователем. Классическая связка: ПДн пользователя — местоположение пользователя — передаваемая пользователем информация. При получении SIM-карты персональные данные фиксируются вместе с телефонным номером. Кроме того, нередко телефонный номер привязывается к банковской карте.

В настоящее время безопасности мобильных устройств уделяется большое внимание. В ней заинтересованы практически все: подразделения, ответственные за безопасность в коммерческих структурах и государственных органах, производители продуктов информационной защиты, специализированные СМИ, регуляторы и, к сожалению, охотники за чужими байтами.

Во-первых, определимся, что мы будем понимать под мобильными платформами. Термин довольно емкий — это ноутбуки, нетбуки, планшетные компьютеры, смартфоны (коммуникаторы), мобильные телефоны. В этот перечень можно добавить еще ряд устройств, например, навигаторы и игровые приставки. Для наглядности ограничимся планшетными компьютерами и смартфонами на базе различных ОС, причем используемыми для оперирования конфиденциальной информацией, не касаясь государственной тайны.

Во-вторых, разберемся, почему с точки зрения ИБ мобильные устройства выделили в отдельное направление. Казалось бы, мобильные устройства вполне подпадают под стандартные определения "ЭВМ", "машинный носитель", "материальный носитель информации", "средства вычислительной техники". Но при этом аппаратные части мобильных устройств и, например, настольных ПК значительно различаются. Скажем, большинство ARM процессоров в смартфонах и планшетных компьютерах имеют на одном кристалле, кроме самого процессора, еще и графическое ядро, контроллеры памяти, различные интерфейсы и т.д.

Отличия мобильных устройств и стандартных ЭВМ

Итак, первая причина — это новая, в том числе с точки зрения безопасности, архитектура, отличная от привычной Intel x86.

Вторая причина — это высокая скорость перехода мобильных устройств из одной среды пере-

дачи информации в другую. Например, смартфон с легкостью меняет подключение по Wi-Fi на 3G-связь. Более того, не исключена возможность "гладкого" перехода между режимами передачи во время одной сессии.

Третья — наличие отдельного класса специализированных ОС для мобильных устройств. Сегодня существует большое разнообразие как видов, так и подвидов таких ОС. Они часто обновляются, причем нередко обновления включают изменения ядра (например, ОС Android).

Четвертая, вытекающая из названия, — это мобильность. Причем не просто возможность физического переноса прибора. При желании можно переносить и настольный ПК, но вряд ли кто-нибудь назовет его мобильным. Современная мобильность подразумевает автономность и свободу от ограничений по времени, месту, способу доступа к необходимой информации, средствам связи и приложениям.

Содержание передаваемой информации

Свобода, о которой мы упоминали при анализе причин (вспомните мобильность), притупляет бдительность. Имея в руках удобный гаджет, человек с легкостью передает сообщения, которые в другой ситуации шепнул бы на ушко только строго адресату.

Существует еще и интеллектуальная обработка информации, которая напрямую не привязана к мобильности. Мы настолько привыкли к ней, что не замечаем. Вряд ли кто-то удивляется, например, что сервис социальной сети каждый мало-мальски длинный набор

цифр в сообщении пытается опознать как телефонный номер.

Задумавшись над всем этим, хочется испугаться и отказаться от использования мобильных устройств. Но не стоит противиться прогрессу. Лучше задуматься о безопасности, а вернее, о средствах защиты информации для мобильных платформ. Поверьте, они есть, и они эффективны.

Модели угроз

Предлагаю подходить классически и для начала определить модель угроз, связанную с имеющимся бизнес-процессом. Несмотря на стремительное обновление технологий, используемых для защиты, с одной стороны, и для атак — с другой, наука о безопасности во многом консервативна, по крайней мере в своих системных подходах. Случай с мобильностью — не исключение.

Одна из угроз мобильности — легкое проникновение в контролируемую зону и выход из нее. Речь конечно, не о том, что есть принципиальная физическая сложность изъять смартфон при входе в здание или поставить генератор шума в соответствующем диапазоне. Но закон перехода количества в качество действует. Массовость мобильных устройств часто требует новых подходов.

Дополнительные угрозы, связанные с мобильностью, — легкость попадания устройства в руки нарушителя, а также заражение этого устройства вирусами и шпионскими программами. Согласитесь, очень неприятно, когда скачанное из Интернета ПО оказывается SMS-трояном и опустошает счет мобильного телефона, отправляя сообщения на платные номера. Но это отдельная тема.

Создадим следующую модель. Есть некая централизованная информационная система, которая базируется на нескольких географически разнесенных ЦОД.

Характеристики, которые нужно определять для информационных систем, прописаны в приказе № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных". Методика определения нарушителей и необходимых криптосредств определена ФСБ России в "Методических рекомендациях по обеспечению с помощью криптосредств безопасности ПДн при их обработке в информационных системах персональных данных с использованием средств автоматизации".

Описание ИС и возможных нарушителей

Постараемся предельно упростить описание.

Примем, что доступ к информационной системе должен быть предоставлен большому количеству пользователей через открытый Интернет. Важно, что большое количество пользователей будет обращаться к данной ИС с разнообразных планшетных компьютеров и смартфонов. Пользователи будут с разными правами доступа: к открытой части ИС, только к своей части информации (посредством "личных кабинетов"), администраторы системы.

Для обеспечения онлайн-взаимодействия пользователей с системой предназначен Web-интерфейс, отображаемый Web-браузером. Система "личных кабинетов" должна обеспечивать изолированное и защищенное механизмами аутентификации и авторизации личное рабочее пространство, позволяющее пользователям самостоятельно настраивать определенные функции.

Возможными источниками угроз для системы являются нарушитель, носитель вредоносной программы, аппаратная закладка. Предположим, в информационной системе могут действовать нарушители категорий Н1 и Н2. Тогда, если система подлежит аттестации, необходимо использовать СКЗИ не ниже класса КС2.

Информационная система описана, конечно, очень сокращенно, но вполне имеет право на существование в реальности.

Сертификация

Итак, исходя из требований к безопасности описанной выше ИС, надо бы найти среди них устройство, сертифицированное в ФСБ по классу КС2.

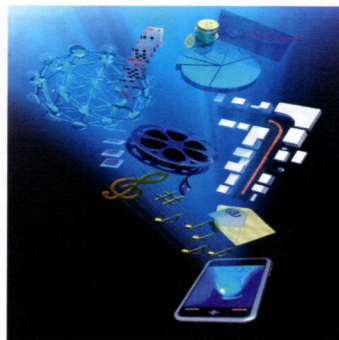
Вот здесь-то и начинаются сложности. Кстати, необходимо уточнение. Проблемы с сертификацией возникают, когда дело касается платформ, работающих на ОС Android или iOS. С ОС Windows сегодня все в порядке, они открыты, и средства защиты для них уже сертифицированы. Но планшетных компьютеров и смартфонов под Windows на рынке не так уж много.

Сертифицировать средства безопасности для таких мобильных устройств можно. Но, судя по тому что на рынке пока нет большого разнообразия сертифицированных средств защиты для планшетных компьютеров и смартфонов, сделать это — непростая задача. Принципиальный момент: при сертификации жестко фиксируется состав мобильной платформы, а именно — связка аппаратной платформы, версии ОС, версии ядра. В этом случае можно сказать "до свидания" такой процедуре, как легкое обновление ОС, а заодно и новым приятным и полезным функциям, которые появляются вместе с обновлением. Ну что ж, безопасность, удобство и мода не всегда дружелюбны друг к другу.

Есть еще одна проблема, мешающая сертификации. Большинство производителей мобильных платформ (напомню, не под Windows) не только не предоставляют данных о своих операционных системах в объеме, необходимом для исследования среды функционирования криптосредств, но и повсеместно не дают пользователям прав администратора ОС. Встраивание средства защиты при этом можно выполнить только полуправильными методами. В этих условиях перспективы сертификации неясны, и добросовестный производитель средств сетевой защиты постарается избежать заявлений о скорой сертификации решений для мобильных платформ.

Безопасное использование

Итак, какие варианты безопасного использования мобильных устройств доступны сегодня? К сожалению, их немного — либо применение устройств на базе ОС Windows, для которой на рынке предла-



гаются сертифицированные средства сетевой информационной защиты, либо применение стандартизованных мобильных платформ на базе других ОС с жестким запретом на их обновления. Для таких ОС большинство вендоров также предлагает средства защиты, правда пока не сертифицированные.

Можно ли на практике применить хотя бы один из этих вариантов? Если это крупная корпорация, в которой есть свои подразделения ИТ и ИБ, то можно обязать пользователя к неудобному, но безопасному варианту. Если это государственная структура, скажем, МВД, организации системы здравоохранения и т.д., то унификация тоже возможна в рамках проекта — пользователь также не имеет особого выбора. Если же речь идет о свободном рынке, на котором, как известно, конкурентоспособность — определяющий фактор, то применимость любого из вариантов под вопросом. Для примера, банковская сфера. Клиенты банков хотят, чтоб им было удобно с множеством их любимых гаджетов. Формально можно обязать к использованию какого-то определенного устройства, прописав, естественно, в договоре, что так безопасно. Но пользователь всегда имеет право сказать: "Не хочешь обеспечить доступ к другому устройству? До свидания, я пошел в другой банк".

Как видите, даже при скромной попытке в рамках статьи подойти к безопасности мобильных устройств с классической точки зрения — построения модели угроз, определения нарушителя и т.д., появляется много проблем, требующих решения. Но тем не менее только при таком подходе мы имеем шанс получить максимально безопасную систему. ●

На подходе уже целый ряд устройств со встроенной возможностью "наблюдения" за пользователем. Уже предлагают фотоаппараты с SIM-картой и встроенным GPS, с якобы безобидной целью тут же передать сделанные снимки в социальную сеть с привязкой фото к координатам, чтобы не забыть, что это вы под пальмой в Египте, а не в Турции. GPS-навигаторы уже давно производятся с поддержкой передачи данных. Вы еще не слышали о бытовых приборах, чайниках и холодильниках со встроенной ОС и опять-таки SIM-картой? Скоро увидите их в магазинах.

Какие выводы? От разнообразия и изменчивости мобильных устройств не уйти. Защиту для этих платформ или же от них обеспечить придется. Спрос есть, есть предложения. Новый рынок, новые возможности.

Ваше мнение и вопросы
присылайте по адресу
infosec@groteck.ru