поверх протокола транспортного уровня. Протокол соединения (*SSH-CONN*), мультиплексирует несколько логических каналов в один зашифрованный туннель. Этот компонент протокола SSH выполняется поверх протокола аутентификации пользователя.

Для аутентификации сервера в SSH-USERAUTH используется протокол аутентификации сторон на основе алгоритмов электронно-цифровой подписи RSA или DSA. Для аутентификации клиента также может использоваться ЭЦП RSA или DSA, но допускается также аутентификация при помощи пароля и даже ip-адреса хоста. Аутентификация по паролю наиболее распространена; она безопасна, так как пароль передаётся по зашифрованному виртуальному каналу. Аутентификация по ip-адресу небезопасна, эту возможность чаще всего отключают. Для создания общего секрета (сеансового ключа) используется алгоритм Диффи — Хеллмана (DH). Для шифрования передаваемых данных используется симметричное шифрование, алгоритмы AES, Blowfish или 3DES. Целостность передачи данных проверяется с помощью CRC32 в SSH1 или HMAC-SHA1/HMAC-MD5 в SSH2. Для сжатия шифруемых данных может использоваться алгоритм LempelZiv (LZ77), который обеспечивает такой же уровень сжатия, что и архиватор ZIP. Сжатие SSH включается лишь по запросу клиента, и на практике используется редко.

Для повышения надежности работы протокола можно принять несколько превентивных мер, заключающихся в проведении ряда организационно-технических мероприятий. К таким мероприятиям относятся:

Запрещение удалённого root-доступа (доступ в качестве администратора системы).

Запрещение подключения с пустым паролем или отключение входа по паролю.

Выбор нестандартного порта для SSH-сервера.

Использование длинных SSH2 RSA-ключей (2048 бит и более). Системы шифрования на основе RSA считаются надёжными, если длина ключа не менее 1024 бит.[6]

Ограничение списка IP-адресов, с которых разрешён доступ (например, настройкой файерволла).

Запрещение доступа с некоторых потенциально опасных адресов.

Отказ от использования распространённых или широко известных системных логинов для доступа по SSH.

Регулярный просмотр сообщений об ошибках аутентификации.

Установка систем обнаружения вторжений (IDS — Intrusion Detection System).

Использование ловушек, подделывающих SSH-сервис (honeypots).

При составлении плана организационно-технических мероприятий по повышению надёжности протокола SSH для конкретного предприятия все вышеперечисленные меры необходимо проанализировать, поскольку они резко отличаются друг от друга по величине капитальных затрат на их внедрение. Действительно, составление и внедрение инструкции или стандарта предприятия, предусматривающих «Отказ от использования распространённых или широко известных системных логинов для доступа по SSH» или «Регулярный просмотр сообщений об ошибках аутентификации», потребует мало денежных средств и времени, в то время как «Установка систем обнаружения вторжений» — это более дорогостоящее и длительное по срокам внедрения мероприятие.

Список использованных источников:

1. Корнеев И. А., Сечко Г.В., Таболич Т.Г. Постановка задачи разработки нового кроссплатформенного программного обеспечения (ПО) для работы с протоколом SSH // Современные средства связи: материалы XVII Междунар. науч.-техн. конф., 16–18 сент. 2012 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2012. – 332 с. – С. 199.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВСКИХ МОБИЛЬНЫХ ПЛАТЕЖЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Королёв Я. П., Лысковец А. М., Масловская А. И.

Сечко Г. В. – канд. техн. наук, доцент

Для обеспечения информационной безопасности мобильных платежей предлагается начать в республике широкую стандартизацию при разработке мобильных приложений, заимствуя при этом передовой зарубежный опыт

Насколько нам известно, в настоящее время банки Беларуси только начинают внедрять приём мобильных платежей через интернет (почти во всех банках клиентам доступен SMS-банкинг). В то же время в России и на Украине этот вид услуг активно развивается. Например, санкт-петербургский банк ОАО АКБ «Балтика» внедрил первую в России России кастомизированную информационно-платежную систему на основе платежного сервиса MasterCard Mobile по модели White-lable при непосредственном участии MasterCard. Разработчиком и сервис-провайдером Baltica Mobile выступила группа компаний Intervale. Сервисом Baltica Mobile могут воспользоваться держатели карт MasterCard и Maestro, эмитированных ОАО АКБ «Балтика». Новый сервис предоставляет возможность оплачивать товары и услуги в режиме он-лайн на

web-портале Банка или через интерфейс мобильного телефона из любой точки мира 24 часа в сутки, 7 дней в неделю [1].

Одновременно с АКБ «Балтика» украинский Приватбанк (филиалы и партнёры в 12 странах) предложил [2] своим клиентам 5 основных (есть и дополнительные) мобильных приложений для платежей со смартфонов. Это 1) Privat24 – приложение для проведения любых финансовых операций с деньгами и картами вне зависимости от дня недели, времени и местонахождения; 2) iPay – позволяет принимать к оплате карточки Visa и MasterCard с мобильного телефона; 3) «Экстренные деньги» – с помощью этого приложения можно снимать деньги в банкоматах ПриватБанка без наличия карты; 4) SMS-банкинг – способ управления своим карт-счётом; владелец банковской пластиковой карты может проводить платежи и получать информацию о проведенных операциях при помощи своего мобильника через SMS; 5) Privat Hot Line – оповещает ПриватБанк о факте мошенничества путём присылки в банк снимка этого факта; если сигнал подтверждается, приславшему выплачивается вознаграждение до 5 000 гривен (5 миллионов рублей).

Перечисленные мобильные приложения подвержены всем угрозам информационной безопасности двух объектов: во-первых, банковских кредитных карт, во-вторых, смартфонов. Для парирования этих угроз в докладе предлагается начать широкую стандартизацию при разработке мобильных приложений, заимствуя при этом передовой зарубежный опыт. Например, в США в 2010 году была организована группа специалистов по работе над безопасностью приёма платежей через мобильные устройства [3]. В том же году с подачи группы разработан стандарт безопасности данных PCI DSS (Payment Card Industry Data Security Standards). В 2012 году Совет по разработке стандартов безопасности PCI (Payment Card Industry Security Standards Council /SSC/) выпустил новый документ «The PCI mobile payment acceptance security guidelines». Согласно документу рекомендуется создавать приложения с поддержкой шифрования данных, защищать приложения паролем. Мобильные приложения, которые осуществляют мобильные платежи, должны обладать функциями обнаружения атак, функциями оповещения об атаках и о введении неправильного пароля или изменении криптографического ключа [3].

Технический директор PCI SSC считает [3], что многочисленные мобильные платформы, различные производители смартфонов и операторы связи чрезвычайно усложняют процесс создания безопасных приложений для приёма платежей через смартфоны. Недостаток практического опыта и необходимой документации позволяет разработчикам мобильного ПО уходить от ответственности за сохранность секретных данных [3].

Анализируя ситуацию с мобильными платежами в Беларуси, несложно заметить, что мобильные платформы в республике, так же как и во всём мире, многочисленны – это и Windows mobile, и Symbian, и Pocket PC, и Android (все перечисленные – различных многочисленных версий), и, в последнее время, Blackberry. Разработкой мобильного ПО в Беларуси занимаются все, кому не лень – от крупных фирм до индивидуальных предпринимателей. В то же время документов, подобных «The PCI mobile payment acceptance security guidelines», в республике нет. В этих условиях широкая стандартизация при разработке мобильных приложений, заимствуя при этом передовой зарубежный опыт, в Беларуси своевременна и актуальна.

Список использованных источников:

1. Мобильные платежи от банка «Балтика» на базе платформы MasterCard Mobile [Электронный ресурс]. – Электронные данные. – Режим доступа www.procontent.ru/news/26942.html. – Дата доступа 23.03.2013.

2. Мобильные приложения ПриватБанка [Электронный ресурс]. – Электронные данные. – Режим доступа privatbank.ua/apps/. – Дата доступа 23.03.2013.

3. Вестервельт Роберт. Новые правила разработки мобильных приложений // Безопасность ИТ-инфраструктуры. – 2012. – № 12 (66). – С. 1-2.

ВРЕДОНОСНОЕ ПО И СМАРТФОНЫ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Королёв Я. П., Рудский А. В., Масловская А. И.

Шпак И. И. – канд. техн. наук, доцент

Анализируется вредоносное программное обеспечение (компьютерные вирусы, программы шпионы и т.д.) как одна из возможных угроз информационной безопасности смартфонов. Предлагаются мероприятия, которые следует осуществить для парирования данной угрозы

Под смартфо́ном (англ. *Smartphone* — умный телефон) — обычно понимают [1] мобильный телефон, сравнимый с карманным персональным компьютером. В [2] в первом приближении проанализированы основные угрозы информационной безопасности смартфонов. В настоящем докладе анализ угроз информационной безопасности смартфонов продолжен в части защиты их от вредоносного программного обеспечения (ПО). При этом под вредоносным ПО понимаются как компьютерные вирусы, так и программы-шпионы. В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Согласно [3] вирусы принято разделять по следующим критериям классификации а) по поражаемым объектам; б) по поражаемым