Е. А. Лагутина

БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЙ МОБИЛЬНЫХ ПЛАТЕЖЕЙ С ПРИМЕНЕНИЕМ TPM MOBILE

Введение

В настоящее время значительно возросло участие мобильных устройств в повседневной жизни: если раньше телефон рассматривался исключительно с точки зрения средства связи, то на сегодняшний день смартфон может выполнять множество других функций. В частности, многие механизмы электронной коммерции и банкинга предполагают использование мобильного устройства в качестве пользовательской платформы.

Согласно данным статистики, количество пользователей систем мобильных платежей выросло со 160,5 млн человек в 2011 г. до 212,2 млн в 2012 г., а оборот по таким операциям увеличился на 61,9 %: 171,5 млрд долларов США в 2012 г. по сравнению со 105,9 млрд долларов США в 2011 г. При подобном темпе роста к 2016 г. число пользователей составит 448 млн человек, а оборот — 617 млрд долларов США. Кроме того, согласно данным компании Symantec, в 2012 г. рост количества вариаций вредоносных программ для мобильных устройств составил 58 %, а мобильных угроз, связанных с кражей информации в целом, — 31 %.

Таким образом, с ростом доверия к мобильным устройствам с точки зрения средства проведения всевозможных финансовых операций более отчетливо проявляется проблема безопасности обработки, хранения и передачи персональных данных и конфиденциальной информации [1].

В настоящей статье предложен вариант решения основных задач безопасности информации, формулируемых при проектировании мобильного платежного приложения. Данное решение предполагает использование TPM Mobile (Trusted Platform Module Mobile — модуль доверенных вычислений, спецификация для создания модуля безопасности, адаптированного для использования в мобильных устройствах; более подробное описание приводится ниже в соответствующем разделе) [2, 3].

Задачи безопасности

В первую очередь следует перечислить задачи, которые необходимо решить при построении прототипа безопасной среды исполнения платежного мобильного приложения:

- аутентификация пользователей;
- защита конфиденциальных данных, предотвращение изменения передаваемых параметров, предотвращение перехватов сеансовых данных;
- экранирование операционной системы и хранилища данных от возможного влияния приложения;
- аудит, протоколирование;
- валидация ввода, авторизация пользователя, обработка исключений, обеспечение безопасной конфигурации;
- кодирование, шифрование, структуризация конфиденциальных данных [4].

TPM Mobile

TPM Mobile представляет собой спецификацию для создания модуля безопасности, адаптированного для использования в мобильных устройствах.

TPM Mobile основывается на спецификации TPM v1.2. Данной спецификацией обеспечиваются средства безопасной генерации криптографических ключей как для подписи, так и для шифрования/дешифрования, средства удаленной аттестации, привязки и надежного защищенного хранения.

Удаленная аттестация позволяет проверить, были ли изменены или скопированы ПО, фильм, музыка и т. д., загруженные пользователем из магазина.

Криптопроцессор производит зашифрование данных так, что расшифрование возможно только на устройстве, где они были зашифрованы, под управлением того же самого ПО.

Привязка шифрует данные, используя ключ подтверждения TPM, записанный в чип в процессе его производства.

TPM Mobile имеет следующие усовершенствования, позволяющие применение в мобильных устройствах:

- безопасная загрузка: загрузочная последовательность не только подвергается измерению, но и останавливается в случае обнаружения неподтвержденного программного обеспечения;
- поддерживается возможность применения только программной части TPM Mobile;
- возможно параллельное использование нескольких TPM Mobile на одном устройстве.

Эти свойства позволяют:

- обеспечить целостность данных устройства;
- разработчикам устройств использовать TPM Mobile в качестве дополнения к уже существующим на устройстве механизмам безопасности;
- разграничить зоны безопасности для нескольких пользователей.

Описание структуры платежного приложения

На основании проведенных автором исследований и сделанных по полученным результатам выводов построен прототип защищенного платежного приложения. Он состоит из приложения на стороне (устройстве) пользователя и приложения на сервере.

Структура приложения на стороне пользователя

На рис. 1 представлена диаграмма классов приложения на стороне пользователя, позволяющая наглядно рассмотреть его предполагаемую структуру, а также реализуемые функции безопасности.

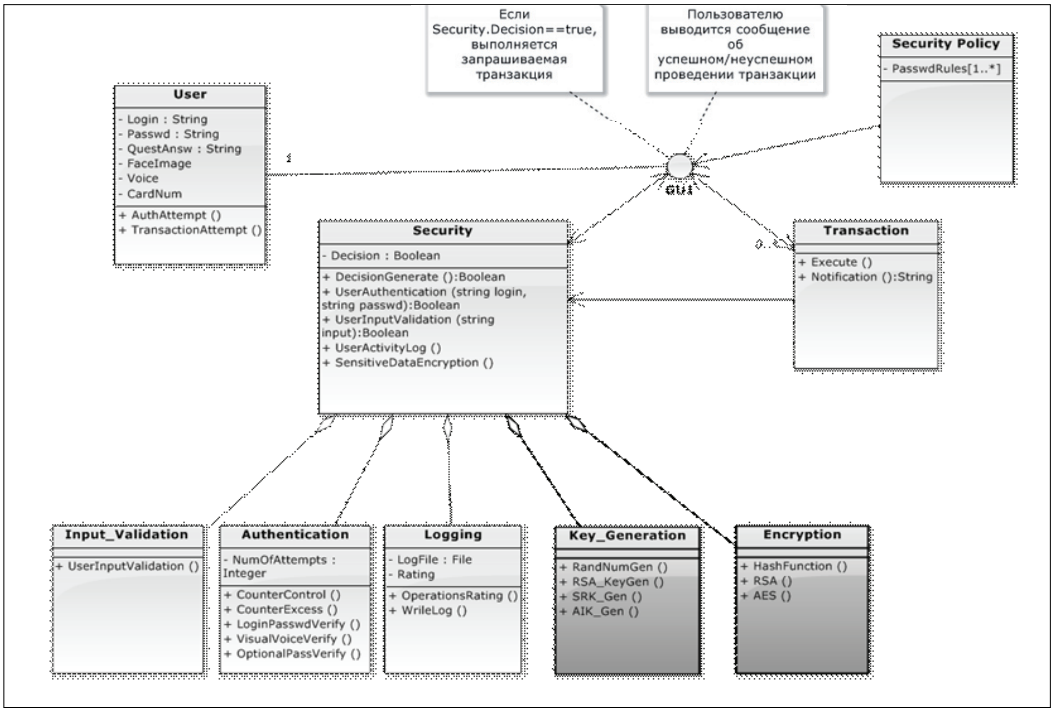

Рис. 1. Диаграмма классов платежного приложения на стороне пользователя

Класс User

Предполагается, что для каждой копии приложения, устанавливаемой на персональном устройстве, существует единственный пользователь, обладающий обязательными уникальными аутентификационными данными: именем пользователя и паролем, данными для речевой аутентификации, сохраненным изображением лица пользователя. Кроме того, к приложению привязывается одна или несколько платежных карт, номер которых хранится в CardNum.

Атрибут QuestAnsw содержит ответ на контрольный вопрос, который необходим для разблокировки приложения. Данное значение выбирается пользователем при первом запуске приложения и не может быть изменено в дальнейшем.

Пользователь может инициировать попытку аутентификации и попытку транзакции с помощью методов AuthAttempt и TransactionAttempt соответственно.

Класс Security

Данный класс является объединением всех реализуемых механизмов безопасности, описание и определение которых приводится в классах Input_Validation, Authentication, Logging, Key_Generation, Encryption.

Класс Security содержит логическую переменную Decision, значение которой устанавливается методом DecisionGenerate на основании данных, генерируемых методами UserAuthentication и (или) UserInputValidation в зависимости от пользовательской операции, безопасность которой проверяется. Если значение Security.Decision — true, разрешается доступ к функциональной части приложения либо выполняется запрашиваемая транзакция.

Класс Input_Validation

Выполняет проверку корректности пользовательского ввода.

Класс Authentication

Содержащаяся в данном классе целочисленная переменная NumOfAttempts представляет собой счетчик попыток аутентификации пользователя и позволяет ограничить их количество.

Управление счетчиком осуществляется в методе CounterControl. В случае превышения допустимого значения счетчика вызывается метод CounterExcess, блокирующий приложение. Блокировка может осуществляться либо на некоторый промежуток времени, либо до ввода пользователем ответа на контрольный вопрос. Ответ на вопрос определяется пользователем при первом запуске приложения. Выбор времени блокировки осуществляется пользователем во время установки приложения и не может быть изменен в дальнейшем.

Методы LoginPasswdVerify, VisualVoiceVerify и OptionalPassVerify выполняют сравнение вводимых пользователем при попытке аутентификации данных с соответствующими сохраненными значениями. LoginPasswdVerify проверяет пару логин — пароль, VisualVoiceVerify сверяет изображение лица пользователя, получаемое от камеры устройства, и (или) выполняет голосовую верификацию.

Класс Logging

Метод данного класса WriteLog выполняет запись сведений о совершаемых пользователем действиях в файл LogFile. Степень детализации записи зависит от критичности действия с точки зрения обеспечения безопасности работы приложения. Все возможные действия пользователя ранжируются с помощью метода OperationsRating, полученное распределение хранится в переменной Rating.

Класс Key_Generation

Методы данного класса выполняют генерацию ключей SRK и AIK, случайных чисел и ключей для RSA. Данный класс реализуется средствами TPM Mobile.

Класс Encryption

Методы этого класса выполняют шифрование данных алгоритмами RSA и AES (методы RSA и AES соответственно), а также вычисление хэш-значений, необходимых для контроля целостности системы. Данный класс реализуется средствами TPM Mobile.

Класс Security Policy

Содержит правила безопасности PasswdRules, согласно которым выбираются способы аутентификации, обеспечивающие различный уровень безопасности, а также ограничения на возможный пароль пользователя: минимальная длина, допустимые символы. С помощью соответствующих настроек пользователь может выбрать желаемый уровень защищенности. В зависимости от выбранного уровня при дальнейшем использовании приложения выполняется аутентификация по логину и паролю и (или) по голосу и (или) визуальная аутентификация.

Класс Transaction

Запускает выполнение транзакции в методе Execute. С помощью этого метода осуществляются связь с платежным терминалом, передача ему всех необходимых для выполнения транзакции данных. В этом классе также предусмотрен метод Notification, сообщающий пользователю о статусе транзакции: успешном проведении или отказе.

Взаимодействие пользовательского класса и классов, реализующих функционал и безопасность приложения, происходит через интерфейс GUI.

Структура приложения на стороне сервера

Часть приложения, хранящаяся на сервере, состоит из единственного класса Card Verification. В данном классе реализуются методы, выполняющие верификацию пользователя приложения как владельца платежной карты. Процесс верификации описывается ниже.

Процесс аутентификации в приложении на стороне пользователя

Аутентификация производится при каждом запуске приложения по схеме, приведенной на рис. 2.

Процесс верификации пользователя в качестве владельца платежной карты

Для прикрепления платежной карты к приложению пользователь должен подтвердить, что он действительно владеет данной картой. Для этого необходимо ввести номер карты, имя владельца, срок действия и CVC21/CVV2 при его наличии. Эти сведения отправляются в часть платежного приложения, располагающуюся на сервере. Затем полученные данные с помощью метода Card_Verification.SendData отправляются в банк клиента вместе с запросом кода подтверждения. Код подтверждения высылается банком на мобильный телефон клиента, который вводит его в соответствующее поле интерфейса. Верификация данного кода производится методом Card_Verification.CodeVerification.

Реализованные механизмы безопасности

В таблице 1 перечислены реализованные в описанном приложении механизмы безопасности.

Таблица 1. Реализованные механизмы безопасности

Аспект безопасности	Решение	Реализация решения
Аутентификация пользователей	Усложненный механизм аутентификации пользователя в приложении	Программный модуль
Защита конфиденциальных данных	Усложненный механизм передачи данных между пользовательским интерфейсом и функционалом приложения	TPM Mobile
Предотвращение нарушения целостности передаваемых параметров		
Предотвращение перехвата сеансовых данных		

Экранирование операционной системы и хранилища данных от возможного влияния приложения	Введение дополнительного ключа безопасности	TPM Mobile
Аудит и протоколирование	Ведение журнала событий	Программный модуль
Валидация ввода, обработка исключений	Проверка пользовательского ввода	Программный модуль

Преимущества предложенного решения

Приложение, проект которого был представлен, может быть реализовано на любой мобильной платформе, что позволяет расширить круг пользователей. Кроме того, решения, существующие в нашей стране на данный момент, по большей части представляют собой приложения мобильного смс-банкинга либо мобильные кошельки, что подразумевает возможность оплаты лишь ограниченного спектра услуг. Описанное же в данной статье приложение ориентировано на перспективы развития применяемых платежных технологий и позволяет не только использовать мобильное устройство для удаленной оплаты, но и безопасно расплачиваться за любые приобретенные товары и услуги непосредственно на месте.

Дальнейшие исследования

В рамках дальнейших исследований предполагаются реализация и тестирование приложения. Для более детального анализа безопасности в максимально приближенных к реальности условиях планируется также проектирование модели возможного нарушителя.

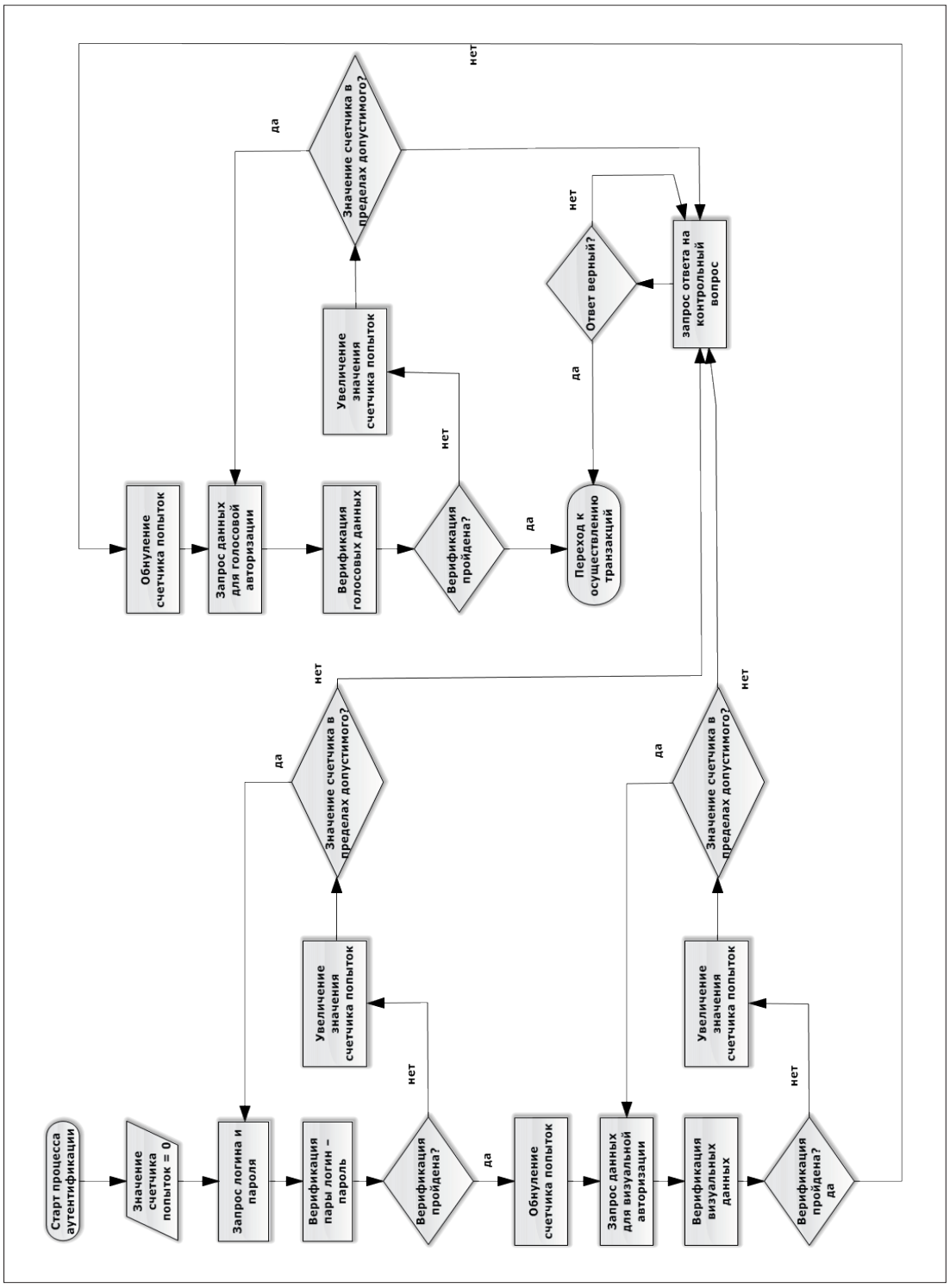

Рис. 2. Алгоритм процесса аутентификации

СПИСОК ЛИТЕРАТУРЫ:

1. *Vasudevan A., Owusu E., Zhou Z., Newsome J., McCune J. M.* Trustworthy Execution on Mobile Devices: What security properties can my mobile platform give me? Carnegie Mellon University. — 19 p.
2. TPM Main Part 1 Design Principles: Specification Version 1.2 Level 2 Revision 103 — 9-08-2007. TCG Published. — 182 p.
3. TCG Mobile Trusted Module: Specification Version 1.0 Revision 7.02 — 29-04-2010. TCG Published. — 103 p.
4. *Сомасегар С., Гатри С., Хилл Д.* Руководство MICROSOFT® по проектированию архитектуры приложений / Пер. с англ. 2-е изд. М.: Изд-во MICROSOFT®, 2009. — 529 с.