International Finance and Accounting

Volume 2018 | Issue 1 Article 7

2-1-2018

PROBLEMS OF INFORMATION SECURITY OF MOBILE APPLICATIONS AND WAYS OF THEIR SOLUTIONS

R. Dadabayeva
Tashkent Financial institute

A. Mahkamov
Tashkent Financial institute

Дадабаева Р.А.,
Махкамов А.А.

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ И ПУТИ ИХ РЕШЕНИЙ

Рассматриваются тенденции развития и основные характеристики мобильного банкинга и дистанционного банковского обслуживания. Отмечается тенденция роста новых рисков и угроз в системах мобильного банкинга. Анализируются проблемы информационной безопасности мобильных приложений: приводятся основные типы угроз, формулируются рекомендации по повышению уровня безопасности.

Ключевые слова: дистанционное банковское обслуживание, мобильный банкинг; аутентификационные данные; межпроцессорное взаимодействие; анализ исходного кода; тестирование приложений; отладочный код; межсайтовый скриптинг; протоколы передач информации; шифрование.

The development tendencies and basic characteristics of mobile banking and remote banking services are considered. There is a trend of growth of new risks and threats in mobile banking systems. The problems of information security of mobile applications are analyzed: the main types of threats are given, recommendations for improving the level of security are formulated.

Key words: remote banking services, mobile banking; Authentication data; interprocess communication; source code analysis; testing of applications; debugging code; crossite scripting; protocols for transmitting information; encryption.

Современный бизнес требует, чтобы доступ к информации осуществлялся быстро, надежно и из любой точки мира. Параллельно идет активное развитие дистанционных услуг, платежные приложения постепенно появляются на наших мобильных устройствах.

Особенно наглядно тенденция использования дистанционных услуг просматривается в банковской сфере. Рост числа пользователей банковскими дистанционными услугами (ДБО) иллюстрирует рис. 1.

Среди всех видов ДБО особое место занимает мобильный банкинг.

Основными преимуществами мобильного банкинга для клиента являются следующие [1]:

- Удобство – клиент может пользоваться услугами из любой точки земного шара;

- Оперативность – оплата услуг при помощи систем мобильного банкинга происходит с большой скоростью, иногда мгновенно;
- Доступность – стоимость пользования услугами удаленного обслуживания невелика, часто банки предоставляют *услуги мобильного банкинга* бесплатно;

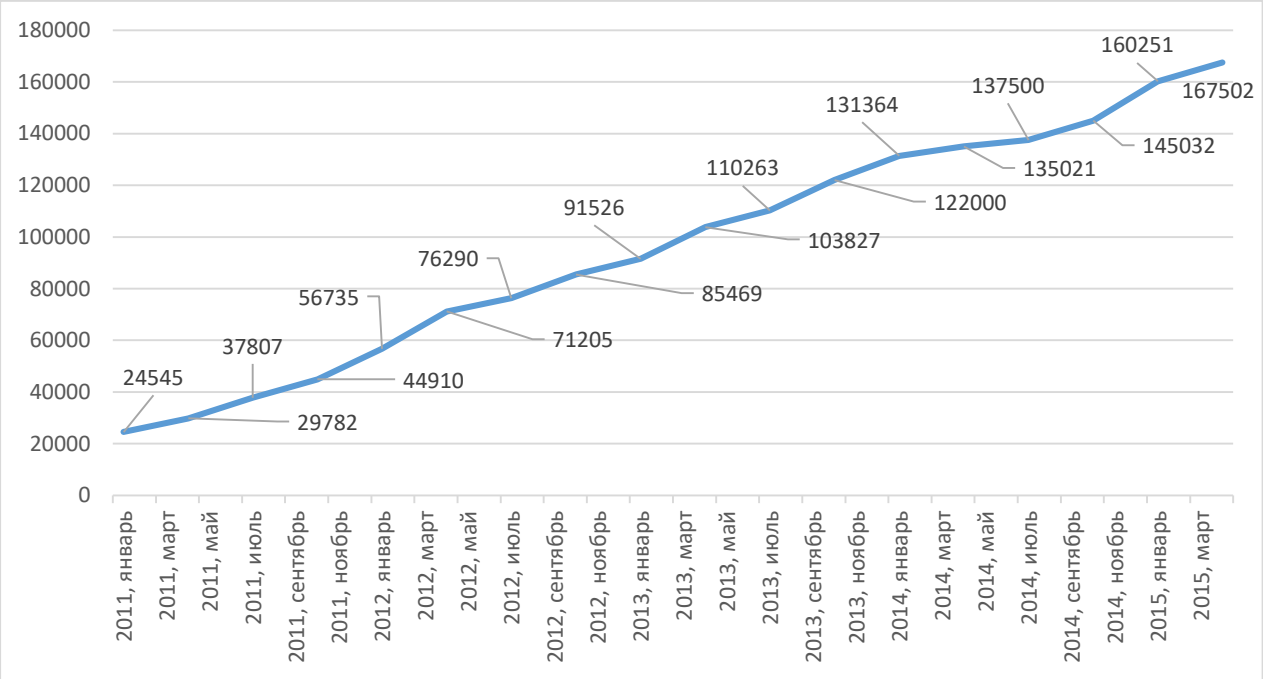

Рис. 1. Количество пользователей ДБО в Узбекистане (состояние на 1 апреля 2015 года)

- Выгодность – часто банки предоставляют клиенту возможность выполнения *удаленных банковских операций* по более выгодным тарифам, чем при обслуживании клиента в офисе;
- Разнообразие – многие банки поддерживают и развивают различные каналы дистанционного обслуживания (например, Интернет, мобильный или стационарный телефон).

Мобильный банкинг имеет преимущества и для банка. Основными из них являются следующие**:**

1. Экономическая выгода за счет сокращения стоимости обслуживания клиента – затраты на оказание услуг клиенту в отделениях банка и точках продаж значительно выше, чем при удаленном взаимодействии. Конечно, банк несет немалые затраты на внедрение *системы мобильного банкинга,* но они окупаются через некоторый период времени и, чем больше клиентов банк подключает к удаленным сервисам, тем короче период окупаемости затрат.

2. Удаленное обслуживание, к которому относится и обслуживание клиентов с помощью терминалов и устройств самообслуживания, гораздо эффективнее, по сравнению с традиционным обслуживанием в офисе банка, так как ни один банк не в состоянии обслужить в своих офисах десятки тысяч клиентов. Вследствие сокращения времени на взаимодействие с клиентом пропускная способность обслуживания увеличивается.

3. Внедрение мобильного банкинга помогает решать задачи развития точек присутствия и обеспечивает доступность для клиента услуг банка в любом месте и в любое время.

4. Появляются возможности привлечения клиентов вне зависимости от их географического местонахождения, банк получает выход на новые клиентские сегменты, которые банк не обслуживал до внедрения удаленных сервисов.

5. Увеличивается скорость и повышается качество обслуживания клиентов.

6. Увеличивается точность совершаемых банковских операций, уменьшается количество возможных ошибок, снижаются операционные риски банка.

7. У банка появляются возможности для решения важных дополнительных задач, например, предоставление клиенту оперативной информации о новых банковских продуктах или сообщение клиенту о необходимых действиях (своевременном погашении просрочки, окончании срока депозита и т.п.).

8. Повышается конкурентоспособность банка благодаря возможности создания принципиально новых банковских продуктов, быстрого масштабирования и интегрирования банковских услуг с другими финансовыми услугами, использующими удаленный доступ к денежным счетам.

Очевидно, что применение мобильных технологий позволяет ускорить, облегчить и удешевить бизнес-процессы в банках, что ведет к повышению эффективности этих процессов. Однако с другой стороны, за «мобилизацией» бизнес-процессов кроются различные риски и угрозы, которые необходимо соотносить с перспективами и выгодами.

Так, подтвердилась тенденция роста риска, отмеченная экспертами в традиционных ежегодных отчетах в области безопасности систем ДБО) [2]. Разработчики мобильных банк-клиентов не уделяют достаточного внимания вопросам безопасности приложений, не следуют руководствам по безопасной разработке. Зачастую отсутствуют процессы разработки безопасного кода и соответствующей архитектуры. Оказалось, что все мобильные 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 операции jailbreak. Около 22% приложений для Android неправильно используют механизмы межпроцессного взаимодействия, тем самым фактически позволяя сторонним приложениям обращаться к критичным банковским данным.

Каждая мобильная операционная система (ОС) имеет свою специфику, в каждой из них можно обнаружить большое количество как новых, так и хорошо известных уязвимостей.

Развитие средств и методов обеспечения безопасности в области информационных технологий (ИТ) всегда отстает от развития самих ИТ. Однако для мобильных технологий этот разрыв существенно шире, чем для стандартных ИТ: постоянно выпускаются новые модели мобильных платформ и ОС с новыми функциями, количество мобильных приложений, включая корпоративные, исчисляется сотнями тысяч, развиваются средства управления. Между тем, средства и методы обеспечения безопасности мобильных технологий уже частично сформированы и продолжают развиваться как самостоятельное направление информационной безопасности (ИБ). Применение средств и методов обеспечения ИБ мобильных технологий в бизнесе позволяет существенно снизить риски «мобилизации» бизнес-процессов. Однако для этого, как минимум, необходимо [2]:

• Четко соотносить перспективы и выгоды, с одной стороны, риски и угрозы, а также затраты на их минимизацию до приемлемого уровня – с другой.

• Знать или хотя бы иметь представление о средствах и методах обеспечения информационной безопасности при использовании мобильных технологий в бизнесе.

• Иметь четкую, внятную и гибкую политику безопасности при использовании мобильных технологий, обеспечить ее безусловное выполнение.

• Иметь подготовленный персонал или доверенных квалифицированных специалистов.

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 хищения денег из мобильных устройств чрезвычайно много, каждый год появляются новые алгоритмы, но вместе с тем растёт и сила противодействия, способная своевременно бороться с угрозами.

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.

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).

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 [3].

По месту расположения приложения выделяют:

- 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.

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.

Компания Digital Security провела аудит безопасности клиентской части приложений на следующих мобильных платформах:

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

В результате этой работы были выявлены следующий типовые угрозы [3]:

– 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.

Компания «Инфосистемы Джет» провела работу и обнародовала свой аналитический отчет по уязвимостям мобильных банковских приложений, функционирующих под управлением iOS, Android и Windows Phone. 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.

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.

В целях защиты мобильных банковских приложений 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.

Для обеспечения защиты от несанкционированного доступа необходимо обновлять ПО на устройстве, использовать программные средства защиты и повышать осведомленность пользователей в вопросах ИБ.

Кроме того, необходима 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 наличие jailbreak устройства (iOS) или 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.

Поэтому в целях обеспечения ИБ мобильных приложений необходимым является [2]:

- 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.

Изложенное выше показывает, что мобильный банкинг содержат уязвимости и недостатки, которые могут привести к хищению денежных средств. Уровень их защищенности 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.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Дадабаева Р.А., Саитходжаева Р.Ш. Мобильный банкинг в системе дистанционного банковского обслуживания. «Халкаро молия ва хисоб» Илмий электрон журнали. №2, 2017

2. Миноженко А. Безопасность мобильных банковских приложений. Журнал. "Information Security/ Информационная безопасность" #4, 2013.

3. Безопасность мобильных технологий в корпоративном секторе. Общие рекомендации. Сайт АРСИБ: *www.aciso.ru.*