Оценка безопасности банковских приложений для мобильных устройств

Носкова И.П.
бакалавр, СПбПУ, Россия, г.Санкт-Петербург
Батаев А.В.
к.т.н. доцент кафедра
"Финансы инновационных и производственных систем"
СПбПУ Россия, г.Санкт-Петербург

Мобильные приложения банков стали настоящим прорывом в банковском обслуживании, а среди всех каналов дистанционного банковского обслуживания являются самым перспективным направлением развития. По оценкам экспертов, в 2014 году банковские приложения для мобильных устройств скачали 6 млн пользователей, и на сегодняшний день количество активных пользователей мобильного банкинга в России составляет 17 миллионов. [1] Учитывая растущую популярность мобильных банковских приложений, существуют опасения относительно их безопасности, так как пробелы в системах защиты могут повлечь за собой финансовые потери тысяч пользователей.

Специализированное мобильное приложение, работающее на основных платформах и отвечающее всем потребностям клиентов, является обязательной составляющей и конкурентным преимуществом любого современного банка. Однако, банки пока не ставят безопасность своих приложений на первое место. Главными причинами являются, во-первых, значительное удорожание разработки приложения, а во-вторых, многократное тестирование, доработка и устранение неисправностей увеличивают время подготовки продукта.

Каждый банк по-своему работает в направлении увеличения безопасности каналов обслуживания. Например, Райффайзенбанк регулярно проверяет код своих приложений на безопасность, а также осуществляет тест на проникновение после каждого обновления. Служба безопасности «ВТБ24» тоже регулярно анализирует уязвимость своих приложений, а Тинькоффбанк вообще не использует внешних подрядчиков для разработки и обслуживания своих программ, этим занимается собственная внутренняя команда программистов. Тем не менее, исследования на уязвимость показывают, что пока на российском рынке не существует ни одного полностью безопасного мобильного приложения [2,3,4,5].

Все атаки на каналы ДБО можно разделить на 3 типа [6,7,8,9]:

1. Физический доступ к устройству клиента.
   При физическом доступе преступник может получить доступ к файловой системе. Если приложение хранит идентификационные данные или другие критичные данные в открытом виде либо данные "утекают" в открытом виде, то для злоумышленника несложно получить эти данные и украсть деньги.
2. Атака «Man in the middle», «MitM» или «человек посередине».
   Данная атака является атакой непосредственно на канал связи: в ходе классической атаки перехватываются данные между устройством клиента и сервером. Для этого необходимо находиться в одной сети с жертвой, к примеру, в публичной сети Wi-Fi, или использовать поддельные беспроводные точки доступа. Для осуществления необходима уязвимость в мобильном приложении, а именно некорректная работа с шифрованием передаваемых данных или полное отсутствие шифрования данных. В результате киберпреступник может

получать и подменять передаваемые данные, что в итоге приводит к краже денежных средств со счета клиента.

3. Загрузка на устройство клиента вредоносной программы различными способами.
   После установки вредоносного приложения на устройство злоумышленник может поднять свои привилегии в системе и получить удаленный доступ к устройству с полными правами доступа, что приводит к полной компрометации устройства: преступник сможет украсть критичные данные пользователя мобильного банкинга или подменять данные платежных операций.

Для каждого типа атак существуют свои способы защиты. Так, для защиты от непосредственно физического доступа к устройству необходимо использовать криптографические возможности устройства, шифровать данные и при необходимости удаленно очищать данные, а также осуществлять постоянный контроль защищенности приложения, который поможет выявить возможные уязвимости.

При атаке «MitM» необходима правильная реализация работы с криптографическим протоколом SSL, который обеспечивает безопасную передачу данных. Также рекомендуется в мобильном приложении при подключении к серверу доверять только SSL-сертификату банка.

Для защиты от вредоносных приложений необходимо постоянно обновлять программное обеспечение на устройстве, использовать программные средства защиты и, что важно, повышать осведомленность пользователей в вопросах информационной безопасности.

Безопасность мобильного банковского приложения – это целый комплекс мер, начиная с архитектуры приложения, разработки с учетом всех возможных уязвимостей, а также непрерывный контроль за его работой и регулярное обновление и доработка.

Угрозы безопасности мобильных банковских приложений создают риски компрометации данных клиентов, хищения денежных средств и нанесения ущерба репутации банка. По мнению экспертов, разработчики мобильных приложений не уделяют достаточного внимания вопросу безопасности приложения, не следуют руководствам по безопасной разработке. В первую очередь это связано с тем, что этого не требует заказчик, то есть банк.

Проведенные исследования показывают, что мобильные банки содержат уязвимости и недостатки, которые могут привести к финансовым потерям клиентов. При этом 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.

У киберпреступников есть множество путей реализации атак. При этом затраты на проведение атаки в реальности могут быть весьма низкими по сравнению с возможной выгодой.

Современные средства защиты для мобильных устройств - антивирусы, MDM-решения и т.д. - помогают сократить риск, но не решают всех проблем. Безопасность должна внедряться еще на этапе проектирования системы и присутствовать на всех этапах жизненного цикла программы, включая разработку и внедрение. Необходимо осуществлять анализ кода, защищенности приложения в целом, тестирование на проникновение и т.д.

Риски при использовании мобильных банковских приложений обратно пропорциональны защищенности приложения. Поэтому необходим комплексный контроль их защищенности. Специалисты по информационной безопасности банков должны уделять безопасности приложений не меньше внимания, чем безопасности интернет-банков.

Учитывая возрастающую популярность мобильных приложений у клиентов, ежегодно

увеличивающиеся объемы транзакций и, соответственно, значительное увеличение случаев взлома и хищения денежных средств, банки должны уделять намного больше внимания безопасности, а не удобству и простоте использования.

СПИСОК ЛИТЕРАТУРЫ

1. П. Кантышев «Мобильность в ущерб безопасности». [Электронный ресурс]. http://www.vedomosti.ru/newspaper/articles/2015/02/24/mobilnost-v-uscherb-bezopasnosti (Дата обращения: 09.10.2015).
2. Д. Евдокимов «Безопасность мобильного банкинга: возможность реализации атаки «MitM». [Электронный ресурс]. http://www.dsec.ru/ipm-research-center/research/a_security_analysis_of_mobile_banking_applications_f... (Дата обращения: 09.10.2015).
3. С. В. Широкова Управление проектами. Управление проектами внедрения информационных систем для предприятия, учебное пособие / С. В. Широкова; М-во образования и науки Российской Федерации, Санкт-Петербургский гос. политехнический ун-т. Санкт-Петербург, 2012.
4. Ильин И.В., Широкова С.В., Эссер М. Управление проектами основы теории, методы, управление проектами в области информационных технологий, учебное пособие, Санкт-Петербург, СПбПУ, 2015, 311 с.
5. Ilin I.V., Lyovina A.I., Shirokova S.V., Hellmann N., Dubgorn A.S. Штil® and prince2® in practice, учебное пособие, Санкт-Петербург, 2014, 128 с.
6. А. Миноженко «Безопасность мобильных банковских приложений». [Электронный ресурс]. http://www.itsec.ru/articles2/25kadr/bezopasnost-mobilnyh-bankovskih-prilozheniy (Дата обращения: 09.10.2015).
7. Батаев А.В. Оценка экономической эффективности внедрения банковских смарт-карт, Молодой ученый. 2015. № 4 (84). С. 334-341
8. Батаев А.В. Анализ использования облачных сервисов в банковском секторе, Молодой ученый. 2015. № 5 (85). С. 234-240.
9. Батаев А.В. Перспективы внедрения облачных технологий в банковском секторе России, Научно-технические ведомости санкт-петербургского государственного политехнического университета, Экономические науки. 2014. № 2. С. 156.