Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.53

Глушень
Руслан, Русланович

Методы и алгоритмы безопасного хранения данных в мобильных устройствах

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1–40 80 02 «Системный анализ, управление и обработка информации»

Научный руководитель
Матвеенко Владимир
Владимирович
кандидат физико-математических
наук, доцент

Минск 2020

ВВЕДЕНИЕ

Люди стремятся защитить свои личные данные и недопустить их утечку к недоверенным лицам. Однако часто при использовании информационных сервисов пользователи даже не подозревают как используются их данные. Зачастую причиной недобросовестной защиты является отнюдь не намерение заработать на этой информации, а трудозатраты необходимые для реализации и отсутствие знаний.

Что же касается в частности ОС Android: за относительно короткий период времени система стала самой популярной мобильной платформой в мире. Хотя изначально она был разработана для смартфонов, теперь она работает на планшетах, телевизорах, автомобилях, голосовых помощниках и т.д..

Исходя из того, что исходный код системы открыт и кастомизируем, многие злоумышленники используют эти факты для поиска уязвимостей. Кроме того, при официальном обнародовании уязвимостей, не все производители устройств стараются исправить проблему с помощью специализированных обновлений системы, и тем более отзывом устройств с рынка.

Однако данные факторы не мешают мобильным устройствам набирать все большую популярность среди пользователей. Исходя из этого, борьба за увеличение числа покупателей чаще способствует внедрению новых возможностей в операционные системы, а не исправлению старых уязвимостей.

Таким образом, даже сейчас в ОС существует много известных и неясных проблем, связанных с безопасностью.

Конечно, в последние годы Android стал более устойчивым к распространенным методам атак, его изоляция приложений (песочница) была усилена, последние версии Android имеют новые функции безопасности, такие как ограниченная поддержка пользователей, введение полного шифрования диска, аппаратное хранилище учетных данных, а также поддержка централизованного управления и предоставления устройств, поддержка биометрической аутентификации.

Однако в последнее время конфиденциальность пользовательских данных вышла на новый уровень, и даже в наше время проблема безопасного хранения стоит очень остро.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Защита данных – непростая задача, особенно, когда специального образования нет и средств на привлечение специалиста также нет. В современных реалиях, мобильные устройства занимают важную роль в жизни человека. Однако очень редко в мобильных устройствах обеспечивается должный уровень защиты данных пользователя или приложения. Одной из причин этого явления служит отсутствие стандартизированного подхода к решению проблемы.

Степень разработанности проблемы

Способов шифрования данных на сегодняшний день очень много, начиная от алгоритмов с тысячелетней историей и заканчивая малоизвестными алгоритмами, применяемыми лишь в очень специфических случаях.

Существуют сервисы, которые за оплату способны произвести инспекцию вашего программного продукта, однако зачастую проверка надежности результатов инспекции стоит под большим вопросом.

Среднестатистический разработчик редко сталкивается с задачами обеспечения безопасности хранения данных. В большинстве же случаев при попытках реализации допускаются типичные ошибки, которые никак не проверяются и соответственно не обнаруживаются.

Цель и задачи исследования

Целью магистерской диссертации является разработка моделей и алгоритмов безопасного хранения данных на мобильных устройствах на основе ОС *Android*.

Объектом исследования являются проблемы, связанные с защищенным хранением данных в ОС *Android*.

Предметом исследования являются алгоритмы, позволяющие безопасно сохранять приватные данные и способы их реализации.

Для достижения поставленной цели необходимо было решить следующие задачи:

1. Провести обзор и анализ проблем связанных с защитой данных на мобильном устройстве.

2. Провести анализ решений, применяемых для обеспечения защиты данных на мобильном устройстве.

3. Разработать простые и доступные в реализации базовые алгоритмы сохранения данных в мобильном приложении.

Теоретическая и методологическая основа исследования

При проведении исследования и написании диссертации использованы научные публикации, техническая документация и интернет-источники, посвященные вопросам компьютерного проектирования электронных систем, разработке многофункциональных клиент-серверных приложений, принципам работы и использования криптографии.

Для решения поставленных задач использованы следующие методы исследования: анализ, синтез, обобщение, сравнение, логический и графический методы.

В работе применялись моделирование и методы компьютерного проектирования.

Научная новизна

Научная новизна заключается в создании простого, доступного и надежного алгоритма шифрования данных, в основе которого лежат уникальные пользовательские данные, не сохраняемые в открытом или зашифрованном виде.

Теоретическая значимость работы заключается в анализе типичных ошибок, связанных с хранением приватных данных, и способов их разрешения.

Практическая значимость работы заключается в разработанном алгоритме, простом, доступном и надежном в реализации.

Основные положения, выносимые на защиту

1. Обзор и анализ проблем связанных с защитой данных на мобильном устройстве.

2. Анализ решений, применяемых для обеспечения защиты данных на мобильном устройстве.

3. Алгоритмы сохранения данных в мобильном приложении, их простота, доступность и надежность.

СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, общей характеристики работы, четырех глав, заключения, библиографического списка и приложения.

В первой главе произведен анализ проблем связанных с хранением данных на мобильных устройствах. Изучены основные виды атак на мобильное приложение, основные уязвимости при хранении данных, вопросы реверс-инжиниринга, вопросы рутования устройств, проблемы скрытой для пользователя посторонней функциональности.

Во второй главе представлено исследование способов безопасного хранения данных. Есть несколько общих для всех мобильных платформ моментов, которые следует соблюдать при разработке: хранение излишних КВД, шифрование КВД, использование встроенных механизмов автоматического шифрования в СУБД, работа при использовании ассиметричного шифрования, использование «самописных» алгоритмов шифрования и защиты, манипуляции с КВД перед выходом за пределы приложения, работа приложения, если удалось понять, что запуск производится на зараженном устройстве, использование встроенного браузера и встроенного веб-движка в операциях с КВД, автоматическая или ручная обфускация кода, защита пользовательским кодом, функционирование клиент-серверного приложения, работа с датами, логгирование и отладочные функции в релизных сборках приложений, принудительный запрет на программное создание скриншотов окна приложения. А также в разделе описаны специфичные для операционных систем способы защиты данных.

В третьей главе произведен анализ методов шифрования данных: симметричных и асимметричных алгоритмов, шифров (*ciphers*) и кодов (*codes*), хеш-функций. Изучены вопросы увеличения надежности защиты различных видов шифрования. Разработан алгоритм безопасного хранения данных, в долговременной памяти мобильного устройств а, на основании пользовательского ввода(*PIN*-кода), *Password-Based Key Derivation Function* стандарта формирования ключа на основе пароля и соли, *Authenticated Encryption with Associated Data(AEAD)* режима блочного шифрования. Также разработан способ безопасного хранения данных на клиентской стороне при клиент-серверном взаимодействии, разработанный на основании предыдущего алгоритма.

В четвертой главе представлен пример использования результатов исследования в *Android*-приложении, а также продемонстрирована работа данного приложения, основной функционал которого включает в себя: аутентификация с помощью *PIN*-кода, сохранение данных зашифрованных с помощью введенного пароля, извлечение данных расшифрованных с

помощью введенного пароля, проверка соответствия введенного пароля с ранее сохраненным. Также продемонстрированы файлы, которые остаются в долговременном хранилище мобильного устройства в результате работы приложения.

В приложении представлен листинг кода, отвечающего за реализацию результатов исследования, приведенную в четвертой главе.

ЗАКЛЮЧЕНИЕ

Мобильные приложения – это постоянно развивающаяся система с историческим прошлым и огромной аудиторией пользователей. Современное общество нацелено на потребление продуктов в сфере услуг, которые также составляют большинство приложений в магазинах ОС.

Большинство приложений требуют, чтобы пользователи предоставили личные данные для проверки или добавления нового пользователя. Часто эти данные должны храниться локально на устройстве. Однако не все разработчики прилагают усилия для защиты этих данных от вторжений. Во многом это связано не с некомпетентностью разработчиков, а с отсутствием единого способа защиты этих данных.

Соответственно, в ходе исследования были изучены основные виды атак на мобильное приложение. Представлено исследование способов безопасного хранения данных, а также описаны специфичные для операционных систем способы защиты данных. Произведена разработка алгоритмов безопасного хранения данных, в долговременной памяти мобильного устройства, а также в произведен анализ методов шифрования данных.

В итоге произведено объединение различных моделей и алгоритмов для простой в реализации и эффективной защиты личных данных пользователя и конфиденциальных данных приложения, необходимых для его правильной работы.

На основании полученных результатов было разработано демонстрационное приложение для мобильной операционной системы, которое позволяет пользователям сохранять на жестком диске устройства приватные данные в зашифрованном виде.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1-А Глушень, Р.Р. Исследование частых ошибок при хранении данных в мобильных приложениях / Глушень, Р.Р. // Материалы 56-ой научной конференции студентов, магистрантов, аспирантов УО «Белорусский государственный университет информатики и радиоэлектроники» Минск, БГУИР, 2020.