ИНФОРИНО 2020
Москва, Россия
14-17 апреля 2020 г.

Развитие средств защиты информации в операционной системе Android

Докладчик:
Павел
Хорев
НИУ «МЭИ»

Авторы:

П.Б. Хорев, Е.П. Кандаурова

Национальный исследовательский университет «МЭИ», Москва

Развитие средств защиты информации в операционной системе Android

Обеспечение информационной безопасности при использовании мобильных устройств основано на многоуровневом подходе к построению системы безопасности. В операционной системе (ОС) устройства должны присутствовать разнообразные средства защиты конфиденциальной информации, позволяющие защитить мобильное устройство от угроз различного рода.

Развитие средств защиты информации в операционной системе Android

Средствами защиты информации в устройстве могут являться средства разграничения прав доступа приложений к объектам ОС и данным владельца устройства, средства идентификации и аутентификации владельца, криптографические средства, антивирусные программы.

Развитие средств защиты информации в операционной системе Android

Целью работы являлась разработка проекта специализированной ОС на базе ОС Android с расширенными средствами защиты информации. Для достижения поставленной цели были решены следующие задачи:

1) анализ средств информационной безопасности в ОС Android;
2) проектирование дополнительных средств идентификации и аутентификации пользователя мобильного устройства;
3) проектирование дополнительных средств ограничения прав устанавливаемых приложений на доступ к различным объектам ОС и пользовательским данным,
4) проектирование дополнительных криптографических средств (шифрования пользовательских данных и снабжения передаваемой информации электронной подписью).

Развитие средств защиты информации в операционной системе Android

Основные методы защиты информации в мобильном устройстве:

- блокировка устройства;
- криптографические методы;
- запрет использования коротких и простых паролей;
- отслеживание поведения приложений;
- установка только проверенных приложений;
- использование средств антивирусной защиты;
- ограничение данных, передаваемых облачным сервисам.

Развитие средств защиты информации в операционной системе Android

Основные недостатки средств защиты информации в ОС Android:

- возможность для владельца устройства разрешить его автоматическую разблокировку дома, с помощью доверенного устройства Bluetooth, по снимку лица;
- отсутствие возможности запрета на использование приложениями так называемых обычных разрешений и недостаточная детализация потенциально опасных разрешений.

Развитие средств защиты информации в операционной системе Android

- Для усиления механизма идентификации и аутентификации владельца устройства при его разблокировке предлагается совместно использовать пароль и отпечаток пальца. Это также даст пользователю возможность ввода пароля для работы «под принуждением», когда разблокировка осуществляется владельцем устройства недобровольно. При этом доступ к конфиденциальной информации владельца будет невозможен.
- После реализации данного предложения владельцу устройства потребуется задать два пароля: пароль для «обычного» входа в устройство, пароль для входа «под принуждением».

Развитие средств защиты информации в операционной системе Android

Также пользователю будут предоставлены следующие возможности:

- возможность настраивать под свои требования ограничения на минимальную длину и сложность пароля;
- возможность выбрать приложения, которые необходимо будет блокировать в случае входа в устройство «под принуждением»;
- возможность отключить разблокировку устройства методом, предоставленным разработанным приложением, если пользователю не требуется дополнительная защита его устройства.

Развитие средств защиты информации в операционной системе Android

Также предлагается внести изменения в систему управления разрешениями устанавливаемых на устройстве приложений:

- при установке приложений уведомлять пользователя обо всех его разрешениях, в т.ч. и из категории обычных;
- позволять пользователю отзывать не только разрешения из категории опасных, но и из категории обычных;
- при одобрении разрешения из категории опасных, относящегося к некоторой группе, приложение получает только одобренное пользователем разрешение, а остальные разрешения из этой группы не одобряются приложению автоматически.

Развитие средств защиты информации в операционной системе Android

- При реализации предложенных изменений не потребуется вносить какие-либо изменения в файл манифеста устанавливаемого приложения.
- При установке приложений будут отображаться два списка разрешений: необходимые разрешения из категории обычных и разрешения из категории опасных. Другие изменения интерфейса при установке приложения не потребуются.

Развитие средств защиты информации в операционной системе Android

Для повышения стойкости шифрования пользовательских данных на устройстве, в том числе и передаваемых по сети, предлагается внести следующие изменения:

- добавить поддержку нескольких алгоритмов шифрования, например, Triple DES и алгоритмов из ГОСТ Р 34.12-2015;
- добавить возможность выбора длины ключа, применяемого для шифрования данных при использовании алгоритма AES;
- для каждого блока шифруемых данных использовать свой уникальный ключ;
- каждый такой уникальный ключ шифровать ключом, полученным из пользовательского пароля или PIN-кода.

Развитие средств защиты информации в операционной системе Android

При реализации этого предложения владелец устройства будет иметь возможность задать ограничения на минимальную длину и сложность парольной фразы, используемой для генерации ключа шифрования и расшифрования данных.

Развитие средств защиты информации в операционной системе Android

Для обеспечения дополнительной защиты передаваемой с устройства информации предлагается использовать электронную подпись. Это позволит осуществлять проверку на отсутствие искажения информации в переданном документе с момента формирования подписи (целостность), принадлежность документа владельцу сертификата открытого ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания им переданного документа (неотказуемость).

Развитие средств защиты информации в операционной системе Android

Предлагается использовать схемы построения электронной подписи на основе алгоритмов асимметричного шифрования (например, алгоритма RSA или российского алгоритма электронной подписи, определенного в ГОСТ Р 34.10-2012).

Потребуется реализовать два процесса: подпись передаваемой информации и проверка подписи под полученным документом. Также необходимо будет реализовать вызов хеш-функции для вычисления хеша передаваемой информации перед ее подписанием или проверкой электронной подписи.

Развитие средств защиты информации в операционной системе Android

Для получения сертификата открытого ключа пользователя, который необходим для проверки подписи под полученным документом, предлагаются следующие варианты:

- использование удостоверяющих центров и инфраструктуры открытых ключей (вариант для владельцев устройств, являющихся пользователями корпоративных информационных систем);
- использование сети взаимного доверия владельцев устройств (вариант для частных пользователей).

Развитие средств защиты информации в операционной системе Android

Необходимо также обеспечить защиту закрытого ключа владельца устройства с помощью шифрования ключа. Для доступа к закрытому ключу потребуется ввод парольной фразы для его расшифрования. Предлагается также добавить возможность экспорта зашифрованного закрытого ключа.

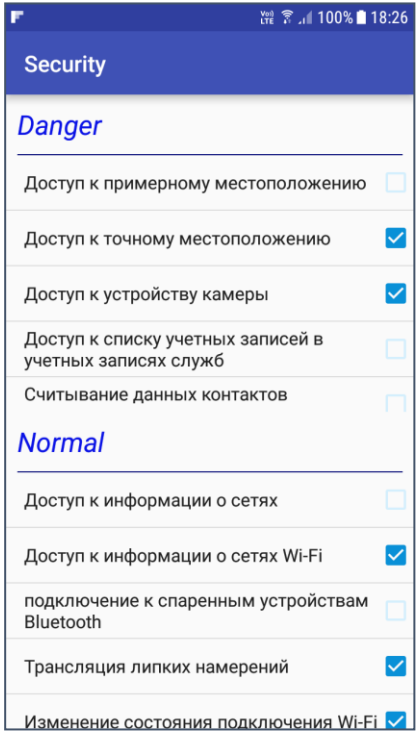
Функция экспорта закрытого ключа может потребоваться в случае кражи или потери устройства, чтобы сохранить для пользователя доступ к закрытому ключу электронной подписи с другого устройства.

Развитие средств защиты информации в операционной системе Android

Для подтверждения эффективности предложенных средств защиты была выполнена их программная реализация. Для этого были использованы интегрированная среда разработки Android Studio и объектно-ориентированный язык программирования Java. Для реализации шифрования пользовательских данных и средств электронной подписи передаваемых данных использовался пакет javax.crypto.

Развитие средств защиты информации в операционной системе Android

Примеры интерфейса разработанных средств защиты



Список разрешений после изменения

Выбор алгоритма и режима блочного шифрования, длины ключа, шифруемого файла

Развитие средств защиты информации в операционной системе Android

Преимущества использования полученных результатов:

1) Возможность реализации входа в устройство «под принуждением» для скрытия наличия на нем ценной информации.
2) Возможность независимого управления паролями (их минимальной длиной и сложностью), используемыми для аутентификации владельца устройства, шифрования и электронной подписи ценной информации на устройстве.
3) Возможность включения криптографической защиты на уровне отдельных пользовательских файлов.
4) Возможность более «тонкой» настройки прав приложений, устанавливаемых владельцем устройства, с функциями просмотра и отзыва таких прав уже после установки приложения.

Спасибо за внимание!

Контакты докладчика:

Павел Хорев

НИУ «МЭИ»

pbkh@yandex.ru

www.appmat.ru