ТЕСТИРОВАНИЕ ТЕХНОЛОГИЙ СОЗДАНИЯ, УПРАВЛЕНИЯ И ЗАЩИТЫ ИНФОРМАЦИИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

В.В. Маликов, А.Н. Бойко, Д.В. Калинин

Согласно отчетным данным по работе защитного алгоритма Google Play Protect, встроенного в приложение Google Play Store на всех авторизованных устройствах на Android и проверяющего устройство при установке/обновлении приложений из каталога Google Play или стороннего источника на признаки потенциально вредоносного приложения (Potentially Harmful Applications, PHA), выявляется значительное количество таких вредоносных приложений.

Для оценки технологического уровня и степени безопасности 3 специализированных приложений КФО для Android проведено их исследование на предмет возможности реверсного инжиниринга программного обеспечения (software reverse engineering, SRE) с изучением структуры построения, алгоритмов функционирования, технологий защиты информации и др.

Для сохранения конфиденциальности: названия КФО заменены порядковыми номерами, идентификаторы приложений изменены, листинг (дизассемблер/декомпилятор) исполняемого кода (classes.dex) и алгоритмы функционирования не приводятся, согласисие владельцев получено.

По результатам исследования можно сделать следующий вывод: APK-сборки (.apk) 3 типовых КФО могут быть подвергнуты реверсному инжинирингу с получением информации по общей структуре, общему алгоритму функционирования (файл AndroidManifest.xml), листингу (дизассемблер/декомпилятор) исполняемого кода (файл classes.dex), построению функциональных графов (декомпилятор) базовых функций (файл classes.dex).

В качестве защиты APK-сборок (.apk) 2 типовых КФО использовался базовой алгоритм (включая обфускацию кода от ProGuard из комплекта Android Studio), в APK-сборке (.apk) 1 типовой КФО были обнаружены признаки дополнительной защиты (усиленная обфускация кода) инструментом, отличным от ProGuard.

ТЕСТИРОВАНИЕ ТЕХНОЛОГИЙ СОЗДАНИЯ И УПРАВЛЕНИЯ СЕТЕВЫМИ РЕСУРСАМИ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

В.В. Маликов, В.А. Гайшун, В.Н. Ярошевич

Исследованы технологии создания и управления сетевыми ресурсами (сайтами) на примере 24 кредитно-финансовых организаций (КФО) Республики Беларусь. Проведено тестирование уровня информационной безопасности (ИБ) библиотек «JavaScript», а также алгоритмов реализации шифрования на основе SSL-сертификатов для сайтов КФО.

Проведенное углубленное тестирование библиотек «JavaScript» сайтов основного домена КФО, позволило выявить детальный перечень уязвимостей ИБ, которые уже были внесены и описаны в базах экспертных знаний (тип потенциальных атак: Regular Expression Denial of Service, Cross-site Scripting, Cross-site Scripting in dialog close Text). Следует отметить, что только 4 сайта основного домена КФО (17 %) не имеют уязвимостей библиотек «JavaScript». Для исследования уровня ИБ сайтов основного домена КФО дополнительно были выполнены оценка наличия и типа используемого SSL-сертификата и оценка качества реализации алгоритма защищенного соединения на основе SSL-сертификата (уровни оценки безопасности: A/A+, B, C, F; где A/A+ - высший уровень, F – низший уровень).

Результаты исследования показали:

– на 2 сайтах КФО (8 %) – нет SSL-сертификата (не реализуется защищенное соединение);

– на 7 сайтах КФО (29 %) – имеются уязвимости при реализации защищенного соединения на основе SSL-сертификата (тип потенциальных атак: Forward Secrecy, Diffie-Hellman key exchange parameters).