УДК 004.056.5

П. П. Урбанович, проф., д-р техн. наук,
А. В. Годун, магистрант
(БГТУ, г. Минск)

БЕЗОПАСНОСТЬ ДАННЫХ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

При разработке мобильных приложений следует учитывать, что данные, которыми оперируют эти приложения, могут представлять определенный интерес для третьих лиц [1]. Особенно это важно в свете распространения мобильных приложений на все сферы электронных услуг, включая финансовые, банковские операции, хранение и передачу личных данных.

Было произведено аналитическое исследование атак на мобильные приложения. Анализ выполнен с учетом рекомендаций и классификации атак и уязвимостей сообщества OWASP (Open Web Application Security Project). Список OWASP состоит из 10 самых опасных атак на web-приложения. Этот список известен как OWASP TOP-10 [2]. В нем сосредоточены самые опасные уязвимости. Основными являются следующие:

1. Декомпиляции файла приложения.
2. Перехват данных, передаваемых по сети.
3. Получение прав суперпользователя.

Основные уязвимости мобильных приложений:

1. Хранение критически важных данных в коде.
2. Использование незащищенных локальных хранилищ.
3. Хранение важных данных в защищенных хранилищах, но в открытом виде.
4. Перевод части функционала во встроенный web-браузер.

Разработано программное средство для проверки системных файлов на устойчивость по отношению к вредоносным программам. Для этого выбран язык программирования Java и среда разработки Android Studio. Пользователь может проверить системные файлы на наличие вредоносной программы. Для этого верифицируется валидный хеш системного файла с текущим хешем. Используется алгоритм хеширования md5.

ЛИТЕРАТУРА

1 Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации / П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

2 OWASP TOP-10: практический взгляд на безопасность веб-приложений [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/simplepay/blog/258499 / – Дата доступа: 10.02.2018.