УДК 004.056 **Информационные технологии**

Комаров А. О., *магистрант кафедры ЖАТС*
Российский университет транспорта (МИИТ)
Россия, г. Москва

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Аннотация: В статье приведена статистика использования мобильных приложений за последние несколько лет, а также рассмотрены основные рекомендации руководства Open Web Application Security Project (OWASP) Mobile Application Security Verification Standard (MASVS) по обеспечению безопасности приложений.

Ключевые слова: мобильные приложения, безопасность, защита, угроза, уязвимость, iOS, Android.

Abstract: the article presents statistics on the use of mobile applications over the past few years, as well as the main recommendations of the open Web Application Security Project (OWASP) Mobile Application Security Verification Standard (MASVS) on application security.

Keywords: mobile applications, security, protection, threat, vulnerability, iOS, Android.

Мобильные приложения стали неотъемлемой частью нашей повседневной жизни. Мы общаемся при помощи мессенджеров, переводим деньги через онлайн-банкинг, работаем удаленно через бизнес-приложения и это лишь малая часть возможностей, которые стали доступны нам благодаря мобильным устройствам. В 2018 году количество загрузок мобильных приложений по всему миру достигло 194 миллиардов [1]. App Annie

прогнозирует, что общее количество загрузок приложений достигнет 260 миллиардов в 2022 году [2].

Согласно статистике, Marketing Land большая часть времени, проводимого в Интернете, сосредоточена в приложениях для смартфонов – 57%, далее по популярности следует использование компьютеров – 34% и планшетов – 9% [3]. Учитывая, что планшеты также относятся к мобильным устройствам, можно сделать вывод, что общее время использования мобильных приложений составляет 66%, и с каждым годом популярность приложений только растет. На рисунке 1 приводится статистика времени, проведенного за использованием устройств по возрастным категориям. Те, кто в возрастной группе 18-24, проводят меньше всего времени за компьютером, в то время как те, кто в категории 65 и старше – наоборот.

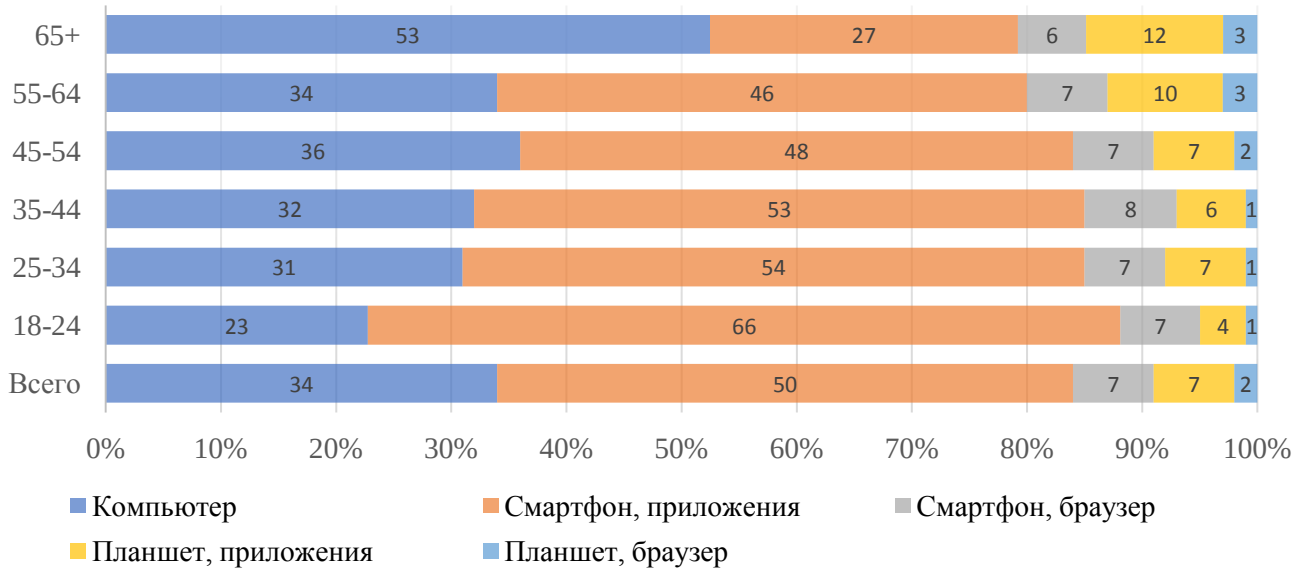

Рисунок 1. Мировое время, проведенное за использованием устройств

Кроме того, статистика App Annie The State of Mobile 2019 показывает, что чаще всего в 2018 году пользовались социальными и коммуникационными приложениями, на которые приходилось 50% времени, проведенного в приложениях по всему миру. Видеоплееры и редакторы также были среди самых быстрорастущих категорий по этому показателю, а время использования

таких приложений выросло на 125% между 2016 и 2018 годами. Другие наиболее быстрорастущие категории – развлечения (120%), финансы (65%) и утилиты (55%). Время, потраченное на использование этих пяти быстро растущих категорий приложений, в совокупности увеличилось на 575%, сообщает App Annie. На рисунке 2 показана диаграмма использования популярных категорий приложений за период с 2016 по 2018 года в млрд. часах [2].

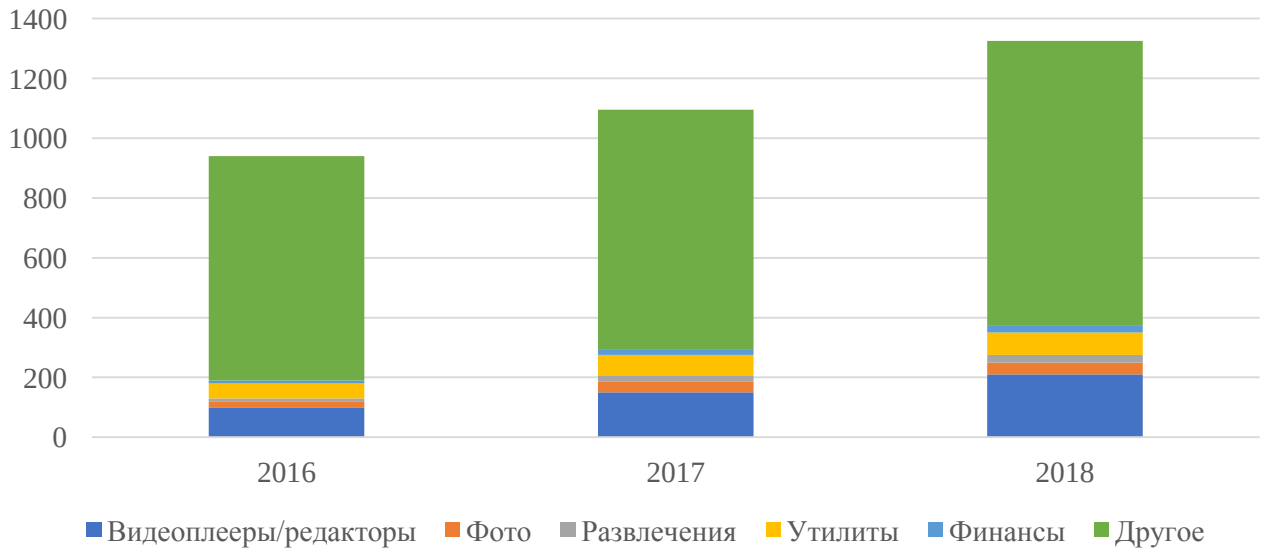

Рисунок 2. Суммарное время в млрд. часах, проведенное в популярных категориях приложений за 2016-2018 годы

Учитывая факты, описанные выше, что мобильные приложения с каждым годом набирают популярность, разработчики столкнулись с тем, что им необходимо понимать, насколько их приложения безопасны для использования и как обеспечить максимальную защиту пользовательских данных.

Сообщество Open Web Application Security Project (OWASP) разработало практическое руководство Mobile Application Security Verification Standard (MASVS) [4]. Данный стандарт предназначен для мобильных разработчиков, аналитиков, системных архитекторов, тестировщиков и всех тех, кто хочет повысить безопасность своих мобильных приложений.

В документе собраны лучшие практики по обеспечению безопасности мобильных приложений, рекомендации не зависят от операционной системы, а сам стандарт открыт и постоянно обновляется благодаря энтузиастам со всего мира. В стандарте описано восемь направлений защиты:

- Архитектура приложения (Architecture);
- Хранение данных и приватность (Data storage);
- Криптография (Cryptography);
- Управление сессиями и аутентификация (Authentication);
- Передача данных (Network Communication);
- Взаимодействие с платформой (Platform Interaction);
- Качество кода (Code Quality);
- Защита от модификаций и отказоустойчивость (Resiliency).

Стандарт состоит из трех уровней, обеспечивающих безопасность:

- Первый уровень содержит 43 рекомендации безопасности;
- Второй уровень дополняет первый еще 13 рекомендациями;
- Третий уровень абстрагирован от двух других и нужен для противодействия реверс-инжинирингу и модификации кода.

Первый уровень (standard security) подходит для всех мобильных приложений, включает основные практики безопасности и предотвращает эксплуатацию распространенных уязвимостей. Например, уровень рекомендует отключить буфер обмена у полей, которые обрабатывают чувствительные данные, потому что к буфер обмену имеют доступ все приложения, а также не записывать чувствительные данные в логи приложения. На рисунке 3 показаны направления защиты, которые покрывает первый уровень.

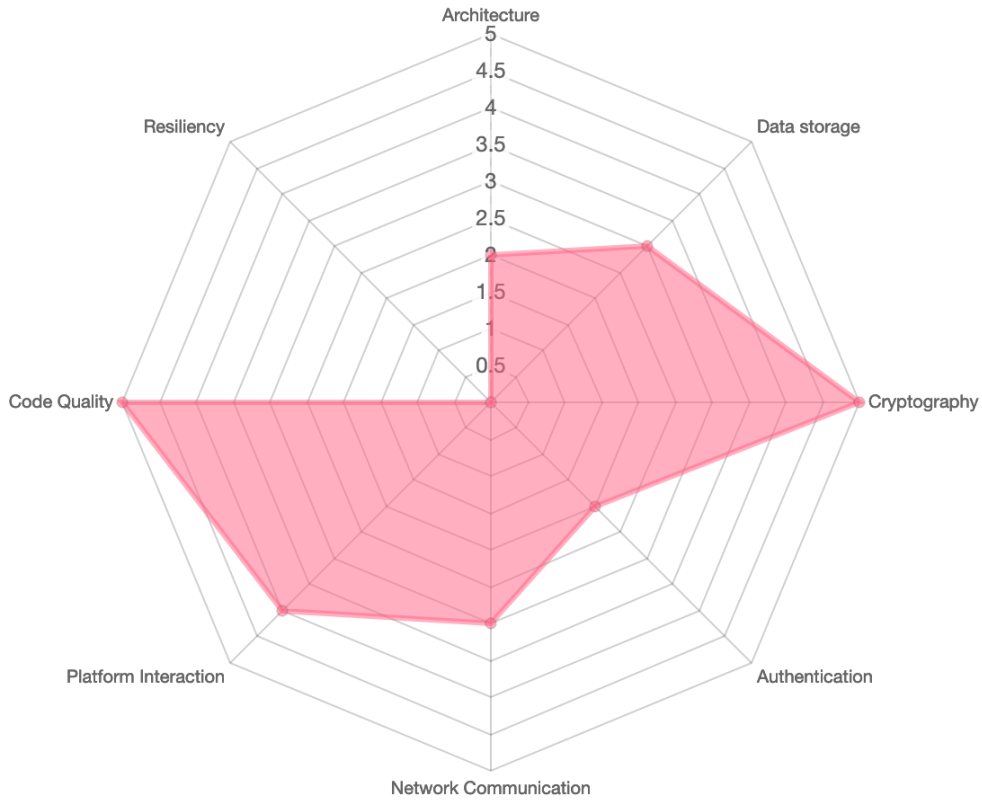

Рисунок 3. Направления защиты, охваченные на первом уровне

Второй уровень (defense-in-depth) предоставляет расширенные возможности управления безопасностью, подходит для мобильных приложений, обрабатывающих конфиденциальные данные, и предотвращает эксплуатацию сложных уязвимостей. При настройке второго уровня используют статистический поиск для проверки исходного кода на функции, классы и ключевые слова, которые чаще всего используются в разработке.

Пример функций и классов:

- android.util.Log.
- Log.d | Log.e | Log.i | Log.v | Log.w | Log.wtf.
- Logger.

Пример ключевых слов:

- System.out.print | System.err.print.
- logfile.
- logging.
- logs.

Также применяют динамический метод, при котором используют все функции приложения, проверяют, что в папке приложения (/data/data/<package-name>) не появляются файлы логов и проверяют logcat на чувствительные данные.

На рисунке 4 показаны направления защиты, охватываемые на втором уровне.

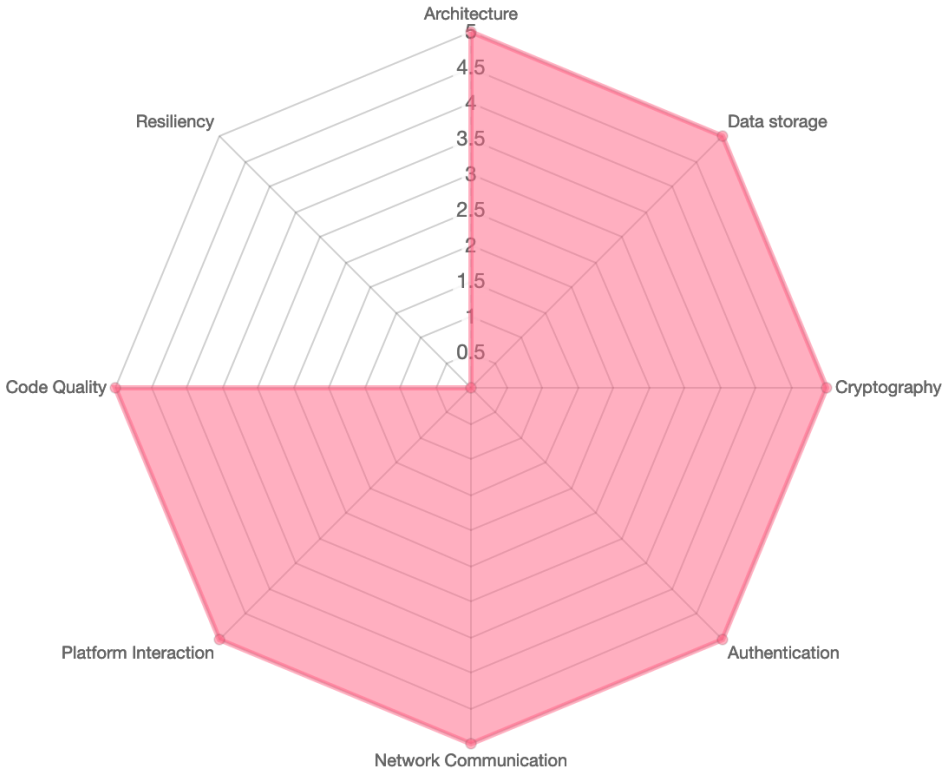

Рисунок 4. Направления защиты, охваченные на втором уровне

Третий уровень (Resiliency against reverse engineering and tampering) используется в дополнение к первому или второму уровням. Данный уровень применим к приложениям, обрабатывающим критичные данные, он служит для защиты интеллектуальной собственности, противодействует реверс-инжинирингу и предотвращает атаки на клиентскую часть сервиса. На рисунке 5 показаны направления защиты, охваченные на третьем уровне.

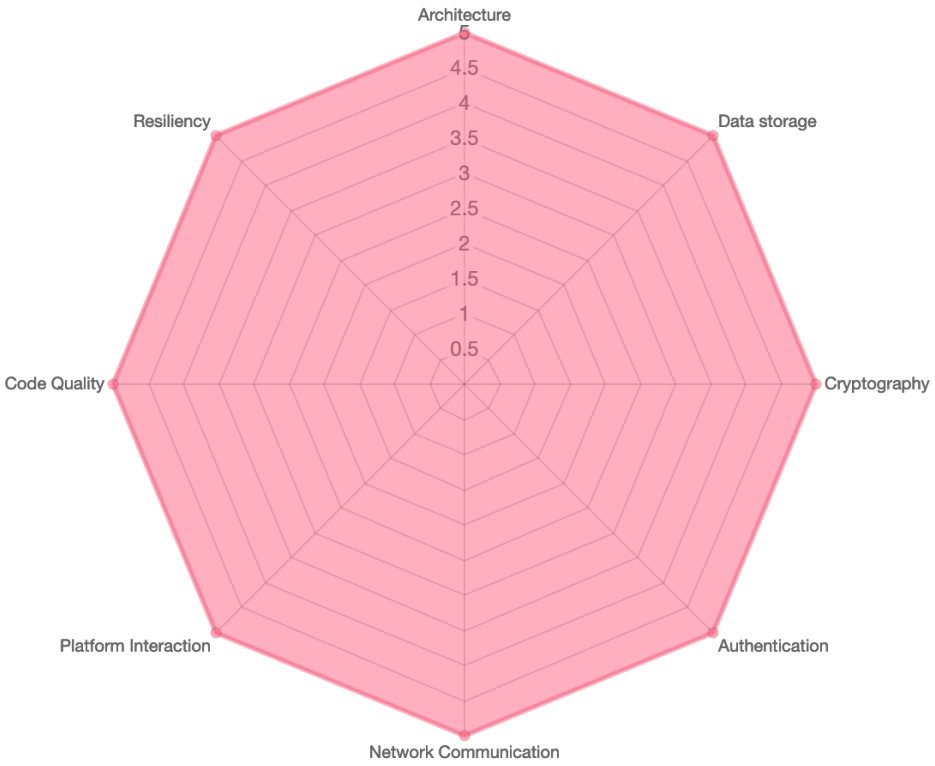

Рисунок 5. Направления защиты, охваченные на третьем уровне

Часто разработчики задаются вопросом, какой уровень выбрать для защиты своего приложения? Допустимы следующие комбинации:

- Использование только первого уровня. Подходит для всех приложений, так как прост в реализации и не усложняет разработку.
- Использование первого и третьего уровней вместе. Подходит для игр (противодействие читерам) или приложений, в которых противодействие модификаций является бизнес требованием.
- Использование только второго уровня. Он требуется для медицинских и финансовых приложений, которые обрабатывают персональные данные пользователей.
- Использование второго и третьего уровней вместе. Этот уровень используют приложения, которые должны работать на всех типах устройств, включая те, где есть Root или Jailbreak.

Необходимо разработать модель угроз для своего мобильного приложения и руководствоваться ей для выбора подходящих уровней безопасности из OWASP MASVS.

Библиографический список:

1. Annual number of global mobile app downloads 2016-2018 [Электронный ресурс]. URL: https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/ (дата обращения: 05.10.2019).

2. The State of Mobile 2019 [Электронный ресурс]. URL: https://www.appannie.com/en/go/state-of-mobile-2019/ (дата обращения: 05.10.2019).

3. Report: More than 50% of digital media time now spent within five mobile apps [Электронный ресурс]. URL: https://marketingland.com/report-50-digital-media-time-now-spent-within-five-mobile-apps-222543 (дата обращения: 05.10.2019).

4. OWASP Mobile Security Testing Guide [Электронный ресурс]. URL: https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide (дата обращения: 05.10.2019).