ПРОБЛЕМЫ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Малюжич М. В., Мирошниченко А. В.

Качалов И.Л. – к.и.н.,доцент

Мобильные телефоны в современном мире являются не просто средством связи, а устройством, которое содержит уязвимые персональные данные, несанкционированный доступ к которым может привести к непредсказуемым результатам. В настоящий момент современные средства защиты не позволяют в полной мере решить вопросы безопасности мобильных систем и оценить возможные риски потенциальных злоумышленных действий. В связи с этим возникает задача систематизировать основные угрозы и уязвимости мобильных приложений для последующего формирования методики по оцениванию угроз информационной безопасности в приложениях для мобильных систем.

В настоящее время компьютерные технологии стали активно применяться во всех сферах человеческой деятельности, в том числе и в образовательном процессе. Существуют компьютерные программы, направленные на развитие зрительного и слухового восприятие, внимания, памяти, словесно-логического мышления, которые можно с успехом применять при обучении детей старшего дошкольного и младшего школьного возраста. Мобильные телефоны в современном мире являются не просто средством связи, а устройством, которое содержит уязвимые персональные данные, несанкционированный доступ к которым может привести к непредсказуемым результатам. В настоящий момент современные средства защиты не позволяют в полной мере решить вопросы безопасности мобильных систем и оценить возможные риски потенциальных злоумышленных действий.

В соответствии с классификацией открытого проекта обеспечения безопасности web-приложений OWASP (Open Web Application Security Project), к основным уязвимостям, которым подвержены мобильные устройства, относятся:

1) системные уязвимости (архитектурных решений мобильной платформы);
2) небезопасное хранение данных;
3) недостаточная защищенность протоколов передачи данных;
4) уязвимости системы авторизации и аутентификации;
5) слабая криптостойкость;
6) уязвимости кода приложения;
7) скрытый функционал приложений;
8) ненадлежащий контроль за клиентскими приложениями.

Большинство из них являются достаточно серьезными и приводят к утечке данных неавторизованных пользователей, возможности выполнения SQL-инъекций, а также возможности получения комбинаций имени пользователя и пароля, сброс в начальное состояние, а также способность повышения своих привилегий.

Несмотря на большое количество методов обеспечения безопасности информации, хранящейся на мобильных устройствах, уровень распространения вредоносных приложений в мобильном сегменте растёт высокими темпами. Угрозы безопасности создают риски персональным данным пользователя, риски компрометации критичных данных вплоть до хищения денежных средств. К тому же разработчики мобильных приложений не всегда уделяют достаточного внимания проблемам безопасности или просто не следуют руководствам по безопасной разработке.

На данный момент, такой гигант информационных технологий как Apple использует в системе безопасности своих основных приложений сквозное шифрование, а так же FaceID для аутентификации. Это означает, что доступ к информации можете получить только вы и только на устройствах, где вы выполнили вход в приложении. Сквозное шифрование требует двухфакторной аутентификации для идентификатора Apple ID. Чтобы защитить свои устройства и данные, необходимо регулярно обновлять программное обеспечение и включить двухфакторную аутентификацию. Другие пользователи, даже компания Apple, не могут получить доступ к информации со сквозным шифрованием. Шанс разблокировать такую систему составляет один на миллион. Не смотря на то, что старший вице-президент по маркетингу корпорации Apple Филипп Шиллер отметил, что абсолютно надежных систем не бывает, данная система со сквозным шифрованием и аутентификацией с помощью FaceID применяется во множестве банковских и платежных приложений. Тем самым в данной работе, в области достижения безопасности мобильных приложений, за основу были взяты и раскрыты все положительные качества технологий Apple, отвечающие всевозможным стандартам безопасности на данный момент, а так же упомянуты уязвимости, которые исправляют, как говорилось ранее, с помощью регулярных обновлений.

На настоящий момент ни высокие рейтинги приложения, ни большое количество скачиваний, ни список ресурсов, доступ к которым пользователь предоставляет приложению перед его установкой, не позволяют оценить возможные риски персональным данным и последствия потенциальных злоумышленных действий. Современные средства защиты (антивирусы, снифферы) могут помочь предотвратить определенный спектр

угроз, но их применение не позволит решить проблему безопасности комплексно.

В связи с этим возникает задача разработки комплексной методики по оцениванию угроз информационной безопасности в приложениях для мобильных систем, а также методики анализа приложений на предмет их соответствия требованиям информационной безопасности.

Список использованных источников:

1. Взлом мобильных онлайн игр [Электрон. ресурс]. Режим доступа: https://habr.com/ru/post/232531/;
2. . Михайлов Д. М. Исследование уязвимости мобильных устройств систем Apple и Google / Д. М. Михайлов, А. В. Зуйков, И. Ю. Жуков и др. // Спецтехника и связь, 2011;
3. Цыганенко Н. П. Статический анализ кода мобильных приложений как средство выявления его уязвимостей / Н. П. Цыганенко // Тр. БГТУ. Сер. 6: Физико-математические науки и информатика, 2015.
4. Петренко С. А., Курбатов В. А. Политики безопасности компании при работе в Интернет. Изд-во ДМК Пресс, 2011. 396 с.