УДК 004.9

ПРИЛОЖЕНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПРИ ПОМОЩИ ЖЕСТОВ ДЛЯ ДОСТУПА К ANDROID УСТРОЙСТВУ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ

Лещенко С.Д. (ИТМО)
Научный руководитель – кандидат технических наук, доцент Штенников Д.Г. (ИТМО)

Введение. Современные Android устройства становятся все более важными составляющими повседневной и рабочей жизни людей. На данные устройства устанавливаются приложения, которые могут быть критически важны для человека. К таким приложениям относятся, например, банковские приложения, генераторы случайных кодов для двухфакторной аутентификации. Если злоумышленнику удастся получить доступ к этим приложениям, то пользователю может быть нанесен ущерб. Поэтому защите таких критически важных приложений необходимо уделить отдельное внимание. Традиционные методы защиты, такие как ПИН-код и графический ключ, уже внедрены в операционную систему Android, однако могут оказаться недостаточно надежными, так как их можно либо украсть, либо просто угадать [1]. Для надежной защиты критических приложений необходим второй фактор защиты, в роли которого могут выступать жесты. Жесты могут быть более уникальными и сложными для воссоздания, чем образцы на экране. Например, графический ключ обычно ограничен шаблоном или комбинацией пальцев на экране, тогда как жесты могут включать в себя разнообразные движения и параметры, такие как скорость и расстояние от камеры, что делает их более сложными для подделки. Пользователи могут находить более естественным использование жестов, так как они больше соответствуют обыденным движениям, чем создание сложных образцов на экране. Также нейронная сеть, используемая для аутентификации на основе жестов, может обнаруживать подозрительные попытки получения доступа, что может улучшить безопасность.

Основная часть. Основной целью работы являлась реализация Android приложения двухфакторной аутентификации на основе жестов пользователя с возможностью выбора блокируемых приложений, а также программы, в которой собирается набор данных для обучения модели нейронной сети, которая в дальнейшем используется в мобильном приложении.

В начале разрабатывалась программа для сбора данных и обучения нейронной сети. В качестве архитектуры модели была выбрана рекуррентная нейронная сеть. Сама нейронная сеть разрабатывалась с помощью библиотеки TensorFlow [2], в качестве формата входных данных для данной нейронной сети были выбраны опорные точки на пяти пальцах кисти руки, получаемые с помощью использования OpenCV [3] и MediaPipe [4]. Далее был осуществлен сбор данных для трех типов жестов: движение, отсутствие движения, жест получения доступа к системе. После сбора данных было выполнено обучение нейронной сети. Далее после обучения нейронной сети было проведено тестирование нейронной сети на корректное распознавание жеста получения доступа к системе. Также было проведено тестирование нейронной сети на устойчивость к состязательным атакам: задавались различные случайные жесты.

Далее осуществлялась разработка Android приложения [5] двухфакторной аутентификации на основе жестов пользователя с возможностью выбора блокируемых приложений. Сначала был спроектирован пользовательский интерфейса приложения. Далее была спроектирована база данных для хранения списка заблокированных приложений, обученной модели и другой служебной информации. Дальше осуществлялась верстка экранов активностей и фрагментов в соотвествии спроектированному ранее интерфейсу. После была реализована спроектированная база данных в виде Object Relation Model с помощью библиотеки Room [6]. Далее были реализованы Back-end части экранов активностей и

фрагментов. После реализации экранов активностей и фрагментов была осуществлена реализация сервиса AccessibilityService для работы приложения в фоновом режиме. Далее была реализована возможность загрузки обученной модели в приложение.

Следующим этапом являлась доработка приложения в соотвествии требованиям информационной безопасности. Была выполнена калибровка параметров сервиса приложения для достижения минимального отклика при запуске приложений из заблокированного списка. Также была осуществлена реализация получения прав администратора в целях устранения угрозы удаления приложения злоумышленником.

Финальным этапом было тестирование готового приложения на уязвимости. Была осуществлена проверка невозможности удаления приложения злоумышленнику, проверка устойчивости нейронной сети, загруженной в приложение, к состязательным атакам, а также проверка невозможности доступа к заблокированным приложениям.

Выводы. В результате было реализовано приложение двухэтапной аутентификации пользователей при помощи жестов для устройства Android с использованием нейронной сети, а также программа, которая собирает данные для дальнейшего обучения данной нейронной сети. Приложение было протестировано на устойчивость к возможным угрозам.

Список использованных источников:

1. Сухова А.Р. ПРОБЛЕМЫ БЕЗОПАСНОСТИ ГРАФИЧЕСКИХ КЛЮЧЕЙ, ИСПОЛЬЗУЕМЫХ ДЛЯ БЛОКИРОВАНИЯ СМАРТФОНОВ // МЕЖДУНАРОДНЫЙ НАУЧНЫЙ ЖУРНАЛ «ИННОВАЦИОННАЯ НАУКА» №2/2016 ISSN 2410-6070.

2. TensorFlow (Открытая программная библиотека для машинного обучения) [Электронный ресурс]: https://www.tensorflow.org/ (дата обращения: 08.01.2024).

3. Павел Дац. Распознавание поднятых пальцев на Python+OpenCV [Электронный ресурс]: https://habr.com/ru/post/177551/ (дата обращения: 08.01.2024).

4. MediaPipe | Google for Developers (фреймворк с открытым исходным кодом) [Электронный ресурс]: https://developers.google.com/mediapipe (дата обращения: 08.01.2024).

5. Developer guides | Android Developers (Справочная информация по Android разработке) [Электронный ресурс]: https://developer.android.com/guide/ (дата обращения: 08.01.2024).

6. Библиотека «Room» для начинающего Android-разработчика [Электронный ресурс]: https://habr.com/ru/articles/713518/ (дата обращения: 11.01.2024).