УДК 004.512

МЕТОДЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ НА МОБИЛЬНЫХ УСТРОЙСТВАХ

Сапиева М.А., студентка 1 курса факультета информационных систем в экономике и юриспруденции
Научный руководитель – Чундышко В.Ю., кандидат технических наук, доцент
ФГБОУ ВО Майкопский государственный технологический университет

Ключевые слова: *идентификация, аутентификация, мобильные устройства, анализ поведения, нейронные сети*

Особенностью статьи является использование нового сценария "блокировки устройства», в данном случае смартфон остается разблокированным и может быть быстро заблокирован, если обнаружены действия не владельца. Предлагается решение, которое представляет собой беспарольный пользовательско-адаптивный контекстно-зависимый метод аутентификации.

Мобильные устройства становятся все более распространенными в бизнес-процессах, которые включают в себя электронную почту, социальные сети, корпоративные информационные системы и банковское дело. В результате на устройстве сохраняется множество конфиденциальной информации. Для защиты такой информации необходимо использование эффективной системы контроля доступа.

Современная система контроля доступа основана на проверке того, что пользователь знает пароль или кодовую фразу, обладает или является (биометрические данные и поведенческие шаблоны). Первый и второй факторы обеспечивают надежную аутентификацию за счет удобства использовании. С другой стороны, решения для аутентификации на основе биометрии позволяют повысить удобство использования за счет сохранения низкой частоты ошибок. Тем не менее, эти решения уязвимы для атаки.

Перспективный подход обеспечивается современными технологиями аутентификации на основе поведения. Однако производительность этих систем существенно зависит от контекста, а именно активности пользователя (неподвижность, ходьба, бег) и используемого приложения. Таким образом, необходимы защищенные от подделки прозрачные и удобные методы аутентификации пользователя.

Перспективным способом повышения точности системы ACS является анализ контекстной информации, а именно использования приложений и физической активности пользователя. Злоумышленнику сложнее манипулировать данными, полученными из контекстно-зависимых источников, что снижает эффективность атаки с подменой. Эти системы постоянно отслеживают как функции, связанные с поведением, так и контекстную информацию, такую как местоположение пользователя во время использования банковских приложений. Несмотря на высокую точность аутентификации и устойчивость к подделке, эти решения могут быть неподходящими для частных пользователей из-за опасений нарушения конфиденциальности и высокого потребления вычислительных ресурсов и батареи. Поэтому необходимо прозрачное решение для аутентификации пользователя на устройстве, обеспечивающее конфиденциальность основе контекстно-зависимого поведения.

Для обеспечения аутентификации на устройстве на основе контекстно-зависимого поведения предлагается следующее решение. Блок-схема обработки функций пользователя с помощью предлагаемого метода представлена на рис. 1.Аутентификация пользователя начинается с инициирующего события, такого как запуск предопределенного приложения. Затем собираются сигналы от встроенных датчиков устройства до события запуска завершения. Например, время работы сенсорной клавиатуры и расположение касаний преобразуются в шаблоны ввода.

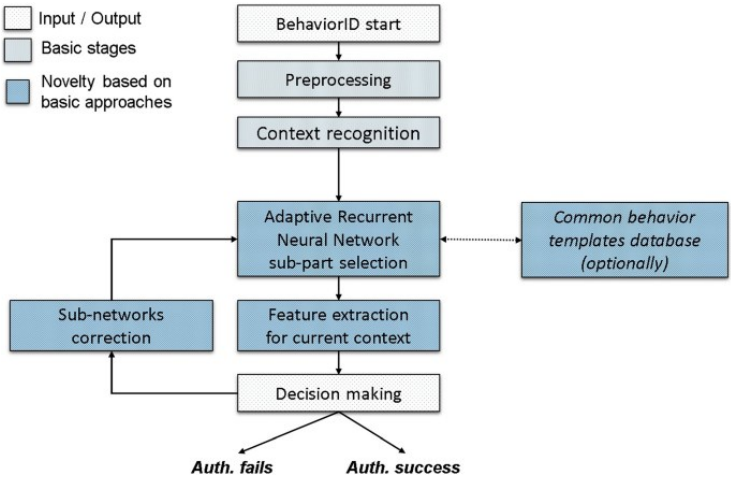

Рис. 1Процедура аутентификации пользователя

Особенностью сети является использование смешанного уровня для повышения производительности в случае обработки последовательностей с несколькими шаблонами, например, смешивания выходных сигналов от встроенных датчиков[1]. Наконец, выходные данные каждого A-RNN, относящиеся к отдельной модальности, обрабатываются модулем принятия решений (рис. 1).Обновление параметров A-RNN с учетом контекста использования позволяет компенсировать изменения профиля поведения пользователя [2].

В последние годы появились некоторые продвинутые механизмы для расширения функциональности LSTM и GRU [3]. Первый - это механизм привлечения внимания, основанный на оценке сходства между закодированным исходным предложением и выходными словами. Механизм особенно полезен в задачах машинного перевода, подписи к изображениям и прогнозирования рейтинга. Другим механизмом являются сети с расширением памяти, которые используют внешнюю память для каждой последовательности. Эти сети нацелены на запоминание недавних полезных образцов и сравнение их с текущими в последовательности ввода. Этот подход часто используется в мета-задачах и одноразовых учебных заданиях. Тем не менее, эти

механизмы нацелены на отслеживание одного шаблона во введенной последовательности [4]. Это ограничивает использование таких методов в приложениях, связанных с анализом поведения, где в собранных данных могут одновременно присутствовать несколько шаблонов.

Библиографический список:

1. М. Пападопули, А. Арнес, Дж.А. Бомбин, Э. Боски, С. Бухеггер, Р.Б. Кортинас и др., Управление мобильной идентификацией. Отчет IDM. Евро. Netw. Inf. Обеспечьте безопасность. Агентство. (2010). https:// www. enisa. europa. eu/ publications/ Mobil e20IDM. Дата обращения 04 октября 2023 года

2. М.А. Ферраг, Л. Магларас, А. Дерхаб, Х. Янике, Схемы аутентификации для интеллектуальных мобильных устройств: модели угроз, контрмеры и открытые вопросы исследований. Дистанционное общение. Система. 73, 317-348 (2020). Дата обращения 04 октября 2023 года

3. Google. Улучшения экрана блокировки и аутентификации в Android 11. (2020). https:// android- разработчик работает. googl электронный блог. com/ 2020/ 09/ блокирует создание и аутентификацию. HTML. Дата обращения 04 октября 2023 года

4. К. Ву, К. Хе, Дж. Чен, З. Чжао, Р. Ду, живучести недостаточно: усиление аутентификации по отпечаткам пальцев с помощью поведенческой биометрии для защиты от кукольных атак. на 29-м симпозиуме по безопасности USENIX (USENIX Security 20) (2020), стр. 2219-2236. https:// www. usenix. org/ конференция/ usenixsecu rity20/ презентация на/ wu. Дата обращения 13 октября 2023 года

USER AUTHENTICATION METHODS ON MOBILE DEVICES

Sapieva M.A.
Scientific supervisor – Chundyshko V.Y.
Maykop State University of Technology

Keywords: *identification, authentication, mobile devices, behavior analysis, neural networks*

A special feature of the article is the use of a new "device blocking" scenario; in this case, the smartphone remains unlocked and can be quickly blocked if actions by someone other than the owner are detected. A solution is proposed that is a passwordless, user-adaptive, context-sensitive authentication method.