УДК 0004.056.53+004.93`1

ПРИЗНАКИ И КРИТЕРИИ НЕСТАНДАРТНОГО ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ

Д.Р. Байдун
Магистрант БГУИР

Е.В. Насуро
Доцент кафедры электронных вычислительных машин БГУИР, кандидат технических наук

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь
E-mail: dima-bajdun@yandex.ru, nasurokv@bsuir.by

Д.Р.Байдун

Окончил Белорусский государственный университет информатики и радиоэлектроники. Магистрант БГУИР. Ведет исследования в сфере выявления нестандартного поведения пользователей.

Е.В. Насуро

Доцент кафедры электронных вычислительных машин БГУИР, основные направления деятельности: проектирование взаимодействия пользователя и сложных программно-аппаратных продуктов, научное руководство магистрантами.

Аннотация. Различные способы идентификации пользователей дают неравнозначные уровни защиты от несанкционированного доступа в систему. Использование комбинаций признаков, полученных при анализе действий пользователя, позволят повысить безопасность систем. Доклад содержит информацию о доступных для анализа характеристиках действий пользователя, сбор которых не требует установки дополнительного оборудования и основан на уже имеющихся аппаратных средствах. Методы машинного обучения позволяют получать персонализированные признаки, характерные для одного пользователя, которые невозможно подделать, так как их сбор проводится неявно в фоновом режиме.

Ключевые слова: идентификация пользователя, распознавание лиц, клавиатурный почерк, машинное обучение, информационная безопасность.

Введение.

Любая система требует надежной защиты, и если от попыток взлома через интернет имеется богатый спектр антивирусных программ, то от взлома физического нас защищают пароли. Но существует шанс, что злоумышленник смог узнать пароль и тогда компьютер и все его данные остаются полностью беззащитными. Однако, каждый человек уникален – имеет свой темперамент, привычки и навыки. В связи с этим, биометрические данные каждого пользователя компьютерной системой будут различаться, как и используемое периферийное оборудование. В данной работе рассматриваются характеристики и признаки уникальные для каждого отдельного пользователя компьютерной системы.

Признаки и характеристики.

Ниже представлены признаки, которые рассматриваются в качестве значимых параметров при отслеживании действий пользователя для выявления аномального поведения.

Распознавание лица. Используя камеру устройства, можно сравнить изображение,

сохраненное ранее с изображением, полученным в режиме реального времени [1].

Имя пользователя и пароль. Проверка подлинности введенного пароля. Надежность этого метода можно повысить, сократив количество неправильных попыток. Дополнительным критерием может выступать скорость ввода пароля [2].

Среднее время и расписание активности. Например, рабочие аккаунты, при необходимости, можно привязывать к режиму работы сотрудника. В остальное время использование служебных учетных записей можно ограничить.

Активность пользователя. Подразумевается время активности пользователя как в отдельно взятых программах, так и в определенных областях программ (например, хранилище паролей в браузерах, поисковые запросы, отключение алгоритмов защиты компьютера – антивирусных программ, брандмауэра, изменение настроек). Например, операционные системы ведут наблюдения и предоставляют некоторую статистику [3]. Кроме того, можно использовать специализированные программы.

Работа с программным обеспечением. Пользователь зачастую имеет устоявшиеся привычки, касающиеся выбора определенных программ, количества единовременно открытых копий программы, количества и типа загруженных из интернета файлов и область работы данных файлов. Кроме того, начало работы характеризуется определенным набором действий – сочетанием запущенных программ, открытием определенных файлов и т.п.

Внешние периферийные устройства. Чтобы исключить внесение изменений в систему и средства защиты при помощи внешних устройств отслеживается ряд параметров: название устройства, активность, область применения, а также – мониторинг файлов, измененных при помощи периферийных устройств.

Клавиатурный почерк [4]. Под данным термином, подразумевается несколько признаков присущих каждому пользователю: количество ошибок при наборе, интервалы между нажатиями клавиш, время удержания клавиш, число перекрытий между клавишами, степень аритмичности при наборе, скорость набора, привычные комбинации клавиш. Кроме того, сюда можно включить особенности работы с мышью/тачпадом. Скорость и ритм клика в каждой отдельно взятой программе.

Коэффициенты критичности.

В связи с разнородностью собираемых данных, а также, с учетом вариабельности некоторых характеристик, необходимо установить коэффициенты критичности критериев и определить уровень ошибок пользователя, при котором будет срабатывать система защиты. Кроме того, нужно предусмотреть разные способы идентификации пользователя при получении тревожных сигналов от системы защиты. В зависимости от комбинации допущенных пользователем ошибок, можно разработать разные реакции алгоритма – от повторного введения пароля или возвращения пользователя в область видимости камеры до полной блокировки системы и учетной записи пользователя с последующим обращением в службу безопасности предприятия.

Заключение.

Сбор всех рассмотренных данных не требует установки дополнительного аппаратного обеспечения и сосредоточен в программной плоскости. Это позволяет расширить сферу применения разрабатываемой системы защиты и сократить расходы на оборудование. При этом, возможно, понадобится регулярная поддержка программного обеспечения, связанная с необходимостью обучать классификаторы при появлении новых пользователей и изменении других условий использования программы.

Различные комбинации перечисленных признаков позволяют разработать универсальный метод, который обеспечит разные уровни надежности в зависимости от поставленной задачи. Разнородность признаков, а также срытое наблюдение за пользователем дают высокий уровень надежности такого метода.

В докладе будет представлен подробный анализ достоинств и недостатков перечисленных признаков, а также – способы повышения надежности за счет

использования различных комбинаций.

Список литературы

[1] Face Recognition Performance Role of Demographic Information. IEEE Transactions On Information Forensics And Security, Vol. 7, No. 6, December 2012

[2] Electronic Authentication Guideline. National Institute of Standards and Technology, USAhttps://csrc.nist.gov/publications/detail/sp/800-63/ver-102/archive/2006-04-30

[3] Журнал действий Windows 10 и конфиденциальность, https://support.microsoft.com/ru-ru/windows/

[4] Нейросетевая идентификация типа личности человека по клавиатурному почерку. Т.В. Жашкова, О.М. Шарунова, Э.Ш. Исянова. Международный студенческий научный вестник. 2015. №3 Ч.1. С. 144-1462.

SIGNS AND CRITERIA OF NON-STANDARD USER BEHAVIOR

D.R.BAIDUN
Postgraduate student of the BSUIR

K.V.NASURO,
Candidate of technical sciences
Belarusian State University of Informatics and Radioelectronics, Republic of Belarus

Belarusian State University of Informatics and Radioelectronics, Republic of Belarus
Email: dima-bajdun@yandex.ru, nasurokv@bsuir.by

Abstract. Different methods of user identification provide unequal levels of protection against of unauthorized access to the system. To raise the level of computer systems security the combinations of features obtained in the analysis of user actions must be used. The report contains information on the characteristics of user actions available for analysis, the collection of which does not require the installation of additional equipment and is based on the already available hardware. Machine learning techniques allow getting personalized traits that are specific to a single user, which cannot be faked, since they are collected implicitly in the background.

Keywords: user identification, face recognition, keyboard handwriting, machine learning, information security.