**Abstract**

Необходимость защиты чувствительных данных сохраненных и доступных с мобильного устройства делает проблему аутентификации пользователей на мобильном устройстве чрезвычайно важной.

Противостояние конфиденциальности и доступности информации на мобильном устройство значительно усложняет данную проблему.

Подход основанный на использовании получения информации с сенсорных экранов мобильных устройств и последующей их обработки методами поиска аномалий и классификации, позволяет обеспечить «прозрачную» непрерывную защиту системы.

Это также обеспечит хорошую защиту от несанкционированного доступа после входа в систему пользователем.

**Introduction**

Технологические достижения в области вычислений и ввода-вывода, а также возможности подключения к сети смещают акцент с ПК на мобильные устройства.

Согласно анализу рынка, в 2015 году во всем мире будет около 1,5 миллиарда смартфонов и 640 миллионов планшетов [3], [12]. Более того, компании, университеты и правительственные учреждения все чаще предоставляют мобильные вычислительные системы и приложения, которые позволяют своим сотрудникам работать удаленно, постоянно подключаясь к инфраструктуре организации.

Популярность мобильных устройств делает их частым носителем информации для конфиденциальной информации (например, конфиденциальных документов, коммерческой тайны, учетных данных).

Поскольку мобильные устройства легко теряются или могут быть украдены, проблема обеспечения доступа пользователей к этим данным приобретает первостепенное значение.

В качестве первого шага защиты аутентификация пользователя является принципиально важной для защиты системы. Однако мобильные устройства вносят компромисс между безопасностью и практичностью большинства существующих решений аутентификации: однократные аутентификационные решения уязвимы для кражи и потери [5], в то время как периодическая аутентификация или автоматический выход из системы после периодов бездействия, скорее всего, будут контрпродуктивными.

Потребность в сильной аутентификации противопоставляется также неуклюжей методологией ввода таких устройств и различными ожиданиями пользователей в отношении моделей взаимодействия, особенно по сравнению со стандартными решениями аутентификации. Как показано в исследовании более 6 000 000 паролей, 91% всех паролей пользователей принадлежат к списку из 1000 общих паролей [4] (например, 8.5% пользователей используют в качестве своих паролей «пароль» или «123456»). Более того, дополнительная стоимость оборудования делает стандартные методы биометрической аутентификации еще непопулярными на мобильных устройствах

Чтобы удовлетворить насущные потребности в более безопасном и удобном для пользователя мобильном решении для проверки подлинности, мы разрабатываем FAST - механизм бесшовной аутентификации пользователей на основе сенсорного экрана, который поддерживает как пассивную, так и непрерывную проверку подлинности для мобильных пользователей на основе жестов прикосновения пользователя. FAST использует тот факт, что во время взаимодействия с мобильными устройствами пользователи раскрывают свои уникальные признаки, такие как давление пальца и траектория движения, скорость и ускорение движения.

Существенным преимуществом нашего подхода является его прозрачность для пользователя: сенсорные данные захватываются датчиками, не нарушая нормальных взаимодействий пользовательских устройств. На этапе postlogin традиционный явный процесс аутентификации запускается только тогда, когда FAST обнаруживает, что текущий пользователь, скорее всего, отличается от владельца смартфона (то есть, потери или кражи устройства).

*Основное содержание:*

* Разработка решения для мобильной аутентификации с сенсорным жестом для нескольких касаний, обеспечивающего дополнительную усиленную защиту мобильных устройств.
* Эмпирическое исследование и оценка применимости использования входов с несколькими касаниями для неявной и непрерывной идентификации пользователей, которая изучает компромисс между ложными отклонениями и ложными ставками принятия

**II Bacground.**

Мы используем следующие два показателя для моделирования компромисса между удобством использования и безопасностью, достигаемым с помощью решения аутентификации.

Определение 1: (FAR) The False Accept Rate (FAR) - процент решений аутентификации, разрешающих доступ к неавторизованному пользователю.

Определение 2: (FRR) The False Reject Rate (FRR) представляет собой процент решений аутентификации, когда авторизованному пользователю запрещен доступ.

Решение, демонстрирующее низкий FAR и высокий FRR, является более безопасным, но не удобным для пользователя. Решение с низким FRR и высоким FAR является более удобным для пользователя, но менее безопасным. Наша цель - свести к минимуму обе метрики.

В предыдущей работе было изучено целесообразность применения динамики нажатия клавиш и шаблонов ввода для идентификации пользователя для персональных компьютеров - нажатия клавиш можно непрерывно производить выборку путем перехвата вывода с клавиатуры. Исследование [7] о восприятии пользователем аутентификации на мобильных устройствах показывает, что пользователи предпочитают систему, которая может неявно и непрерывно выполнять аутентификацию пользователя, не нарушая нормальное взаимодействие между пользователем и мобильным устройством. Кроме того, Jakobsson и соавторы [14] предложили неявную структуру аутентификации пользователей и изучили использование записанной истории телефонных вызовов и место для непрерывной аутентификации пользователей.

В отличие от ПК, сенсорный экран является основным средством ввода на смартфонах и планшетах. Входы мультитач включают характеристики поведения, которые являются специфическими для пользователя и могут использоваться для обнаружения мобильных пользователей.

Мы предлагаем систему идентификации пользователей на основе жестов, основанную на сенсорном жесте, FAST (Fingergestures Authentication System с использованием сенсорного экрана), которая фокусируется на аутентификации пользователей после входа в систему. На рисунке 2 показана диаграмма высокого уровня конструкции. Пока смартфон используется, FAST непрерывно аутентифицирует пользователя. После входа пользователя FAST продолжает аутентифицировать мобильного пользователя в фоновом режиме, используя перехваченные сенсорные данные из обычных пользовательских взаимодействий с смартфоном. Для достижения этой цели FAST полагается на обнаружение владельцев смартфонов на жесте. Метод обнаружения активируется по требованию, когда сенсорные входы принимаются и прозрачны для пользователя смартфона. Только при наличии достаточных доказательств того, что текущий пользователь не является владельцем смартфона, активируется традиционная аутентификация пользователя.

FAST собирает выбранную информацию касания жестов, включая тип жестов, координаты X и Y, направления движения пальца, скорость движения пальца, давление в каждой точке сэмплирования и расстояние между несколькими точками касания. В общей сложности для каждого жестов касания предусмотрено 53 функции. Мы рассматриваем только шесть наиболее часто встречающихся и полезных жестов: вплоть до салфетки, прокручивание сверху вниз, прокрутку слева направо, прокрутку справа налево, увеличение и уменьшение. Поскольку пользователь смартфона может применять разные уровни касания на разных этапах жесткого касания FAST также делит каждый жест на три сегмента, (i) начало касания, (ii) основное касание, которое является самым длинным сегментом И (iii) конец касания.

Необходимо проявлять осторожность, чтобы добиться надлежащего баланса значений FAR и FRR. В период после входа в систему, из-за постоянного мониторинга пользователя и частой прозрачной проверки подлинности, основанной на сенсорных жестах и входах сенсорных перчаток, низкая FRR является основной задачей - во время обычных пользовательских взаимодействий с смартфоном важнее удобство использования. Это связано с тем, что частота операций аутентификации обеспечивает быстрое обнаружение злоумышленников даже при больших значениях FAR.

Touch Sequence Length и Authentication Threshold. Во время фазы после входа FAST непрерывно контролирует подлинность мобильного пользователя прозрачным образом. FAST достигает этого, перехватывая жесты касания и виртуальные вводные данные, и стремится достичь низкого FRR. Тем не менее, жесты пользователя и соответствующие входы датчиков перчаток могут изменяться во времени. Таким образом, решение аутентификации пользователей, которое полагается только на отдельные экземпляры входных жестов прикосновения, вряд ли будет надежным и точным

Защита базы данных не срабатывает, если злоумышленник имеет физический доступ к мобильному устройству, находящемуся в состоянии после входа. То есть, BASE достигает FAR 100%: он не аутентифицирует пользователя после процедуры входа в систему. Значение FRR для BASE равно 0%.

Напротив, FAST использует поведение жестов прикосновений для пользователя, чтобы улучшить безопасность мобильных устройств. Мы количественно оцениваем улучшения безопасности FAST, сравнивая его значение FAR с FAR 100% BASE. Мы измеряем юзабилити FAST с точки зрения достигнутого FRR, где меньшее FRR означает более высокое удобство использования.

В качестве классификаторов мы применили те же три алгоритма: Random Forest, J48 и Bayes Net. Результаты показаны на рисунке 6. R, J и B обозначают случайный лес, дерево решений J48 и Bayes Net. Наборы данных делятся в соответствии с типами жестов: DU, UD, LR, Rl, ZI, ZO и Total соответственно обозначают, проведите пальцем вниз вниз (DU), проведите пальцем сверху вниз (UD), проведите пальцем слева направо Вправо (LR), проведите справа налево (RL), увеличьте масштаб (ZI), уменьшите масштаб (ZO) и общую производительность всех комбинированных типов

жестов (Total).

**VI. RELATED WORK**

В общем, существует три типа подходов аутентификации пользователей: «что у вас есть», «что вы знаете» и «кто вы». Подход «что у вас есть» зависит от смарт-карты, USB-флэш-накопителя или некоторых других типов объектов, которые должны иметь пользователи. Для проверки подлинности пользователя смарт-карты и USB-накопители должны быть физически вставлены в компьютер. Тем не менее, сам мобильный телефон можно считать признаком «того, что у вас есть», а проблемы связаны с утратой контроля над самим смартфоном.

Искусство подхода «кто ты» можно разделить на две группы, включая неявную идентификацию пользователя и классификацию по мультимодальности, особенно биометрические данные с мультимодальными характеристиками.

Для десктопов исследователи в прошлом исследовали возможность применения динамики нажатия клавиш и набора символов для идентификации пользователя. Клавиши нажатия клавиш можно непрерывно отбирать, перехватывая вывод с клавиатуры. Ailisto et al. [17] использовали акселерометры в телевизионных пультах дистанционного управления для идентификации людей. Cuntoor et al. [8] и Gafurov et al. [11] экспериментировал с идентификацией пользователя, используя анализ и распознавание походки. Koreman и Morris et al. [16] предложил непрерывный мультимодальный подход для идентификации пользователей. В [14] Jakobsson и соавторы предложили неявную структуру аутентификации пользователей и изучили использование записанной истории и местоположения телефонных вызовов для непрерывной аутентификации пользователей.

Некоторые исследования проводились по методу графической аутентификации, который использует неявные функции рисования для аутентификации пользователей. Jermyn, et al. [15] предложил метод - «Нарисуй секрет (DAS)». Пользователи будут рисовать график в 2DGrid и информацию о том, какая сетка занята, и в которой будут записываться заказы. При попытке входа в систему пользователи будут повторять рисунок. Согласно Jermyn et al., Относительно небольшая сетка на самом деле достаточно безопасна. Но согласно исследованию Торпа и др. [19], безопасность DAS, возможно, не так хороша, как когда-то считалось. В реальном мире люди обычно используют подпись для подтверждения своей личности. Поэтому естественно, что Сюкри

и другие. [18] предложил аналогичный метод в кибер-мире. В их схеме пользователи должны рисовать свои подписи мышью, и система будет нормализовывать данные и записывать их в базу данных. Во время аутентификации система извлекает характеристики из вновь введенной подписи и сравнивает их с предварительно сохраненной версией. Кроме того, Varenhorst et al. [20] предложил метод рисования каракулей вместо подписей. Они использовали несколько методов для анализа данных, в том числе сетки, скорости, каракули дисперсии и сочетание всех вышеперечисленных и достигли очень высокой точности на основе их оценки

Был составлен литературный материал по объединению множества биометрических входов для получения агрегированных результатов идентификации пользователей. В [13], Indovina et al. Определили, что биометрическая интеграция может происходить на уровне функций или уровне баллов. При интеграции на уровне функций все исходные функции измерений группируются в один вектор признаков для классификации. Хотя на данный момент доступно наибольшая информация, интеграция на уровне функций страдает от так называемого проклятия размерности. Кроме того, функции некоторых измерений могут не всегда быть доступными

**VII Conclusion**