Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.52

Байдун
Дмитрий Русланович

СИСТЕМА АНАЛИТИЧЕСКОГО ОБЗОРА ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ ДЛЯ ВЫЯВЛЕНИЯ НЕСТАНДАРТНОГО ПОВЕДЕНИЯ

АВТОРЕФЕРАТ
диссертации на соискание степени магистра

по специальности 1-40 80 01 Компьютерная инженерия. Хранение и обработка данных

Научный руководитель
Насуро Екатерина Валериевна
кандидат технических наук,
доцент кафедры ЭВМ, БГУИР

Минск 2021

Введение

Развитие аппаратных и программных средств, повсеместное распространение локальных и глобальных сетей и возрастающая популярность облачных хранилищ привели к увеличению количества видов и способов несанкционированного проникновения в систему компьютера. Новые угрозы безопасности информации стали причиной для изменения требований к средствам защиты. В нынешнее время, существует разрыв между теоретическими моделями безопасности и современными информационными технологиями. Большинство систем защиты направлены на предотвращение взлома системы – пароли, биометрическая идентификация, электронные ключи и т.д. В случае, когда вход был осуществлен незаконно, система остается незащищенной от дальнейших действий.

Аналитическая система обзора действий пользователя будет направлена на решение этой проблемы. Мониторинг поведения оператора ЭВМ позволит выявлять непривычные действия, что позволит предположить взлом или незаконное завладение паролем. Такая система повысит уровень безопасности информации и защиты компьютерных систем.

Общая характеристика работы

Цель и задачи исследования. Разработать аналитическую систему обзора действия пользователя для выявления нестандартного поведения.

Для этого необходимо решить некоторые задачи:

- выявить критерии для анализа действий пользователя
- разработать систему коэффициентов значимости критериев
- разработать модель работы системы, с учетом временных меток
- провести минимизацию ложных срабатываний системы

Объектом исследования является защита компьютерных систем от неправомерных действий пользователя.

Предметом исследования является взаимодействие пользователя с компьютерными системами.

Обоснование темы. Развитие аппаратных и программных средств, повсеместное распространение локальных и глобальных сетей и возрастающая популярность облачных хранилищ привели к увеличению количества видов и способов несанкционированного проникновения в систему компьютера. Новые угрозы безопасности информации стали причиной для изменения требований к средствам защиты. В нынешнее время, существует разрыв между теоретическими моделями безопасности и современными информационными технологиями. Большинство систем защиты направлены на предотвращение взлома системы – пароли, биометрическая идентификация, электронные ключи и.т.д. В случае, когда вход был осуществлен незаконно, система остается незащищенной от дальнейших действий.

Аналитическая система обзора действий пользователя будет направлена на решение этой проблемы. Мониторинг поведения оператора ЭВМ позволит выявлять непривычные действия, что позволит предположить взлом или незаконное завладение паролем. Такая система повысит уровень безопасности информации и защиты компьютерных систем.

Апробация результатов диссертации. Результаты исследований были представлены на 56 СНТК, 57 СНТК и BigData 2021.

Опубликованность результатов исследований. Результаты исследований были опубликованы в сборниках СНТК 56 и 57, а также в сборнике тезисов BigData 2021.

Структура и объем диссертации. Диссертация имеет полный объем в 74 страниц, из них: 2 страницы занимают 4 рисунка, 3 страницы занимают 5 таблиц, приложение А состоящее из 15 страниц, а также использовано 33 библиографических источника.

Краткое содержание работы

Во введении обосновывается актуальность исследования, ставятся цели и задачи, определяются предмет, объект исследования, научная новизна и практическая ценность.

В обзоре литературы рассматриваются различные способы и средства аутентификации пользователя.

Множество способов и средств аутентификации пользователей позволяет разрабатывать различные системы защиты с учетом различных требований к скорости, надежности и стоимости таких систем. Каждый из способов имеет свои достоинства и недостатки, которые необходимо учитывать при проектировании для достижения наилучших результатов.

1. Распознавание лица. Плюсы: скорость работы системы, низкая стоимость. Минусы: чувствительность к освещению, положению головы, точность распознавания, необходимость обучения системы.
2. Пароль. Плюсы: простота в реализации, низкая стоимость, хороший уровень защиты. Минусы: высокий шанс подбора, кражи, негативно влияющий человеческий фактор.
3. Действия пользователя при запуске системы. Плюсы: самообучение, скрытая работа, не требует от пользователя специальных действий. Минусы: необходимость в обучении, сильная зависимость от настроения и самочувствия человека.
4. Среднее время активности. Плюсы: простота реализации, высокий показатель защиты при установленном графике работы. Минусы: высокая зависимость от человеческого фактора.
5. Отключение алгоритмов защиты компьютера (антивирусные программы, брандмауэр и т.п.). Плюсы: простота реализации. Минусы: человеческий фактор.
6. Активность пользователя. Плюсы: высокая эффективность для офисных либо рабочих компьютеров. Минусы: сложность реализации, малоэффективен для персональных компьютеров.
7. Работа с программным обеспечением. Плюсы: скрытый режим работы. Минусы: необходимость обучения, сложности в анализе данных.
8. Внешние периферийные устройства. Плюсы: простота в реализации, скрытый режим работы.
9. Клавиатурный почерк. Плюсы: высокий уровень идентификации, удобство для пользователя, скрытый режим работы. Минусы: зависимость от состояния пользователя, сложность в обучении.
10. Жесты. Минусы: сложность в реализации и анализе, высокий шанс ошибки, долгое обучение, зависимость от состояния пользователя.

11. Работа с мышью/тачпадом. Теже плюсы и минусы, что и у клавиатурного почерка.
12. Идентификация по радужной оболочке глаза. Плюсы: высокий уровень защиты, дополнительное оборудование находится в средней ценовой категории. Минусы: скорость работы, чувствительность к свету и положению человека, необходимость в дополнительном оборудовании.

Подводя итог всего выше сказанного, можно смело утверждать, что ни один вариант защиты не гарантирует полную защиту от несанкционированного доступа. Однако появляется возможность комбинировать несколько способов аутентификации для компенсации несовершенств отдельных методов, что позволит повысить надежность защиты.

Во втором разделе рассмотрены методы биометрической идентификации, такие как:

Оптический метод идентификации по отпечатку пальца. Плюсы: уникальность отпечатков пальца, возможность идентификации пользователя даже с поврежденным рисунком (определяться может по краям рисунка, как в варианте с умышленным затирании кислотой отпечатка). Считыватели отпечатков пальцев имеют ряд недостатков: в связи с архитектурой устройства, присутствует вероятность фальсификации, есть необходимость в дополнительном оборудовании и вопросы к скорости работы.

Мультиспектральный метод идентификации по отпечатку пальца. Имеет те же плюсы и минусы, что и у оптического считывателя, кроме вероятности фальсификации. Считается что с данным комплексом она максимально мала.

Способ аутентификации по сердечному ритму обладает рядом преимуществ, таких как высокая точность, высокая сложность подделки и получения эталона, анализ физического состояния реципиента. Среди недостатков этого способа выделяется скорость работы и финансовые затраты.

Радужная оболочка глаза. Плюсы: радужная оболочка каждого человека уникальна, что дает высокий уровень защиты. Минусы: стоимость оборудования, скорость идентификации.

Сетчатка глаза. Плюсы: высокая степень безопасности, сетчатка глаза остается неизменной в течение всей жизни (не считая изменения в связи с хроническими заболеваниями). Минусы: высокая стоимость оборудования, низкая скорость идентификации.

Рисунок вен. Плюсы: имеет высокую степень защиты в связи с индивидуальностью рисунка вен для каждого человека, трудности в

несанкционированном получении шаблона. Минусы: стоимость и размеры сканеров, время обработки и сравнения результатов.

После подробного рассмотрения методов биометрической аутентификации, некоторые из них были признаны не приемлемыми для использования в системе. Например, идентификация по сетчатке глаза либо по рисунку вен были признанными не пригодными в связи с дороговизной дополнительного оборудования, по отпечатку пальца – самый высокий коэффициент ложного срабатывания.

Так же были рассмотрены методы анализа данных. В данной работе наиболее удачно применимый будет метод кластерного анализа.

В третьем разделе рассматриваются методы аутентификации и биометрическая аутентификация, в частности.

Все рассмотренные в данном разделе критерии имеют свои плюсы и минусы:

1. Многоразовые пароли. Не требуют каких-либо дополнительных средств для реализации, имеют среднюю степень удобства для пользователя и низкую стоимость установки и обслуживания, однако имеют минусы в виде возможности подобрать пароль.
2. Одноразовые пароли менее удобные для пользователя, однако данный способ аутентификации исключает возможность использования оптимизированного перебора. Минус – требуется специальное ПО.
3. Биометрическая аутентификация. Данный способ более дорогой, по сравнению с паролями, имеет шанс на ложное срабатывание и требует в некоторых вариантах реализации специальное оборудование. Но в тоже время, является более удобным для пользователя, полностью исключает возможность перебора.
4. Графическая аутентификация. Главные плюсы заключаются в высоком показателе удобства для пользователя, отсутствии возможности подмены. Однако данный способ имеет и минусы: высокая стоимость установки и обслуживания, требует установку специального ПО, оставляет возможность к подбору и присутствует вероятность ложного срабатывания.
5. Аутентификация через географическое местоположение. Плюсы: дешевый вариант в установке и обслуживании, защищен от варианта с подбором. Минусы: присутствует шанс возникновения ошибки, подмены данных, требует спец оборудование.
6. ЭЦП и интеллектуальные карты. Плюсы: открытый интерфейс, отсутствуют вероятность ложного срабатывания и подбора.

Минусы: дорого, требует специальное оборудование, есть вероятность подмены.

В четвертом разделе рассматривается разрабатываемая система, ее алгоритмы работы, критерии отслеживания и анализа.

Имея в своей основе простой алгоритм работы, данная система имеет хороший запас помехоустойчивости. Благодаря скрытому варианту работы системы и постоянному сбору, и анализу данных, имеет высокие шансы на выявление несанкционированного доступа. При помощи комплексного анализа действий пользователя, уменьшается шанс ложных срабатываний некоторых методов аутентификации.

Однако у данной системы присутствуют и минусы. Хоть комплексный подход и снижает шанс ложных срабатываний, он не опускает данный вариант развития событий до нуля. Имея комплексный подход, система так же получила и уязвимости каждого из методов. В случае если злоумышленник будет точно знать все используемые методы, и будет уверен в наличии данной защиты, получить доступ к системе он все-таки сможет, пусть и не сразу.

Данные минусы указывает на возможность для ее будущих модернизаций. Ведь пока будут развиваться алгоритмы взлома, будут совершенствоваться и алгоритмы защиты.

Заключение

В ходе выполнения работы была разработана аналитическая система обзора действия пользователя для выявления нестандартного поведения.

Для этого были выполнены все поставленные ранее задачи:

1. Рассмотрены и проанализированы основные способы и методы аутентификации. На основе плюсов и минусов данных методов, были выявлены критерии для анализа действий пользователя.

2. Проанализировав все варианты пересечения между собой выбранных критериев, а также возможные положительные либо отрицательные комбинации была разработана система коэффициентов значимости критериев.

3. Основываясь на критериях, выявленных ранее, и системе коэффициентов получилось разработать модель работы системы, с учетом временных меток и провести минимизацию ложных срабатываний системы.

По итогу работы, полученная система имеет определенные плюсы и минусы.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

[1-А] Байдун, Д. Р. Обзор характеристик и признаков, определяющих поведение пользователя ПК / Байдун Д. Р. // Радиотехника и электроника : сборник тезисов докладов 56-й научной конференции аспирантов, магистрантов и студентов (Минск, апрель-май 2020 г). - Минск : БГУИР, 2020. - С. 10.

[2-А] Байдун, Д.Р. Обзор признаков и критериев нестандартного поведения пользователя / Д.Р. Байдун // Компьютерные системы и сети: материалы 57 научной конференции аспирантов, магистрантов и студентов БГУИР (Минск, 20-21апреля 2021г.). – Минск : БГУИР, 2021.

[3-А] Байдун, Д. Р. Признаки и критерии нестандартного поведения пользователя / Д. Р. Байдун, Е. В. Насуро // BIG DATA and Advanced Analytics = BIG DATA и анализ высокого уровня: VII Международная научно-практическая конференция [Электронный ресурс]: сборник материалов VII Международной научно-практической конференции, Минск, 19-20 мая 2021 года / Белорусский государственный университет информатики и радиоэлектроники; редкол.: В. А. Богуш [и др.]. – Минск, 2021. – С. 50–52. – Режим доступа: http://bigdataminsk.bsuir.by/files/2021_materialy.pdf.