обнаружения аномалий для постоянного подтверждения личности пользователя // T-Comm: Телекоммуникации и транспорт. – 2022. – Т. 16, № 5. – С. 48-55. – DOI: 10.36724/2072-8735-2022-16-5-48-55.

7. *Уймин А.Г.* Интеллектуальный анализ динамики трехпозиционного графического манипулятора типа «мышь» как элемента поведенческой биометрии // Системы управления и информационные технологии. – 2022. – № 2(88). – С. 92-96. – DOI: 10.36622/VSTU.2022.88.2.018.

Саломатин А.А.

Алгоритм аутентификации пользователей на основе статических характеристик аппаратного обеспечения компьютеров

Аннотация: Работа посвящена разработанному алгоритму аутентификации пользователей на основе статических характеристик аппаратного обеспечения компьютеров. Подробно изложены основные шаги алгоритма, описывающие используемые данные и их обработку для генерации характеристических профилей пользователей. Предложено программное обеспечение, реализующее алгоритм. Результаты работы могут быть использованы для дальнейшего усовершенствования алгоритма и его апробации.

Ключевые слова: информационная безопасность, аутентификация, цифровой след, аппаратное обеспечение, статические характеристики

Введение

В эпоху информационных технологий особую важность приобретает вопрос информационной безопасности (ИБ) пользователей сетей. Данные пользователей различных устройств должны обладать высокой степенью защиты от кибератак, направленных на потерю пользовательских данных, их сбор злоумышленниками и/или др.

Одним из направлений исследований в этой области является адаптивная аутентификация, позволяющая на основе анализа различных параметров, определяющих поведение пользователя в сети, выявить его подлинность [1-2]. Набор необходимых статических и динамических характеристик в данной задаче называют цифровым следом.

Как показывают работы [3-7] аутентификация на основе статических характеристик аппаратного обеспечения (АО) способна повысить уровень ИБ пользователя в качестве дополнительного фактора аутентификации. Однако, необходимо уделить внимание разработке алгоритмов аутентификации пользователей, учитывающих новые ранее не представленные статические характеристики АО компьютеров, поскольку это может гипотетически повысить уровень ИБ пользователей, выраженный в рациональном сочетании точности и времени аутентификации.

1. Разработка алгоритма аутентификации

Пусть имеется множество $U = \{U_1, U_2, \dots, U_n\}$ пользователей компьютеров, обладающих соответствующими характеристическими профилями K_i. Каждый характеристический профиль отражает некоторое множество статических характеристик, характеризующих пользователей. Отметим эти множества D_i.

Возникает запрос о входе пользователя U_l, идентифицирующего себя как U_k пользователь. Необходимо, принять или отклонить запрос, тем самым определяя аутентификацию входящего пользователя. Обозначим булевую переменную, отвечающую за это действие F.

Таким образом, информационная модель задачи выглядит следующим образом:

$$\langle U, K, U_l; F \rangle. \quad (1)$$

Алгоритм аутентификации на основе статических характеристик АО компьютеров состоит из следующих этапов.

1) Сбор статических характеристик АО D_l входящего пользователя U_l. Получают следующие данные с помощью специальных программных средств или интерфейсов,

предоставляемые операционной системой через API:
– идентификационные характеристики процессора: частота работы, количество потоков и др.;
– объем и тип оперативной памяти: объем оперативной памяти (RAM), тип используемой памяти (например, DDR4), скорость работы и др.;
– характеристики жесткого диска: объем, количество разделов и др.;
– сведения о сетевых устройствах: MAC-адреса сетевых адаптеров, IP-адреса, информацию о сетевых соединениях и другие данные, которые могут быть полезными для идентификации устройства в сети;
– другие важные компоненты: данные о видеокартах, звуковых картах, USB-устройствах и т.д.

2) Создание уникального идентификатора UP_l на основе полученных данных D_l. На этом этапе используются алгоритмы хеширования, шифрования или другие методы обработки данных для того, чтобы представить информацию в виде уникального набора символов или чисел, который может быть использован для дальнейшей аутентификации. Одним из способов создания уникального идентификатора является использование хеш-функций для обработки собранных данных. Хеш-функция преобразует входные данные произвольной длины в строку фиксированной длины, которая является уникальной для каждого набора входных данных. Применение хеш-функции к данным аппаратного обеспечения обеспечивает уникальность идентификатора или характеристического профиля, поскольку даже незначительные изменения во входных данных приводят к значительным изменениям в выводе хеш-функции.

3) Генерация специального ключа K_l. Этот ключ является криптографически защищенным представлением характеристик АО. Полученный характеристический профиль используется как основа для генерации ключа с использованием криптографических методов. Например, можно использовать алгоритм симметричного шифрования, такой как AES (Advanced Encryption Standard), где характеристический профиль служит в качестве ключа

шифрования. Также важно обеспечить безопасное хранение сгенерированного ключа за счет хранения в зашифрованном виде, использования аппаратных средств защиты, хранения в безопасном хранилище и/или др.

4) Принятие решения о запросе. Происходит сравнение ключей K_k и K_l. При совпадении ключей пользователь аутентифицируется как подлинный, и доступ к системе разрешается. Если данные не совпадают, доступ ограничивается (полностью или частично).

2. Программное обеспечение для апробации алгоритма аутентификации

Для будущей апробации разработанного алгоритма разработано программное обеспечение для сбора данных о компьютере и создания ключа устройства, который может быть использован для аутентификации пользователей на основе аппаратных характеристик.

Для сбора информации о системе, включая аппаратные характеристики компьютера, используются стандартные библиотеки Python: "platform", предоставляющая информацию о том, какой процессор, сколько оперативной памяти установлено, и какая операционная система запущена на компьютере, а также "psutil", дающая сведения о жестких дисках, сетевых интерфейсах и некоторых других аппаратных частях.

Для создания уникального идентификатора устройства все собранные данные о статических характеристиках аппаратного обеспечения используемого компьютера обрабатываются в строку с использованием специальной хеш-функции SHA-256 (библиотека "hashlib"), которая является одной из наиболее надежных и широко используемых хеш-функций. SHA-256 использует комбинацию операций битовых сдвигов, побитовых операций И, ИЛИ и исключающего ИЛИ, а также нелинейных функций, известных как раундовые функции, чтобы обеспечить равномерное распределение данных в процессе хеширования. Присутствует стойкость к коллизиям, что означает, что вероятность обнаружения двух разных сообщений с одинаковым хэшем крайне низка.

На рисунке 1 представлен пример результата работы программного обеспечения.

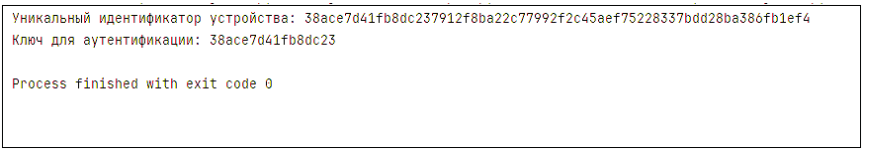

Рисунок 1 – Пример результата работы программного обеспечения

При условии наличия ключей всех пользователей последним шагом для работы алгоритма остается сравнение полученного ключа для аутентификации с ключом, соответствующим тому пользователю, которого задавал входящий.

Заключение

Предложен алгоритм аутентификации пользователей на основе статических характеристик АО компьютеров. Определен рациональный набор статических характеристик АО компьютеров, характеризующих пользователей. Предложены подходы к созданию уникальных идентификаторов пользователей и генерации ключа, при сравнении которого определяется возможность доступа к данным. С использованием языка программирования Python и стандартных библиотек, обеспечивающих доступ к системным ресурсам и криптографическим функциям, разработано ПО, реализующее основные шаги алгоритма. В дальнейшем планируется усовершенствовать данное ПО для апробации разработанного алгоритма аутентификации и определения его эффективности в результате проведения эксперимента.

Литература:

1. *Исхаков А.Ю., Саломатин А.А.* Подход к выявлению связанных с пользователем сущностей веб-пространства в задаче адаптивной аутентификации / Материалы Международной научно-практической конференции «Актуальные задачи математического моделирования и информационных технологий» (АЗММиИТ 2020, Сочи). – Сочи: Сочинский государственный университет, 2020. – С. 128-132.

2. *Bakar K., Haron G.* Adaptive authentication: Issues and challenges / 2013 World Congress on Computer and Information Technology (WCCIT). – IEEE: Sousse, Tunisia, 2013. – P. 1-6.

3. *Bogacheva D., Salomatin A.* The Hardware-Based User Authentication Method for Personal Emergency Rescue Systems / Proceedings of 2023 International Russian Automation Conference (RusAutoCon). – IEEE: Sochi, 2023. – P. 610-615.

4. *Dong S., Farha F., Cui S., Ning H., Ma J.* CPG-FS: A CPU performance graph based device fingerprint scheme for devices identification and authentication / Proceedings of the 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing. – IEEE: Fukuoka, 2019. – P. 266-270.

5. *Salomatin A.* Method of user identification based on dynamic characteristics of mobile device hardware // E3S Web of Conferences. – 2024. – Vol. 548. – P. 1-6.

6. *Salomatin A., Iskhakov A., Meshcheryakov R.* Formation of a Digital Footprint Based on the Characteristics of Computer Hardware to Identity APCS Users / Proceedings 2021 International Russian Automation Conference (RusAutoCon). – IEEE: Sochi, 2021. – P. 314-320.

7. *Takasu K., Saito T., Yamada T., Ishikawa T.* A survey of hardware features in modern browsers: 2015 Edition / Proceedings of the 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. – IEEE: Santa Catarina, 2015. – P. 520-524.

Фейзов В.Р.

Влияние государственной системы управления на протестный потенциал общества

Аннотация: В работе рассматривается взаимосвязь между протестным потенциалом общества и системой управления государством. Проанализированы основные факторы, влияющие на развитие протестных настроений, а также роль государственных акторов в управлении этими факторами. Описаны конкретные действия, которые ключевые государственные структуры (правительство, судебная система, правоохранительные органы, социальные службы, экономические структуры и местные