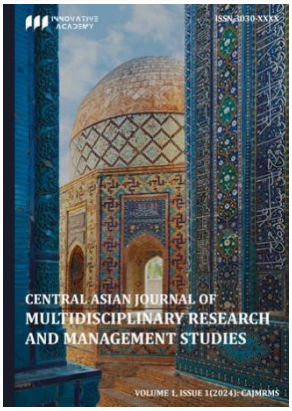


МЕТОДИКА ОБУЧЕНИЯ ИСПОЛЬЗОВАНИЮ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ПАРОЛЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вохидов Дилшод Аликулович

(Ассистент Самаркандского государственного медицинского университета)

Ниятқобилова Мохинур Мухтор қизи

(студент Самаркандского государственного медицинского университета, 121 –группа педиатрия факултет).

Нодиршоева Зулфия Сирожиддин қизи

(студент Самаркандского государственного медицинского университета, 121 –группа педиатрия факултет).

Махсудова Баҳор Жўрабек қизи

(студент Самаркандского государственного медицинского университета, 121 –группа педиатрия факултет)

https://doi.org/10.5281/zenodo.14234992

ARTICLE INFO

Received: 19 th November 2024
Accepted:20th November 2024
Published:28th November 2024

KEYWORDS

идентификация, контроль разрешений, аутентификация, авторизация, смарт-карта, жетон.

ABSTRACT

Основная цель – изучение теоретических и практических аспектов компьютерной безопасности, знание методов парольной защиты, а также формирование и развитие навыков и умений использовать их на практике.

Введение: Для проблемы безопасности, связанной с управлением системными ресурсами, будет использоваться термин "контроль разрешений" —как общий термин. При проведении разъяснений, относящихся к данной области, выделяют 3 основные важные области: идентификация, аутентификация и авторизация.

Идентификация – это процесс обращения с человеком как с кем-то. Например, когда вы идентифицируете себя по телефону, можно сказать, что идентификация прошла. При этом вы представляетесь, например, «Я Шерзод». В этом случае Боходир служит вашей личностью. Таким образом, идентификация - идентификация субъекта - это процесс предъявления системе или запрашивающему субъекту. Кроме того, почтовый адрес можно рассматривать как идентификатор в системе электронной почты. Процесс предоставления почтового адреса можно рассматривать как процесс идентификации. В системе электронной почты почтовый адрес уникален. Можно предположить, что идентификатор пользователя уникален и неповторяем в системе.

Аутентификация — это процесс проверки того, что пользователь (или сторона) имеет право использовать систему. Для примера возьмем процесс использования пользователя с персонального компьютера. При первоначальном входе в систему

пользователь вводит свой идентификатор (т. е. имя пользователя) и через него представляется системе (проходит процесс идентификации). Затем система запрашивает у пользователя пароль для проверки предоставленной личности. Если в идентификатор введен соответствующий пароль (т. е. прошел проверку подлинности), пользователь сможет получить доступ к компьютеру. Другими словами, можно сказать, что аутентификация — это процесс проверки подлинности пользователя или объекта.

После прохождения аутентификации пользователь получает доступ к системному ресурсу. Однако пользователю, прошедшему аутентификацию, не разрешается выполнять необязательные действия в системе. Например, требовать, чтобы пользователю с привилегиями аутентификации была предоставлена возможность устанавливать приложения. Итак, как ограничить разрешения пользователю, прошедшему аутентификацию? Этими вопросами занимается именно сфера авторизации.

Авторизация-это процесс авторизации действий, которые пользователь, прошедший процессы аутентификации, может выполнять в системе.

В области безопасности термины используются отдельно от их стандартизированных значений. В частности, контроль разрешений во многих случаях используется как синоним авторизации. Однако в этом курсе контроль разрешений рассматривается более широко. То есть процессы авторизации и аутентификации рассматриваются как части контроля разрешений.

Обобщая определения, данные вышеупомянутым терминам, можно сделать следующий вывод:

Идентификация - кто вы?

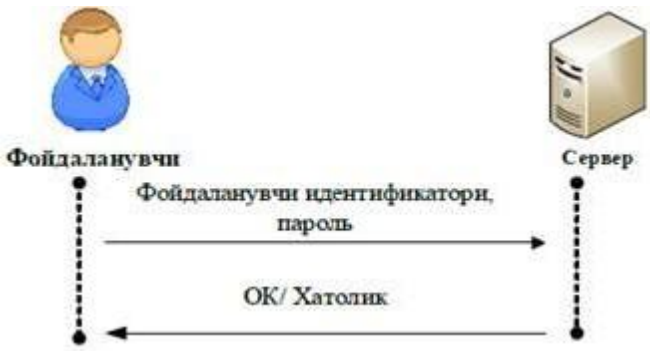
Аутентификация: вы тот, кто вы есть на самом деле?

Авторизация - есть ли у вас разрешение на это?

Анализ литературы и методология: В процессах аутентификации или идентификации субъекты могут принимать форму человека или устройства (компьютера). То есть человек может аутентифицировать человека, машина может аутентифицировать человека или машина может аутентифицировать машину. В этой лекции основное внимание будет уделено сценариям аутентификации человека или машины.

Примером состояния "что-то, что вы знаете" является пароль. С другой стороны, примером состояния" что-то у вас есть " являются смарт-карты, токен, пульт дистанционного управления или ключ от машины. Состояние" что-то ваше " обычно рассматривается как синоним биометрических параметров. Например, прямо сейчас вы можете купить ноутбук и пройти аутентификацию через сканер отпечатков пальцев на нем.

Пароль-некая информация, известная только пользователю и обеспечивающая прохождение процесса аутентификации в системе. Пароль на практике является широко используемым параметром в процессе аутентификации. Например, нам нужно будет ввести пароль, необходимый для получения прав на использование наших



компьютеров. Этот чехол также можно использовать для мобильных телефонов. Обзор процесса аутентификации в состоянии на основе пароля показан на рисунке 3.1.

Рисунок 3.1. Процесс аутентификации машины и человека на основе пароля

Аутентификация на основе пароля имеет следующие особенности:

- легко реализовать аутентификацию на основе пароля (низкая стоимость, простота замены);
- пароль пользователя обычно содержит информацию об алокадоре (например, его любимую футбольную команду, номер телефона и Хак.) (123456, 12345, DM > yeg (U) и поэтому "легко идентифицируется злоумышленниками;
- запоминание сложных паролей сложно (например, }De}(43}Yett+U);
- широко используемый на практике метод аутентификации на основе пароля метод.

Смарт-карта или жетон

Для аутентификации применяются токены в виде смарт-карт или устройств. Смарт-карта-это устройство размером с кредитную карту с небольшим объемом памяти и вычислительными возможностями. Смарт-карта обычно хранит в себе какой-то секретный размер, ключ или пароль, хранит и даже выполняет вычисления. На рисунке 3.2 показана смарт-карта специального назначения и устройство для ее считывания (устройство для чтения смарт-карт).

Рисунок 3.2. Смарт-карта против считывателя смарт-карт

Методы аутентификации на основе чего-либо могут быть реализованы в различных формах. Возьмем, к примеру, генератор паролей. Генератор паролей-это небольшое устройство, которое используется при входе в систему. Предположим, у Алисы есть генератор паролей, и она хочет пройти аутентификацию у Боба, используя его. Для этого Боб отправляет случайное число k (—вопрос) Алисе. Алиса вводит полученное число K и PIN-код, необходимый для использования генератора паролей, в генератор паролей. Генератор паролей, с другой стороны, предоставляет ответ Алисе, и он передается Бобу. Если ответ правильный, Алиса проходит аутентификацию, иначе она не сможет пройти. Обзор этого сценария показан на рисунке 3.3.

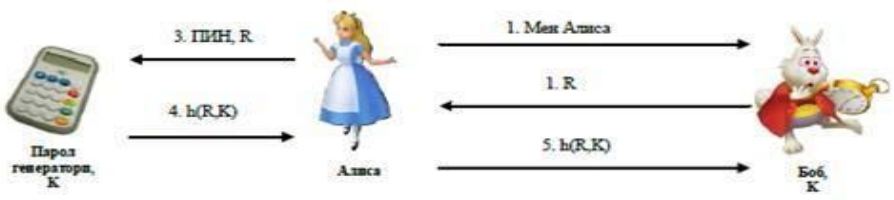


Рисунок 3.3. Процесс аутентификации на основе токенов

Согласно приведенной схеме, генератор глав и паролей должен иметь распределенный ключ K. В этой схеме использовался механизм вопросов-ответов. То есть в качестве вопроса Боб передает Алисе число R и получает соответствующий ей ответ - h(r, k). Проверяя полученную информацию, Боб проверяет Алису на подлинность.

Смарт-карта или-методы аутентификации, основанные на чем-то, что у вас есть, имеют следующие характеристики:

- аутентификация на основе смарт-карты не требует запоминания чего-либо;
- высокая стоимость реализации и устройства (в частности, замена токена в случае его утери обходится дорого);
- есть проблема с потерей токена или смарт-карты и выгоранием;
- обеспечивает высокий уровень безопасности, если токен надежно переносится.

Аутентификация на основе биометрических параметров

В методе аутентификации на основе биометрических параметров биометрический параметр служит ключом к УЗИ человека. Существует гораздо больше биометрических параметров, таких как отпечаток пальца, изображение лица, зрачок глаза, голос, стиль движения, форма уха, форма руки и взлом. На практике широко используется метод аутентификации, основанный на биометрических параметрах. Например, метод аутентификации по отпечатку пальца широко используется на входных дверях многоквартирных домов или при входе в организации, а на ноутбуках и мобильных телефонах-на основе изображения лица или аутентификации по отпечатку пальца (рис.3.4).

Отпечаток пальца Изображение лица Зрачок глаза Голос

Рисунок 3.4. Примеры биометрических образцов

В области информационной безопасности биометрические параметры рассматриваются как альтернатива паролям, обеспечивающая более высокую безопасность. Метод аутентификации, основанный на биометрических параметрах, имеет следующие особенности:

- метод, основанный на биометрических параметрах, не требует необходимости запоминать и носить с собой;
- реализация аутентификации на основе биометрических параметров к паролю
- считается дороже, чем метод на основе токенов, и дешевле, чем метод на основе токенов (есть некоторые исключения);
- нет возможности заменить биометрический параметр, то есть, если биометрический параметр поддельный, то система аутентификации считается полностью скомпрометированной для этого пользователя;
- методы аутентификации, основанные на различных биометрических параметрах, воспринимаются людьми в разной степени.

Идеальный биометрический параметр для использования в области аутентификации должен соответствовать:

-быть универсальным-биометрический параметр обязателен для всех пользователей;

-быть другим-выбранный биометрический параметр должен быть разным для всех людей;
-свойство-выбранный биометрический параметр должен оставаться неизменным с течением времени;
-аккумулируемость-физическое свойство обязательно должно быть легко аккумулируемым.

***Результаты**:* На практике концентрация физического свойства также будет зависеть от внимания человека к процессу.

Биометрический параметр широко используется не только при решении задачи аутентификации, но и при идентификации. То есть —кто ты? может ответить на вопрос: "почему?" Например, у BI есть базы данных отпечатков пальцев, относящиеся к преступникам. В этой базе он скачивается в виде отпечатка пальца (изображение отпечатка пальца, имя пользователя) и с помощью него может проверить человека на наличие в списке преступников. Для этого от проверяемого человека берется изображение отпечатка пальца, и если оно присутствует в базе данных RV1, то имя проверяемого человека совпадает с именем пользователя, соответствующим изображению отпечатка пальца.

Заключение. Если одна из сторон проверяет подлинность другой, это называется односторонней аутентификацией. Если обе стороны аутентифицируют друг друга, это называется двусторонней аутентификацией. Например, во время использования электронной почты только сервер аутентифицирует пользователя (с помощью пароля) и поэтому может называться односторонней аутентификацией. Однако при совершении электронных платежей как сервер аутентифицирует пользователя, так и пользователь аутентифицирует сервер. Поэтому данный случай можно назвать двойной аутентификацией.

ЛИТЕРАТУРЫ:

1. Вохидов, А. М., Вохидов, Д. А., Фармонова, Р. Ф., & Хафизова, Д. Ш. (2022). Разработка Графическим Пользовательским Интерфейсом-Программ В Пакете Tkinter С Использованием Современных Педагогических Технологий В Области Медицины. *Miasto Przyszłości*, *30*, 181-184.

2. Vohidov, D., Maxmudova, Z., & Sayfullayev, R. (2022). TIBBIYOT YO'NALISHIDA ZAMONAVIY PEDAGOGIK TEXNOLOGIYALARINI QO 'LLAB TKINTER PAKETIDA GUI DASTURLARINI TUZISH. *Евразийский журнал математической теории и компьютерных наук*, *2*(12), 31-35.

3. Voxidov, A., Voxidov, D., Avazov, A., & To'layev, A. (2023). TIBBIYOT UNIVERSITETI PEDIATRIYA FAKULTETI TALABALARI UCHUN TA'LIMDA ISHLAB CHIQISH AMALIYOTINING KONTEKST SIFATIDA TA'LIM. *Евразийский журнал академических исследований*, *3*(2 Part 4), 150-154.

4. Melitoshevich, V. A., & Alikulovich, V. D. (2023). Development by a Graphic User Interface-Programs in the Tkinter Package Using Modern Pedagogical Technologies in the Field of Medicine. *Miasto Przyszłości*, *32*, 13-17.

5. Вохидов, Д. А., Вохидов, А. М., Аминов, Ж., & Хабибжон, Л. (2023). Роль Информационных Технологий В Управлении Ресурсами Персонала Здравоохранения. *Miasto Przyszłości*, *34*, 299-305.

6. Voxidov, A. M., Malikov, M. R., Voxidov, D. A., & Nurmuxammadiyeva, L. A. (2022). Tibbiy-biologik tadqiqotlarda statistik tahlil jarayonlari. *Academic research in educational sciences*, *3*(3), 287-293.

7. Alikulovich, V. D., & Melitoshevich, V. A. (2023). Use of Interactive and Modern Pedagogical Software in the Process of Freelancing Sites in Medicine. *Eurasian Scientific Herald*, *17*, 1-6.

8. Voxidov, A. M., Malikov, M. R., & Voxidov, D. A. (2021). TIBBIYOTDA DIFFERENSIAL TENGLAMALARNI FARMATSIYA SANOATIDA QO'LANISHI. *Academic research in educational sciences*, *2*(12), 1096-1102.

9. Voxidov, D., & Voxidov, A. (2023). TIBBIYOT XODIMLARI RESURSLARINI BOSHQARISHDA AXBOROT TEXNOLOGIYANING O 'RNI. *Евразийский журнал медицинских и естественных наук*, *3*(3), 114-120.

10. Вохидов, Д. А., Вохидов, А. М., Аминов, Ж., & Хабибжон, Л. (2023). Роль Информационных Технологий В Управлении Ресурсами Персонала Здравоохранения. *Miasto Przyszłości*, *34*, 299-305.

11. Вохидов, Д. А., Вохидов, А. М., Хайдарова, Х. Р., & Тураева, А. Б. (2023). Ключевые Особенности Learningapps В Повышении Знаний Студентов Медицины. *Miasto Przyszłości*, *42*, 607-609.

12. Melitoshevich, V. A., Alikulovich, V. D., Janaboyevna, A. A., & Baxtiyorovna, D. S. (2024). TIBBIY-BIOLOGIK MASALALANI CHIZIQLI KORRELYATSIYA USULIDAHISOBLASH. *BARQARORLIK VA YETAKCHI TADQIQOTLAR ONLAYN ILMIY JURNALI*, *4*(4), 1-6.

13. Alikulovich, V. D., Melitoshevich, V. A., & Kizi, O. F. O. (2024). KEY FEATURES OF LEARNINGAPPS IN IMPROVING THE KNOWLEDGE OF MEDICAL STUDENTS. *Eurasian Journal of Academic Research*, *4*(3-2), 142-145.

14. Voxidov, D., Voxidov, A., & Aminov, J. (2023). MAIN FEATURES OF TRAINING APPLICATIONS IN INCREASING THE KNOWLEDGE OF MEDICINE STUDENTS. *Modern Science and Research*, *2*(12), 226-229.

15. Jaloliddin, A., & Alikulovich, V. D. (2023). TIBBIYOT YO'NALISHIDAGI TALABALARNI BILIMINI OSHIRISHDA LEARNINGAPPS NING ASOSIY XUSUSIYATLARI.

16. Вохидов, А. М., Вохидов, Д. А., & Давронова, З. М. (2023). Статистического Анализа В Медико-Биологических Исследованиях. *Miasto Przyszłości*, *42*, 232-237.

17. Voxidov, D., & Voxidov, A. (2023). PEDAGOGICAL CONDITIONS FOR EFFECTIVE DISTANCE LEARNING IN THE SYSTEM OF TRAINING OF ENVIRONMENTAL SPECIALISTS. *Modern Science and Research*, *2*(10), 436-442.

18. Вохидов, А. М., Вохидов, Д. А., Фармонова, Р. Ф., & Хафизова, Д. Ш. (2022). Разработка Графическим Пользовательским Интерфейсом-Программ В Пакете Tkinter С Использованием Современных Педагогических Технологий В Области Медицины. *Miasto Przyszłości*, *30*, 181-184.

19. Akhmedova, F., Shagazatova, B., Artikova, D., & Mirxaydarova, F. (2018, October). The course of Parkinson's disease in patients with impaired carbohydrate metabolism. In MOVEMENT DISORDERS (Vol. 33, pp. S176-S177). 111 RIVER ST, HOBOKEN 07030-5774, NJ USA: WILEY.

20. Shagazatova, B. X., Mirkhaydarova, F. S., Artikova, D. M., Axmedova, F. S., & Kudratov, N. A. (2019). FEATURES OF DIABETES MELLITUS IN HIV-INFECTED PATIENTS. Toshkent tibbiyot akademiyasi axborotnomasi,(1), 149-152.