Тип работы: Контрольная работа

Предмет: Информатика

Введение
В эпоху, когда цифровые взаимодействия и транзакции стали таким же обычным явлением, как и физические, необходимость точной проверки личности человека никогда не была столь острой. Целью данной статьи является изучение набора инструментов и протоколов, составляющих сложную структуру проверки и аутентификации личности. От традиционных методов, которые уже давно стали краеугольным камнем безопасности, до инновационных технологий, открывающих новые горизонты, в этом исследовании рассматривается, как функционируют эти механизмы, их применение и сложности, связанные с обеспечением подлинности человека в различных контекстах.
После этого мы рассмотрим различные средства аутентификации, начиная от факторов, основанных на знаниях, таких как пароли и PIN-коды, до факторов, основанных на владении, таких как смарт-карты и токены, а также факторов, основанных на природе, где в игру вступают биометрические данные.
Мы критически проанализируем сильные и слабые стороны, присущие этим методам, включая соображения удобства пользователя, финансовых последствий и уровня безопасности, обеспечиваемого каждым из них.
В последних разделах этого исследования основное внимание будет уделено системам многофакторной аутентификации, обсуждается их растущая необходимость перед лицом изощренных киберугроз и рассматривается их будущее в поясе постоянно меняющихся цифровых ландшафтов.
Наше исследование направлено на то, чтобы дать четкое представление о нынешнем состоянии средств идентификации и аутентификации, их значении в обеспечении личной и институциональной безопасности, а также проекции их траектории по мере нашего продвижения к все более цифровому будущему.
I. Идентификация и аутентификация: Основные понятия
Идентификацию и аутентификацию можно рассматривать как краеугольный камень программных и аппаратных средств безопасности, поскольку другие службы ориентированы на обслуживание идентифицированных объектов. Идентификация и аутентификация образуют основную линию защиты, представляя собой «ворота» в информационный домен организации.
Идентификация дает возможность субъекту (пользователю, процессу, действующему от имени конкретного пользователя, или программно-аппаратному компоненту) заявить о себе (озвучить свое имя). Посредством аутентификации другая сторона подтверждает, что субъект действительно является тем, за кого себя выдает. Этот процесс иногда называют синонимом «проверки подлинности».
Стоит в скобках отметить, что происхождение термина «аутентификация» в русском языке несколько неясно [9]. Английский термин «аутентификация» можно понимать более прямо как «аутентификация»; Происхождение дополнительного «фи» в середине неясно – возможно, из-за «идентификации»? Тем не менее, этот термин получил признание, закрепился в методических указаниях Государственной технической комиссии России и используется в многочисленных публикациях, поэтому корректировка его сейчас невозможна.
Аутентификация может быть односторонней (чаще всего клиент доказывает серверу свою подлинность) или двусторонней (взаимной). Примером односторонней аутентификации является процедура входа пользователя в систему.
В сетевой среде, где стороны территориально разделены, эта услуга имеет два основных аспекта:
- что служит аутентификатором (то есть используется для подтверждения подлинности предмета);
- как организован (и защищен) обмен идентификационными/аутентификационными данными.

Субъект может подтвердить свою подлинность, предъявив хотя бы одно из следующих документов:
- что-то известное им (пароль, персональный идентификационный номер, криптографический ключ и т. д.);
- что-то, чем они обладают (личная карта или подобное устройство);
- что-то присущее им (их голос, отпечатки пальцев, т. е. их биометрические характеристики).
В открытой сетевой среде без доверенного пути между сторонами это означает, что, как правило, данные, отправленные субъектом, могут не совпадать с данными, полученными и используемыми для проверки подлинности [15]. Требуется защита как от пассивного, так и от активного наблюдения за сетью – перехвата, изменения или воспроизведения данных. Открытая передача паролей явно неадекватна; шифрование паролей также не решает проблему, так как не защищает от повтора данных. Требуются более сложные протоколы аутентификации.
Надежной идентификации препятствуют не только сетевые угрозы, но и ряд причин. Во-первых, почти все объекты аутентификации можно узнать, украсть или подделать. Во-вторых, возникает дилемма между надежностью аутентификации и удобством как пользователя, так и системного администратора [8]. В целях безопасности необходимо периодически предлагать пользователю повторно ввести данные аутентификации (поскольку его место мог занять кто-то другой), что раздражает и повышает вероятность того, что кто-то проконтролирует ввод данных. В-третьих, чем надежнее средство защиты, тем оно дороже. Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. Прежде всего, единый вход необходим для удобства пользователя. Если в корпоративной сети имеется множество информационных сервисов, обеспечивающих независимый доступ, множественная идентификация/аутентификация становится слишком обременительной [13]. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, и доминирующих решений пока не сформировано.

1. Барабанова М. И., Кияев В. И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях [Текст]: Учебное пособие/ Барабанова М. И., Кияев В. И. СПб.: Изд-во СПбГУЭФ, 2010.- 267 с.
2. Басов О.О., Сайтов И.А. Основные каналы межличностной коммуникации и их проекция на инфокоммуникационные системы / Труды СПИИРАН. 2013. Вып. 7(30). С. 122—136.
3. Болл Руд М. и др. Руководство по биометрии // Москва, Техносфера. 2007. 368 с.
4. Варлатая, С. К. Биометрические данные как способ идентификации личности / С. К. Варлатая, Н. С. Рудных, В. М. Лужин. — Текст : непосредственный // Молодой ученый. — 2016. — № 7 (111). — С. 49-51. — URL: https://moluch.ru/archive/111/27402/ (дата обращения: 03.04.2024).
5. Выскуб В.Г., Прудников И.В. Повышение эффективности распознавания личности при использовании биометрической идентификации // Электротехнические и информационные комплексы и системы. 2011. Вып. 1. С. 28—32.
6. Денисова Д.М. Методы исследования воздействия сенсорных стимулов на психофизиологическое состояние человека, Труды СПИИРАН. 2009 г. Вып. 9. С. 219—227.
7. Жвалевский О.В., Рудницкий С.Б. Биометрический комплекс для инструментальной оценки психосоматического статуса человека, Труды СПИИРАН, 2009 г. Вып. 8. С. 61—77.
8. Иванов А. И. Биометрическая идентификация личности по динамике подсознательных движений [Текст]: Монография./ Иванов А. И. — Пенза: Изд-во Пенз. гос. ун-та, 2000. — 188 с.
9. Казарин М. Н. Разработка и исследование методов скрытного клавиатурного мониторинга [Текст]: автореф. дис... канд. техн. наук; 05.13.19. /Таганрог, 2006.- 181 с.
10. Рудаков, О. М. Метод биометрической аутентификации, основанный на анализе клавиатурного почерка / О. М. Рудаков. — Текст : непосредственный // Молодой ученый. — 2016. — № 11 (115). — С. 448-451. — URL: https://moluch.ru/archive/115/30980/ (дата обращения: 03.04.2024).
11. Скубицкий А.В. Анализ применимости метода реконструкции динамических систем в системах биометрической идентификации по клавиатурному почерку // Инфокоммуникационные технологии. Т. 6. № 1. 2008.
12. Чистяков, М. В. Методы идентификации пропусков и основные требования к системе контроля и управления доступом и безопасностью учреждения / М. В. Чистяков. — Текст : непосредственный // Молодой ученый. — 2016. — № 11 (115). — С. 241-243. — URL: https://moluch.ru/archive/115/30686/ (дата обращения: 03.04.2024).
13. Шарипов Р. Р. Разработка полигауссового алгоритма аутентификации пользователей в телекоммуникационных системах и сетях по клавиатурному почерку: автореферат диссертации на соискание ученой степени канд. техн. наук: 05.12.13 / Р. Р. Шарипов. — Казань, 2006. — 16 с.
14. G. Leggett, J. Williams and D. Umphress. Verification of User Identity via Keystroke Characteristics. Human

Factors in Management Information Systems, 1989.
15. Hiromasa Fujihara, et al. Speaker Identification under Noisy Environments by Using Harmonic Structure Extraction and Reliable Frame Weighting // INTERSPEECH 2006 — ICSLP September 17—21, Pittsburgh, Pennsylvania, pp 1459— 1462.
16. L. Rothkrantz et al. Voice Stress Analysis. Text, Speech and Dialogues, ISBN 3-540-23049-1, Lecture Notes in Artificial Intelligence, P. 449—456, Springer, Berlin-Heidelberg-New York, 2004.
17. M. Sigmund Spectral Analysis of Speech under Stress. Int. Journal of Computer Science and Network Security, vol. 7. P. 170—172. 2007.