УДК 004.4

С. А. Айвазян
Л. М. Куперштейн

ДОСЛІДЖЕННЯ СИСТЕМИ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ГОЛОСУ

Вінницький національний технічний університет

Анотація

Розроблено систему двофакторної автентифікації програмного додатку на основі голосу. Розпізнавання голосу реалізовано за допомогою інтелектуального хмарного сервісу. Оцінено достовірність автентифікації, що показала досить високі показники.

Ключові слова: кібербезпека, автентифікація, двофакторна автентифікація на основі голосу, база даних, хмарний сервіс.

Abstract

A two-factor voice-based authentication system software has been developed. Voice recognition is implemented through an intelligent cloud service. Authentication was evaluated, which showed fairly high performance.

Keywords: cybersecurity, authentication, two-factor voice-basis authentication, database, cloud service.

Вступ

У міру розвитку комп'ютерних мереж і розширення сфер автоматизації цінність інформації неухильно зростає.

Розвиток науки стає вихідним пунктом для створення нових галузей виробництва, продуктивною силою суспільства, що відбивається у глибоких змінах у взаємовідносинах науки й виробництва [1].

На сьогоднішній день для надійного захисту від несанкціонованого доступу використовується двофакторна автентифікація, яка забезпечує доступ до ресурсу зазвичай на основі паролю (1-й фактор) та ще одного унікального ідентифікатора (одноразовий пароль, апаратний токен, біометричний тощо) [2].

Метою роботи є дослідження доцільності використання двофакторної автентифікації на основі голосу від несанкціонованого доступу при розробці програмного засобу.

Результати дослідження

При дослідженні було розроблено алгоритми роботи системи автентифікації на основі голосу, зокрема визначено роботу кожного процесу та їх взаємодію із користувачем, впроваджено режими роботи програми при збереженні, читанні, записі та передачі даних до локальної бази даних, інтегровано роботу із хмарним сервісом, реалізовано систему двофакторної автентифікації на основі голосу у вигляді програмного десктопного додатку та проведено тестування [3].

Для тестування були обрані два критерії, які обов'язково повинні бути забезпечені для нормальної роботи програмного забезпечення. Перший критерій – відсутність помилок при роботі програми. Другий критерій і найважливіший, забезпечення всіх покладених на програму вимог, тобто мінімально можливу кількість помилкових спрацьовувань алгоритму порівняння зразків голосу користувача з еталонними зразками, збереженими в базі даних. Дослідження якості ідентифікації помилок першого роду та другого роду сприятиме до визначення порогового значення достовірності автентифікації для користувача.

FRR є добутком відношення числа відмов у доступі користувачам до загального числа спроб отримання доступу клієнтами і 100%. FAR є – добутком відношення числа надання доступу зловмисникам до загального числа спроб отримання доступу зловмисниками і 100% [4].

Хмарний сервіс має підготовлений набір даних, що складається із приблизно трьох тисяч людських голосів (жіночих та чоловічих) для подальшого використання при розпізнаванні голосу.

В цілому, проведено 25 тестувань з наступними результатами – 19 з 25 разів, хмарний сервіс розпізнав слово «лампа», з середнім значенням достовірності у 94-95%. Серед схожих слів найчастіше

розглядались слова «рампа» – 90%, «лама» – 88%, «ламб» – 88%, «лава» – 88%, «ламбада» – 86%, “Трамп» – 80%. При невдалих спробах пройти автентифікацію, хмарний сервіс розпізнавав слова «рампа» – 86-94%, «лама» – 81-90% та «лава» – 80-87%.

FRR – є значенням кількості «своїх», що не пройшли поріг, відповідно проведеному тестування його значення = 6 / 25 * 100% = 24%, що є задовільним результатом, адже важливішим фактором для системи автентифікації на основі голосу є відсутність можливості отримання доступу зловмисником.

FAR – є значенням допуску «чужих», що пройшли поріг, відповідно результатам тестування, значення FAR = 3 / 25 * 100 = 12%. Даний відсоток є не поганим результатом, адже зловмиснику доведеться витратити чимало часу, щоб досягнути результату при проходженні систем автентифікації.

Значення EER (точку перетину FAR та FRR) дорівнює:

$$(FAR + FRR) / 2 = 18\%$$

Тестування проводилось при різних умовах введення голосу від людини, зокрема коли людина була здоровою, хворою, знаходилась в умовах без шуму та навпаки. Для успішної автентифікації людина повинна мати ймовірність ідентифікації більше 85%, інакше автентифікації не буде пройдено. Середній час створення облікового запису – 2,5 хвилини, автентифікації – 2 хвилини.

У таблиці 1 описано усі варіації тестування та ймовірності ідентифікації людини, а рисунки 1-2 відображують її дані.

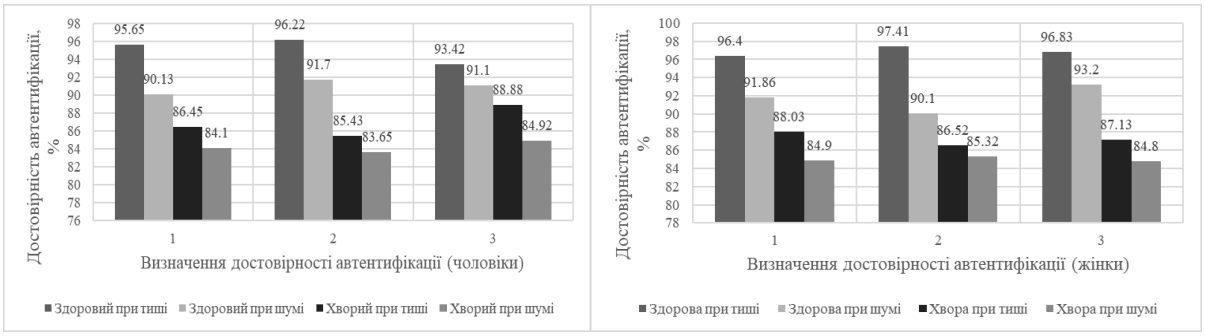

Рисунок 1 – Діаграма результатів визначення достовірності автентифікації жінок та чоловіків

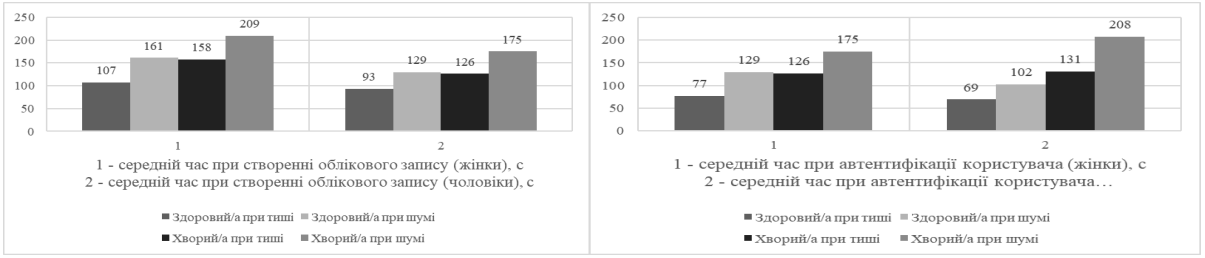

Рисунок 2 – Діаграма результатів визначення середнього часу при автентифікації для жінок та чоловіків

Таблиця 1 – Тестування процесу автентифікації людини за голосом при різних умовах

№	Людина	Умови	Достовірність автентифікації, %			Середній час при створенні облікового запису, хв	Середній час при автентифікації користувача, хв
1	Чоловік №1	Здоровий при тиші	95.65%	96.22%	93.42%	01:33	01:09
2	Чоловік №2	Здоровий при шумі	90.13%	91.7%	91.1%	02:13	01:42
3	Чоловік №3	Хворий при тиші	86.45%	85.43%	88.88%	02:38	02:11
4	Чоловік №4	Хворий при шумі	84.1%	83.65%	84.92%	03:29	03:28

Продовження таблиці 1

5	Жінка №1	Здорова при тиші	96.4%	97.41%	96.83%	01:47	01:17
6	Жінка №2	Здорова при шумі	91.86%	90.1%	93.2%	02:41	02:09
7	Жінка №3	Хвора при тиші	88.03%	86.52%	87.13%	02:45	02:06
8	Жінка №4	Хвора при шумі	84.9%	85.32%	84.8%	03:59	02:55

Час реєстрації облікового запису в середньому займав від 1,5 до 3 хвилин, найбільше часу займає процес запису «голосового відбитку» через стан здоров'я людини і шуми (чи їх відсутність) та надіслання його до хмарного сервісу, що займається розпізнаванням голосу. Чоловіки при цьому, впоралися за коротший час, ніж жінки (дельта між виконанням – приблизно 30 секунд).

На автентифікацію користувача було витрачено менше часу, ніж на створення облікового запису, через просту форму класичної автентифікації та швидку перевірку хмарним сервісом ідентифікації користувача на основі його голосу. При часу автентифікації між чоловіками і жінками визначилась гендерна рівність (з невеликою перевагою чоловічої статі).

Для збільшення значення достовірності автентифікації користувач повинен забезпечити умови відсутності шумів, не дивлячись на наявність в хмарному сервісі засобу фільтрації, а також мати гарний стан здоров'я.

Тестування проводилося на застарілій звуковій карті, що інтегрована в материнську плату. Картка з високим рівнем шуму та ігноруванням високих і низьких частот, а також зі слабким мікрофоном, який не забезпечує необхідний рівень запису. З хорошою звуковою картою, можна домогтися значно кращих результатів. Помилок в програмі в ході тестування виявлено не було.

Висновки

У процесі дослідження проведено тестування та визначено похибку при тестуванні помилок першого та другого роду, достовірність автентифікації користувача при різних варіантах порівняння «голосового відбитку». Виявлено відсоток похибки при автентифікації користувача, середній час, що необхідний для створення облікового запису та автентифікації у систему.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи / Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.
2. Лужецький В. А., Кожухівський А. Д., Войтович О. П. Основи інформаційної безпеки: навчальний посібник – Вінниця: ВНТУ, 2013. – 221 с.
3. Куперштейн Л., Лукічов В., Айвазян С. Система двофакторної автентифікації на основі голосу. [Електронний ресурс]. – Режим доступу: http://www.konferenciaonline.org.ua/arhiv-konferenciy/arhiv-konferenciy11-06-2019 – Назва з екрану.
4. Джейн А. К., Флінн П., Росс А. А. Посібник з біометрики – Springer Science, 2008. — 553 с.

Айвазян Самвел Арманович — студент групи 1БС-19м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: 1bs15b.ayvazian@gmail.com

Куперштейн Леонід Михайлович — кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Ayvazian Samvel A. — Student of 1BS-19m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: 1bs15b.ayvazian@gmail.com

Kupershtein Leonid M. — Candidate of Technical Sciences, Docent of the Information Security department, Vinnytsia National Technical University, Vinnytsia, email: kupershtein.lm@gmail.com