ЗАХИСТ ІНФОРМАЦІЇ У СИСТЕМАХ ГОЛОСОВОЇ АВТЕНТИФІКАЦІЇ

Квашенко В.Р.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

E-mail: vladyslav.kvashenko@nure.ua

Abstract

Voice authentication has gained significant attention as a biometric security measure in various applications, including mobile devices, financial services, and access control. However, it introduces unique cybersecurity challenges. This paper explores the evolving landscape of voice authentication, delving into vulnerabilities and countermeasures to ensure the integrity and privacy of user data. From voice imitation attacks to the intricacies of secure voice biometrics, we discuss the multifaceted dimensions of voice-based security. This research aims to contribute to the growing field of cybersecurity in voice authentication systems.

Голосова автентифікація – це форма ідентифікації людини на основі унікальних біометричних характеристик — у цьому випадку голосу. Голос унікальний, як відбиток пальця, і складається з комбінації таких характеристик, як діалект, висота та швидкість вимови. Голосову автентифікацію важче підробити, ніж відбитки пальців, і її не можна зламати, як паролі, що робить її більш безпечнішим методом автентифікації. Крім того, голосова автентифікація зручніша за інші форми біометричної автентифікації (наприклад, сканування райдужної оболонки ока), оскільки людина може автентифікуватись віддалено.

З часом все більше можливостей стають нам доступні віддалено, наприклад, під час використання таких сервісів як електронний банкінг, електронна охорона здоров'я, компанії стикаються з реальною потребою в надійних та легких у використанні методах автентифікації для захисту конфіденційної та персональної інформації. Точна автоматична ідентифікація особи стає критичною для широкого спектру застосувань.

Зловмисник може отримати доступ до персональних банківських акаунтів, електронних медичних кабінетів, підтвердити списання грошей або збирати конфіденційну інформацію для використання у своїх цілях.

Види атак на системи голосової автентифікації

Атакам на системи голосової автентифікації приділяється все більше уваги як серед зловмисників так і серед спеціалістів з кібербезпеки. Так, згідно з [1], в 2019 році впровадження голосової автентифікації в компаніях допомогло зменшити втрати від телефонних атак на 300 мільярдів. А по прогнозам Reports and Data [2], глобальний ринок голосових біометричних рішень становитиме 3,9 мільярда доларів США до 2026 року, при середньорічному темпі зростання у 23,5%.

Атаки на запис голосу (Voice Recording Attacks) є одними з найпоширеніших способів атак на системи голосової автентифікації. У цих атаках зловмисники намагаються отримати запис голосу користувача без його належного дозволу і використовувати цей запис для автентифікації в системі. Серед методів отримання зразку запису голосу вирізняють соціальну інженерію – зловмисники можуть переконати користувача сказати певні фрази, представляючись як довірені особи. Також зразок голосу може бути отриманий з соціальних мереж – зловмисники можуть отримати голосові профілі з соціальних мереж користувачів, або використовувати записи з онлайн-засобів спілкування або мессенджерів. Для протидії атакам на запис голосу пропонують використовувати двофакторну аутентифікацію, використовувати активну голосову автентифікацію, під час якої користувач має повто-

рити назване випадкове слово. Зловмисники використовують цей метод через простоту отримання голосового запису. Атаки імітації голосу (Voice Impersonation Attacks) є способом атаки на системи голосової автентифікації, коли зловмисники намагаються вимушити систему вважати, що голос, яким користується зловмисник, є голосом авторизованого користувача. Інструментами атаки може бути – голосове моделювання, штучний інтелект. Для протидії атаці можна використовувати двофакторну аутентифікацію, аналіз голосового зразку на аномалії, або згідно з [3], використовувати машинне виявлення уособлення голосу, яке аналізує зміну в магнітному полі динаміків для виявлення машинного імітатора, замість аналізу акустичних характеристик зразків. Атаки на передачу голосу (Voice Transmission Attacks) це атаки, які спрямовані на отримання голосових даних користувача під час їх передачі через комунікаційну мережу, таку як телефонний додаток або голосовий чат. Зловмисники можуть намагатися перехопити, записати або використовувати ці голосові дані для недозволеної автентифікації в системі. Методами виконання таких атак може бути – перехоплення голосового трафіку—зловмисники можуть намагатися перехопити трафік для подальшого його аналізу та використання для проведення атак, маніпуляція голосовим записом– якість, тембр, частота або швидкість голосового запису може бути змінена, щоб видати себе за іншого користувача. Методи захисту від таких атак є шифрування голосових даних, моніторинг мережі на предмет виявлення аномальної активності, використання заходів безпеки на рівні мережі. Атаки на внутрішні системи (Internal System Attacks) це атаки, спрямовані на отримання несанкціонованого доступу до систем, що зберігають голосові дані користувачів і голосові моделі для голосової автентифікації. Ці атаки можуть бути надзвичайно небезпечними, оскільки зловмисники можуть мати доступ до чутливих особистих даних і використовувати ці дані для недозволеної аутентифікації або для інших шкідливих цілей. Методами виконання таких атак є – будь-який несанкціонований доступ до серверів та баз даних, витік конфіденційної інформації. Методами захисту може бути шифрування даних, встановлення параметрів доступу, використовуючи принцип least privilege, та періодичне оновлення та актуалізація даних.

Висновки

Голосова автентифікація є важливим інструментом для ідентифікації користувачів на основі їх унікальних голосових характеристик. Вона забезпечує високий рівень безпеки і комфорту для користувачів у різних галузях, таких як банківська сфера та охорона здоров'я. Проте голосова автентифікація не є безпечною від усіх можливих атак.

Зловмисники активно працюють над знаходженням способів атак на системи голосової автентифікації, такі як атаки на запис голосу, імітацію голосу, атаки на передачу голосу та атаки на внутрішні системи. Для протидії цим атакам, потрібно впроваджувати ефективні методи безпеки, такі як двохфакторна аутентифікація, шифрування голосових даних, та інші. У майбутньому голосова автентифікація продовжить розвиватися і розширюватися в різних галузях. Очікується, що розвиток передових технологій розпізнавання голосу та використання штучного інтелекту значно підвищить точність та надійність систем голосової автентифікації. Збільшена усвідомленість щодо безпеки серед користувачів також сприятиме покращенню захисту від потенційних атак.

В цілому, голосова автентифікація залишається важливою складовою сучасних систем безпеки, і її майбутній розвиток спрямований на підвищення безпеки та зручності користувачів у цифровому світі.

Література

1. DEREK T. Opus Research Report: “2019 Intelligent Authentication and Voice Biometrics Intelliview” [Електронний ресурс] / TOP DEREK. – 2019. – Режим доступу до ресурсу: https://opusresearch.net/wordpress/2019/06/27/opus-research-report-2019-intelligent-authentication-and-voice-biometrics-intelliview/.

2. Voice Biometrics Market To Reach USD 3.91 Billion By 2026 [Електронний ресурс] // Reports And Data. – 2019. – Режим доступу до ресурсу: https://www.globenewswire.com/news-release/2019/10/08/1926845/0/en/Voice-Biometrics-Market-To-Reach-USD-3-91-Billion-By-2026-Reports-And-Data.html.

3. You Can Hear But You Cannot Steal: Defending against Voice Impersonation Attacks on Smartphones [Електронний ресурс] / [C. Si, R. Kui, P. Sixu та ін.] – Режим доступу до ресурсу: https://par.nsf.gov/servlets/purl/10042568.