УДК 004.056.53 **DOI:10.30837/rt.2022.4.211.12**

О.Й. ДОВНАР, канд. техн. наук, М.Ф. БАБАКОВ, канд. техн. наук, В.І. ЧЕРКІС

ВИКОРИСТАННЯ СКАНЕРУ ВІДБИТКІВ ПАЛЬЦІВ ДЛЯ ЗАХИСТУ ДАНИХ У МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Вступ

В умовах інформаційних війн та постійних DoS нападів бази та сервери підпадають під постійну загрозу. Більшість баз захищені лише стандартними системами авторизації, що може стати фатальним, особливо для закладів охорони здоров'я. Так, на офіційному інформаційному ресурсі Державної служби спеціального зв'язку та захисту інформації України [1] зазначено, що у ІІІ кварталі 2022 р. кількість кібератак на критичну інформаційну інфраструктуру України значно зросла і з 15-го лютого Україна зазнала понад 3000 DDoS-атак.

Таким чином, актуальність обмеження доступу до коитичної інформації наразі має найвищу степінь, а розробка систем або проистроїв може повністю змінити погляд на інформаційне устаткування та його захист. Задля убезпечення захисту інформації наразі застосовують DNS маски та блокування надмірних запитів. Це певною мірою покращує ситуацію або дозволяє швидше переналаштувати сервер, що знаходиться під атакою. Альтернативне рішення цієї проблеми (наприклад, для закладів охорони здоров'я) – це просте устаткування для авторизації сесії, а у всіх інших випадках – ігнорування або блокування доступу.

Рішення, яке може спростити та покращити заходи безпеки, – заміна технології, що використовує звичайну пару логін/пароль, зчитування відбитків пальців.

Ідентифікація за допомогою відбитків пальців – найбільш поширений біометричний спосіб визначення особистості. У сучасному світі відбитки пальців застосовується все більше, а саме: в криміналістиці, в медичній сфері, науці, в сучасній оборонній промисловості.

Метою розробки є забезпечення надійного захисту для серверів та баз даних шляхом ідентифікації користувачів до створення сесії.

Об'єктом для убезпечення доступу до аккаунту стане пристрій з можливостями сканування відбитків.

Вибір прототипу

Відбиток пальця – це відбиття, що залишає папілярні лінії (або візерунок) людського пальця. Відбиток пальця дуже легко залишається на відповідних поверхнях (наприклад, скло, метал або шліфований камінь) через фізіологічну властивість виділенню поту з екзокринних залоз, які присутні на епідермальній нерівності. Інколи існує можливість отримати неякісне зображення відбитка. Причинами цього є: жирна або ж суха шкіра рук, випадкові рухи під час зняття відбитка та великі пори. Використання неякісних зображень відбитків знижує прохідну здатність біометричних систем. Для уникнення таких проблем існують алгоритми визначення та поліпшення якості зображення відбитків пальців [2 – 7].

Біометричні прилади для доступу до баз даних зазвичай використовують FTIR сенсори або NFC датчики при авторизації за телефоном. Найчастіше використовують такі методи контроля доступу [6 – 8]:

- застосування ключ-карти;
- ідентифікація за райдужкою ока;
- ідентифікація за обличчям;
- застосування NFC датчика телефону.

У всіх цих методів є свої недоліки [9]. Так, вадою ключ-карти є простота копіювання, ідентифікація за райдужкою ока – складний та дорогий метод, ідентифікація скануванням обличчя не є достатньо достовірним методом. Окрім того, ці методи потребують драйверів для своєї працездатності. Таким чином, можна стверджувати, що використання сканеру відбитка пальця є найбільш придатним для рішення поставленої задачі ще й тому, що більшість питань стосовно його роботи та безпеки вже розглянуті.

Основним недоліком системи з авторизацією за відбитком є проблеми зі зчитуванням (у випадку відсутності відбитків людина не зможе пройти авторизацію), а також муляжі відбитків (залежить від схеми та типу сканеру).

Подібні схеми вже наявні на мобільних пристроях з скануванням відбитків. Їх основна мета – спростити та забезпечити безпеку, коли створюється нова сесія. При завантаженні додатка на мобільний пристрій записується відбиток пальця, а при наступній спробі відбувається ідентифікація – зчитування відбитку та порівняння його з записаним еталоном і у випадку успішної авторизації – створення сесії.

Що стосується комп’ютерів, то для подібної авторизації буде необхідний додатковий портативний пристрій – біометричний сканер відбитку та спеціальна програма для роботи з цим обладнанням, що ускладнює наш критерій простоти для роботи медичного персоналу. А влаштовані подібні рішення є лише у системі Windows 10, 11 у ideapad та thinkpad.

Таким чином, за технічними характеристиками необхідно розробити подібний до вбудованого пристрою сканер відбитків. Розглянемо основні типи сканерів, що застосовуються на даний час [10 – 15].

Оптичні сканери. Такі сканери працюють на основі використання оптичних методів отримання зображення. Існує кілька основних способів реалізації оптичного методу.

1. Оптичний метод відображення. У цьому методі використовується ефект повного внутрішнього відображення (Frusted Total Internal Reflection). Провідними виробниками таких сканерів є BioLink, Digital Persona, Identix.

2. Оптичний метод на просвіт. Сканери даного типу є оптоволоконною матрицею, в якій всі хвилеводи на виході з'єднані з фотодатчиками. Чутливість кожного датчика дозволяє фіксувати залишкове світло, що проходить через палець, у точці зіткнення пальця з поверхнею матриці. Цей метод характеризується високою надійністю зчитування та стійкістю до використання муляжів. Даний тип сканерів випускається американською компанією Security First Corp.

3. Оптичні безконтактні сканери. В оптичних безконтактних сканерах (touchless scanners) не потрібно безпосередньо контакту пальця з поверхнею скануючого пристрою. Провідний виробник сканерів цього типу Touchless Sensor Technology. Перевагами оптичних сканерів є відносно низька ціна та компактність. Недоліки: чутливість до забруднення, стану шкіри та слабка захищеність від муляжів та інших способів обману [8, 18 – 20]

Ємнісні сканери є найбільш поширеними напівпровідниковими пристроями для отримання зображення відбитка пальця. Їхня робота заснована на ефекті зміни ємності *p*-*n*-переходу напівпровідника при дотику гребеня папілярного візерунка з елементом напівпровідникової матриці. Перевагами таких сканерів є низька собівартість та висока надійність, а недоліками – слабка захищеність від муляжів. Провідними виробниками сканерів цього типу є Veridicom та STMicroelectronics

Радіочастотні сканери використовують матрицю елементів, що працюють як мініантени. Оскільки аналізуються фізіологічні властивості шкіри, ймовірність обману даного сканера прагне до нуля, але при поганому контакті з пальцем робота такого сканера може бути нестійкою. Відомим виробником радіочастотних сканерів є компанія Authentec.

Сканери, які використовують метод тиску у своїй конструкції, мають матрицю п'єзоелектричних елементів, чутливих до натискання. Чутливі до тиску сканери випускає компанія BMF. Недоліками таких сканерів є низька чутливість, неефективний захист від муляжів та схильність до пошкоджень при надмірно докладних зусиллях.

Термосканери використовують датчики, що складаються з піроелектричних елементів, та дозволяють фіксувати різницю температури і перетворювати її на напругу. Такий метод має безліч переваг: висока стійкість до електростатичного розряду, стійка робота в широкому температурному діапазоні, ефективний захист від муляжів. До недоліків цього методу можна віднести те, що зображення швидко зникає через те, що палець і датчик приходять до температурної рівноваги.

Ультразвукові сканери сканують поверхню пальця ультразвуковими хвилями. Перевагами таких сканерів є підвищена якість зображення та повний захист від муляжів. Недоліком є висока собівартість.

Таким чином, у якості прототипу було використано оптичний сканер завдяки його розповсюдженості та відносно невисокої вартості, а саме FPM10A, зображений на рис. 1.

Рис. 1. Сенсор сканування відбитків FPM10A

Технічні рішення

Оскільки доступ до серверу відбувається через браузер, то використовувати COM порт проблематично. Окрім того, є труднощі із драйверами. Тобто, потрібно мати пристрій, сумісний з стандартним набором драйверів. Саме таким апаратним рішенням є Arduino Pro Micro рис. 2, котра може імітувати мишку, клавіатуру, або джойстик.

Рис. 2. Arduino Pro Micro

Для збільшення об’єму пам’яті тут можлива комбінація з Micro sd, а для передачі даних через мережу – ESP8266. Схема підключення елементів показана на рис. 3.

Для взаємодії зі сканером задіяна стандартна бібліотека Arduino Fingerprint. Записати до пристрою можливо 255 відбитків, а перевірку правильності буде виконувати саме Arduino Pro Micro.

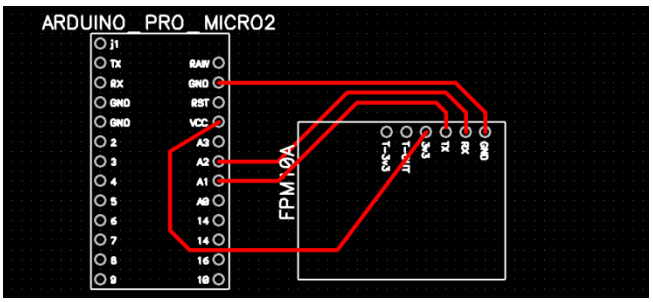
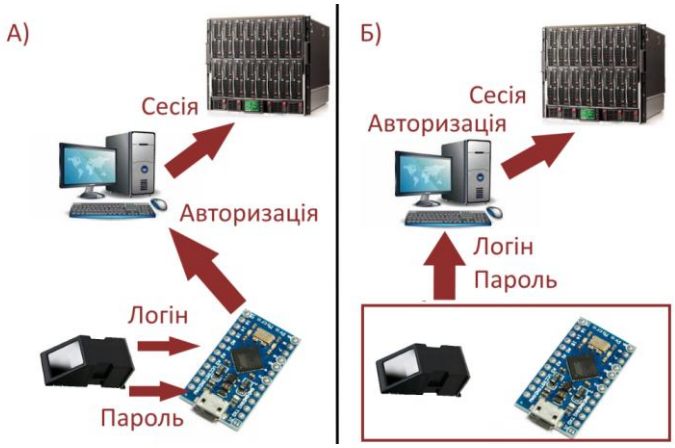


Рис. 3. Принципіальна електрична схема підключення

Можливі два варіанти взаємодії (рис. 4). Перший має на увазі перевірку та авторизацію прямо на Arduino Pro Micro, при цьому використовуються одразу два відбитки: один відповідає за логін, а інший – за пароль. У другому випадку авторизацію виконує комп'ютер за запитом програмного пристрою (рис. 4, *а*), або усі запити пристрою перевіряє комп'ютер (рис. 4, *б*). В обох варіантах потрібна спеціальна програма, котра перевірить особу у внутрішній базі та дозволить отримати доступ до веб-ресурсу. Оскільки локальні бази наявні майже у всіх закладах охорони здоров'я, то перехід до такого устаткування не викликатиме суттєвих змін, а лише дозволить забезпечити високий рівень захисту серверу, а також ідентифікувати користувачів.



а *б*

Рис. 4. Спосіб авторизації: *а* – сканер – пристрій; *б* – пристрій – комп'ютер

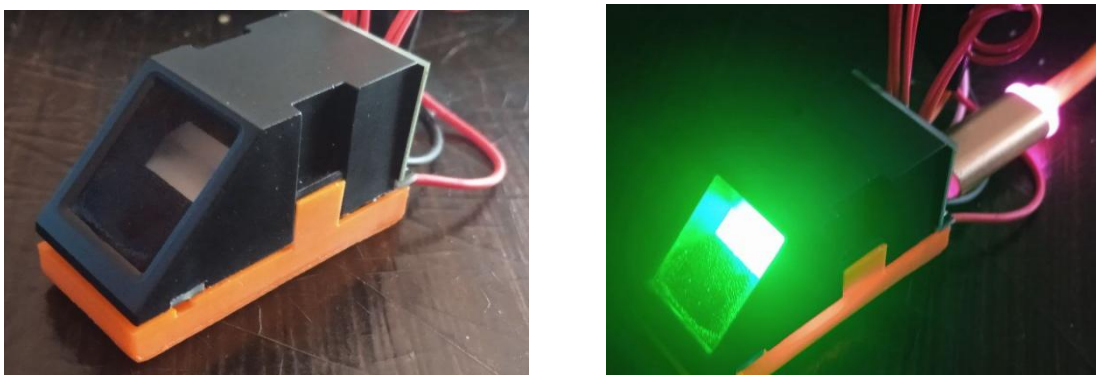
Більш надійним та зручним вважається другий спосіб, оскільки отримати доступ до серверу буде складніше за умови імітації одразу трьох складових частин.

Що стосується способів підробки та муляжів подібних пристроїв – захисний механізм використання передбачає наявність запрограмованої дати компіляції і весь програмний код на Arduino Pro Micro підпорядкований цьому формату дати та часу, що унеможливлює спосіб використання муляжу, а дата при повторній компіляції буде переналаштована, що зробить пристрій нефункціонуючим. Таким чином, пристрій важко підробити та легко налаштувати під конкретний заклад.

Перевірка технічних рішень

Для простоти збірки була розроблена та надрукована 3D модель, що покращує властивості передачі та збільшує строк роботи пристрою. Результат зображено на рис. 5. Загальний розмір прототипу склав 46x25x23 мм, що робить його аналогом кишенькового носія пам'яті, а також економним та зручним у застосуванні. Пристрій не потребує зовнішнього джерела електроенергії та підключається звичайним USB кабелем зарядки до користувацького

комп’ютеру. Для застосування потрібно лише перейти до програми та прикласти спочатку палець-логін, а після підтвердження – палець-пароль, що забезпечує максимальну надійність.



а *б*

Рис. 5. Прототип пристрою сканування: *а* – загальний вигляд пристрою; *б* – пристрій у робочому стані

Тестування прототипу проводилось на серверній програмі VinGo v2.3 (рис. 6) та VsLabLite v4.2. Авторизація пройшла успішно у 28 випадках із 30, а у категорії з помірними знаннями та навичками у комп’ютерній сфері успішних було 26 спроб з 30. При цьому не було жодної помилкової авторизації.

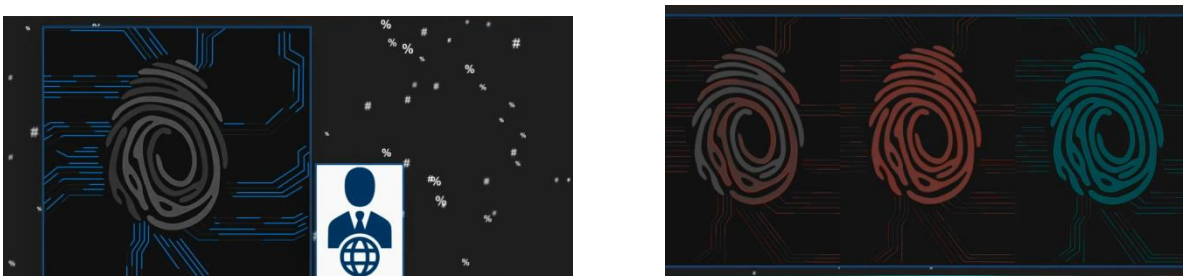


Рис. 6. Вікна тестування прототипу

Розробка функціонує строго за заданим алгоритмом та заблокує пристрій у разі декількох невдалих спроб авторизації, а спосіб авторизації дозволить отримати доступ до акаунту та сесії лише у випадку успішного зчитування обох пальців, що майже унеможливлює напад на сервери та бази даних.

Висновки

Розроблений простий та ефективний пристрій для попередньої авторизації до цільового об’єкту за відбитком. В основу входить плата, що надає стандартний набір драйверів та зумовлює простоту використання на будь-якій платформі (Windows, Linux, Mac). Розробка не потребує батареї та постійного джерела живлення, що робить її економною. Виріб є компактним та зручним у застосуванні, що для медичного персоналу є суттєвим. Пристрій має високий рівень захисту від помилкової авторизації завдяки двохетапній автентифікації, а також надійний захист від муляжів та спроб злому, що дозволяє застосовувати його у медичних та військових сферах.

Список літератури:

1. Державна служба спеціального зв’язку та захисту інформації України [Електронний ресурс] Режим доступу: https://cip.gov.ua/ua/news/kilkist-kiberatak-na-ukrayinu-prodovzhuye-zrostati

2. Л. Монастирський, В. Лозинський, Я. Бойко, Б. Соколовський. Розпізнавання відбитків пальців у недорогій біометричній системі // Електроніка та інформаційні технології. 2018. Випуск 9. С. 120 – 124.

3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. Москва : ДМК Пресс, 2012. 544 С.
4. Патент 67772 України МПК 7G06K9/20, A61B5 / 117. Спосіб та пристрій для ідентифікації особи шляхом безконтактного розпізнавання ліній руки і пальців / Хауке Рудольф, DE, Айнігхаммер Хайнс Й., DE, Айнігхаммер Йєнс, DE., заявник і патентовласник – ТСТ-ТАЧЛЕСС СЕНСОР ТЕКНОЛОДЖИ СЕЙЛЗ ЕНД МАРКЕТІНГ АГ, СН
5. Унгул В., Проценко М. Метод поліпшення якості зображення відбитків пальців за допомогою фільтра Габора // Междунар. научн. журнал // 2016. № 6, т. 2. С. 15 – 18.
6. Fingerprint Sensor FPC1011F [Електронний ресурс] // Fingerprint. Режим доступу: http://www.fingerprint.se/en/Products/All%20products%20overview.aspx?sc_lang=en.
7. Product Specifications TCS5 TouchStrip® Fingerprint Sensor (TCEEA4 (TCS4C+TCD50A)) [Електронний ресурс] // Upek. Режим доступу: http://www.upek.com/solutions/productfinder/
8. AuthenTec Fingerprint Sensors AES2660 [Електронний ресурс] // Authentec. Режим доступу: http://www.authentec.com/products-pcsandperipherals.cfm.
9. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. Москва : Горячая линия Телеком, 2010. 272 с.
10. NI Vision Assistant Tutorial [Електронний ресурс]. Режим доступу: http://www.ni.com/pdf/manuals/372228a.pdf
11. International biometrics and idenity association [Електронний ресурс]. Режим доступу: www.ibia.org.
12. Biolink біометричні системи [Електронний ресурс].
13. Biometric terminals add security to a variety of processes [Електронний ресурс]. Режим доступу: www.bioscrypt.com
14. From identity and secure access to biometric identity [Електронний ресурс]. Режим доступу: www.crossmatch.com
15. Everywhere Identity Matters [Електронний ресурс]. Режим доступу: www.identix.com

Надійшла до редколегії 20.10.2022

Відомості про авторів:

Довнар Олександр Йосипович – канд. техн. наук, доцент, Національний аерокосмічний університет ім. М.Є Жуковського «Харківський авіаційний інститут», доцент кафедри Радіоелектронних та медичних комп'ютеризованих засобів та технологій, Україна; email: a.dovnar@khai.edu; ORCID: https://orcid.org/0000-0001-7171-0024

Бабаков Михайло Федорович – канд. техн. наук, доцент, Національний аерокосмічний університет ім. М.Є Жуковського «Харківський авіаційний інститут», професор кафедри Радіоелектронних та медичних комп'ютеризованих засобів та технологій, Україна; email: m.babakov@khai.edu; ORCID: https://orcid.org/0000-0001-8642-3693

Черкіс Владислав Ігорович – студент, Національний аерокосмічний університет ім. М.Є Жуковського «Харківський авіаційний інститут», Україна, email: v.i.cherkis@student.khai.edu