ВИДИ БІОМЕТРІЇ В МОБІЛЬНИХ ДОДАТКАХ

Соколова В. К.
Науковий керівник – к.т.н., ст. викл. Ткачов В. М.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. ЕОМ, тел. (057) 702-13-54)
e-mail: d_ec@nure.ua

User identification is required in many applications that process personal data, such as online banking. According to a Spiceworks study, more than 60% of companies in Europe and North America use biometrics to protect their data and believe that this method is more reliable than a pin code or a combination of login and password. 10% of respondents are sure that only biometrics is enough for identification, while other companies insist on using additional methods. This publication provides an overview of biometrics and data security in today's world.

Для ідентифікації користувача в додатку можна використовувати біометрії - наприклад, відбиток пальця, сканери райдужної оболонки ока або геометрії обличчя.

Популярні способи біометричної ідентифікації:

- сканер відбитка пальця (fingerprint) - 57%;
- сканер геометрії особи (face ID) - 14%;
- сканер райдужної оболонки ока (IRIS) - 5%;
- геометрія руки - 4%.

Існують і інші способи аутентифікації, наприклад, голосова біометрія проте, їх надійність нижче, тому звертаються до них рідше.

Сканер відбитка пальця (fingerprint).

Кожен виробник мобільних пристроїв пропонує свої методи отримання та зберігання даних користувача. Так, на пристроях Apple зразок відбитка пальця проводиться через хеш-функцію перед збереженням в захищений обчислювальний модуль. Всі процеси, що пов'язані з Touch ID, відбуваються саме в цьому модулі, і такі дані неможливо витягти з нього. На пристроях Android ступінь безпеки залежить від виробника та які він використовує підходи і рішення. Як правило, робота зі сканерами відбитка пальця регламентується окремими документами, в тому числі специфікаціями Google. Провідні виробники смартфонів, такі як Samsung, використовують досить надійні та точні ємнісні сенсори, що забезпечують високу ступінь безпеки даних. Однак, окремі невеликі компанії можуть застосовувати менш надійні сенсори і зберігати відбитки на пристрої, іноді навіть у вільному доступі.

Сканер геометрії особи (face ID).

Якщо додаток ідентифікує користувача по обличчю, то сканування здійснюють за рахунок ємнісної камери. У порівнянні з попереднім способом, тут потрібно ще більш складний алгоритм, що вимагає високої точності захоплення зображення та розподілу більше ніж 30 тисяч

контрольних точок по зображенню особи користувача. У свою чергу, це визначає більш високі вимоги до камери смартфона. На практиці ємнісний сканер вивчає обличчя користувача, вибудовуючи геометричну модель і перетворюючи її в результати обчислення, які можна зберігати. Під час авторизації результат обчислення (з урахуванням похибки) для конкретного користувача зіставляється з результатом, що зберігаються в пам'яті. При цьому не всі пристрої надають повноцінні можливості для розпізнавання осіб. Інколи виробники обмежуються 2D-скануванням за допомогою звичайної камери. Як правило, при цьому на зображенні виділяється особа, яку можна порівняти з іншими зображеннями в базі. Якщо з додатком не вдасться знайти відмінності, то користувач може бути розпізнаний як власник.

Сканер райдужної оболонки ока (IRIS).

IRIS - це не сканер сітківки ока. Ця технологія сканує райдужну оболонку, яка оточує зіницю, тоді як сітківка розташовується всередині очі на задній стінці. Сканер визначає особливості зовнішності користувача і геометричну форму райдужки, використовуючи ємнісні камери. Хоча такий спосіб біометричного захисту може здатися перспективним, у нього є свої уразливості. З одного боку, для зняття блокування недостатньо знайти і пред'явити фотографію власника, адже камера визначає обсяг зображення. Однак, такий ризик вище при одночасному використанні фотографії та контактних лінз. Сканер сітківки ока в цьому відношенні може бути безпечніше, оскільки дані власника неможливо отримати у відкритих джерелах або вгадати.

Список використаної літератури:

1. Vitalii Tkachov, Anna Budko, Kateryna Hvozdetska and Daryna Hrebeniuk. Method of Building Dynamic Multi-hop VPN Chains for Ensuring Security of Terminal Access Systems // IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T): Kharkiv 06-09 oct. 2020, Kharkiv.

2. Tkachov, V., Bondarenko, M., Ulyanov, O., & Reznichenko, O. (2019, December). Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT) (pp. 161-165).

3. Tkachov, V., Hunko, M., Volotka, V.: Scenarios for Implementation of Nested Virtualization Technology in Task of Improving Cloud Firewall Fault Tolerance. In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), pp. 759-763. IEEE (2019).