Недоліки біометричної системи аутентифікації для захисту інформації

Бордюг Георгій
зав. кафедри ННІІДС ЗЗІ НАУ, професор, д.т.н. Козловський В.В,
ННІІДС, Національний авіаційний університет
м. Київ
georgebordiuh@gmail.com

***Анотація* — Розглядаються основні системи біометричної аутентифікації: аутентифікація по відбиткам пальців, по геометрії обличчя та по голосу. Визначені недоліки кожної з систем, наведені принципи роботи кожної з систем.**

Ключові слова — біометрія; аутентифікація; біометрична система захисту; захист інформації

I. Вступ

В наш час одним з найбільш перспективних напрямків в системах контролю доступу стає використання біометричних даних людини. Такий спосіб аутентифікації дуже зручний. Однак біометрія знаходиться на самому початку свого довгого шляху, і існує ряд проблем, пов'язаних з відносною новизною даної технології.

II. Види біометричної аутентифікації

A. Аутентифікація по відбиткам пальців

На даний момент існують три типи сканерів відбитків: оптичні (FTIR, оптоволоконні, оптичні протяжні та ін.), напівпровідникові (термосканери, протяжні термосканери, ємнісні та ін.) та ультразвукові. Всі вони працюють за різними принципами, але в підсумку отримують схожі зображення, які відповідно до визначених математичних алгоритмів перетворюються в контрольну суму. Можливими вразливостями даної технології можуть бути:

- Створення муляжу на основі латексу або желатину. Подібний муляж може спрацювати на простих сканерах.
- Перехоплення сигналу в разі, якщо сканер пов'язаний з основною системою через провідний інтерфейсом.
- Конденсація (напрямок струменя теплого повітря на сканер і, як результат, відновлення останнього відбитка).

Крім того, існує проблема розпізнавання пальця з порізами, "зморщуванням" шкіри та іншими дефектами, яку можна обійти за рахунок зняття декількох відбитків.

B. Аутентифікація по геометрії обличчя

Системи з розпізнавання геометрії особи працюють на основі фізичних і структурних ознак (форми особи, симетрії / асиметрії особи, форми та розміру губ, носа, очей та ін.). Отримавши зображення особи, система унікальний шаблон, який порівнюється зі зразком, що зберігається в базі данних. Дані системи вже застосовуються на вулицях і в аеропортах багатьох міст світу. Мінуси даної технології:

- Зміна освітленості, міміки, волосяного покриву, наявність або відсутність макіяжу та інші зміни перешкоджають розпізнаванню особи.
- Обман системи за допомогою фотографії особи зареєстрованого користувача або перебір фотографій з різними типами осіб спрацьовує на біометричних системах, встановлених на ноутбуках декількох великих виробників.
- Система не може відрізнити близнюків.

C. Аутентифікація по голосу

Її впровадження викликано постійним зростанням і поширенням телефонних ліній різного типу. Даний вид біометрії заснований на аналізі характеристик голосу: гучності, швидкості, манері мови і ін.

Основні проблеми даного виду аутентифікації:

- зміна голосу (емоції, стан здоров'я);
- перешкоди в мікрофоні і лініях зв'язку;
- перехоплення конфіденційної інформації порушником.

III. Висновок

Біометрична система аутентифікації є новинкою у сфері технічного захисту інформації. Для її належного використання потрібно розуміти, коли її використання буде доцільним. Варто не забувати про основні проблеми подібних систем і, за можливості, виправити їх при її використанні.

Список використаних джерел

[1] Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. - Пенза: ПГУ, 2000.

[2] Гузик В.Ф., Десятерик М.Н. Биометрический метод аутентификации пользователя. // «Известия ТРТУ» №2 (16), ТРТУ, Таганрог, 2000.

[3] Задорожный В. Обзор биометрический технологий // Защита информации. Конфидент. -2003. - № 5

Фор А. Восприятие и распознавание образов. - М .: Машиностроение