АНАЛІЗ МЕТОДІВ ЗАХИСТУ БІОМЕТРИЧНИХ ШАБЛОНІВ

Ляшенко Г. Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Використання біометричних характеристик людини для автентифікації швидко замінює звичайні паролі. Унікальність біометричних характеристик дає великі переваги для вірного надання доступу під час автентифікації, але вони потребують надійного захисту, тому передача їх у відкритому вигляді не є можливою.

Метою доповіді є огляд процесів, які проходять під час передачі даних для віддаленої автентифікації мережею, огляд можливих атак в мережі та обрання методів, які підвищують захищеність даних під час віддаленої автентифікації під час передачі відкритими каналами зв'язку.

В доповіді наводяться існуючі типи атак, що можуть виникнути під час віддаленої автентифікації. До таких атак можна віднести можливе використання фальсифікованих біометричних характеристик користувача, поновлення та використання старих даних, які були використані раніше під час автентифікації; несанкціонований доступ до сформованого біометричного шаблону під час автентифікації, його підміна або підміна шаблону, який зберігається в базі даних; вплив з метою підміни рішення під час порівняння біометричних шаблонів; перехоплення даних під час передачі каналами зв’язку. Також в роботі розглядаються основні підходи до захисту біометричних шаблонів. Одним з ефективних методів є метод «соління», необхідний в цьому методі ключ збільшує ентропію та призводить до збільшення відстані Хемінга між даними біометричних зразків, що стає перевагою використання цього методу. Інший метод на основі однобічних перетворень дозволяє при компрометації ключа замінити шаблон та анулювати за допомогою специфічних функцій. Також ефективними є методи мережної стеганографії, які дозволяють скрити сам факт передачі даних, які необхідні для автентифікації. Наведені в роботі дані дозволяють обирати ефективні методи захисту шаблонів в залежності від мережі, якою передаються дані.

Список літератури

1. Astrakhantsev A. Noise resistance of remote authentication via LTE network / A. Astrakhantsev, G. Liashenko, A. Shcherbak // Information and Telecommunication Sciences – 2020 – Vol. 2, – P. 38-43.

2. Dodis. Y. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data / Y. Dodis, R. Ostrovsky, L. Reyzin, A. D. Smith. // SIAM J. Comput. – 2008. – Vol. 38, no. 1. – pp. 97-139.