https://www.business-gazeta.ru/news/362049 (дата звернення: 27.10.2017).

Одержано 30.10.2017

УДК 004.93

Владислав Вячеславович БОРОДАВКА,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»

Михайло Віталійович ЦУРАНОВ,
старший викладач кафедри комп'ютерних систем та мереж Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»

ВИКОРИСТАННЯ БІОМЕТРИЧНОГО КОНТРОЛЮ ДОСТУПУ ДО LINUX СЕРВЕРІВ ДЛЯ ПРОТИДІЇ НЕСАНКЦІОНОВАНОМУ ДОСТУПУ

З розвитком інформаційних технологій все більша кількість сервісів переноситься на хмарні платформи і використовує технологію клієнт-сервер для забезпечення безпечної обробки і зберігання даних. Для забезпечення контролю доступу до серверів і серверних приміщень використовуються різні СКУД (Системи контролю управлінням доступом). У цих системах використовуються різні токени для автентифікації користувачів: RFID мітки, смарт-карти, uaTocken і т.д.

Останнім часом все більшого поширення в СКУД отримують системи біометричної автентифікації (БА) користувача. Системи БА – системи, що використовують для ідентифікації особи людей їх біометричні дані [1]. Біометрія передбачає систему розпізнавання людей по одній або кільком фізичним, або поведінковим характеристикам людини. В даний час методи БА стали більш досконалими, а надійна авторизація та автентифікація стають важливими атрибутами повсякденного життя [2, с. 18]. Широке застосування біометричних технологій (БТ) призводить до появи принципово нових видів загроз. Зараз БТ трансформувалися в повноцінний компонент систем захисту, інтеграція яких вимагає продуманого підходу.

Стрімкий розвиток технології клієнт-сервер призвело до виникнення значної кількості нових загроз, багато з яких отримали подальший розвиток в середовищі ОС Linux. Це стало можливим в результаті того, що Linux використовується в якості серверної ОС і за даними компанії Netcraft на вересень 2017 року, вісім з десяти найбільш надійних інтернет-

компаній, що надають хостинг, використовують Linux на своїх веб-серверах [3]. Linux є ключовим компонентом комплексу, що поставляється з серверним комплектом ПЗ LAMP (Linux, Apache, MariaDB / MySQL, Perl / PHP / Python), а також для управління суперкомп'ютерами, за даними на червень 2017, 99,6% комп'ютерів зі списку 500 найпотужніших працювали під управлінням Linux [4].

Метою даної роботи є аналіз особливостей методів і алгоритмів БА, можливості їх застосування в різних промислових системах безпеки та операційних системах, розгляд вразливостей біометричних систем, а також розробка програмного засобу БА для ОС Linux.

Результатом роботи є модель загроз для БА, матриця аналізу методів і алгоритмів БА, а також готовий програмний засіб БА для ОС Linux. Наведені результати дозволять підвищити безпеку і ефективність автентифікації в серверах на базі Linux, а також зменшити ризики обходу СКУД.

Список використаних джерел:

1. Wikipedia: Биометрические системы аутентификации URL: https://ru.wikipedia.org/wiki/Биометрические_системы_аутентификации (дата звернення: 24.10.2017).
2. Каклаускас А. Биометрическая и интеллектуальная поддержка решений. Вильнюс: Техника, 2012. с. 344.
3. Most Reliable Hosting Company Sites in September 2017 Netcraft. URL: https://news.netcraft.com/archives/2017/ (дата звернення: 24.10.2017).
4. Operating system family/Linux URL: https://www.top500.org/statistics/details/osfam/1. (дата звернення: 24.10.2017).

Одержано 25.10.2017

УДК 004.056

Олександр Юрійович ГОРЕЛОВ,
студент факультету комп'ютерних наук Харківського національного університету радіоелектроніки

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОДНОГО КЛАСУ ВЕБ-ДОДАТКІВ

Однією з актуальних проблем кібербезпеки є забезпечення безпеки веб-додатків і хмарних додатків, які дуже активно розвиваються в останні роки. З огляду на те, що величезне число додатків цих класів розробляються з використанням мови Java, особливу актуальність здобуває завдання забезпечення безпеки саме додатків цього класу.