УДК 681.327.12

Тетяна Грищук, Володимир Дубовой, В'ячеслав Ковтун (Вінниця)

КОНЦЕПЦІЯ ВПРОВАДЖЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ РОЗПІЗНАВАННЯ МОВЦЯ У ПРОЦЕС АВТЕНТИФІКАЦІЇ ДЛЯ ДОСТУПУ ДО КРИТИЧНОЇ СИСТЕМИ

Розвиток інформаційних систем критичного застосування у напрямку впровадження мультисерверної архітектури призвів до ускладнень при забезпеченні їх інформаційної безпеки, зокрема, у вирішенні задачі надійної автентифікації складових елементів цих систем. Існуючим концепціям забезпечення надійності процесу автентифікації у інформаційних системах критичного застосування властиві недоліки, основні з яких – невідповідність актуальному стандарту безпеки інформаційних систем ISO/IEC 27001:2013 [1], обчислювальна неефективність та низький комфорт процесу автентифікації.

Автори пропонують позбавлену цих недоліків концепцію надійної автентифікації для мультисерверної інформаційної системи критичного застосування, до складу якої входить, зокрема, множина користувачів, множина серверів та виділений сервер-реєстраційний центр для обліку об'єктів системи без ведення верифікаційних таблиць. Інформаційний обмін між об'єктами системи організовано у вигляді захищених сесій на основі ключів із механізмом узгодження із застосуванням односторонніх хеш-функцій та криптографії еліптичних кривих, яка на даний час забезпечує найкраще співвідношення надійності шифрування по відношенню до довжини ключа серед існуючих криптосистем. Роботу із користувачами персоніфіковано за допомогою індивідуальних карт доступу, які захищено на основі положень криптографічної теорії еліптичних кривих. На картах доступу, окрім ідентифікаційної інформації та паролю, зберігається індивідуальна біометрична інформація про особливості голосу користувача. Додаток для автентифікації, який встановлюється на обчислювальному засобі користувача, ініціюється двохступінчатою процедурою розпізнавання користувача (за умови наявності ідентифікаційної карти) – за індивідуальними особливостями його голосу та за введеним паролем, що поряд із зручністю, забезпечує надійність процесу автентифікації.

Запропоновану базову концепцію впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до системи критичного застосування протестовано та обґрунтовано її відповідність стандарту ISO/IEC 27001:2013, включаючи наявність механізмів захисту від таких типів атак: атаки із вгадуванням паролю, атаки із відтворенням запису паролю, атаки із використанням викрадених засобів верифікації, атаки із використанням викрадених ідентифікаційних карт, атаки на основі авторизованих аккаунтів користувачів (інсайдерів), спуфінг-атаки, атаки із підбором паролю, атаки із спробою підробки ключа сесії, атаки на основі частини відомих ключів сесій, атаки на основі ключів сесій довготривалого використання, атаки на основі одноразових паролів, атаки в процесі оновлення паролю, атаки із перевантаженням апаратних засобів. Втім, досвід практичної експлуатації системи автентифікації для доступу до ресурсів інформаційної системи критичного застосування виявив у базовій концепції ряд вразливостей, з метою позбавлення яких було створено удосконалену концепцію впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до системи критичного застосування, яка містить відповідні механізми захисту і також повністю задовольняє вимогам стандарту ISO/IEC 27001:2013.

Автори оцінили обчислювальну ефективність запропонованих концепцій шляхом підрахунку кількість найбільш обчислювально складних операцій – масштабованого множення T_m та обчислення хеш-функції T_h, при проведенні автентифікації об'єктів у складі інформаційної системи критичного застосування (користувача, сервера, реєстраційного центру та всіх цих об'єктів разом). Ітогова обчислювальна складність базової концепції склала $4T_m + 15T_h$, а удосконаленої - $6T_m + 17T_h$, що є середнім результатом порівняно із аналогами, але застосування криптографії еліптичних кривих робить операції хешування приблизно у 6 разів швидшою від використовуваної у аналогах криптографії із відкритим ключем.

Література

1. ISO/IEC 27001:2013, "Information technology - Security techniques - Information security management systems – Requirements". [Electronic resource], Access mode: https://trofisecurity.com/assets/img/iso27001-2013.pdf.