УДК 003.26.09:004.032.24-004.272.3
А. Луцків, О. Кравець
(Тернопільський національний технічний університет імені Івана Пулюя)

РОЗРОБКА ВЕБ-ПОРТАЛУ ГРІД-ОРІЄНТОВАНОЇ ВІРТУАЛЬНОЇ ЛАБОРАТОРІЇ

На даний час все частіше для розв'язання обчислювальних задач, що потребують значного обсягу ресурсів, використовуються грід-мережі. У науковій роботі здійснюється розробка та формування вимог до веб-порталу GRID-орієнтованої віртуальної лабораторії.

Можна зазначити, що в більшості випадків для того, щоб завантажити в кластер власну програму і подати дані для обчислень, користувач повинен пройти кілька не надто зручних кроків, які можуть бути дуже неочевидними для нього, наприклад, науковця хімічної спеціальності. Тому постає задача спрощення процесу користування grid-мережею і розробки інтуїтивного інтерфейсу, водночас забезпечивши йому розширюваність, гнучкість і захищеність.

Важливим питанням взаємодії користувача з grid-мережею через веб-портал є питання безпеки. Очевидно, що для таких завдань незахищеної передачі даних по протоколу HTTP буде зовсім недостатньо, оскільки він передає незашифровані дані і надає великі можливості для сніфінгу та атаки типу «man-in-the-middle», зокрема, у недостатньо захищених безпровідних мережах. Тому для з'єднання і передачі даних до грід-мережі використовують SSL- або TLS-сертифікат [1], що в реалізації схеми HTTPS (комбінації взаємодії HTTP через SSL) надає достатній захист від вказаних атак. Загалом, більшість спроб і способів зламу SSL та TLS не мали практичного успіху, оскільки потребують значних допрацювань або/та ресурсних затрат.

Проте, останнім часом було проведено декілька успішних зламів HTTPS, захищеного вищевказаними криптографічними протоколами, що однозначно мало б змусити звернути увагу на можливі їх вади і провести аналіз.

У доповіді буде розглянуто і проаналізовано сучасні способи захисту з'єднання веб-порталу, що працює з конфіденційними даними та здійснено порівняння їх захищеності. Також будуть розглянуті різні види атак на протоколи шифрування SSL та TLS, котрі є реалізовні практично [2] або можуть бути здійснені теоретично. Водночас буде проаналізовано варіанти захисту від таких атак. У доповіді пропонуються можливі варіанти покращення схеми реалізації захисту веб-порталу на базі даних технологій.

1. SSL/TLS Overview [Електронний ресурс]. - Режим доступу: URL: https://sites.google.com/site/tlsssloverview/ssl-v-tls/

2. Moxie Marlinspike. New Tricks For Defeating SSL In Practice [Електронний ресурс]. - Режим доступу: URL: https://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf