АВТОМАТИЗОВАНИЙ ЗАСІБ АНАЛІЗУ ПРОТОКОЛІВ AVISPA

Рой Є.О., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі інформаційна безпека постає як один з ключових викликів, з якими стикаються організації, державні структури та звичайні користувачі. Для гарантування необхідного рівня захисту інформації надзвичайно важливим є аналіз криптографічних та комунікаційних протоколів на предмет слабких місць і потенційних атак. Однією з найефективніших систем автоматизованого аналізу безпеки протоколів є AVISPA (Automated Validation of Internet Security Protocols and Applications).

AVISPA – це інструмент, призначений для автоматизованого аудиту захищеності криптографічних та комунікаційних протоколів. Він використовує формальні методи для моделювання та подальшого аналізу протоколів. Це дозволяє виявляти потенційні вразливості ще на стадії розробки, що суттєво зменшує ймовірність їхнього експлуатування в реальних системах. Процес використання AVISPA складається з кількох етапів: від специфікації протоколу, використовуючи мову HLPSL, до застосування одного з вбудованих аналізаторів задля перевірки безпеки [1, 2].

Ключовими перевагами AVISPA є автоматизація аудиту безпеки, висока швидкість аналізу та здатність виявляти різноманітні атаки. З іншого боку, є й певні недоліки, наприклад, труднощі з моделюванням надто складних протоколів, чи нездатність оцінити всі потенційні загрози у деяких сценаріях.

В доповіді надані результати аналізу та дослідження потенціалу та специфіки використання AVISPA для аналізу криптографічних та комунікаційних протоколів, і як приклад застосування AVISPA, надані результати аналізу безпеки протоколу TLS.

Отже, AVISPA є потужним інструментом для автоматизованого аналізу безпеки криптографічних та комунікаційних протоколів. Його функціонал дає змогу зменшувати вірогідність появи вразливих протоколів у реальних інформаційно-комунікаційних системах, що вкрай важливо для сьогоденної інформаційної безпеки. Завдяки використанню формальних методів та багатьох аналізаторів, зокрема на основі моделювання, обмежень логіки, AVISPA може стати незамінним помічником при розробці та тестуванні нових мережевих протоколів.

Список літератури

1. AVISPA v1.0 User Manual. AVISPA Team. 2006. URL: https://people.rennes.inria.fr/Thomas.Genet/Crypt/AVISPA_manual.pdf.

2. F. Kammuller. Verification with AVISPA to Engineer Network Security Protocols. *International Journal on Advances in Security*. 2012. No. 3,4. P. 112-120. URL:https://personales.upv.es/thinkmind/dl/journals/sec/sec_v5_n34_2012/sec_v5_n34_2012_4.pdf