УДК 004.056.5

МОДЕЛЬ ЗАГРОЗ ТА АНАЛІЗ ЗАХИЩЕНОСТІ ПРОТОКОЛУ SSL/TLS ВІД КРИПТОАНАЛІТИЧНИХ АТАК

Якименко І.З.[1)], Бабюк Д.В. [2)], Гнатишин Ю.А.[3)]
Тернопільський національний економічний університет,
[1)] к.т.н.; [2)] магістр; [3)] ст. лаборант

I. Постановка проблеми

На даний час під Web–транзакцією розуміється потік даних у глобальному середовищі Internet, більша частина інформації в якому передається за допомогою SSL/TLS–протоколу. Тому розгляд питань, пов'язаних з безпекою Web–транзакцій, є досить актуальною задачею. Знаючи принцип роботи даного протоколу та існуючі атаки, можна забезпечити потрібний захист даних, які передаються.

II. Мета роботи

Метою дослідження є побудова моделей загроз і розробка методів захисту для Web–транзакції, в яких використовуються стандартні протоколи TLS\SSL.

III. Модель атаки посередника на протоколу TLS\SSL та методи її запобігання

Атака «посередника» (man–in–the–middle) передбачає участь у комунікаційної сесії трьох суб'єктів: клієнта, сервера і посередника–зловмисника, що знаходиться між ними. Таке становище дозволяє зловмисникові перехоплювати всі повідомлення, які прямують в обох напрямках, і при бажанні підміняти їх.

«Посередник» видає себе сервером для клієнта і клієнтом для сервера. Для моделювання та реалізації даної атаки повинні бути такі вхідні дані: клієнт, сервер і зловмисник знаходяться в одній мережі; є програми–шкідники (Snifer, Nmap (Win), WinNuke, Smurf); обмін ключами ведеться по мережі. Схема атаки наведена на рисунку 1.

Рисунок 1 – Схема атаки посередника на протокол SSL/TLS

Щоб запобігти даній атаці під час діалогу про встановлення безпечного з'єднання з сервером необхідно надати сертифікат, який підписаний сертифікаційним центром. У цьому сертифікаті розміщується загальнодоступний ключ сервера, його ім'я та ім'я емітента сертифікату. Клієнт верифікує підпис сертифіката, а потім перевіряє ім'я емітента. Якщо посередник надає підроблений сертифікат, то він не пройде перевірку підпису, так як зловмисник не може знати секретного ключа сервера. Оскільки зловмисник не може згенерувати довірений сертифікат, то цю атаку легко виявити (в браузері буде з'являтися повідомлення про помилку).

Висновок

У роботі побудовано модель загроз для атаки посередника і запропоновано методи захисту для Web–транзакції, в яких використовуються стандартні протоколи TLS\SSL.

Список використаних джерел

1. Васильев Г.А. Политика безопасности при работе в Internet / Г.А.Васильев. – СПб: Питер, 1997. – 848с.
2. Мартин Дж. Об Internet и о безопасности / Дж.Мартин. – М.: Мир, 2000. – 608с.