МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І
ПРОГРАМНОЇ ІНЖЕНЕРІЇ

ЗИМНИЦЬКИЙ ОЛЕГ ГЕННАДІЙОВИЧ

УДК 004.056.5

Дослідження вразливостей реалізації криптографічних методів захисту протоколу SSL/TLS

Спеціальність 125 «Кібербезпека»

Автореферат

дипломної роботи на здобуття освітньо-кваліфікаційного
рівня «магістр»

Тернопіль — 2019

Роботу виконано на кафедрі кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя

Керівник роботи: кандидат технічних наук, зав. кафедри кібербезпеки
Загородна Наталія Володимирівна
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: д.к.н., професор
Кунанець Наталія Едуардівна,
Тернопільський національний технічний університет
імені Івана Пулюя, кафедра комп'ютерних наук, доцент.

Захист відбудеться 23 грудня 2019 р. о 9.00 годині на засіданні екзаменаційної комісії №33 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд. 806.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Протокол TLS та його окремі реалізації отримали широке розповсюдження для криптографічного захисту інформації при її передачі по мережі, тому наявні у цих реалізаціях вразливості становлять загрозу інформації широкого кола користувачів.

Метою даного дослідження є розробка методології, що дозволить суттєво зменшити ймовірність виникнення вразливостей під час імплементації SSL/TLS, аналіз порядку розробки відкритих імплементацій протоколу та формування рекомендацій, які можуть використовувати їх розробники, або їх приватні форки, що надає практичне значення даному дослідженню.

Завданнями, які ставляться перед дослідженням це провести всебічний аналіз уже виявлених вразливостей бібліотек (OpenSSL, GnuTLS, NSS); виявити причин виникнення цих вразливостей ; проаналізувати способи, які дозволили виявити ці вразливості; сформувати методологію, що дозволить уникати подібних вразливостей під час імплементації протоколу SSL/TLS.

Об'єктом дослідження є відкриті реалізації протоколу SSL/TLS, які часто використовуються розробниками ПЗ і на які припадає основна частина трафіку. До таких імплементацій належать: OpenSSL, GnuTLS, Mozilla NSS.

Предметом дослідження є вразливості програмного коду цих реалізацій.

Методи дослідження. В процесі дослідження використано загальнонаукові методи пізнання: порівняння, системний аналіз. А також методи статичного та динамічного аналізу коду.

Наукова новизна полягає у створенні методології, що дозволяє виявляти вразливості реалізації протоколу TLS за допомогою вільного програмного забезпечення.

Апробація результатів. Основні положення дослідження доповідалися й обговорювалися на науково-практичних конференціях: на VII Науково-технічної конференції "Інформаційні моделі, системи та технології" (Тернопіль, 11-12 грудня 2019 року).

Структура роботи. Робота складається зі вступу, семи розділів, висновків, переліку джерел посилань. Робота містить 24 рисунки, 5 таблиць. Обсяг основного тексту становить 82 сторінки, перелік джерел посилань — 6 сторінок. Загальний обсяг дипломної роботи складає 94 сторінки.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність проблеми, визначено об’єкт і предмет дослідження, сформульовано його мету, завдання, розкрито теоретичну та методологічну основу, методи дослідження; висвітлено наукову новизну, практичне значення роботи.

У першому розділі — “*Загальні передумови виникнення реалізацій протоколу TLS*” — було проаналізовано історію виникнення мережі Інтернет, появи на розповсюдження World Wide Web, розвиток сучасних методів криптографічного захисту інформації та умови виникнення протоколів криптографічного захисту інформації.

У другому розділі — *“Аналіз вразливостей реалізацій протоколу TLS”* — було проведено глибокий аналіз вразливостей реалізацій протоколу TLS, що були виявлені у трьох найбільш широко використовуваних відкритих реалізаціях протоколу TLS, а саме OpenSSL, GnuTLS та Network Security Services. Дані вразливості можна поділити на наступні типи:

- відмова в обслуговуванні (DoS);
- загроза виконання коду;
- переповнення буферу;
- обхід чогось, а саме певного етапу встановлення з’єднання чи передачі інформації каналом, що становить загрозу конфіденційності чи цілісності інформації;
- псування пам’яті.

Кожен тип розглянуто окремо, щоб визначити основні причини появи цих вразливостей.

У третьому розділі — *“Методи виявлення вразливостей реалізації протоколу TLS”* — представлено методологію виявлення вразливостей реалізації протоколу TLS за допомогою вільного програмного забезпечення, а саме Cppcheck, Clang Static Analyzer, Gcov та Valgrind.

Кожен крок детально розглянутий окремо на прикладі відкритої реалізації протоколу SSL/TLS OpenSSL.

ВИСНОВКИ

У дипломній роботі запропоновано методологію пошуку вразливостей у реалізаціях протоколу SSL/TLS на стадії розробки. Для цього пропонується проводити наступні заходи:

1. Статичний аналіз коду за допомогою двох відкритих аналізаторів коду — Cppcheck та Clang Static Analyzer.
2. Написання модульних тестів паралельно з кодом протоколу та визначення покриття коду тестами за допомогою вбудованої у компілятор GCC функції та застосунків gcov та lcov.
3. Проведення динамічного аналізу коду реалізації протоколу TLS за допомогою аналізатора Valgrind для пошуку вразливостей, що пов’язані з неправильною роботою з оперативною пам’яттю програми.

Запропонована методологія може легко розширюватися та проводитися автоматизовано за допомогою засобів для неперервної інтеграції, наприклад Gitlab CI. Також, вона може бути легко застосовано до ПЗ інших типів.

1. Зимницький О.Г. Вразливості реалізації криптографічних методів захисту протоколу SSL/TLS/ Тези доповіді на VII Науково-технічної конференції «інформаційні моделі, системи та технології» 11-12 грудня 2019 року. — Тернопіль, 2019. — С. 196 ст.

АНОТАЦІЇ

Ключові слова: КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, РОЗРОБКА ЗАХИЩЕНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, SSL, TLS.

Робота об’ємом 90 сторінок, яка містить 25 рисунків, 6 таблиць, 62 джерела за переліком посилань.

Метою даної кваліфікаційної роботи є аналіз вразливостей реалізації протоколу SSL/TLS та розробка методології виявлення цих вразливостей з використанням існуючих технік та програмного забезпечення.

Об’єктом вивчення є вразливості відкритих реалізацій протоколу SSL/TLS.

Методами дослідження є як загальнонаукові методи пізнання: порівняння, системний аналіз, так і спеціальні, зокрема методи статичного та динамічного аналізу коду.

Наукова новизна полягає у створенні методології аналізу реалізацій протоколу TLS на етапі розробки з використанням методів статичного та динамічного аналізу коду, а також модульного тестування.

Результати роботи можуть бути використані для пошуку вразливостей у реалізаціях протоколу SSL/TLS мовою програмування C на всьому етапі розробки.

Keywords: CYBERSECURITY, INFORMATION SECURITY, SECURE SOFTWARE DEVELOPMENT, SSL, TLS.

Work with 90 pages containing, 25 illustrations, 6 tables, 62 sources by list of links.

The purpose of this qualification work is to analyze the vulnerabilities of the SSL/TLS open-source implementations and to build a methodology for their detection during the development process.

The object of the research is the vulnerabilities of the SSL/TLS open-source implementations.

The scientific methods that are used in the study are both general-purpose methods, like comparing or system analysis, and specific methods, such that methods of static and dynamic code analysis.

Scientific innovation is a creation of a methodology for analyzing implementations of TLS protocol at the development stage using static and dynamic code analysis.

Results of the work can be used for detecting vulnerabilities of SSL/TLS protocol implementations that are written in C programming language during the whole development process.