Авторська довідка

(реферату дипломної роботи магістра)

Назва дипломної роботи магістра: дослідження вразливостей реалізації криптографічних методів захисту протоколу SSL/TLS

назви записувати нижнім регістром (як у реченні)

Назва (англ.): study of vulnerabilities of cryptographic methods implementation of SSL/TLS security protocol

переклад англійською

Освітній ступінь : ***магістр***

Шифр та назва спеціальності: 125 «Кібербезпека»

Екзаменаційна комісія:

напр.: Екзаменаційна комісія №1

Установа захисту: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 23.12.2019 **Місто:** Тернопіль

Сторінки:

Кількість сторінок дипломної роботи: Кількість сторінок реферату:

УДК: УДК 004.056.5

Автор дипломної роботи

Прізвище, ім’я, по батькові (укр.): Зимницький Олег Геннадійович

розкривати ініціали

Прізвище, ім’я (англ.): Zymnytskyi Oleh

використовувати паспортну транслітерацію (КМУ 2010)

Місце навчання (установа, факультет, місто, країна): ТНТУ, ФІС, Тернопіль, Україна

Керівник

Прізвище, ім’я, по батькові (укр.): Загородна Наталя Володимирівна

повністю

Прізвище, ім’я (англ.): Zahorodna Hatalia

використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ, кафедра КБ, Тернопіль, Україна

Вчене звання, науковий ступінь, посада: кандидат технічних наук, доцент кафедри кібербезпеки

Рецензент

Прізвище, ім’я, по батькові (укр.): Кунанець Наталія Едуардівна

повністю

Прізвище, ім’я (англ.): Kunanets Nataliia

використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ, Факультет комп’ютерно-інформаційних систем і програмної інженерії, Кафедра комп’ютерних наук м.Тернопіль, Україна

Вчене звання, науковий ступінь, посада: доктор наук із соціальних комунікацій, професор кафедри комп'ютерних наук

Ключові слова

українською: КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, РОЗРОБКА ЗАХИЩЕНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, SSL, TLS

англійською: CYBERSECURITY, INFORMATION SECURITY, SECURE SOFTWARE

DEVELOPMENT, SSL, TLS.

Анотація

українською: Робота об’ємом 90 сторінок, яка містить 25 рисунків, 7 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 С на всьому етапі розробки.

англійською: Work with 90 pages containing, 25 illustrations, 7 tables, 62 sources by the 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.

Бібліографічний опис:

українською: Зимницький О.Г. Дослідження вразливостей реалізації криптографічних методів захисту протоколу SSL/TLS: автореферат дипломної роботи магістра за спеціальністю 125 – Кібербезпека / О.Г. Зимницький: Тернопільський національний технічний університет імені Івана Пулюя – Тернопіль: ТНТУ, 2019. – 6с.

англійською: Zymnytskyi O. Study of vulnerabilities of cryptographic methods implementation of SSL/TLS security protocol: abstract of master’s thesis on speciality 125 – Cybersecurity / O. Zymnytskyi; - Ternopil Ivan Puluj National Technical University – Ternopil: TNTU, 2019 – 6p.