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

ЛЕНЬО ВІКТОРІЯ МИХАЙЛІВНА

УДК 004.056

АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ НА ПРИКЛАДІ ПРОТОКОЛУ АВТЕНТИФІКАЦІЇ KERBEROS

125 "Кібербезпека"

Автореферат
дипломної роботи на здобуття освітнього рівня "магістр"

Тернопіль
2019

Роботу виконано на кафедрі кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: доктор технічних наук, доцент кафедри кібербезпеки
Александер Марек Богуслав,
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: доктор технічних наук, доцент кафедри автоматизації технологічних процесів і виробництв
Приймак Микола Володимирович,
Тернопільський національний технічний університет імені Івана Пулюя,

Захист відбудеться ___ грудня 2019 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії № ___ 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 теми роботи. Сучасні комп'ютерні розподілені системи характеризуються високим рівнем інтегрованості функціональних можливостей, підтримкою взаємодії декількох апаратних та програмних платформ, часто з використанням принципів розподіленості та паралельної роботи користувачів. Цей факт обумовлює високу складність проектованих систем та необхідність керування доступом до спільних ресурсів. Керування доступом – це механізм авторизації, який базується на автентифікації користувачів розподіленої системи.

Отже, автентифікація користувачів – важлива частина забезпечення інформаційної безпеки. Одним з методів автентифікації є використання протоколу Kerberos, з доступом до відповідного сервера. Тому тема роботи є актуальною.

Мета роботи: Метою роботи є аналіз методів і засобів автентифікації користувачів комп'ютерної розподіленої системи на основі сервера Kerberos.

Об’єкт, методи та джерела дослідження. Об’єкт дослідження: процеси забезпечення, контролю та управління безпекою у комп'ютерних системах.

Предмет дослідження: протокол авторизації на основі виділеного сервера Kerberos.

Методи дослідження. Для досягнення мети дипломної роботи використовувались:

– методи узагальнення та аналізу – при проведенні огляду стану механізмів автентифікації;

– формалізації та математичного моделювання – при аналізі методу стійкості шифрування паролів.

Наукова новизна отриманих результатів:

- Наукова новизна полягає у вирішенні задачі забезпечення захищеності особистих даних користувача розподіленої комп'ютерної системи. При цьому було отримано такі результати:
- систематизовано моделі автентифікації користувачів;
- запропоновано практичний приклад налаштування процесу автентифікації користувачів розподіленої системи.

Практичне значення отриманих результатів.

Всі проаналізовані методи та засоби автентифікації можуть використовуватись практично при вивченні відповідних дисциплін, що стосуються адміністрування розподілених комп'ютерних систем, а також при побудові розподілених систем, для котрих критичним параметром є процес надійної автентифікації користувачів з використанням виділеного сервера.

Апробація. Основні положення роботи доповідались, розглядались та обговорювались на наукових конференціях Тернопільського національного технічного університету. Результати дипломної роботи опубліковані у тезах доповіді на студентській науковій конференції, яка проводились у ТНТУ.

Структура роботи. Робота складається з розрахунково-пояснювальної записки. Розрахунково-пояснювальна записка складається з вступу, 7 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – ____ арк. формату А4.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі проведено огляд задч, які потрібно вирішити під час підготовки дипломної роботи магістра.

В першому розділі проведено аналіз важливості, методів та засобів забезпечення безпеки в комп'ютерних розподілених системах.

В другому розділі виконано дослідження протоколу автентифікації користувачів з використанням віддаленого сервера Kerberos.

У третьому розділі запропоновано практичну реалізацію системи автентифікації користувачі на основі віддаленого сервера для операційної системи Windows.

В спеціальній частині виконано дослідження можливостей пакету прикладних програм WireShark для аналізу мережевого трафіку на оснрові наочного представлення пакетів даних..

В розділі «Обґрунтування економічної ефективності» розглянуто питання організації виробництва і проведено розрахунки техніко-економічної ефективності проектних рішень.

В частині «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання планування робіт по охороні праці при роботі з комп'ютерною технікою, правові основи забезпечення безпеки в надзвичайних ситуаціях.

В розділі «Екологія» проаналізовано сучасний екологічний стан України, розглянуто питання забруднення довкілля, що виникає внаслідок реалізації технологічного процесу, а також запропоновано заходи зі зменшення забруднення довкілля.

У загальних висновках щодо дипломної роботи описано прийняті в проекті технічні рішення і організаційно-технічні заходи, які забезпечують виконання завдання на проектування; оригінальні технічні рішення, прийняті автором в процесі роботи; технічні рішення роботи, які можуть бути впроваджені у виробництво; техніко-економічні показники та їх порівняння з базовими.

ВИСНОВКИ

У магістерській роботі виконано дослідження способів забезпечення автентифікації користувачів розподіленої комп'ютерної системи на основі протоколу Kerberos.

Основні наукові та практичні результати полягають в наступному.

1. Проведено аналіз наукових публікацій, протоколів та практичних рішень в області реалізації методів автентифікації користувачів розподіленохї комп'ютерної системи.
2. Проаналізовано можливості протоколу на основі віддаленого сервера автентифікації.
3. Здійснено аналіз ризиків при використанні методу автентифікації з віддаленим сервером.
4. Запропоновано практичну реалізацію методу для операційної системи Windows.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Яворський Р. ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ РОЗГОРТАННІ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ [Текст] / Р. Яворський, В. Амбок, В. Леньо. Матеріали науково-технічної конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя. – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2019. – с. 108.

АНОТАЦІЯ

АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ НА ПРИКЛАДІ ПРОТОКОЛУ АВТЕНТИФІКАЦІЇ KERBEROS

У магістерській роботі виконано дослідження способів забезпечення необхідного рівня захищеності комп'ютерних мереж на основі авторизації користувачів з використанням віддаленого сервера Kerberos. Здійснено огляд принципів авторизації та аутентифікації.

В дипломній роботі показано актуальність оцінювання рівня захищеності комп'ютерних систем з на основі ОС Windows з використанням служби автентифікації Kerberos. Проаналізовано основні механізми авторизації та принципи роботи такої системи з виділеним сервером Kerberos.

Ключові слова: БЕЗПЕКА, АВТЕНТИФІКАЦІЯ, ШИФРУВАННЯ, ДОВІРЕНИЙ КОРИСТУВАЧ, KERBEROS, СЕРВЕР, ПРОТОКОЛ

ANNOTATION

ANALYSIS OF SECURITY PROBLEMS IN DISTRIBUTED INFORMATION SYSTEMS (KERBEROS AUTHENTIFICATION PROTOCOL AS A CASE OF STUDY)

The master's thesis investigates how to provide the necessary level of security of computer networks based on user authorization using a remote Kerberos server. Authorization and authentication principles are reviewed.

The diploma thesis shows the relevance of assessing the security level of computer systems based on Windows using Kerberos authentication service. The basic authorization mechanisms and principles of operation of such a system with a dedicated Kerberos server are analyzed..

Key words: SECURITY, AUTHENTIFICATION, ENCRYPTION, TRUSTED USER, KERBEROS, SERVER, PROTOCOL