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

МАРКОВСЬКИЙ АНДРІЙ ВАСИЛЬОВИЧ

УДК 004.73

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В BLUETOOTH-МЕРЕЖАХ ПЕРЕДАВАННЯ ДАНИХ

123 «Комп'ютерна інженерія»

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль, 2018

Роботу виконано на кафедрі комп'ютерних систем та мереж Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: **Баран Ігор Олегович**
кандидат технічних наук, доцент
декан факультету комп'ютерно-інформаційних систем та програмної інженерії
Тернопільський національний технічний університет імені Івана Пулюя

Рецензент: **Литвиненко Ярослав Володимирович,**
доцент, кандидат технічних наук, доцент кафедри комп'ютерних наук
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться _26_ грудня 2018 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії № 34 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд. 603.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Стрімко зростаюча сфера стільникової телефонії породила вже не один новий канал витоку інформації. У їх число потрапив і популярний протокол зв'язку Bluetooth (базується на стандарті IEEE 802.15), яким оснащені сьогодні всі моделі смартфонів і планшетів. Пристрої зв'язку, що використовують протокол передачі даних Bluetooth, незважаючи на всі зусилля фахівців з питань зв'язку та криптографії, стають сьогодні легкою здобиччю навіть хакерів-початківців. Розроблено доступні відповідні методики проникнення в телефон, програми злому і навіть необхідне обладнання (спеціальні антени), що дозволяє зловмисникові "бачити" конкретний телефон на відстані до двох кілометрів. Подібні атаки загрожують для власника телефону масою проблем. У їх числі копіювання адресної книги, SMS-повідомлень, фотографій і будь-яких інших даних, використання сервісів телефону, тобто Інтернету, WAP і GPRS, отримання доступу до АТ-команд телефону, а саме, до можливості відсилати повідомлення (в будь-якій кількості) і дзвонити на будь-які номери. Найприкріше, що все це відбувається без будь-яких демаскуючих ознак і, звичайно, без відома користувача телефону. Мобільному пристрою зв'язку може бути завдано і істотну шкоду, зокрема внаслідок зараження його вірусами, здатними повністю відключити Bluetooth, вбудований файлменеджер, телефонну книгу, заблокувати і зіпсувати операційну систему та ін.

В період інтенсивного розвитку і поширення технологій, коли стільниковий зв’язок став частиною повсякденного життя, надзвичайно актуальними є питання захисту інформації, представленої у цифровому вигляді, яка може передаватися через Bluetooth-мережі.

Мета роботи: дослідженні методів і засобів захисту інформації в Bluetooth мережах.

Об’єкт та методи дослідження. Основним об’єктом дослідження є процес забезпечення захисту інформації в безпровідних мережах на основі технології Bluetooth. Програмна система захисту мереж передачі даних розробляється з використанням теорії надійності програмних засобів, методів шифрування та аутентифікації, чисельних методів та методів верифікації ПЗ.

Предмет дослідження: методи і засоби для забезпечення захисту від НСД в безпровідних мережах.

Наукова новизна отриманих результатів:

- удосконалено способи захисту інформації від НСД в безпровідній мережі (пасивні, активні та програмні);
- сформульовані та реалізовані рекомендації, щодо практичних способів захисту Bluetooth мереж передавання даних;
- спроектовано та реалізовано комп’ютерну систему для дослідження захищеності Bluetooth мережі, яка складається з апаратного та програмного забезпечення.

Практичне значення отриманих результатів. Впровадження методів та засобів захисту інформації в Bluetooth мережах дає змогу підвищити їх захищеність від різного роду НСД.

Апробація. Окремі результати дослідження доповідалися на VII Міжнародній науково-технічній конференції молодих учених та студентів «Актуальні задачі сучасних технологій» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 28-29 листопада 2018 р.)

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 7 частин, висновків, переліку посилань, додатків. Обсяг роботи: розрахунково-пояснювальна записка – ____ арк. формату А4, графічна частина – 9 аркушів формату А1.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі проведено аналіз актуальності та мети роботи, поставлено задачі дослідження, сформульовано об’єкт та предмет дослідження, наведена наукова новизна та практичне значення одержаних результатів.

В першому розділі «Аналітичний огляд стандарту IEE 802.15 щодо забезпечення отримання НСД до безпровідних мереж» сформульовано основні цілі і завдання дослідження, виконано постановку задачі на дипломну роботу, виконано загальний аналіз інформаційної бази дослідження, проведено аналіз стандарту 802.15 та протоколу 802.15.1 (загальні принципи роботи, архітектура ядра системи, взаємодія під мереж, взаємопов’язаність технології з різними стандартами).

В другому розділі «Дослідження архітектури, режимів роботи, протоколів та методів захисту від НСД BLUETOOTH мереж» описано архітектуру передачі даних, режими роботи пристроїв Bluetooth, протоколи технології 802.15, зокрема кореневі, RFCOMM, інтерфейс HCI. Проаналізовано схожі технології IrDA, Home / SWAP, ZigBee, IEEE 802.11. Наведено основні методи захисту систем передачі даних на базі протоколу 802.15.

В третьому розділі «Практичний аналіз системного програмного забезпечення для отримання НСД до BLUETOOTH мереж» описано основні види Bluetooth-атак (в т.ч. Bluesnarfing, BluePrinting, BlueBugging, Blueover, Backdoor, BlueBumping, BlueSmack, Car Whisperer) та способи і засоби захисту від них. Показано процес отримання НСД за допомогою алгоритму BlueSnarf.

В четвертому розділі «Спеціальна частина» описано аналіз аналіз дистрибутиву Backtrack, тестування захисту протоколу 802.15.1 та процес аутентифікації за допомогою Bluetooth-телефону в ОС Linux.

В п’ятому розділі «Обґрунтування економічної ефективності» розглянуто питання розрахунку економічної ефективності і терміну окупності капітальних вкладень.

В шостому розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання санітарних норми і вимоги до ПК, освітленості виробничих приміщень для роботи з відеодисплейними терміналами та Забезпечення безперебійного електроспоживання об’єкту при надзвичайних ситуаціях техногенного характеру.

В сьомому розділі «Екологія» описано процес енергозбереження і його роль у вирішенні екологічних проблем, а також статистичний аналіз тенденцій і закономірностей динаміки в екології.

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; наведено рекомендації по розробці схожих систем.

В **графічній частині** представлені характеристика сімейства протоколів 802.15, специфікація ядра системи та передачі даних Bluetooth, взаємодія підмереж, порівняння технологій безпровідної передачі даних, аутентифікація та шифрування в Bluetooth, алгоритм програми для отримання НСД, перелік Bluetooth-атак.

ВИСНОВКИ

Дослідивши архітектуру ядра системи є очевидним те, що протокол 802.15 є простим для реалізації на фізичному рівні. Специфікація ядра системи вимагає автоматизованого тестування, що відповідає реалізації Bluetooth. Це досягається шляхом дозволу програмі тестування контролювати реалізацію Bluetooth через інтерфейс радіоканалу. На даний час Bluetooth є повністю суміною технологією до моделі IEEE 802. Фізичний рівень протоколу відповідає базовим принципам моделей OSI та 802.

Основні заходи захисту систем передачі даних в Bluetooth-мережах: організація безпечних каналів аутентифікації в Bluetooth (використання алгоритму аутентифікації E1 на основі алгоритму шифрування SAFER+; шифрування даних на основі алгоритму E0, управління з використанням ключів).

В ході проведення дослідження виконано наступне:

- проаналізовано існуючі технології безпровідної передачі даних (IrDA; Home / SWAP; ZigBee; IEEE 802.11);
- досліджено, що специфікація ядра системи вимагає автоматизованого тестування, що відповідає реалізації Bluetooth. Це досягається шляхом дозволу програмі тестування контролювати реалізацію Bluetooth через інтерфейс радіоканалу;
- проведено аналіз існуючих програмних засобів для перевірки захищеності Bluetooth-мереж від НСД;
- виконано аналіз системи захисту Bluetooth-мереж та алгоритмів шифрування передачі даних;
- побудовано комп’ютерну систему для дослідження захищеності мережі, яка складається з апаратного та програмного забезпечення.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Марковський А.В. Методи та засоби захисту інформації в Bluetooth-мережах передавання даних / А.В. Марковський – Матеріали VII Міжнародної науково-технічної конференції молодих учених та студентів. Актуальні задачі сучасних технологій. Т.2 – Тернопіль, ТНТУ, 28-29 листопада 2018 – с. 113

АНОТАЦІЯ

Марковський А.В. Методи та засоби захисту інформації в Bluetooth-мережах передавання даних

Дипломна робота на здобуття освітнього ступеня магістра, 123 «Комп'ютерна інженерія». – Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль 2018

Дипломна робота присвячена дослідженню сучасних методів, способів та засобів захисту інформації в безпровідних мережах з використанням технології передачі даних Bluetooth, виявлення їх недоліків та перспектив подальшого розвитку.

В роботі проведено аналіз сучасного стану в області забезпечення отримання НСД до безпровідних мереж на основі стандарту IEE 802.15, досліджено його основні характеристики, протоколи роботи. Також визначено особливості функціонування протоколів роботи, досліджено режими шифрування даних, режими безпеки Bluetooth та надано рекомендації щодо можливостей їх подальшого розвитку.

Наведено заходи захисту систем передачі даних на базі протоколу 802.15, проаналізовано системне ПЗ для отримання НСД та проведено порівняння можливостей основних атак для отримання НСД до мереж стандарту 802.15. Описано особливості тестування системи захисту технології 802.15 з використанням алгоритмів BlueBug, BlueBug AT-shell та програмним продуктом FAT.PL

Ключові слова: BACKTRACK, BLUEBUG, BLUETOOTH, BLUESNARF, BLUESMACK, IEEE 802.15, PIN-КОД, RFCOMM, АУТЕНТИФІКАЦІЯ, НСД, ШИФРУВАННЯ

ANNOTATION

Markovskiy A.V. Methods and tools of information security in Bluetooth-networks data transfer

The diploma paper for obtaining the Master's degree, 123 «Computer Engineering» – Ternopil Ivan Puluj National Technical University, Ternopil 2018

The thesis deals with the research of modern methods and tools of information security protection in wireless networks using the technology of Bluetooth data transfer, revealing their shortcomings and prospects for further development.

The first chapter thesis analyzes the current state of software in obtaining unauthorized access to wireless networks based on the standard IEE 802.15, studied its basic characteristics, protocols work. Then were described the peculiarities of operation of the work protocols, examines data encryption modes, Bluetooth security modes, and provides guidance on the possibilities for their further development. Provided security measures for data transfer systems based on the 802.15 protocol, analyzes the system software for obtaining unauthorized access and compares the capabilities of the main attacks to obtain unauthorized access for networks of the standard 802.15. The peculiarities of testing the 802.15 technology protection system using the BlueBug algorithms, the Bluebug AT-shell and the software FAT.PL are presented

Keywords: BACKTRACK, BLUEBUG, BLUETOOTH, BLUESNARF, BLUESMACK, IEEE 802.15, PIN-COD, RFCOMM, UTHENTICATION, UNAUTHORISED ACCESS, ENCRYPTION