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

СИТНИК ОЛЕКСАНДР ІГОРОВИЧ

УДК 004.056.53

СТВОРЕННЯ ЗАХИЩЕНОГО МЕТОДУ РЕПЛІКАЦІЇ ДАНИХ З ВИКОРИСТАННЯМ NFC-ТЕХНОЛОГІЇ

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

Рецензент: доктор наук із соціальних комунікацій, професор кафедри комп'ютерних наук
Кунанець Наталія Едуардівна,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 26 грудня 2019 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії №32 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. Підтримка призначених для користувача даних в актуальному стані і можливість доступу до них з будь-якого пристрою - головний принцип забезпечення зручності взаємодії користувача з інформаційними системами.

Кількість пристроїв для особистого користування вже не обмежується тільки телефоном і комп'ютером. У багатьох людей так само присутні планшети, ігрові приставки, «розумна побутова техніка». Часто виникає необхідність роботи з розрахованими на багато користувачів пристроями - наприклад, комп'ютери в інтернет-кафе або в навчальній аудиторії. Щоб забезпечити максимально зручну взаємодію користувача незалежно від пристрою, з яким в даний момент відбувається робота, необхідно використовувати синхронізацію даних профілю користувача з можливістю безпечної передачі даних та знищення налаштувань профілю після закінчення роботи з пристроєм та відключення телефону.

Мета роботи: створення захищеного методу реплікації даних використовуючи NFC-технологію.

Об’єкт та предмет дослідження. Об’єктом дослідження є процес реплікації даних, які потребують захисту. Предметом дослідження є методи та засоби реплікації.

Наукова новизна отриманих результатів:

З урахуванням виявлених слабких і сильних сторін існуючих каналів реплікації, проведеного аналізу загроз та методів їх подолання запропоновано та представлено новий метод реплікації, заснований на застосуванні технології NFC в якості каналу установки сеансового ключа. Проведений аналіз захищеності запропонованого методу реплікації за допомогою технології NFC мобільного телефону на ОС Android показав, що отриманий метод є більш стійким до існуючих загроз при передачі інформації, є більш гнучким і простим у використанні, і може використовуватись для тимчасової реплікації профілю користувача, наприклад, при створенні спеціальних додатків для ОС Android.

Практичне значення отриманих результатів полягає в тому, що даний метод може бути покладений в основу інформаційної системи та створення мобільного застосунку для тимчасової реплікації профілю користувача на необхідний пристрій.

Апробація. Окремі результати роботи доповідались на VII науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 11 – 12 грудня 2019 р.

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з

вступу, 7 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 104 арк. формату А4, ілюстративна частина– 13 слайдів.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі сформульовано актуальність проблеми створення нового методу реплікації з метою створення тимчасового профілю користувача та сформульовано мету і основні завдання роботи.

У першій главі проводиться аналіз існуючих механізмів синхронізації призначених для користувача даних і протоколу NFC.

У другій главі досліджується перелік загроз, що виникають при передачі даних за технологією NFC та визначаються особливості встановлення безпечного каналу для NFC. Досліджується технологія NFC в мобільних телефонах на базі ОС Android.

У третій главі розробляється метод, що полягає у використанні технології NFC для автоматизованої реплікації профілю користувача та визначається прототип системи реплікації профілю користувача за допомогою технології NFC.

В спеціальній частині приведено опис застосунку «SyncManager».

В п’ятому розділі обчислено основні показники економічної ефективності від розробки і реалізації запропонованого алгоритму.

У підрозділі "Охорона праці" розглянуто вимоги щодо охорони праці в приміщеннях та їх оснащення. У підрозділі "Безпека життєдіяльності" описано безпеку приміщень та розлади здоров'я користувачів, що формуються під впливом роботи за комп'ютером.

В розділі "Екологія" описано формування бази статистичних даних в екології. Також розглянуто джерела шуму і вібрацій та методи їх знешкодження.

У загальних висновках щодо дипломної роботи наведено короткий опис основної частини; сформульовано основні результати.

В додатках до пояснювальної записки приведено тези.

В ілюстративній частині приведено класифікацію реплікацій, Застосування NFC-технології, Загрози та методи захисту для технології NFC, Схема запропонованого методу реплікації, Функціональна схема прототипу, Встановлення захищеного каналу за допомогою NFC та Передача даних за альтернативним каналом.

ВИСНОВКИ

На основі аналізу загроз, що виникають при передачі даних за технологією NFC, запропоновані методи і шляхи їх усунення, де новим основним шляхом їх

подолання є використання засобів рівня додатків, завдяки яким можна домогтися переваг, які не існують на канальному рівні. Було розв'язано наступні задачі:

1. Проведений аналіз рівнів реплікації на основі хосту, мережі та контролеру системи зберігання даних показав, що реплікація на основі контролеру системи є одною з найгнучкіших для проведення реплікації, основною перевагою якої є об'єднання всіх переваг систем реплікації на рівні мережі, проте визначені недоліки кожного з рівнів реплікації доводить необхідність шукати нові шляхи і рівні для проведення більш захищеної реплікації.

2. Аналіз загроз, що виникають при передачі даних за технологією NFC показав, під час реплікації даних цією технологією можуть бути загрози пов’язані з пасивним прослуховуванням каналів, пошкодженням переданих даних, модифікацією даних, вставки даних та атак типу Relay, проте на основі проведених досліджень, можна стверджувати що атака типу «людина посередині» для протоколу NFC є практично нездійсненою.

3. На основі аналізу загроз, що виникають при передачі даних за технологією NFC, запропоновано методи і шляхи їх усунення, де основним новим шляхом їх подолання є використання засобів рівня додатків, завдяки яким можна домогтися переваг які не існують на канальному рівні.

4.Створено методику реплікації та прототип системи, що відповідає сформульованим вимогам.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Ситник О. Метод реплікації даних з використанням NFC-технології [Текст] / Ситник О., Лазорко А**.** Збірник тез VII науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» – Тернопіль (11 – 12 грудня 2019 р.), ТНТУ, 2019. – с.97

АНОТАЦІЯ

Дана магістерська кваліфікаційна робота присвячена створенню захищеного методу реплікації даних використовуючи NFC-технологію. Проводиться аналіз існуючих механізмів синхронізації призначених для користувача даних і протоколу NFC та представляються їхні переваги та недоліки.

Ключові слова: NFC-ТЕХНОЛОГІЯ, РЕПЛІКАЦІЯ, ОС ANDROID, ДВОХФАКТОРНА АУТЕНТИФІКАЦІЯ, ВІДКРИТИЙ КЛЮЧ, СЕАНСОВИЙ КЛЮЧ, ШИФРУВАННЯ, ПРОФІЛЬ MOZILLA.

ANNOTATION

This master's qualification paper is devoted to the creation of a secure data replication method using NFC technology. An analysis of the existing mechanisms for synchronizing user data and NFC protocols and their advantages and disadvantages are presented.

Key words: NFC TECHNOLOGY, REPLICATION, ANDROID OPERATING SYSTEM, TWO-FACTOR AUTHENTICATION, PUBLIC KEY, SESSION KEY, ENCRYPTION, MOZILLA PROFILE.