УДК 004.056.53

АНАЛІЗ АТАК ПРИ ПЕРЕДАЧІ ДАНИХ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ NFC

Вовчак А.Б.
Західноукраїнський національний університет
магістрант

I. Вступ

Технологія NFC (NearFieldCommunication) - це бездротовий спосіб обміну даними між пристроями, який базується на використанні радіочастотного ідентифікаційного модуля, який дозволяє надсилати та приймати дані через магнітні поля [1-3]. Ця технологія стала надзвичайно популярною останнім часом і використовується для передачі даних між різними пристроями, такими як смартфони, планшети, смарт-картки та інші гаджети. NFC дозволяє зручно проводити оплати, обмінюватися контактами, відкривати двері та виконувати багато інших завдань [3-5]. Проте разом з перевагами при використанні цієї технології існують і загрози для безпеки даних користувачів [6-9].

В технології NFC обмін інформацією відбувається лише при безпосередньому контакті пристроїв на відстані не більше 10 см [1]. Однак питання про те, наскільки близько має знаходитися потенційний зловмисник, щоб успішно перехопити радіочастотний сигнал, який було б можливо подальше використовувати, не має однозначної відповіді [4,5]. Ця невизначеність обумовлена безліччю факторів, що впливають на відстань, на якій можливе прослуховування, таких як характеристики передавача та антени атакуючого, якість обладнання атакуючого, умови локації, наявність бар'єрів у вигляді стін і потужність NFC пристрою. Оцінка цих параметрів робить неможливим надання універсального значення, яке підходило б до більшості ситуацій.

II. Мета роботи

Метою роботи є аналіз атак при передачі даних із використанням технології NFC.

III. Дослідження безпеки технології NFC

В NFC існують два основних режими - активний та пасивний. В активному режимі один пристрій генерує радіочастотні сигнали та ініціює комунікацію, в той час як в пасивному режимі інший пристрій відповідає на запити та не генерує сигнали.NFC використовує магнітні поля для передачі даних. Кожен пристрій має NFC-комп'ютер, який генерує радіочастотні сигнали на частоті 13,56 МГц. Пристрої взаємодіють через ці магнітні поля та мають вбудовані механізми безпеки, такі як шифрування та аутентифікація, щоб захистити дані від несанкціонованого доступу [1,2]. Принцип роботи технології зображено на рисунку 1.

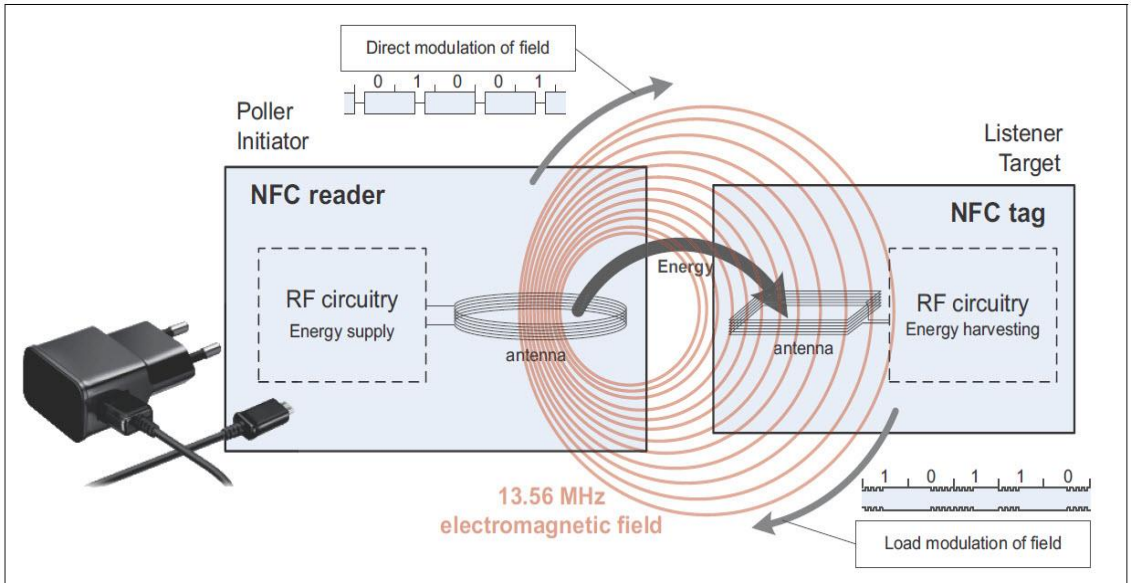

Рисунок 1 – Принцип роботи технології NFC

В рамках дослідження безпеки технології NFC була розглянута можливість проведення різних атак на канал передачі даних. Перелік атак представлений в таблиці 1.

Таблиця 1

Безпека технології NFC

Атаки на бездротові канали	Актуальність для технології NFC	Методи захисту
Пасивне прослуховування	+	Криптографічні методи
Пошкодження даних	+	Криптографічні методи
Модифікація даних	багато обмежень	Криптографічні методи
Вставка даних	багато обмежень	Криптографічні методи
Relay атаки	+	Екранування, Авторизація користувача
MITM атаки	-	-

Наведений перелік відображає можливість атак на незахищений за замовчуванням канал передачі даних. Уникнути багатьох таких атак можливо на рівні додатків, використовуючи криптографію та інші засоби захисту. Оскільки NFC є бездротовою технологією, існує загроза прослуховування каналу. Під час з'єднання двох пристроїв, вони взаємодіють за допомогою радіохвиль. Потенційний зловмисник може використовувати спрямовану антену для прослуховування передаваних сигналів. Шляхом експериментів або вивчення специфікацій протоколів взаємодії пристроїв атакуючий може виявити, як отримати інформацію з перехопленого сигналу. Слід відзначити, що існують доступні на ринку пристрої для перехоплення та розкодування радіочастотних сигналів.

Також важливо враховувати режим роботи передавача даних. У залежності від активного чи пасивного режиму роботи, методи перехоплення даних можуть значно відрізнятися. Загалом можна сказати, що в активному режимі радіус можливого прослуховування може сягати 10 метрів, тоді як в пасивному режимі ця відстань обмежується 1 метром.

Аналіз атак на безпеку технології NFC вказує на необхідність вдосконалення заходів безпеки для захисту даних та пристроїв, що використовують цю технологію. Деякі загальні рекомендації включають:

-Використання криптографічних методів для шифрування та аутентифікації даних.

-Встановлення захищених NFC-карток і пристроїв з високим рівнем безпеки.

-Валідація даних та перевірка їхньої цілісності під час передачі.

-Використання надійних каналів зв'язку для запобігання Relay атакам.

-Регулярне оновлення програмного забезпечення та виправлення виявлених вразливостей.

Висновок

Технологія NFC пропонує безліч можливостей для зручної бездротової передачі даних та використання в різних додатках та пристроях. Проте, зростаюча популярність технології NFC призвела до збільшення загроз та атак. Проведений у роботі аналіз різних атак на безпеку NFC показує, що безпека має бути важливою складовою розробки та використання цієї технології.

Список використаних джерел

1. Albattah, A., Alghofaili, Y., &Elkhediri, S. (2020). NFC Technology: Assessment Effective of Security towards Protecting NFC Devices & Services. 2020 International Conference on Computing and Information Technology (ICCIT-1441), 1–5.
2. Alrawais, A. (2020). Security Issues in Near Field Communications (NFC). International Journal of Advanced Computer Science and Applications, 11(11). https://doi.org/10.14569/IJACSA.2020.0111176
3. Ghosh, S., Goswami, J., Kumar, A., &Majumder, A. (2015). Issues in NFC as a form of contactless communication: A comprehensive survey. 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 252. https://doi.org/10.1109/ICSTM.2015.7225422
4. M. Dyvak, I. Darmorost, R. Shevchuk, V. Manzhula, and N. Kasatkina, “Correlation analysis traffic intensity of the motor vehicles and the air pollution by their harmful emissions,” in 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 2018, pp. 855–858.
5. Krepych S. The task of synthesis of analog filter with the specified admissible values of the output characteristics and computing complexity of the methods of theis solution / S. Krepych, M. Dyvak, P. Stakhiv, R. Shevchuk //13-th International Conference “The Experience Of Designing And Application Of CAD Systems in Microelectronics” Polyana Svalyava (Zakarpattya) Ukraine, 2015. – P.119-121.
6. Chen, C. H., Lin, I. C., & Yang, C. C. (2014). NFC Attacks Analysis and Survey. 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 458–462. https://doi.org/10.1109/IMIS.2014.66
7. Noh, S.-K., & Choi, D.-Y. (2013). Standard technical analysis, trend and future of NFC. Smart Media Journal, 2(3), 10–16.
8. Chen, I.-F., Peng, C.-M., & Yan, Z.-D. (2019). A simple NFC parameters measurement method based on ISO/IEC 14443 standard. 2019 IEEE International Conference on RFID Technology and Applications (RFID-TA), 33–36.
9. Комар М.П. Нейросетевой подход к обнаружению сетевых атак на компьютерные системы / М.П. Комар, И.О. Палий, Р.П. Шевчук, Т.Б. Федысив // Інформатика та математичні методи в моделюванні – 2011. – Том 1, №2. – С. 156-160.