УДК 004.021
DOI: 10.31673/2409-7292.2023.010005

Хворостяний Р. В.

ПРОБЛЕМИ БЕЗПЕКИ ТА ЗАХОДИ ПРОТИДІЇ АТАКАМ В NFC

Технологія Near Field Communication (NFC), широко поширена через зручність у використанні. Разом з тим, NFC уразлива до атак безпеки, таких як людина посередині; відмова в обслуговуванні (DOS) та ін. Ці атаки призводять до витоку важливих даних користувача, що може вплинути на будь-яку організацію, яка використовує програми та технології NFC. У цій статті розглядаються вразливості NFC та різні види атак на NFC. Також у статті розглянуто можливі рішення, які могли б захистити NFC від цих загроз безпеці.

Ключові слова: NFC, зв'язок ближнього доступу, атака, безпека.

Вступ

NFC (Near Field Communications) забезпечує двонаправлений безпроводовий безконтактний зв'язок між двома пристроями з підтримкою NFC або тегами NFC на короткій відстані менше 10 см. Він походить від технології радіочастотної ідентифікації (RFID), в той час, як RFID здатна лише для односторонньої передачі. NFC базується на індуктивному з'єднанні двох пристроїв NFC або тегах на центральній частоті 13,56 МГц, що підтримується стандартами ISO14443. NFC має три режими роботи: одноранговий режим, режим читання/запису та режим емуляції карти NFC. Одноранговий режим роботи дозволяє двом пристроям NFC передавати дані між собою. Режим читання/запису дозволяє пристроям NFC отримувати доступ до певних цифрових даних. Режим емуляції картки NFC змушує пристрої NFC працювати як карта NFC. На основі активності задіяних пристроїв або тегів NFC режими зв'язку можна класифікувати як режими зв'язку «активний-активний», «активний-неактивний», «неактивний-активний».

Постановка проблеми

Як нова технологієя, NFC має багатообіцяюче та широке майбутнє для застосування в різноманітних програмах. NFC надає зручні інструменти, такі як продаж квитків, електронні гаманці, фінансові операції, смарт-постери тощо. NFC має перевагу швидкого встановлення приватного зв'язку на короткій відстані і, тим самим, протистоїть зловмисним спробам, оскільки на дуже короткій відстані вони є малоймовірними. Але чи достатньо захищена технологія NFC? NFC є прикладом безпроводового зв'язку, що робить його вразливим до прослуховування, пошкодження даних і атак із заглушенням. Іншими словами, технологія NFC не включає надійну схему безпеки для захисту додатків, які створені на її основі. Крім того, NFC поділяє базові стандарти та методи з технологією proximity RFID. Деякі з атак, які можуть бути здійснені проти комунікацій RFID, є також загрозою і для NFC. Це залишає розробникам програмного забезпечення необхідність пошуку шляхів уникнення будь-яких загроз, які можуть бути спричинені цією технологією.

Аналіз публікацій

У роботі [1] описується рішення безпеки, яке можна використовувати для безпечного встановлення транзакцій мобільних платежів через радіоінтерфейс NFC. Пропоноване рішення є легким – воно використовує симетричні криптографічні примітиви на пристроях, які мають обмеження пам'яті та ресурсів ЦП. У статті [2] розглядається уразливість NFC, що вимагає поглиблених досліджень як безпеки, так і конфіденційності. Зосереджуючись на таких атаках, як DOS і пошкодження даних, існуючі моделі оцінки ризиків оцінюються за допомогою підходу аналітичного ієрархічного процесу (AHP).

У [3] розглядаються дві системи, які зосереджені на захисті даних, що передаються між двома пристроями з підтримкою NFC, використовуючи комбінацію RSA та AES та інші комбінації алгоритмів шифрування AES і Deffie Hellman. В публікації [4] представлено концепцію технології NFC у цілісному підході з різних точок зору, включаючи вдосконалення та оптимізацію апаратного забезпечення, основи зв'язку та стандарти, додатки, елементи

захисту, конфіденційність і безпеку, аналіз зручності використання, а також питання екосистеми та бізнесу.

Предметом роботи [5] є інформаційна безпека технологій RFID та NFC. У роботі описано та класифіковано деякі відомі на даний момент уразливості відповідних протоколів і пристроїв, які їх реалізують, а також розглянуто засоби та програмне забезпечення криптоаналізу. Результатом роботи є оцінка ризику використання окремих специфічних NFC-пристроїв, наприклад, безконтактних банківських карток.

Незважаючи на широке коло публікацій, на теперішній час не існує глибокого узагальнення проблем безпеки технології NFC, не досліджені основні типи атак та методи запобігання таким атакам.

Метою цього дослідження є розгляд механізмів безпеки NFC у їх відповідності до можливих кіберзагроз та вибору раціонального методу протидії таким загрозам.

Аналіз проблем безпеки NFC

NFC не надає жодного механізму безпеки для захисту свого зв'язку, що призводить до того, що дані користувачів потрапляють в ефір [6]. Розглянемо можливі атаки на NFC, і заходи протидії їм (рис. 1).

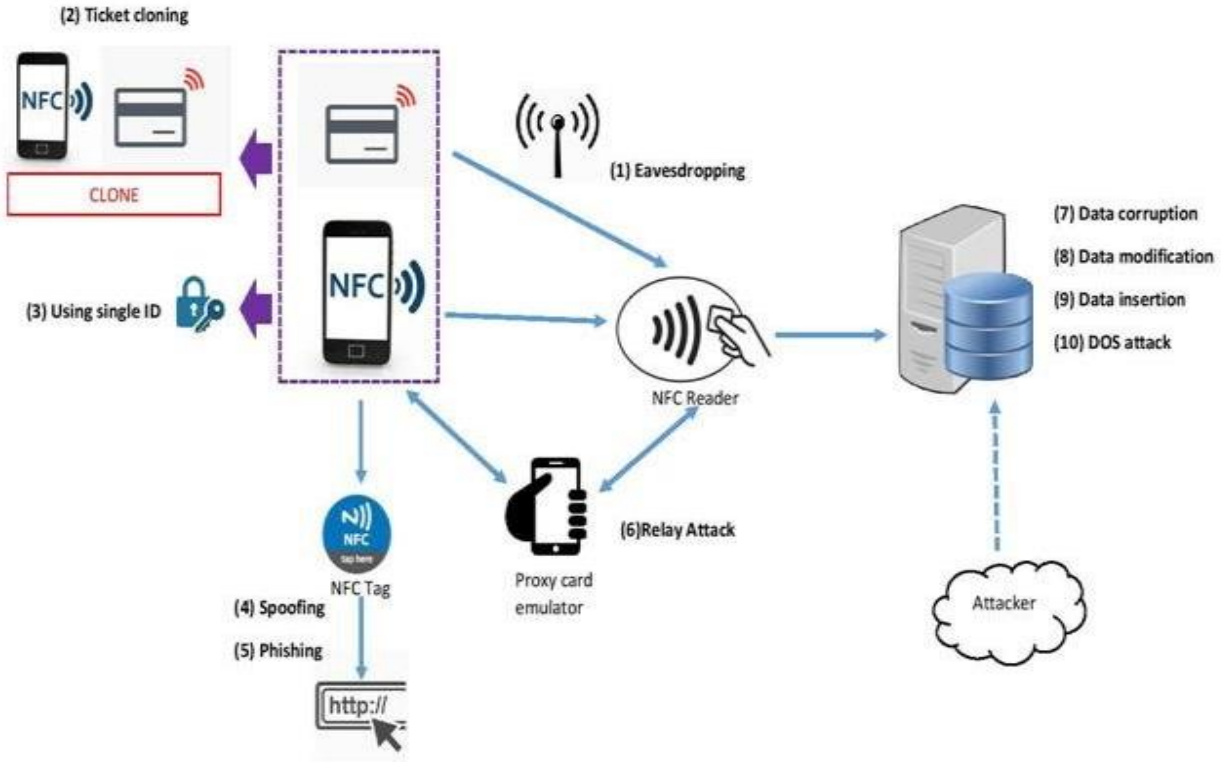

Рис. 1. Сукупність атак NFC [2]

(1) Прослуховування. Однією з поширених атак на безпроводовий зв'язок та, зокрема на NFC, є атака прослуховування [7].

Обмежений діапазон зв'язку пристроїв NFC, який становить близько 10 см, не повністю запобігає ризику атаки прослуховування. Будь-який зловмисник із достатнім обладнанням може прослухати зв'язок між двома пристроями NFC. Головне питання полягає в тому, наскільки близько потрібно підійти зловмиснику, щоб мати можливість провести атаку підслуховування пристроїв NFC. Це здебільшого залежить від умов комунікації: антен, приймача, потужності випромінюваного сигналу та шумів. Крім того, на атаку впливає режим зв'язку, оскільки існує різниця між прослуховуванням пристрою NFC у пасивному чи активному режимі [8].

© Хворостяний, Р. В. (2023). Проблеми безпеки та заходи протидії атакам в NFC. Сучасний захист інформації, 1(53), 39–46. https://doi.org/10.31673/2409-7292.2023.010005.

Важче слухати пристрій NFC у пасивному режимі, оскільки цільовий пристрій може отримувати живлення від електромагнітного поля, яке генерує активний пристрій. Відповідно до [9], коли пристрій NFC надсилає дані в активному режимі, атака підслуховування може здійснюватися на відстані до 10 м, тоді як в пасивному режимі ця відстань зменшується приблизно до 1 м.

Встановлення безпечного з'єднання та використання стандартних алгоритмів шифрування між двома пристроями NFC може захистити від атак підслуховування. Стандартний протокол узгодження ключів, такий як RSA або Elliptic Curves, можна використовувати для встановлення спільного секретного ключа між двома пристроями NFC. Потім секретний ключ можна використовувати для шифрування зв'язку за допомогою алгоритму симетричного ключа, такого як AES або 3DES [9]. Цей контрзахід забезпечить конфіденційність зв'язку NFC і захистить від атак підслуховування.

(2) Клонування. Технологія NFC застосовується в таких службах, як електронний або цифровий квиток. Клонування квитка з NFC може статися, якщо квитки були скопійовані та передані іншим перед перевіркою. Кожен може використати клон квитка як новий квиток, наприклад, для отримання знижки при покупці товарів. Якщо квиток перевірений, ним можна користуватися до закінчення терміну його дії [2].

(3) Скімінг. Є два режими захищеного елемента – зовнішній і внутрішній.

1) Зовнішній режим: щоб емулювати тег, у пристроях NFC потрібні чіпи смарт-карт. У зовнішньому режимі зовнішній зчитувач отримує доступ до захищеного елемента й не може розрізнити смарт-карту від пристрою NFC із захищеним елементом. Наприклад, у захищеному елементі є аплет кредитної картки, який перетворює смартфон NFC на мобільний платіжний пристрій.

2) Внутрішній режим: у внутрішньому режимі контролер хоста отримує доступ до захищеного елемента (читання та зміна). Запущені програми на головному контролері смартфону можуть змінювати інформацію в захищеному елементі. Таким чином, користувачі можуть дистанційно керувати інформацією в захищеному елементі за допомогою онлайн-з'єднання. У захищеному елементі індекс додатків надається як картами пам'яті (наприклад, Mifare Application Directory NXP), так і процесорними картами (наприклад, JCOP). Таким чином, він вразливий для сторонніх гравців, оскільки інші програми в захищених елементах піддаються впливу. Отже, проблема існує не лише в технології NFC, а й в індустрії смарт-карт взагалі.

(4) Спуфінг. Для кожного чіпа безконтактної смарт-картки є унікальний ідентифікатор (ISO14443 A: UID, ISO14443 B: PUPI, Felica: IDm). Їх довжина становить 4, 7 або 10 байт. Коли під час процесу зчитування відбувається колізія, необхідний унікальний ідентифікатор, щоб запобігти цьому шляхом ідентифікації. Ідентифікатор можна отримати вже під час вибору транспондера. Процес зчитування не включає шифрування чи автентифікацію пристрою зчитування.

Для запобігання колізії в стандарті вказано унікальний ID. Просте апаратне забезпечення, таке як OpenPICC [10], може підробити чиюсь особу, імітуючи ідентифікатор. Таким чином, якщо програма використовує фіксований унікальний ідентифікатор, можна легко отримати конфіденційні дані власника. Оскільки процес зчитування транспондера не включає шифрування, легко перервати зв'язок між зчитувачем і чіпом смарт-картки, щоб отримати фіксований унікальний ідентифікатор. Щоб уникнути цієї ситуації, унікальний ідентифікатор може бути створений випадковим чином під час колізії, що вже використовується в NFC електронних паспортів [11]. Це запобігає відстеженню користувачів однак не працює, якщо жертва використовує RFID (смарт-карту або пристрій NFC).

(5) Фішинг – це спроба отримати в електронному повідомленні конфіденційну інформацію, таку як паролі та дані кредитної картки, під виглядом надійної особи. Фішингові атаки можна легко здійснити проти середовища NFC шляхом зміни або заміни тегів NFC. Наступні алгоритм пояснює, як зловмисник може отримати конфіденційну інформацію, таку

© Хворостяний, Р. В. (2023). Проблеми безпеки та заходи протидії атакам в NFC. Сучасний захист інформації, 1(53), 39–46. https://doi.org/10.31673/2409-7292.2023.010005.

як дані кредитної картки, запустивши фішингову атаку на паркомат, який використовує технологію NFC для завершення процесу оплати [8]:

1) зловмисник спочатку створює шкідливий тег, який містить неправдиву інформацію, наприклад URL-посилання, яке спрямовує на фішинговий сайт;

2) зловмисник знаходить паркомат, який використовує технологію NFC, і заміняє оригінальну мітку на паркоматі на шкідливу;

3) щоб сплатити за паркомат жертва зі смартфоном NFC сканує тег паркомата;

4) користувачеві буде запропоновано встановити шкідливу програму (наприклад pork-mobile), яка є веб-переглядом фішингового сайту;

5) користувач вводить конфіденційну інформацію (наприклад дані кредитної картки) а зловмисник збирає її за допомогою встановленої шкідливої програми,.

Існує декілька контрзаходів, які можна застосувати для запобігання або зменшення ризику фішингової атаки. Одним з ключових факторів здійснення фішингової атаки є обман користувачів шляхом видавання за надійну особу. Обізнаність і освіта користувачів щодо фішингових атак є важливим заходом протидії, оскільки це допомагає мінімізувати кількість успішних атак. Обережні користувачі розпізнають процес встановлення нової програми з підозрілою назвою, наприклад – детальніше дослідять назву та оригінальність програми.

(6) Ретрансляція – це тип атаки людини в середині, коли зловмисник намагається маніпулювати зв'язком через ретрансляцію дослівних повідомлень між двома пристроями. Ретрансляція може бути виконана лише в тому випадку, якщо хоча б один з пристроїв атаки підтримує емуляцію карти. Існує багато можливих сценаріїв здійснення цієї атаки.

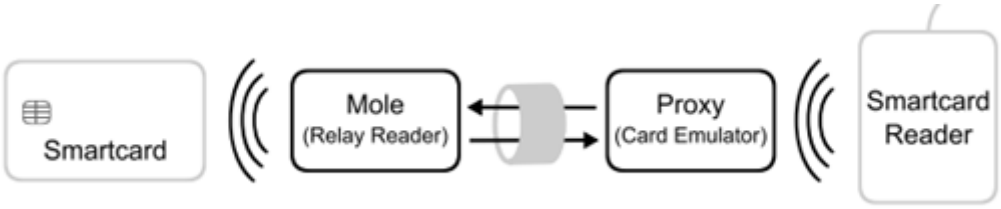

Рис. 2. Атака Ретрансляції [11]

Перший сценарій – коли NFC завжди ввімкнено на смартфоні, навіть якщо телефон не використовується. Смартфон із платіжною програмою може легко здійснювати транзакції. Як наслідок, це робить смартфон вразливим для ретрансляції. У цьому сценарії є два зловмисники, які підключені один до одного через Інтернет. Перша атака стосується проксі-пристрою, а друга – ретранслятора з двома пристроями з підтримкою NFC або смартфонами. У громадському місці, наприклад у транспорті, де збирається багато людей, очікуючи прибуття автобуса чи метро, зловмисник за допомогою надійного пристрою може наблизитися до смартфону жертви. Потім проксі-пристрій здійснює платіж NFC на платіжній станції. З'єднання між платіжною станцією та смартфоном жертви передається на два пристрої [12].

Другий сценарій можна реалізувати на сучасному смартфоні, де є деякі привілеї (відомі як взлом або рутинг), які дають повний контроль над смартфоном. Але він також втрачає деякі функції безпеки смартфона, такі як пісочниця. Крім того, функції безпеки захищають елементи безпеки, де знаходиться платіжна програма NFC. Таким чином, на рутованому смартфоні елементи безпеки більш вразливі. У цьому випадку зловмисник намагається дозволити користувачеві встановити шкідливу програму. Потерпілий вважає, що він отримав права доступу програми для функції. Тоді шкідлива програма отримає право доступу для виконання функцій. Тим часом програма отримує доступ до захищених елементів і інформує зловмисника через Інтернет. Тепер зловмисник має можливість здійснити оплату за платіжними реквізитами жертви [12].

Для захисту від ретрансляції користувач смартфона повинен переконатися, що NFC у смартфоні завжди вимкнено. Крім того, користувач смартфона повинен зберегти функції безпеки для виявлення будь-якої шкідливої діяльності в будь-якій встановленій програмі.

(7) Пошкодження даних. Щоб мати можливість пошкодити дані під час передачі між двома пристроями NFC зловмиснику потрібна висока потужність. Цю атаку можна виявити, оскільки пристрої NFC можуть перевіряти радіочастоту, подану під час передачі даних, і визначати тип атаки. Крім того, для здійснення атаки з пошкодженням даних зловмиснику потрібна більша потужність, ніж може виявити пристрій NFC. Отже, ця атака може бути виявлена пристроями NFC [6].

(8) Модифікація даних. Під час модифікації даних зловмисник може змінити дані, якими обмінюються пристрої NFC, таким чином пристрій-одержувач отримає деякі дійсні, але підроблені дані. Здійсненність атаки модифікації даних залежить від амплітуди модуляції [9]. Важко запустити атаку модифікації даних проти середовища NFC, коли модуляція кодування становить 100% тому, що при 100% модуляції зловмисник не може змінити біт значення 0 на біт значення 1 оскільки кожен біт для радіочастотного сигналу перевіряються декодером.

Однак легко провести атаку модифікації даних, коли модуляція становить 10%. При 10% модуляції декодер порівнює та оцінює рівні сигналу 82% і повний. Зловмисник намагається вставити сигнал до сигналу 82%, щоб сигнал 82% став видимим як повний сигнал, а фактичний повний сигнал відображався як сигнал 82%. Таким чином, дійсний біт зворотного значення біта буде декодований декодером. Підсумовуючи, можна сказати, що атака можлива у всіх бітах для 10% модуляції, тоді як неможливий для всіх бітів при 100% модуляції.

Іншим прикладом модифікації даних є обмін електронними візитними картками або інформацією про сполучення. Оскільки в протоколі транзакцій немає шифрування або автентифікації, засоби безпеки для забезпечення автентичності, цілісності та конфіденційності повинні бути реалізовані на прикладному рівні. Поточний загальний протокол, NFCIP-1, не включає засоби безпеки. У цій ситуації зловмисники можуть порушити зв’язок і змінити дані.

Існує кілька способів захисту від атаки модифікації даних. По-перше, зловмисник не зможе змінити всі дані, що передаються радіочастотним каналом, якщо в активному режимі використовується швидкість 106 Кбод. Чітко видно, що активний режим важливий, однак цей режим вразливий для атак підслуховування. Крім того, деякі біти в 106 КБ можуть бути змінені. По-друге, пристрій-відправник постійно перевіряє радіочастотне поле під час передачі даних, щоб виявити будь-яку потенційну атаку. По-третє, встановлення безпечного з’єднання між двома пристроями NFC є найкращим підходом для захисту від атаки модифікації даних [6].

(9) Вставка даних. Мета атаки із вставкою даних полягає в тому, щоб вставити повідомлення в дані, якими обмінюються два пристрої NFC, коли автовідповідачу потрібен час, щоб відповісти вихідному пристрою. Атака може бути запущена лише в тому випадку, якщо пристрій має певну затримку, завдяки якій зловмисник може передати своє повідомлення раніше, ніж пристрій-відповідач. Якщо і зловмисник, і автовідповідач передають дані одночасно, дані будуть перекриватися та бути пошкодженими.

Атака вставки даних може бути запущена між пристроями NFC за наступним сценарієм:

1) зловмисник розміщує свій зчитувач біля оригінального зчитувального пристрою;

2) потерпілий користувач використовуватиме мобільний смартфон NFC для передачі даних на пристрій зчитування;

3) шкідливий зчитувач відповідає безпосередньо користувачеві-жертві раніше, ніж оригінальний зчитувач;

4) оригінальний зчитувач відповідає жертві після зловмисника і відповідь буде проігнорована мобільним NFC-смартфоном жертви.

Щоб запобігти атаці вставки даних між двома пристроями NFC, можна застосувати три контрзаходи. По-перше, автовідповідач має відповідати оригінальному пристрою без затримки. Таким чином зловмисник не зможе вставити повідомлення в дані, які обмінюються

© Хворостяний, Р. В. (2023). Проблеми безпеки та заходи протидії атакам в NFC. Сучасний захист інформації, 1(53), 39–46. https://doi.org/10.31673/2409-7292.2023.010005.

між двома пристроями NFC, оскільки зловмисник не може бути швидшим за пристрій, що відповідає. По-друге, автовідповідач повинен слухати канал під час передачі даних, щоб пристрій міг виявити будь-яку потенційну атаку. По-третє, встановлення захищеного каналу між двома пристроями NFC є найкращим підходом для запобігання будь-якій атаці [9].

(10) Відмова в обслуговуванні (DoS). Безпроводовий зв'язок може бути дуже вразливим до атак типу «Відмова в обслуговуванні» (DoS-атак). Результати DoS-атак можуть бути різними: від погіршення безпроводового зв'язку до повної втрати доступності. Запустивши DoS-атаку, зловмисник може спробувати зробити NFC недоступним для користувачів.

Одним зі сценаріїв DoS-атаки є використання пристрою завад, націленого на середовище NFC для порушення зв'язку між двома пристроями [9]. Наприклад, зловмисник із пристроєм для завад, наприклад завади RFID, передає сигнал, який заважає передачі між мобільним смартфоном NFC і зчитувачем постачальника послуг. Ці завади можуть знищити передані дані та спричинити відмову в обслуговуванні. Практично, немає способу запобігти глушінню, однак існує рішення для протидії цьому сценарію шляхом виявлення глушіння. Рішення полягає в тому, щоб дозволити пристроям NFC перевіряти радіочастотне поле під час передачі. Це означає, що пристрій, що відправляє, може постійно перевіряти наявність глушіння та може зупинити передачу даних, коли хтось намагається перешкодити передачі.

Інша DoS-атака пояснюється в [13], де метою атаки є знищення довірчих відносин між клієнтами та постачальником послуг.

Сценарій цієї атаки пояснюють наступні кроки.

1) зловмисник створює тег, який викликає збій у смартфоні NFC після сканування;

2) зловмисник проникає до жертви або постачальника послуг і розміщує шкідливий тег поверх тегу постачальника послуг;

3) будь-який клієнт, який відвідує жертву або постачальника послуг, щоб отримати послугу за допомогою смартфону NFC, завершує роботу після сканування;

4) оскільки шкідливий тег виглядає так само, як і звичайний тег, то цей інцидент може зруйнувати довірчі відносини між клієнтом та постачальником послуг.

Для цієї атаки немає рішення, однак її можна виявити за допомогою деяких інструментів, наприклад фаззингу [13].

Інший сценарій DoS-атаки може бути запущений за допомогою порожнього тегу NFC. У [7] показано, що просто торкання NFC-пристрою з порожньою міткою викликає реакцію пристрою. Пристрій згенерує повідомлення про помилку, що є простим способом зайняти пристрій і зробити його недоступним. Запобігти цьому сценарію атаки може додавання механізму керування пристроєм NFC, наприклад комутатора NFC. Недоліком цього рішення є те, що користувачеві доводиться вмикати та вимикати функцію NFC кожного разу, коли йому потрібно сканувати.

(11) Людина в середині. У Man in The Middle Attack (MITM) зловмисник змушує дві сторони повірити, що вони підключаються одна до одної безпосередньо, тоді як насправді вся розмова керується зловмисником. У класичному сценарії припустимо, що Аліса та Боб хочуть поговорити між собою, а Єва є зловмисником, який контролює всю розмову. Обидві сторони, Аліса та Боб, вважають, що вони отримують і надсилають дані один одному, тоді як усі дані надходять від Єви (рис. 3).

Розглянемо той самий сценарій, але зв'язок між Алісою та Бобом є з'єднанням NFC, де Аліса буде в активному режимі, а Боб у пасивному. Аліса хоче надіслати дані Бобу і для цього вона генерує радіочастотне поле. Дані можуть бути підслухані Євою, якщо Єва достатньо закрита та активно перешкоджає передачі даних Бобу. Теоретично, у цій ситуації Аліса може виявити атаку шляхом перевірки наявності активних завад та відключити зв'язок [9]. Припустимо, що з'єднання триває і Аліса його не перевірила. Єва генерує радіочастотне поле, щоб мати можливість надіслати дані Бобу. Але це спричинить два активних радіочастотних

© Хворостяний, Р. В. (2023). Проблеми безпеки та заходи протидії атакам в NFC. Сучасний захист інформації, 1(53), 39–46. https://doi.org/10.31673/2409-7292.2023.010005.

поля. Перше генерує Аліса, а друге генерує Єва. У такому випадку Боб отримає незрозумілі дані. Як наслідок, у цій ситуації практично неможливо провести атаку Людина в середині.

Інший сценарій, але цього разу дві сторони Аліса та Боб будуть в активному режимі. Аліса надсилає дані Бобу і Єва може підслухати дані. Єва порушує передачу, щоб Боб не отримав дані. Знову ж таки, якщо Аліса не перевірила наявність активних завад, протокол продовжиться. Припустимо, що протокол триває активно – радіочастотне поле активного зв'язку було вимкнуто Алісою, тому Єва може надсилати дані Бобу. Єва включила радіочастотне поле і відправляє дані. У цій ситуації Аліса чекає відповіді від Боба. В результаті вона слухає і отримує дані від Єви. Аліса виявляє проблему в протоколі та від'єднує протокол. Отже, для Єви неможливо надсилати та отримувати дані від двох учасників. Підсумовуючи, можна сказати, що у реальному житті атака між двома пристроями NFC практично неможлива [9].

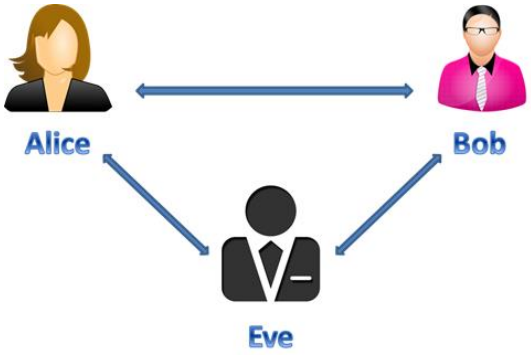

Рис. 3. Атака «Людина в середині» [11]

Хоча, атака людини в середині практично неможлива в NFC-з'днанні, однак настійно рекомендується використовувати активний режим. Крім того, щоб виявити будь-які збурення, викликані будь-якою атакою, активна сторона повинна слухати та перевіряти радіочастотне поле під час передачі.

Вибір засобів протидії атакам NFC. Оцінка ефективності протидії атакам на NFC виконується на основі чотирьох факторів: вартість атаки, практичність атаки, вартість контрзаходу та практичність контрзаходу. Основна мета цієї оцінки та аналізу полягає в тому, щоб одночасно оцінити та розрізнити згадані атаки та обрати методи протидії.

Вартість атаки описує витрати, необхідні для здійснення атаки на ближнє комунікаційне середовище. Ціною може бути таке обладнання, як обладнання для створення завад або обладнання для підслуховування, або вартість необхідного часу та зусиль для проведення атаки. Деякі атаки вимагають придбання додаткового обладнання, щоб розпочати атаку, наприклад, атака ретранслятора потребує двох пристроїв NFC та проксі-пристрою та двох залучених зловмисників. З іншого боку, є кілька атак, пов'язаних із NFC, які є недорогими та легкими для запуску, наприклад атака на відмову в обслуговуванні.

Практичність атаки є важливим фактором, який описує практичність атаки та можливість її виконання. Не всі атаки, пов'язані з NFC, практичні; фактично деякі атаки неможливо здійснити, наприклад людина в середині атаки [9]. Крім того, атака модифікації даних майже неможлива для всіх бітів у 100% модуляції. Однак; інші атаки, такі як підслуховування, відмова в обслуговуванні, фішинг-атаки та атаки на довіру, є практичними і можуть бути запущені з достатніми знаннями та обладнанням.

Вартість контрзаходів описує необхідні витрати для виконання контрзаходів, наприклад додаткові ресурси або технічні механізми. Для деяких атак, таких як атака на відмову в обслуговуванні, рішення може бути дорогим, оскільки вимагає найму служби безпеки або впровадження системи камер замкнутого телебачення (CCTV) для моніторингу та запобігання

© Хворостяний, Р. В. (2023). Проблеми безпеки та заходи протидії атакам в NFC. Сучасний захист інформації, 1(53), 39–46. https://doi.org/10.31673/2409-7292.2023.010005.

доступу до зчитувача. Однак інші атаки, такі як ретрансляція, вимагають дешевших технічних засобів протидії, таких як вимкнення NFC у смартфоні.

Іншим важливим фактором є практичність контрзаходів, яка описує практичність контрзаходів і можливість їх виконання. Деякі розглянуті контрзаходи є непрактичними для реалізації, наприклад, одним із контрзаходів модифікації даних є використання 106 Кбод в активному режимі, що зробить пристрої NFC вразливими до атак підслуховування [14]. З іншого боку, інші запропоновані контрзаходи практичні та дуже корисні для реалізації, наприклад встановлення безпечного з'єднання між пристроями NFC. Встановлення безпечного з'єднання є дуже практичним засобом протидії та може бути корисним для запобігання кільком атакам, пов'язаним із NFC.

Висновки

Комунікація ближнього поля NFC є багатообіцяючою технологією, і очікується, що вона буде більш інтегрованою з майбутніми смартфонами та стане невід'ємною частиною нашого повсякденного життя. Однак, безпека NFC все ще викликає занепокоєння та потребує більш глибокого аналізу та подальших досліджень. Технологія зв'язку на невеликій відстані не може забезпечити захист від багатьох досліджуваних атак, таких як прослуховування або модифікація даних. Встановлення захищеного каналу між пристроями NFC є ключовим механізмом для зменшення багатьох ризиків безпеки.

Майбутня робота щодо захисту NFC може полягати в тому, як розробити надійні операції зв'язку ближнього поля. Крім того, слід більше досліджувати інші атаки, пов'язані з безпекою, такі як викрадення сесії NFC, атака клонування, атака відповіді та атака NFC skimming, яка полягає в зчитуванні пристрою NFC у кишені людини. Крім того, використання NFC в платіжних системах створює багато питань безпеки, які слід більше вивчати та аналізувати.

Перелік посилань

1. Mohamad Badra, Rouba Borghol Badra, A Lightweight Security Protocol for NFC-based Mobile Payments, Procedia Computer Science, Volume 83, 2016, Pages 705-711.
2. Mahinderjit Singh, Manmeet (Mandy) & Adzman, Ku & Hassan, Rohail. (2018). Near Field Communication (NFC) Technology Security Vulnerabilities and Countermeasures. International Journal of Engineering and Technology. 7. 298-305. 10.14419/ijetv7i4.31.23384.
3. Shreya Parikh, 2017, Security of NFC, International Journal of Engineering Research & Technology (IJERT) ICIATE – 2017 (Volume 5 – Issue 01),
4. Coskun V, Ozdenizci B, Ok K. The Survey on Near Field Communication. Sensors (Basel). 2015 Jun 5;15(6):13348-405. doi: 10.3390/s150613348. PMID: 26057043; PMCID: PMC4507650.
5. M A Masyuk 2019 Information security of RFID and NFC technologies. Journal of Physics: Conference Series, Volume 1399, Issue 3. 033093
6. Arwa Alrawais. Security Issues in Near Field Communications (NFC). (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 11, 2020. 621-628.
7. S. H. Omkar Ghag, "A comprehensive study of google wallet as an NFC application," International Journal of Computer Applications, 2012.
8. V. Damme, Gauthier, K. Wouters, and B. Preneel, "Practical experiences with nfc security on mobile phones," in Workshop on RFID Security, 2009.
9. E. Haselsteiner and K. Breitfuß, "Security in near field communication (nfc)," 2006.
10. "Openpcd http://www.openpcd.org/," 2007.
11. Pierluigi Paganini. Near field communication (NFC) technology, vulnerabilities and principal attack schema. https://resources.infosecinstitute.com/topic/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/
12. R. Vermaas, "The security risks of mobile payment applications using near-field communication," 2013.
13. C. Mulliner, "Vulnerability analysis and attacks on nfc-enabled mobile phones," in Availability, Reliability and Security, 2009.
14. M. Riyazuddin, "Nfc: A review of the technology, applications and security." [Online]. Available: http://123seminarsonly.com/Seminar-Reports/023/46910687-Near-Field-Communications-Review.pdf.

Надійшла: 28.12.2022 Рецензент: д.т.н., професор Савченко В.А.