УДК 004.491.22

БЕЗПЕКА ВИКОРИСТАННЯ ТЕХНОЛОГІЇ NFC

А.О. Кабанов, Ю.В. Ковальова
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. Активне використання технології NFC вже стало повсякденною справою при оплаті товарів та послуг. Зі сторони маркетингу – це полегшення процедури оплати і зменшення витрат часу на цей процес, зі сторони фінансів – універсальний платіжний засіб, не потребуючий введення паролю, зі сторони технологій – використання новітніх розробок в повсякденному житті. А як щодо безпеки використання? Саме це питання є ключовим у розгляді розповсюдженої технології NFC.

NFC (Near Field Communication, «комунікація ближнього поля») – система бездротового високочастотного зв'язку малого радіусу дії, що дозволяє обмінюватися даними між пристроями, які перебувають на відстані близько 10 см. Це означає, що за допомогою NFC-гаджетів можна оплачувати покупки та послуги безконтактним способом, отримувати додаткову інформацію про товари і т.п.

За принципом дії NFC схожий з Bluetooth, але при підключенні до іншого пристрою NFC не потрібно витрачати багато часу на ідентифікацію, зв'язок встановлюється майже миттєво (за десяті частки секунди). Для передачі даних NFC використовує кодування з різним коефіцієнтом модуляції в залежності від швидкості передачі даних. При цьому пристрої NFC в змозі одночасно і отримувати, і передавати дані. Таким чином, вони можуть контролювати радіочастотне поле і виявляти невідповідність, якщо отриманий сигнал не відповідає переданому [1].

Технологія NFC в Україні використовується в трьох виглядах:

1. У вигляді мітки (коли до мітки підносять активний NFC-зчитувач, вона активується й передає інформацію зчитувачу. Здебільшого мітки доступні лише для зчитування).
2. У вигляді картки (дана технологія використовується в банківських платіжних картках та в проїзних у метрополітені).
3. У вигляді мобільного пристрою:
   - передавання даних з використанням NFC-чипа та Bluetooth або Wi-Fi модулів;
   - зчитування NFC міток для отримання додаткової інформації;
   - емуляція віртуальних карток для оплати товарів та послуг [2].

На сьогоднішній день в Україні функціонують дві системи електронних платежів з мобільних пристроїв: Google Pay (для мобільних пристроїв під керуванням операційною системою Android) та Apple Pay (для мобільних пристроїв під керуванням операційною системою iOS/iPadOS/WatchOS).

Успішне використання технології NFC призводить до її широкого застосування, наприклад:

– для контролю доступу в приміщення або на територію (великі об'єкти - заводи, готелі, готелі, аквапарки, публічні заходи - концерти, виставки, саміти, заходи з інформаційної безпеки, гірськолижні курорти, олімпіади та інші спортивні заходи);
– для доступу в автомобіль і його подальшого керування;
– для управління розумним будинком;
– для оплати транспорту (транспортні карти, електронні квитки);
– для відстеження переміщення товарів;
– для посвідчення особи.

Широке використання технології NFC передбачає широкий спектр можливостей для скоєння злочинів. З точки зору інформаційної безпеки основні слабкості і недоліки NFC пов'язані з тим, що стек протоколів NFC не передбачає криптографії при передачі. Стандарти зберігання даних в мітках і картах, а також їх емуляції - не передбачають криптографічного захисту при зберіганні. В реалізаціях багатьох карт, смарт-карт і їх емуляції застосовуються слабкі криптографічні алгоритми.

В NFC сервісах традиційно закладається надмірна довіра до інформації, що зберігається на картах і мітках, і в результаті чого фактично не виконується фільтрація даних. Раніше, коли пристрої для зчитування і запису інформації на карти були не так поширені, це можна було зрозуміти. Зараз в смартфонах з підтримкою NFC можна легко створити емуляцію карти і записати туди довільні дані (SQL-ін'єкції, виконання команд на стороні сервісу і т.п.).

Серед найбільш розповсюджених атак на NFC є:
– Прослуховування інформації при передачі по NFC;
– Несанкціоноване зчитування інформації з NFC пристроїв;
– Lock Attack (переведення емульованої карти (мітки) в режим тільки читання і блокування запису інформації зчитувачем);
– Time Attack (в разі якщо термін дії карти або послуг прописаний на самій карті, то можна замінити цю дату);
– Reply Attack (перехоплення інформації і багаторазове її повторення або застосування - дозволяє отримувати доступ до послуг, товарів від імені іншої особи);
– Clone attack (клонування NFC пристроїв);
– Relay attack (зловмисник використовує два NFC пристрої, одне з яких зчитує дані з пристрою жертви, передає дані на другий пристрій, а другий пристрій видає отримані дані зчитувачу і отримуємо послугу від імені жертви);
– Класичні атаки на серверну та інфраструктурну частину NFC сервісів [3].

Висновки. Використання технології NFC стало повсякденною справою в житті сучасної людини. Однак, з розвитком технологій та їх використання в мережі IoT (інтернет речей), розробники NFC-пристроїв та сервісів відкладають питання забезпечення безпеки даних сервісів на останній план, а згодом і взагалі не повертаються до нього. Перелічені типи атак на NFC-модуль стануть в нагоді розробникам NFC-пристроям для усунення вразливостей, а

організаціям, які використовують такі прилади, нададуть освіченість в цьому питанні.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Near Field Communication (NFC) Ближняя бесконтактная связь – 2018 – [Електронний ресурс]. – Режим доступу https://bit.ly/2NcCv5C

2. Near Field Communication – 2019 – [Електронний ресурс]. – Режим доступу https://uk.wikipedia.org/wiki/Near_Field_Communication

3. NFC – 2016 – [Електронний ресурс]. – Режим доступу https://www.securitylab.ru /news/tags/NFC/

УДК 514.18

ПРОБЛЕМА АВТОМАТИЗАЦІЇ СТВОРЕННЯ ГРАФУ ДОРІГ ДЛЯ ГЕОМЕТРИЧНОГО МОДЕЛЮВАННЯ

С.Я. Кравців, О.М. Соболь
(Україна, Харків, Національний університет цивільного захисту України)

Робота присвячена автоматизації графу доріг для використання їх у комп’ютерних програмах для визначення областей покриття.

Ключові слова: граф доріг, геометричне моделювання, дискретні області, пожежно-рятувальний підрозділ.

S. Kravtsiv, O. Sobol. Problem of automation of the creation a graph of roads for geometric modeling. The work is devoted to the automation of the graph of roads for use in computer programs to determine the coverage areas/

Keywords: graph of roads, geometric modeling, discrete areas, fire and rescue unit.

С.Я. Кравцив, О.Н. Соболь. Проблема автоматизации создания графу дорог геометрического моделирования. Работа посвящена автоматизации графу дорог для использования в компьютерных программах для определения областей покрытия.

Ключевые слова: граф дорог, геометрическое моделирование, дискретные области, пожарно-спасательное подразделение.

Постановка проблеми. Одною із проблем для геометричного моделювання є збір необхідної інформації (масштаб карти, геолокації доріг та всіх елементів на карті, відомості про аварійні ділянки тощо), що необхідна для покриття області з дискретними елементами.

Для автоматичної побудови області покриття території в геометричному моделюванні досить важливим є те, що навігаційні карти необхідно будувати за допомогою графів доріг, що представляють собою цифрову векторну карту, що складаються з топологічно пов'язаних дуг і вузлів, розташування і властивості яких з заданою точністю та повнотою передають маршрути і організацію руху наземного транспорту.