Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерної інженерії та управління _____
(повна назва)

Кафедра _____Безпеки інформаційних технологій _____
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____перший (магістерський)_____

_____Метод захисту інформації при використанні технології NFC_____

(тема)

Виконав:

студент __2_ курсу, групи _БДІРм-20-1_
___Сенченко А.О._____

(прізвище, ініціали)

Спеціальність _____125 Кібербезпека ____

(код і повна назва спеціальності)

Освітня програма __«Безпека державних інформаційних ресурсів»_

(повна назва освітньої програми)

Керівник __проф. Заболотний В.І._____

(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ _____Халімов Г.З.__
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет_____Комп'ютерної інженерії та управління _____

Кафедра_____Безпеки інформаційних технологій_____

Рівень вищої освіти_____перший (магістерський)_____

Спеціальність_____125 Кібербезпека _____
(код і повна назва)

Освітня програма_____«Безпека державних інформаційних ресурсів»_____
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові_____Сенченку Антону Олеговичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи ___ Метод захисту інформації при використанні технології NFC_____
_____
затверджена наказом по університету від _1_____09___2021 р. № __1684ст__ ___
2. Термін подання студентом роботи до екзаменаційної комісії _13 грудня_____2021 р.
3. Вихідні дані до роботи _дослідження технології NFC, створення та аналіз моделі порушника, аналіз та створення моделі загроз, розробка рекомендацій що до більш безпечного застосувуання технології NFC_ _
_____
_____
_____
_____
_____
_____
_____
_____
_____
4. Перелік питань, що потрібно опрацювати в роботі _____
Технічні аспекти роботи технології NFC.
Сфера використання технології NFC.
Аналіз загроз та методів захисту при передачі данних в NFC.
_____
_____
Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _презентаційний матеріал у вигляді слайдів _____

_____
_____
_____
_____
_____
_____
_____
_____
_____

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім’я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання	1.09.2021	Виконано
2	Робота з джерелами за тематикою роботи	1.09.2021-1.10.2021	Виконано
3	Вивчення основних понять в сфері загроз безпеки для технології NFC	1.10.2021-22.10.2021	Виконано
4	Аналіз технічних аспектів NFC	22.10.2021-29.10.2021	Виконано
5	Аналіз загроз безбеки для технології NFC	29.10.2021-6.11.2021	Виконано
6	Аналіз безпеки технології технології NFC	6.11.2021-12.11.2021	Виконано
7	Розробка захищеного каналу під час передачі за інтерфейсом NFC	12.11.2021-25.11.2021	Виконано
8	Оформлення пояснювальної записки	25.11.2021-13.12.2021	Виконано

Дата видачі завдання _1__ _____вересня_____2021 р.

Студент _____
(підпис)

Керівник роботи _____ _____проф. Заболотний В.І._
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Звіт про передатестаційну практику містить : 72 с., 28 рис., 4 табл., 27 джерел.

БЕЗПЕКА NFC, ЗАГРОЗИ ТА МЕТОДИ ЗАХИСТУ ПРИ ПЕРЕДАЧІ ДАНИХ В NFC, СТАНДАРТИ ТА ПРОТОКОЛИ NFC , ТЕХНІЧНІ ХАРАКТЕРИСТИКИ ТЕХНОЛОГІЇ NFC.

Об’єкт дослідження – забезпечення безпеки даних під час передавання технологією NFC.

Предмет дослідження – безпека стандартів та протоколів в технології NFC.

Мета роботи – аналіз та дослідження загроз в інформаційній безпеці для засобів які використовують технологію NFC; аналіз стандартів та протоколів які використовуються в технології NFC.

Методи дослідження – аналіз технічних характеристик технології NFC; аналіз загроз, які можуть виникати для системи NFC.

У ході виконання роботи була розглянута система роботи технології NFC. Було виявлено її технічні характеристики та стандарти розробки NFC. Була створена модель загроз та модель правопорушника. Був запропонований варіант розробки захищеного каналу для передачі даних за інтерфейсом NFC.

ABSTRACT

The report on pre-certification practice contains: 72 pp., 28 pictures, 4 table, 27 sources.

NFC SAFETY, THREATS AND PROTECTION METHODS WHEN TRANSMITTING DATA TO NFC, NFC STANDARDS AND PROTOCOLS, TECHNICAL CHARACTERISTICS OF NFC TECHNOLOGY.

The object of research is to ensure data security during NFC technology transmission.

The subject of research is the security of standards and protocols in NFC technology.

Purpose - analysis and study of information security threats for tools that use NFC technology; analysis of standards and protocols used in NFC technology.Research methods - analysis of threats that may arise to the NFC system.

Research methods - analysis of technical characteristics of NFC technology; analysis of threats that may arise to the NFC system.

In the course of the work, the system of NFC technology operation was considered. Its technical characteristics and NFC development standards were identified. A threat model and an offender model were created. An option for the development of a secure channel for data transmission over the NFC interface was proposed.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

RFID – радіочастотна ідентифікація;

NFC – комунікація ближнього поля;

SE – безпечний елемент;

NFC-WI – Бездротовий інтерфейс;

ISO/IEC 14443 – стандарт, що описує частотний діапазон, метод модуляції та протокол обміну безконтактних пасивних карток (RFID) ближнього радіусу дії (до 10 см) на магнітозв'язаних індуктивностях;

ISO / IEC 18092 – определяет режимы связи для интерфейса и протокола связи ближнего поля (NFCIP 1) с использованием индуктивно связанных устройств, работающих на центральной частоте 13,56 МГц для соединения периферийных устройств компьютера;

SWP – протокол, що забезпечує з'єднання однопровідного зв'язку між інтерфейсом елементом безпеки на сім-карті;

NFCIP-1 – стандарт визначає режими зв'язку для інтерфейсу та протоколу зв'язку ближнього поля;

NFCIP-2 – визначає механізм вибору між різними режимами зв'язку;

PCD – пристрій працює як зчитувач ISO / IEC 14443 сумісних карт;

PICC – пристрій емулює безконтактну смарт-карту, в так званому режимі емуляції карт;

NDEF – стандарт, що визначає формат даних між NFC-сумісними пристроями і мітками;

RTD – стандарт, визначає типи записів для різних цілей у повідомленнях NDEF;

LLCP – протокол для підтримки P2P зв'язку між двома пристроями;

Digital Protocol – цифровий протокол для NFC-пристроїв зв'язку, забезпечує специфікації з реалізації на вершині стандартів ISO/IEC 18092 та ISO/IEC 14443;

SNEP – простий протокол обміну NDEF-повідомленнями, використовується у верхній частині LLCP, дозволяє проводити обмін повідомленнями NDEF.

ВСТУП

Near Field Communication (NFC) – це розширення технології радіочастотної ідентифікації (RFID), яка працює на короткій відстані . RFID в основному використовується для відстеження та ідентифікації шляхом передачі радіохвиль. NFC працює на низькій частоті 13,56 МГц на відстані від 4 см до 10 см і має максимальну швидкість передачі даних 424 кілобіт на секунду (кбіт/с).

Підтримка технології смартфонами почалася з виходом версії ОС Android 4.0 "Ice Cream Sandwich" у 2011 році, а також з виходом у 2014 році Apple iPhone 6 і смартфонів на базі Windows Phone 8.1

Використання NFC в реальних програмах насправді не гарантує безпечного застосування. Таким чином, технологія NFC має свої власні проблеми, як-от загрози безпеки RFID застосовні до NFC, оскільки NFC є аналогом RFID, і всі пристрої NFC діють як засоби зчитування або засоби запису, які можуть створювати різні загрози. Інший фактор, що призводить до вразливості безпеки в NFC, пов’язано з відсутністю специфікації NFC, яка охоплює всі контрзаходи для служб безпеки x.800, такі як аутентифікація та контроль доступу. Поточна специфікація призначена лише для надання вказівок для розробників додатків NFC для захисту даних і зв’язку в пристроях NFC. Далі проблеми з конфіденційністю, що виникають при використанні NFC, можуть витікати зловмисними атаками. Наприклад, користувачі, які використовують NFC як цифровий гаманець для зберігання інформації про свій банківський рахунок, схильні до атаки на конфіденційність даних, коли інформація на гаманці захоплюється зловмисником без будь-якого відома користувача в будь-який час і в будь-якому місці. Оскільки технологія NFC стикається з проблемами, зростають питання безпеки щодо безпечного середовища.

Об’єкт дослідження – забезпечення безпеки інформації під час передавання технологією NFC.

Предмет дослідження – безпека стандартів та протоколів, які використовуються в технології NFC.

Мета роботи – дослідження загроз в інформаційній безпеці для засобів які використовують технологію NFC; аналіз стандартів та протоколів які використовуються в технології NFC.

Методи дослідження – аналіз фізичних характеристик технології NFC; аналіз загроз, які можуть виникати для системи NFC.

У кваліфікаційній роботі досліджуються існуючі стандарти, які стосуються технології NFC. Аналізується набір протоколів, які можуть забезпечувати захист інформації під час обміну ключами та шифрування трафіку під час передачі даних за технологією NFC.

1 ПРОЦЕС ПОЯВИ ТЕХНОЛОГІЇ NFC

1.1 Історія RFID

RFID – це радіочастотна ідентифікація (РЧІ). Технологія RFID створена з метою автоматизації та зручності проведення багатьох виробничих процесів на Вашому підприємстві. Основи технології RFID були закладені ще в 40-ті роки XX століття (час Великої Вітчизняної війни). Вже на літальних апаратах з'явилися ідентифікуючі системи, які дозволяли розпізнати своїх союзників і ворогів. Але оскільки вся електронна техніка на той час була побудована на ламповій основі, то про розвиток технології RFID не могло йтися й мови.

Після війни були зроблені нові відкриття в галузі електроніки (зокрема напівпровідникових елементів), що дозволило ввести технологію RFID і розділити її на активний і пасивний напрямки. Активний метод ідентифікації вже передбачав використання RFID-мітки, обладнаної приймально-передавальними схемами і має власне джерело живлення, яке дистанційно читалося на дуже великих відстанях. Пасивна ідентифікація вимагає застосування тієї ж RFID-мітки, але не має власного джерела живлення. Вона отримує енергію від зчитувального пристрою.

У період 1950-1970-х років. XX століття ця технологія була засекречена і використовувалася лише у військовій промисловості, а також застосовувалася розвідувальними військами. Вартість застосування цієї технології на той час була фантастичною.

Вже 80-ті рр. XX століття напівпровідники значно зменшилися у розмірах і різко знизилася їхня вартість. Нова технологія вже ні для кого не була секретом і почалося її активне впровадження. Першим кроком у впровадженні в народні маси цієї технології стало застосування штрих-

коду. Спосіб простий, швидкий, із захистом від шкідливих зовнішніх впливів. Але в той же час цей спосіб має суттєві недоліки:

1. Пряма видимість між зчитувачем та штрих-кодом

2. Неможливість перезапису закладеної у штрих-коді інформації

3. Не універсальність штрих-коду як ідентифікатора

4. Вартість даної технології не набагато менша за вартість більш досконалої технології

У той самий час (80-ті рр.) виникла гостра необхідність запровадження технології RFID з можливістю дистанційного зчитування інформації, одночасного зчитування кількох RFID-меток. Також передбачалося позбавитися прямого контакту RFID-мітки використовуючи RFID-зчитувач. Звісно, розпочалися розробки за світовими стандартами запису, зберігання та відтворення ідентифікаційної інформації. А на початку 90-х років були розроблені активні та пасивні RFID-технології, що орієнтуються на різні сфери діяльності. У компанії rfid-m ви можете купити будь-які з представлених технологій rfid, наші спеціалісти з rfid обладнання, повністю вас проконсультують та нададуть усі необхідні консультації.

Будь-яка RFID-система складається зі зчитувального пристрою (зчитувач, рідер або інтерогатор) і транспондера (він же RFID-мітка, іноді також застосовується термін RFID-тег).

Більшість RFID-міток складається з двох частин. Перша - інтегральна схема (IC) для зберігання та обробки інформації, модулювання та демодулювання радіочастотного (RF) сигналу та деяких інших функцій. Друга - антена для прийому та передачі сигналу.

З введенням RFID-міток у повсякденне життя пов'язана низка проблем. Наприклад, споживачі, які не мають зчитувачів, не завжди можуть виявити мітки, прикріплені до товару на етапі виробництва та упаковки, і позбутися їх. Хоча під час продажу, як правило, такі мітки

знищуються, сам факт їхньої наявності викликає побоювання у правозахисних та релігійних організацій.

Вже відомі додатки RFID (безконтактні смарт-картки в системах контролю керування доступом та в платіжних системах) набувають додаткової популярності з розвитком інтернет-послуг.

Існує кілька способів систематизації RFID-міток та систем:

1. За робочою частотою
2. За джерелом живлення
3. За типом пам'яті
4. По виконанню

За джерелом живлення

За типом джерела живлення RFID-мітки поділяються на:

1. Пасивні
2. Активні
3. Напівпасивні

Пасивні RFID-мітки не мають вбудованого джерела енергії. Електричний струм, індукований в антені електромагнітним сигналом від зчитувача, забезпечує достатню потужність для функціонування кремнієвого CMOS-чіпа, розміщеного в мітці, і передачі сигналу у відповідь.

1.2 Історія розвитку технології NFC

Технологія NFC бере свій початок в далекому 1983 році. 14 травня 1983 року Чарльз Велтон, електротехнік за освітою, отримує патент на портативний радіочастотний випромінювач-ідентифікатор. Так виникає саме поняття RFID.

Стандарт ISO/IEC для NFC був прийнятий 8 грудня 2003, а через деякий час - був прийнятий і ECMA стандарт.

Стандартами, що описують відкриту технологічну платформу NFC, є ECMA-340 and ISO/IEC 18092. Ці стандарти описують режими модуляції, кодування, швидкості передачі даних і частоту кадру в рамках радіообміну пристроїв з підтримкою NFC, а також процедури ініціалізації зв'язку та протокол виправлення помилок під час встановлення з'єднань, як активного, так пасивного режиму роботи. Потім описується транспортний протокол, включаючи активацію протоколу і способи обміну даними. Радіоінтерфейс для NFC описується стандартами ISO/IEC 18092/ECMA-340 (Near Field Communication Interface and Protocol-1 (NFCIP-1)) та ISO/IEC 21481/ECMA-352 (Near Field Communication Interface and Protocol-2 (NFCIP-2))).

У 2004 році, 18 березня, анонсовано створення NFC Forum (Форум NFC) – некомерційної організації, організованої компаніями NXP Semiconductors, Sony та Nokia для просування технології NFC у її застосуваннях у споживчій електроніці, мобільних пристроях та ПЕОМ. NFC Forum займається питаннями стандартизації технології NFC, з метою забезпечення можливості взаємодії між пристроями та сервісами різних компаній.

У 2006 році з'являється початкова специфікація NFC-тегів та виходить перший комерційний телефон з NFC-чіпом.

У травні 2009 року NFC Forum представляє режим peer-to-peer передачі між пристроями з NFC-чіпами різної інформації: посилань, контактів, даних встановлення зв'язку через Bluetooth.

У березні 2011 року до NFC Forum приєднується компанія Google.

У травні 2011 року Google анонсує Google Wallet, мобільний додаток для прив'язування банківських карт до смартфонів із NFC-чіпами. Незабаром користувачі можуть замінити кредитки своїм смартфоном.

У серпні 2011 року Nokia повідомляє про те, що всі майбутні Symbian-смартфони будуть комплектуватися чіпами NFC.

NFC Forum розробив для NFC загальний формат даних NDEF (NFC Data Exchange Format, Формат Обміну Даними для NFC), придатний для зберігання та передачі різних видів інформації, включаючи об'єкти MIME (MIME - стандарт, що описує передачу різних типів даних електронною поштою, а також, у загальному випадку, специфікація для кодування інформації та форматування повідомлень таким чином, щоб їх можна було пересилати через Інтернет) та короткі текстові повідомлення, наприклад URL.

Концептуально, NDEF дуже близький до MIME, і використовує щільно упаковані бінарні «записи». Кожен запис може зберігати різні види об'єктів. Відповідно до прийнятих угод, тип першого запису визначає тип всього повідомлення.

Крім того, у розробці та впровадженні NFC бере участь асоціація GSMA (GSM Association, Асоціація GSM), що об'єднує 700 мобільних операторів із 218 країн світу. GSMA створено три ініціативні групи:

Mobile NFC initiative (Ініціативна група мобільного NFC) - працює над розвитком користувацьких додатків NFC і включає 14 операторів стільникового зв'язку, що займають близько 40% світового ринку, а саме: Bouygues Тйлйcom, China Mobile, AT&T, KPN, Mobilkom Austria, Orange, , SK Telecom, Telefonica Myviles Espaca, Telenor, TeliaSonera, Telecom Italia Mobile (TIM), Vodafone, Deutsche Telecom.

Pay buy mobile initiative (Ініціативна група мобільної купівлі та продажу) – працює над загальним підходом до розвитку взаємодії мобільних пристроїв із безконтактними платіжними терміналами. На даний момент до ініціативи входять 30 мобільних операторів.

ISIS - ініціативна група, що об'єднує AT&T, Verizon та T-Mobile з метою стимуляції широкого розвитку технології NFC, та надання двомстам мільйонам користувачів трьох мобільних операторів у США функціональності кредитної картки у їхніх мобільних пристроях.

StolPan (Store Logistics and Payment with NFC, Логістика Магазинів та Оплата за допомогою NFC) - всеєвропейський консорціум, створений за підтримки програми Information Society Technologies (Інформаційні Технології Товариства) Європейської Комісії для вивчення можливостей інтеграції NFC, бездротових мереж обміну даними.

Форум NFC визначив три комунікаційні режими роботи NFC-чіпов:

1. Режим peer-to-peer. У цьому випадку два пристрої зв'язуються один з одним для обміну інформацією між собою. За допомогою p2p передаються контакти між смартфонами з NFC-чіпами, відбувається миттєва передача налаштувань з WiFi-роутера на мобільний пристрій . У цьому режимі можна буде поєднувати смартфони для створення мультиплеєрних ігор. Для Nokia є NFC-версії хітів Angry Birds та Fruit Ninja, частина рівнів у яких відкриваються лише при з'єднанні через NFC з іншим смартфоном.

2. Режим зчитувача. У цьому режимі ваш смартфон виступає в ролі сканера сучасних аналогів штрих-кодам - NFC-міткам, що містить різну додаткову інформацію. До речі, NFC-мітки останнім часом все частіше витісняють штрих-коди: їх можна зустріти на продуктах харчування в супермаркетах (щоб швидко дізнатися про термін придатності та склад), а також рекламних щитах з метою швидко передати рекламну інформацію.

3. Режим емуляції карт. Саме цей режим найчастіше асоціюється із технологією NFC. Завдяки режиму емуляції карт ваш смартфон може «прикинутися» вашою банківською картою або проїзним квитком на метро, тим самим звузивши товщину вашого гаманця .

2 ТЕХНІЧНІ ХАРАКТЕРИСТИКИ ТЕХНОЛОГІЇ NFC

2.1 NFC інтерфейс

Основним компонентом пристрою NFC є бездротовий NFC-інтерфейс, який безпосередньо спілкується з іншими пристроями NFC або RFID. Інтерфейс NFC поєднує в собі функціональність приймача даних, читання RFID-міток і передачі RFID-міток. Інтерфейс NFC, як правило, складається з контролера NFC і NFC-антени. Крім того, іноді безконтактний кінцевий модем (NFC CLF -Contactless Front-End) також заявлений як частина NFC інтерфейсу, він відповідає за управління специфічними для NFC протоколами зв'язку між антеною і кінцевим NFC-пристроєм . Контролер NFC має аналоговий радіочастотний інтерфейс, який включає в собі передавач для відправки сигналів на частоті 13,56 МГц, приймач на тій же частоті, та інший приймач для завантаження модульованих сигналів на частоті 848 кГц (такі модульовані сигнали генеруються пасивними NFC пристроями). Радіочастотний інтерфейс також може включати модулятор навантаження, який використовується в режимі емуляції карти для модуляції відповідей на активних NFC-пристроях.

Інша частина контролера - безконтактний універсальний синхронний приймач (UART), де дані кодуються і декодуються у відповідні форми сигналів, необхідних для передачі ядру контролера, який обробляє протоколи повідомлень. Ядро контролера - мікропроцесор, який обробляє протоколи повідомлень. Контролер NFC забезпечує кілька інтерфейсів для зв'язку з хост-контролером і Елементом Безпеки (через спеціальні протоколи - Single Wire Protocol (SWP) і інтерфейс NFC

Wireless Interface (NFC-WI)). Блок-схема контролера NXP PN544 NFC, що використовується , щоб проілюструвати типові компоненти та інтерфейси управління .

При використанні NFC-WI безпечний елемент приєднаний за допомогою двох проводів до RF-інтерфейсу контролера NFC. NFC-WI інтерфейс в контролері NFC показаний на рисунку 2.1. Провіду передають сигнали модуляції між приймачем NFC і NFC-контролером. Елемент безпеки кодує і декодує сигнали від проводів, а також робить обробку протоколу передачі даних. NFC-WI повністю сумісний зі стандартами NFCIP-1 та ISO/IEC 14443, які будуть розглянуті далі. Підтримувані швидкості передачі - 106, 212 та 424 кбіт/с.

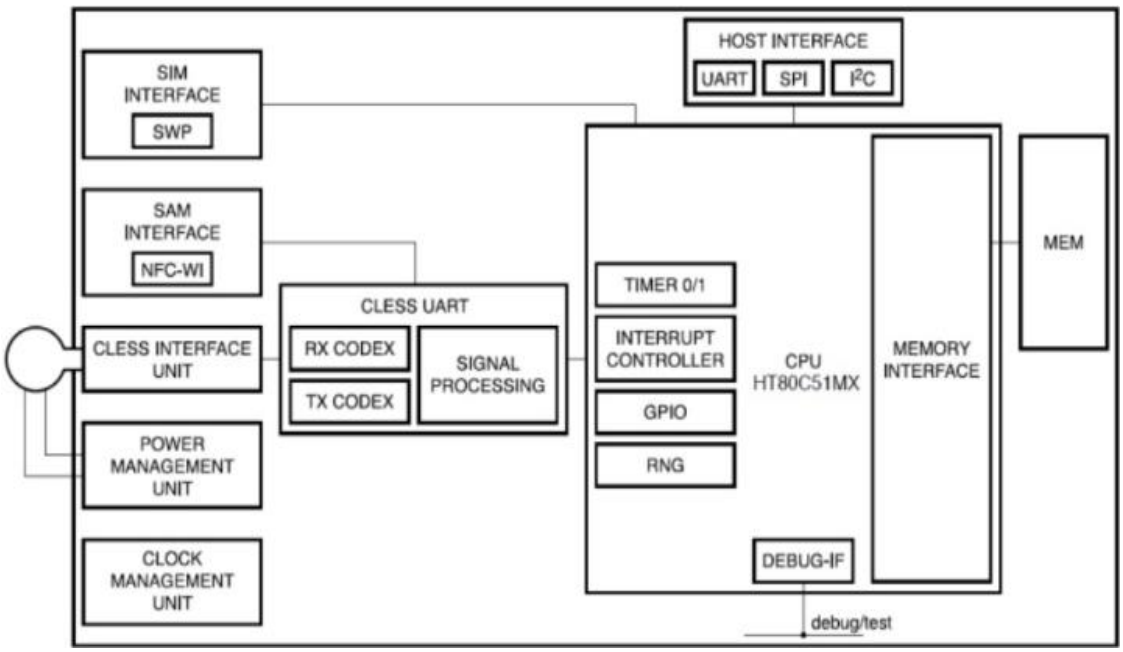


Рисунок 2.1 — NXP PN544. Приклад контролера NFC, вбудованого у сучасних смартфонах.

Протокол Single Wire Protocol (SWP) - протокол, що забезпечує з'єднання однопровідного зв'язку між інтерфейсом елементом безпеки на сім-карті (UICC SE) і NFC. Використовується лише один провід передачі даних, оскільки лише одне з восьми контактних шляхів на поверхні SIM-

карти, доступний передачі даних. На відміну від NFC-WI, протокол передачі даних (ISO / IEC 14443) обробляється мікропроцесором інтерфейсу NFC і лише дані програми направляються в елемент безпеки за допомогою SWP. Елемент безпеки на сім-карті може бути безпосередньо підключений до інтерфейсу NFC, навіть коли напруга подається не по телефону, а через інтерфейс NFC замість цього. Це дозволяє елементу безпеки спільно працювати з інтерфейсом NFC в режимі емуляції карти, навіть коли акумулятор телефону практично розряджений.

2.2 Елемент безпеки

Деякі програми, що використовують NFC, наприклад, програми для проведення платежу, або покупки електронних квитків вимагають, щоб дані, що зберігаються в пам'яті, були захищені, оскільки зловмисник потенційно може маніпулювати даними або читати їх з пам'яті. Дані, доступ до яких може отримати зловмисник, можуть бути дуже критичні – наприклад, відомості про банківську карту, отримавши доступ до яких, зловмисник може створювати клони карт.

Тому ці критичні програми повинні працювати в захищеному середовищі, бажано на окремому чіпі, а не в основному процесорі телефону. які забезпечують механізми захисту для підтримки безпечного середовища для зберігання та виконання.

ЕБ повинен мати операційну систему, в якій додатки встановлюються та використовуються (як правило, додатки встановлюються у вигляді JAVA-аплетів). Приклад таких ОС: MULTOS (Multi Application Card Operating System) або Java Card OS . Існує кілька варіантів апаратних модулів, які можуть служити як елемент безпеки в смартфонах (Рисунок 2.2)

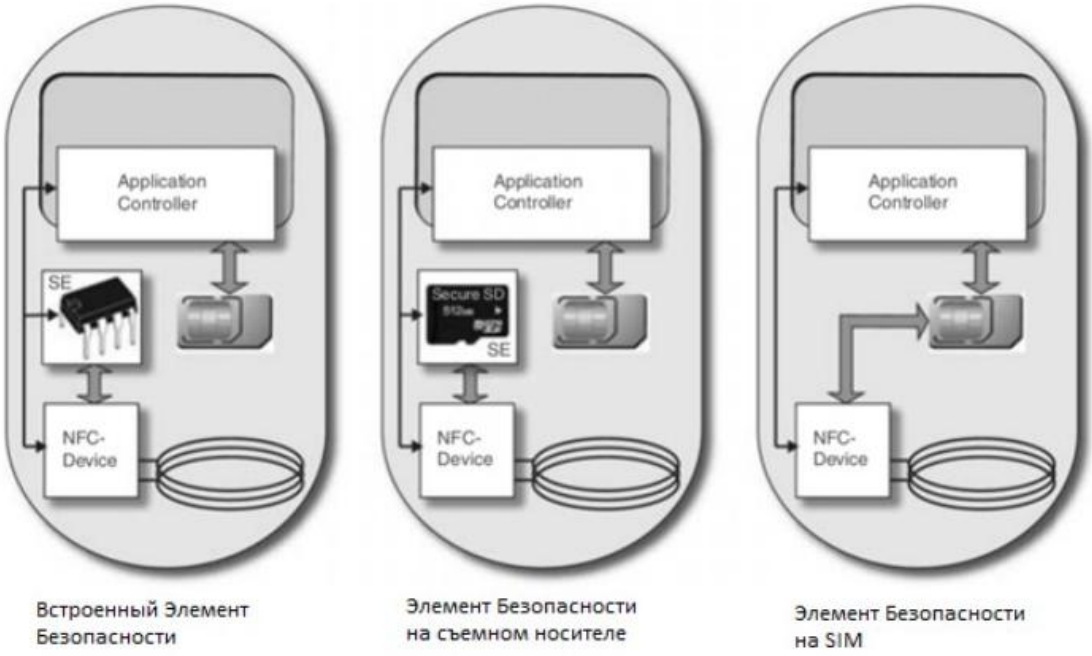


Рисунок 2.2 — Варіанти апаратних модулів, що використовуються як ЕБ.

Вбудований апаратний ЕБ може бути безпосередньо вбудований у телефон. Тому він не може бути видалений або переведений в інший пристрій. Це рішення має деякі недоліки: права доступу до вбудованого ЕБ повністю контролюються виробником телефону і якщо вони суворі, то ЕБ не може навіть дозволити встановити програми користувача.

UICC (Universal Integrated circuit card). ЕБ міститься на SIM/USIM-карті мобільного телефону і може обслуговувати декілька програм, випущених різними постачальниками програм.

Знімний носій (наприклад, SD-карта) складається з пам'яті, вбудованої смарт-елемента картки та смарт-картки контролера. Він забезпечує такий самий високий рівень безпеки, як смарт-карта і сумісний з більшістю основних стандартів для смарт-карт. Його переваги в тому, що він легко змінюється в діапазоні від телефону до телефону - на відміну від UICC, який пов'язаний з певним номером мобільного телефону.

Елемент безпеки містить операційну систему, яка дозволяє запускати кілька додатків у віртуальній машині поверхневої ОС

смартфона. Типова ОС використовується в ЕБ - JavaCardOS. Вона має фреймворк під назвою Java Card Runtime Environment (JCRE), який підтримує програми, реалізовані в обмеженій версії мови Java (підмножина конструкцій оригінальної мови Java і бібліотечних функцій).

Використання віртуальної машини дозволяє відокремити критично важливі дані від усіх інших. Однак і тут є свої підводні камені. Операційна система елемента безпеки може запускати обмежену кількість додатків і тримати в пам'яті обмежену кількість даних. Залишається питання, що буде з важливими даними, що містяться в пам'яті елемента безпеки, якщо необхідно зберегти нові дані, але місця в пам'яті для збереження не буде. Крім того, не виключена помилка розробника, який може не вказати, що його додаток повинен запускатися з використанням елемента безпеки. Сам же елемент безпеки, не може розпізнавати програми, які передають дані захисту.

2.3 Режими роботи NFC-контролера

Пристрій NFC може працювати в пасивному режимі та в активному режимі. Якщо пристрій генерує власне радіочастотне поле, то воно працює в активному режимі, і називається «Ініціатор». В іншому випадку пристрій працює в пасивному режимі, і називається "Таргет". Активні пристрої - як правило, мають джерело живлення (наприклад, смартфон), пасивні - джерела живлення не мають (наприклад, смарт-карти, nfc-теги).

Можливі два варіанти обміну даними між пристроями: коли обидва пристрої NFC активні, і коли один пристрій активний, другий пасивний.

Коли перший пристрій надсилає запит — він генерує радіочастоту, поки очікується відповідь другого пристрою, частота не генерується. Таким чином, коли два пристрої обмінюються даними, вони генерують

частоту по черзі. Приклад такого взаємодії: два смартфони, що обмінюються даними - фото, відео-ролики, посилання і т.п.

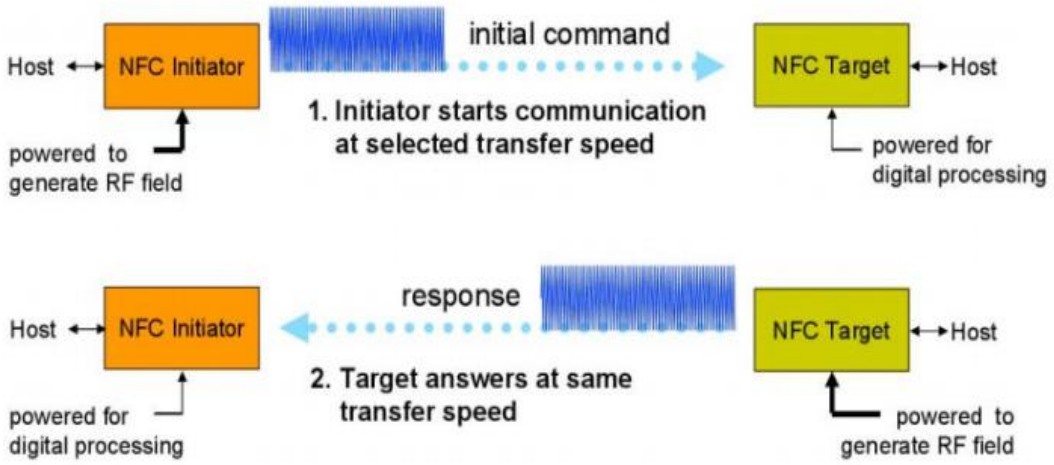


Рисунок 2.3 — Схема роботи пристроїв в активному режимі.

В активному режимі базовий радіочастотний сигнал (13,56 МГц) модулюється з даними відповідно до схеми кодування. Якщо активний пристрій передає дані зі швидкістю 106 кбіт/с, тоді використовується модифікований код Міллера зі 100% модуляцією. У всіх інших випадках використовується манчестерське кодування з коефіцієнтом модуляції 10%

Пасивний режим (Рисунок 2.4) взаємодії NFC-пристроїв відбувається тоді, коли електромагнітне поле генерує лише ініціатор сеансу зв'язку. Така взаємодія може відбуватися, коли активный пристрій (наприклад, смартфон) зчитує дані з пасивного пристрою (наприклад, NFC-тег).

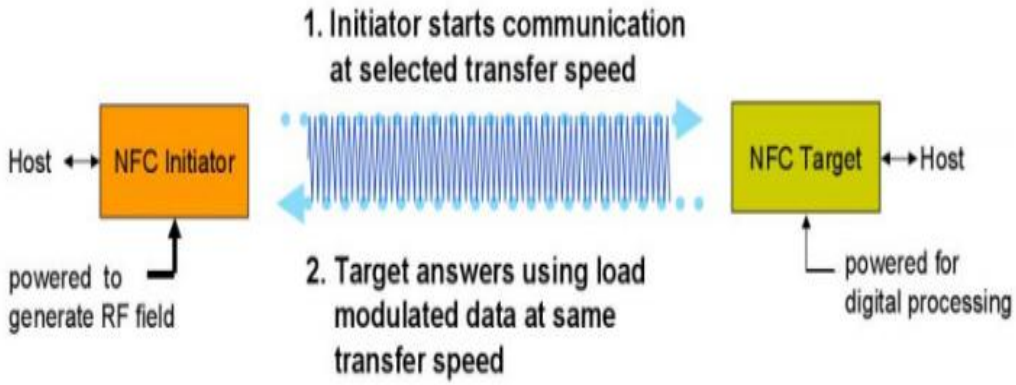


Рисунок 2.4 — Схема роботи пристроїв пасивному режимі.

Так як пристрої використовують радіочастотні хвилі, щоб обмінюватися повідомленнями та даними, з'являється можливість для прослуховування повідомлень за допомогою спрямованих антен, пошкодження даних, розриву сесії шляхом створення перешкод, модифікації даних.

У NFC визначено три основні режими роботи:

1.Пасивний (емуляція смарт-карти). Пасивний пристрій поводиться як безконтактна карта одного з існуючих стандартів.

2. Передача між рівноправними пристроями. Здійснюється обмін між двома пристроями. При цьому за рахунок власного джерела живлення у пристрою, що прослуховує, можна використовувати NFC навіть при вимкненому живленні опитувального пристрою.

3. Активний режим (читання чи запис).

У кожному режимі може застосовуватися один із трьох способів передачі: NFC-A (14443 A), NFC-B (14443), NFC-F (JIS X 6319-4). Для розпізнавання способу передачі пристрій, що ініціює, посилає запит. Характеристики режимів кодування та модуляції наведені у таблиці 2.1.

Таблиця 2.1 — Характеристики режимів NFC

Стандарт	Тип пристрою	Кодування	Модуляція	Швидкість передачі кб/с
NFC-A	Опитуючий пристрій	Модифікований код Міллера	ASK 100%	106
	Прослуховующий пристрій	Манчестерське кодування	Модуляція навантаження (ASK)	106
NFC-B	Опитуючий пристрій	NRZ-L	ASK 10%	106
	Прослуховующий пристрій	NTZ_L	Модуляція навантаження (BPSK)	106
NFC-F	Опитуючий	Манчестерське кодування	ASK 10%	212/424
	Прослухову-юще	Манчестерське кодування	Модуляція навантаження (ASK)	212/424

У пасивному режимі використовуються мітки NFC — пасивні пристрої, призначені для обміну активними NFC-пристроями. Як і мітки RFID, мітки NFC використовуються для зберігання невеликої кількості даних. Усього визначено 4 типи міток (див. табл. 2.2).

Таблиця 2.2 — Типи міток

Тип	1	2	3	4
Стандарт	14443A	14443 B	jis 6319-4	14443 A/B
Сумісні продукт	Innovision Topaz	NXP Mifare	Sony Felica	NXP DESFire, SmartMX-jCOP
Швидкість передачі кб/с	106	106	212,424	106,212,424
Обсяг пам’яті	96 б	48 б	до 1 Мб	До 32 кб

2.4 Режими роботи NFC-пристрою

Як було зазначено вище, NFC-контролер відповідає за комунікації. Він містить інтерфейси для різних режимів використання NFC-пристроїв: емуляція картки оплати, режим точка-точка, режим читання/запису.

NFC-пристрій може працювати у трьох режимах (Ринусок 2.5): емуляція NFC-карти, піринговий режим та режим читання/запису.

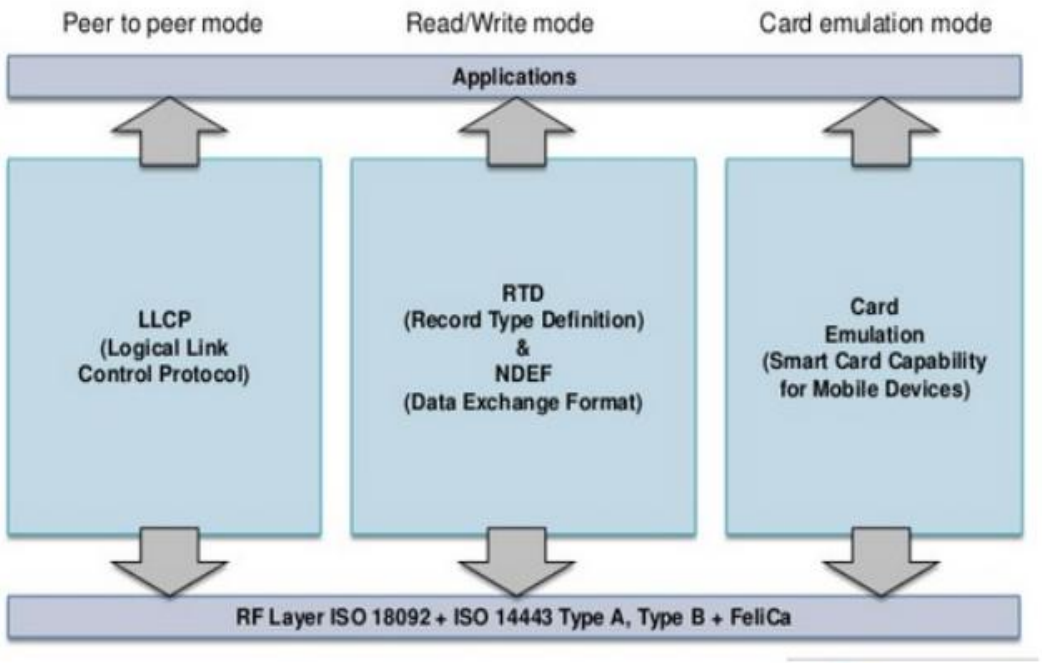


Рисунок 2.5 — Режими роботи NFC-контролера

Режим читання/запису: в режимі читання/запису, пристрій NFC працює як RFID-зчитувач і здатний читати пасивні мітки NFC, а також писати в них. До додатків, які використовують цей режим, належать передусім інформаційні додатки, що дозволяють одержувати дані з RF або NFC-міток і створених на їх основі смарт-постерів, завантажувати різні квитки, дисконтні ваучери і т. д. для подальшого пред'явлення. Цей режим також ефективний при реалізації транспортних додатків. Він може використовуватися й у додатках, що мають допоміжний характер стосовно інших NFC-додатків. Наприклад, при купівлі транспортного квитка за технологією NFC можна додатково завантажити схему проїзду або розклад роботи транспорту. Цей режим може стати основним для роботи транспортного NFC-додатка, якщо йдеться про завантаження в мобільний телефон транспортного квитка з подальшою оплатою на основі виставленого оператором рахунку.

Режим точка-точка (P2P): у режимі P2P, пристрій NFC має двонаправлене з'єднання з іншим NFC пристроєм для обміну даними. Цей

режим може бути використаний для обміну невеликою кількістю даних між телефонами (наприклад, URL), обмін контактними даними або WiFi-налаштуваннями. Слід зазначити, що універсальність стандартів NFC дозволяє обмінюватися даними в режимі точки не тільки між смартфонами, але і між іншими пристроями - NFC-зчитувачами, комп'ютерами, фотоапаратами, музичними центрами.

Режим емуляції карт: у цьому режимі, NFC-пристрій емулює безконтактні смарт-картки (ISO/IEC 14443 або FeliCa карти) і діє як пасивний пристрій. Емуляція прозора і для інших пристроїв, такий пристрій-емулятор виглядає як традиційна смарт-картка. Пристрій у такому режимі може бути використаний як проїзний у суспільному транспорті, як банківська карта, що використовується для оплати покупок. Пристрій в режимі емуляції картки також може бути використаний в ідентифікаційних програмах для організації доступу.

Тільки в одному з цих режимах, в режимі емуляції картки, задіяний елемент безпеки. В інших режимах немає аутентифікації, немає шифрування - дані передаються у відкритому вигляді, і можуть відразу зберігатися у файловій системі. Це дає простір для дій зловмисників. Вони можуть створювати некоректні NFC-повідомлення, що відключають телефон, що зчитує їх, передавати шкідливі посилання і файли, а також підміняти NFC-мітки на помилкові. Помилкові NFC-мітки навіть при використанні елемента безпеки в режимі емуляції карток можуть призвести до несанкціонованого списання коштів.

Для реалізації криптографічного захисту персональних даних підійде тільки режим точки. Так як режим емуляції карти і так уже захищений за допомогою Елементу безпеки. А в режимі читання/запису немає сенсу шифрувати загальнодоступні мітки. Проте, слід зазначити, що використання емуляції карт разом із ЕБ дуже обмежена для сторонніх розробників ПЗ. Поки що виробники ЕБ можуть створювати програми,

захищені за допомогою цього елемента. Для інших розробників така корисна можливість залишається закритою. Діаграма роботи технології NFC у смартфоні (Рисунок 2.6).

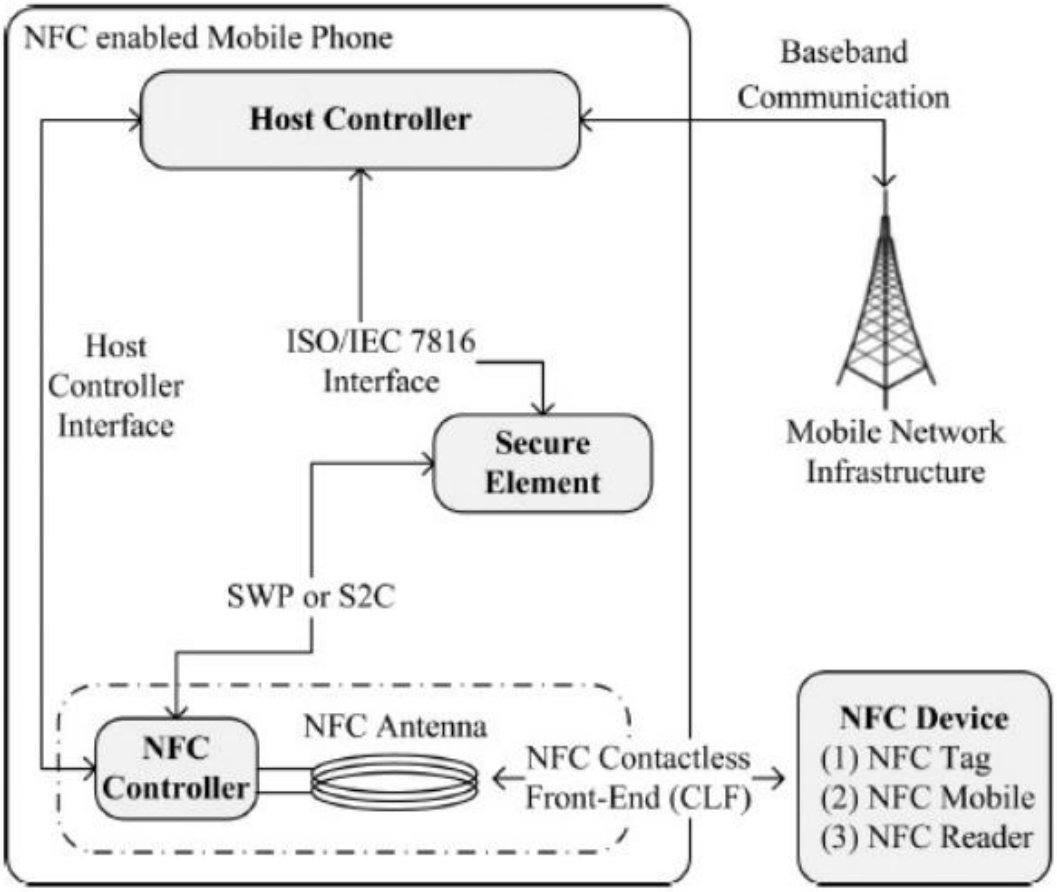


Рисунок 2.6 — Схема роботи технології NFC у смартфоні

Дана схема наочно показує взаємодію елементів телефону один з одним. У центрі схеми - контролер NFC, Host Controller -процесор самого телефону та антена.

NFC-контролер за допомогою антени взаємодіє з іншим NFC-пристроєм за низькорівневим протоколом NFC Contactless Front-End і передає дані хост-контролеру пристрою для їх подальшої обробки.

Якщо контролер працює в режимі емуляції карти, то при взаємодії з іншим NFC-пристроєм, NFC-контролер безпосередньо з'єднується з Елементом безпеки. Елемент безпеки обробляє дані, при цьому додаток

NFC використовує режим емуляції карти, запускається не на основному процесорі телефону, а на чипі елемента безпеки. І лише після цього деякі дані передаються основному процесору.

3 СТАНДАРТИ ТА ПРОТОКОЛИ NFC

Технологія NFC була схвалена як ISO/IEC стандарт 8 грудня 2003 року і пізніше як стандарт ECMA . NFC — технологія з відкритою платформою, стандартизована в ECMA-340 і ISO/IEC 18092. Ці стандарти визначають схеми модуляції, кодування, швидкості передачі і радіочастотну структуру інтерфейсу пристроїв NFC, а також схеми ініціалізації та умови, необхідні для контролю за конфліктними ситуаціями. для пасивних та для активних режимів NFC. Крім того, вони також визначають протокол передачі, включаючи протокол активації і спосіб обміну даними. NFC об'єднує безліч раніше існуючих стандартів, включаючи ISO 14443, ISO 15693.

Особливо в "режимі емуляції карти" пристрій NFC повинен, принаймні, передати унікальний ідентифікаційний номер існуючому раніше зчитувачу. Крім основних стандартів, існують також стандарти, створені організацією NFC Forum. NFC Forum є некомерційною асоціацією, заснованою 18 березня 2004 року компаніями NXP Semiconductors, Sony і Nokia, щоб просунути використання NFC в побутовій електроніці, мобільних пристроях та персональних комп'ютерах . NFC Forum сприяє реалізації та стандартизації технології NFC, щоб гарантувати здатність до взаємодії між пристроями та послугами. Стандарти NFC Forum не є обов'язковими, але вони сприяють створенню універсального способу зв'язку NFC-пристроями різного типу - смартфонами, комп'ютерами, NFC-зчитувачами та побутовими електричними приладами.

3.1 Основні стандарти

Наведемо перелік основних стандартів NFC:

1. ISO/IEC 18902 або ECMA-340 (NFCIP-1). Стандарти описують фізичний рівень і зв'язок між двома пристроями NFC.

2. ISO / IEC 21481 або ECMA 352 (NFCIP-2). Стандарт визначає механізм вибору режиму зв'язку між пристроями, які працюють на частоті 13,56 МГц.

3. ISO / IEC 14443 (Proximity-Coupling Smart Cards). Стандарт описує безконтактні смарт-карти, методи роботи та протоколи передачі даних для зв'язку між картою та пристроєм зчитування. Такі смарт-карти працюють на відстані до 7-15 см.

4. ISO/IEC 15693 (Vicinity-Coupling Smart Cards). Стандарт описує спосіб функціонування та експлуатації Vicinity-Coupling смарт-карт. Основна відмінність від безконтактних карт є те, що дані скарти можуть бути зчитані з більшої відстані (до 1-1,5 метрів).

3.2 Стандарт ISO/IEC 14443

ISO/IEC 14443 - основний стандарт визначає методи роботи безконтактних смарт-карт. Він включає наступні 4 частини:

1. Фізичні характеристики;
2. Радіочастотна потужність і сигнальний інтерфейс;
3. Ініціалізація та запобігання колізій;
4. Протокол передачі.

ISO/IEC 14443 може бути прийнятий як еквівалент протоколу ISO/IEC 7816, який стандартизує методи роботи для контактних смарт-карт. Взаємини обох протоколів та їх відображення на рівні моделі OSI можна побачити на рисунку 3.1

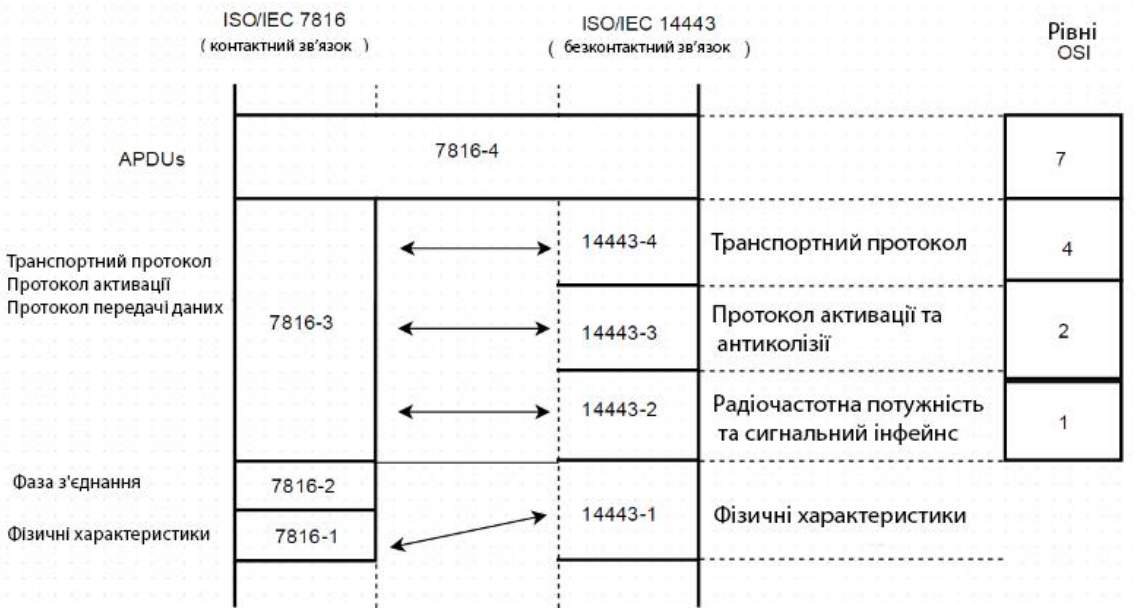


Рисунок 3.1 — Схема взаємовідносин стандартів ISO/IEC 14443 та ISO/IEC 7816

3.3 Інтерфейс та протокол зв’язку ближнього поля

NFCIP-1 стандарт частково заснований на стандарті ISO/IEC 14443. Він визначає два режими зв'язку, активний і пасивний режим. На відміну від пасивного режиму, активний режим підтримує зв'язок двох пристроїв, які мають власне джерело живлення.

Стандарт визначає схеми модуляції, кодування, швидкість передачі та формат кадру RF-інтерфейсу, а також схеми ініціалізації та умови, необхідні для контролю колізій даних під час ініціалізації.

Крім того, він визначає транспортний протокол, званий протоколом обміну даними (DEP - Data Exchange Protocol). DEP є напівдуплексним протоколом, що підтримує передачу блочно-орієнтованих даних з обробкою помилок. Для даних, що не вписуються в одному кадрі, визначено механізм передачі по ланцюжку. Режим точка-точка NFC може використовувати NFCIP-1 як базовий протокол. Протокол передачі, радіо

інтерфейс та методи антиколізій задаються аналогічно тим, які визначені в стандарті ISO/IEC 14443.

3.4 Механізм вибору між режимами зв’язку

NFCIP-2 визначає механізм вибору між різними режимами зв'язку, що реалізують ISO/IEC 14443, ISO/IEC 15693, NFCIP-1 . Кожен NFC-сумісний пристрій, що реалізує NFCIP-2, вибирає (на початку кожного повідомлення) між заданими режимами:

1. PCD - пристрій працює як зчитувач ISO / IEC 14443 сумісних карт;
2. PICC - пристрій емулює безконтактну смарт-карту, в так званому режимі емуляції карт;
3. NFC – у цьому режимі пристрій працює відповідно до NFCIP-1 специфікації, і може працювати як в активному так і пасивному режимі.

3.5 Високорівневі NFC стандарти

Високорівневі стандарти не є офіційною назвою, але вона характеризує групу норм, виданих організацією NFC Forum, в основі яких лежать стандарти ISO/IEC . NFC Forum - міжнародна організація метою якої є розвиток технології NFC. Деякі з цих стандартів підводять різні технології під один загальний стандарт (наприклад, Цифровий протокол (Digital Protocol)), інші забезпечують розширену функціональність та нові методи роботи для NFC-пристроїв:

1. Стандарт NDEF (NFC Data Exchange Format) визначає формат даних між NFC-сумісними пристроями і мітками;
2. Стандарт RTD (Record Type Definition) визначає типи записів для різних цілей у повідомленнях NDEF;

3. Протокол Connection Handover визначає, як використовувати NFC для встановлення з'єднання з використанням інших технологій бездротового зв'язку (наприклад, Bluetooth, Wi-Fi);

4. Logical Link Control Protocol (LLCP) - протокол для підтримки P2P зв'язку між двома пристроями, що використовуються на вершині NFCIP-1;

5. Digital Protocol - цифровий протокол для NFC-пристроїв зв'язку, забезпечує специфікації з реалізації на вершині стандартів ISO/IEC 18092 та ISO/IEC 14443;

6. NFC Activity Technical Specification — пояснює, як настроїти протокол зв'язку з іншим пристроєм NFC або NFC мітками;

7. Simple NDEF Exchange Protocol (SNEP) - простий протокол обміну NDEF-повідомленнями, використовується у верхній частині LLCP, дозволяє проводити обмін повідомленнями NDEF.

3.6 Стандарт ISO/IEC 7816-4

Відповідно до стандарту, ISO/IEC 7816-4 визначає організацію, безпеку та команди для обміну між зчитувачем і карткою. Це включає:

1. Зміст пар команда-відповідь обміну між інтерфейсами карт. Кожна пара складається з двох блоків даних прикладного протоколу (скорочено APDU - Application Protocol Data Units);

2. Структура файлів та даних на карті пам'яті;

3. Структура і змістом так званих історичних байтів, що описують експлуатаційні характеристики карти - байтикоманди Answer To Reset (ATR), відправлені за допомогою карти. Ця команда є спеціальною командою, відправленою картою після її електричного перезапуску за допомогою зчитувача;

4. Методи доступу до файлів та даних в архітектурі карти та безпеки, що визначають права доступу до файлів

5. Методи безпечного обміну повідомленнями.

Блоки даних прикладного протоколу (Application Protocol Data Unit-APDUs) використовуються для обміну даними між смарт-картою читачем на прикладному рівні. APDUs завжди утворюють пари повідомлень команда та відповідь. По-перше, команда APDU (позначається як CAPDU) відправляється від зчитувача на карту, яка відповідає, посилаючи відповідь APDU (позначений як R-APDU). Формат даних призначений, щоб бути незалежним від основного протоколу передачі.

C-APDU складається з заголовка і тіла. Заголовок має фіксовану довжину, тіло має змінну довжину і може бути відсутнім у деяких випадках. Заголовок складається з прапорів CLA, INS, P1, P2, інше тіло. Структура блоку команди прикладного протоколу представлена в таблиці 3 .

Таблиця 3.1 — Структура блоку команди прикладного протоколу

Поле	CLA	INS	P1	P2	LC	Data	Le
Довжина	1	1	1	1	0,1 або 3	змінна	0-3

Опис структури блоку:

1. CLA - байт класу інструкція;

2. INS - байт номера інструкції;

3. P1, P2 - Додаткові параметри;

4. Lc-довжина даних команди;

5. Le-довжина очікуваної відповіді.

Довжина полів Lc і Le залежить від можливості карти до спілкування, ця можливість називається «розширений APDUs». Про можливості карти йдеться в історичних байтах або ATR картки. Якщо

карта підтримує розширений APDU, то Lc дорівнює 3 байтам і поле даних команди має довжину до 65535 байт. Le у разі розширеного APDU, також як і Lc має максимальну довжину 3 байти і довжина поля даних для відповіді становить до 65535 байт. У випадку звичайного APDU, як Lc так і Le мають максимальну довжину 1 байт і довжина поля даних команд і поле даних відповіді очікується до 255 і 256 байт відповідно.

Структура блоку відповіді прикладного протоколу представлена у таблиці

Таблиця 3.2 — Структура блоку відповіді прикладного протоколу

Поле	Дані	SW1	SW2
Довжина	Змінна	1	1

Тіло (опціонально) складається лише з області даних. Заголовок складається з двох прапорів-статусів: SW1 та SW2. Вони кодують стан обробки команди. Наприклад, код стану '90' означає, що команда була виконана повністю та успішно. Інші коди стану знаходяться у описі стандарту .

4 ВИКОРИСТАННЯ ТЕХНОЛОГІЇ NFC

4.1 Читання та запис міток

Android Beam використовує можливість передачі та обробки коротких інформаційних повідомлень. Однак насправді їх можна не лише передавати з телефону, а й зчитувати з пасивних міток. У певному сенсі ця технологія аналогічна відомим QR-кодам, які зчитують фотокамеру телефону. При цьому корисна інформація (наприклад, посилання на сторінку сайту) займає кілька десятків байт. Мітки можуть використовуватись компаніями, наприклад, для просування своїх товарів чи послуг. Враховуючи компактний розмір пасивної мітки, вона може бути розміщена практично в будь-якому місці: на коробці з товаром, в журналі, на інформаційній стійці та інших місцях.

Рисунок 4.1 — приклад пасивної мітки NFC

WifiTap WiFi NFC: дозволяє записати мітку для підключення до бездротової мережі. Фактично вона є текстовим посиланням (URI) виду wifi://ssid/wpa/key. Її можна використовувати для швидкого підключення гостей до домашньої точки доступу без введення складних і довгих паролів на клавіатурі телефону. Людині достатньо лише зчитати мітку, і в його телефон буде записано нову точку доступу.

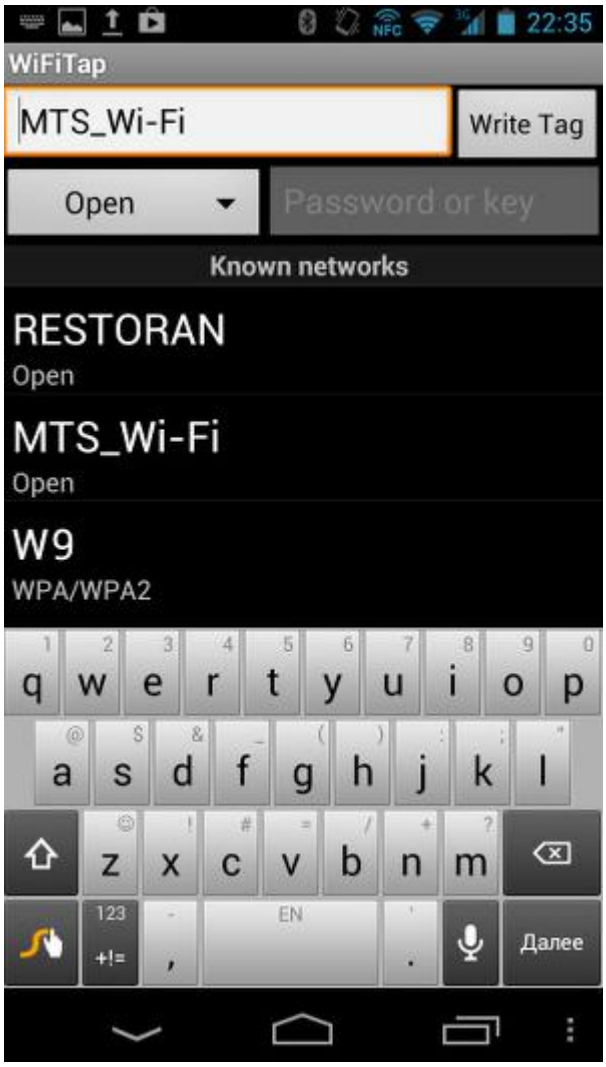


Рисунок 4.2 — приклад роботи WiFiTap

App launcher NFC tag maker: запис міток додатків в один дотик. Можна вибрати одну з встановлених програм і зробити мітку з

посиланням на нього. При читанні мітки відкриється програма (якщо вона встановлена) або її сторінка в Play Store.

Smart Tag Maker: записування міток для Sony Xperia Smart Tags.

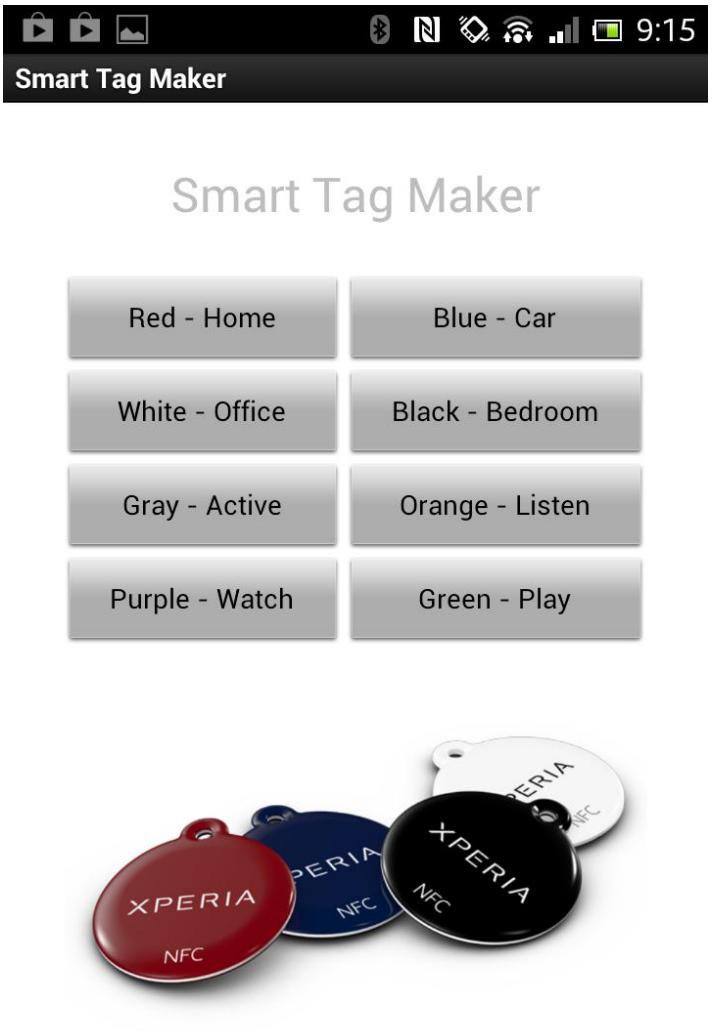


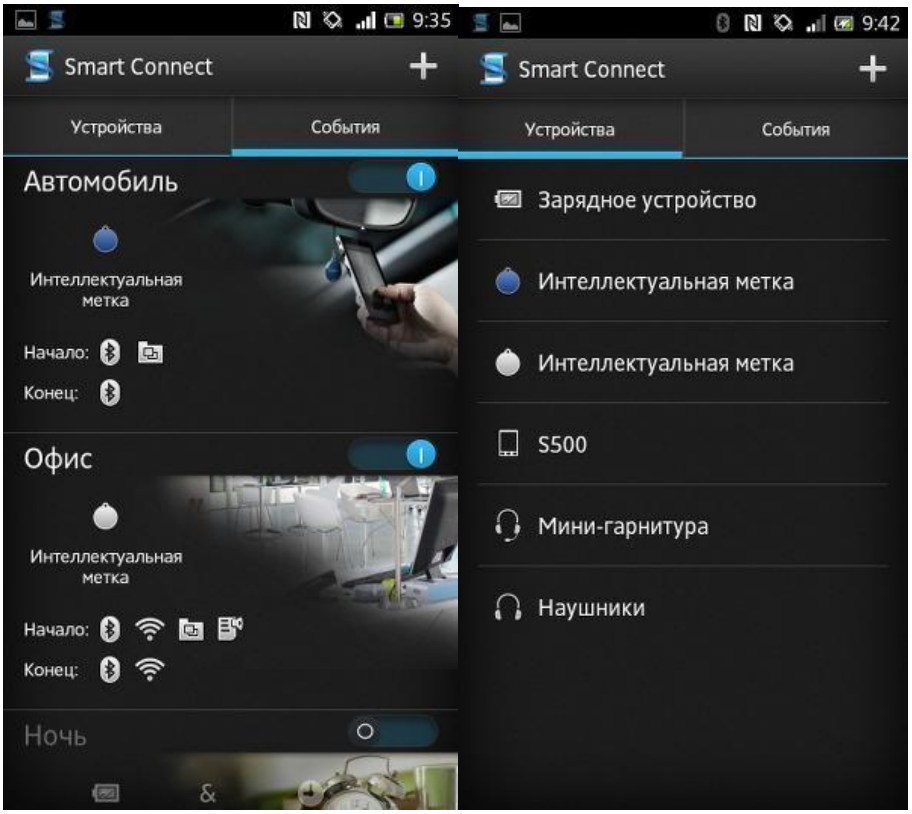
Рисунок 4.3 — Smart Tag Maker

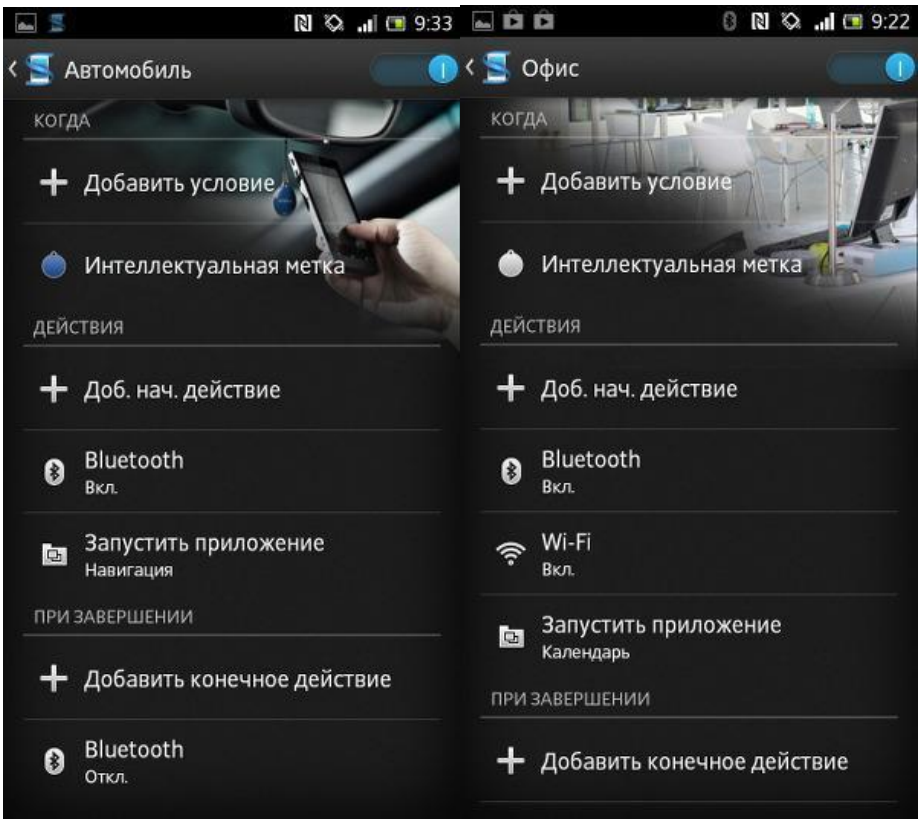
4.2 Smart Connect

Sony є одним із активніших учасників процесу впровадження NFC. В її продуктах вже предустановленна програма Smart Connect, яка підтримує роботу з оригінальними мітками Sony. Для створення своїх міток можно використовувати утиліти Smart Tag Maker . NDEF URI це формат, який використовується для роботи системи з кодуванням номера / кольору мітки в текстовому посиланню. Всього система передбачає до восьми міток, які позначені як: «будинок», «машина», «офіс»,, «спальня», «слухати»,, «активності», «перегляд», «грати».

Рисунок 4.4 – Один із варіантів оригінальних міток Sony Smart Tags

Програма Smart Connect працює й з іншими пристроями, а не тільки з NFC пристроями, які підключаються до телефону , включаючи гарнітури, пристрої Bluetooth, блок живлення. При цьому користувач може перепрограмувати всі схеми; в кожній з них вказується набір з умови і дій.


9:35
Smart Connect
Устройства
События
Автомобиль
Интеллектуальная метка
Начало:
Конец:
Офис
Интеллектуальная метка
Начало:
Конец:
Ночь
9:42
Smart Connect
Устройства
События
Зарядное устройство
Интеллектуальная метка
Интеллектуальная метка
S500
Мини-гарнитура
Наушники


9:33
Автомобиль
КОГДА
Добавить условие
Интеллектуальная метка
ДЕЙСТВИЯ
Доб. нач. действие
Bluetooth
Вкл.
Запустить приложение
Навигация
ПРИ ЗАВЕРШЕНИИ
Добавить конечное действие
Bluetooth
Откл.
9:22
Офис
КОГДА
Добавить условие
Интеллектуальная метка
ДЕЙСТВИЯ
Доб. нач. действие
Bluetooth
Вкл.
Wi-Fi
Вкл.
Запустить приложение
Календарь
ПРИ ЗАВЕРШЕНИИ
Добавить конечное действие

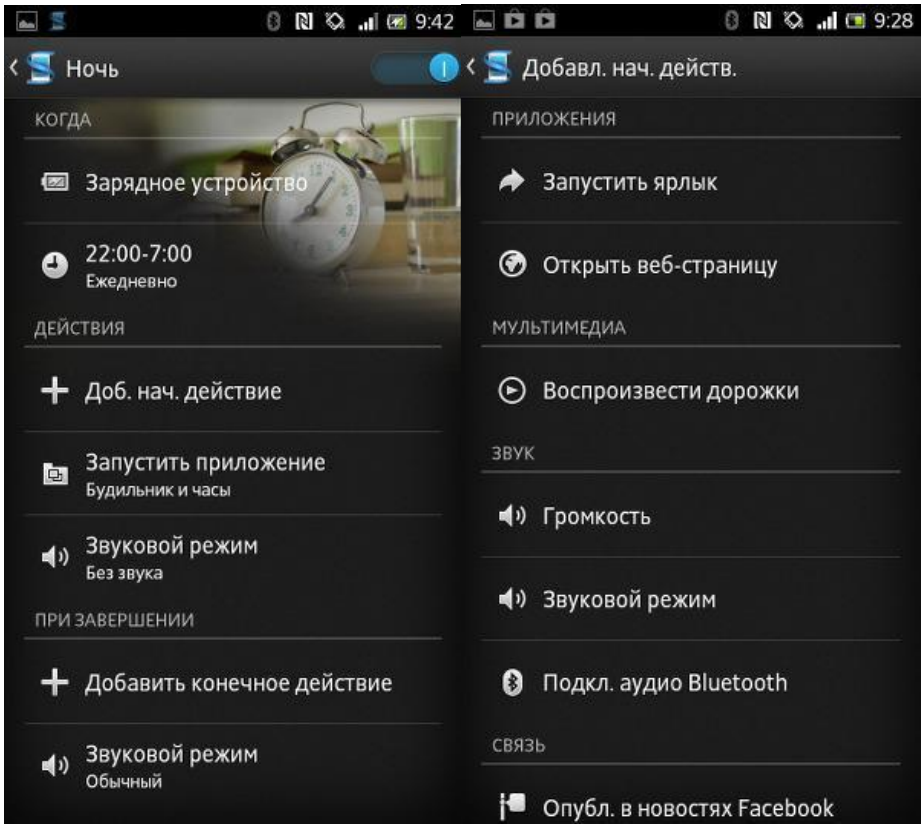


Рисунок 4.5 – Робота з мітками в програмі Sony Smart Connect

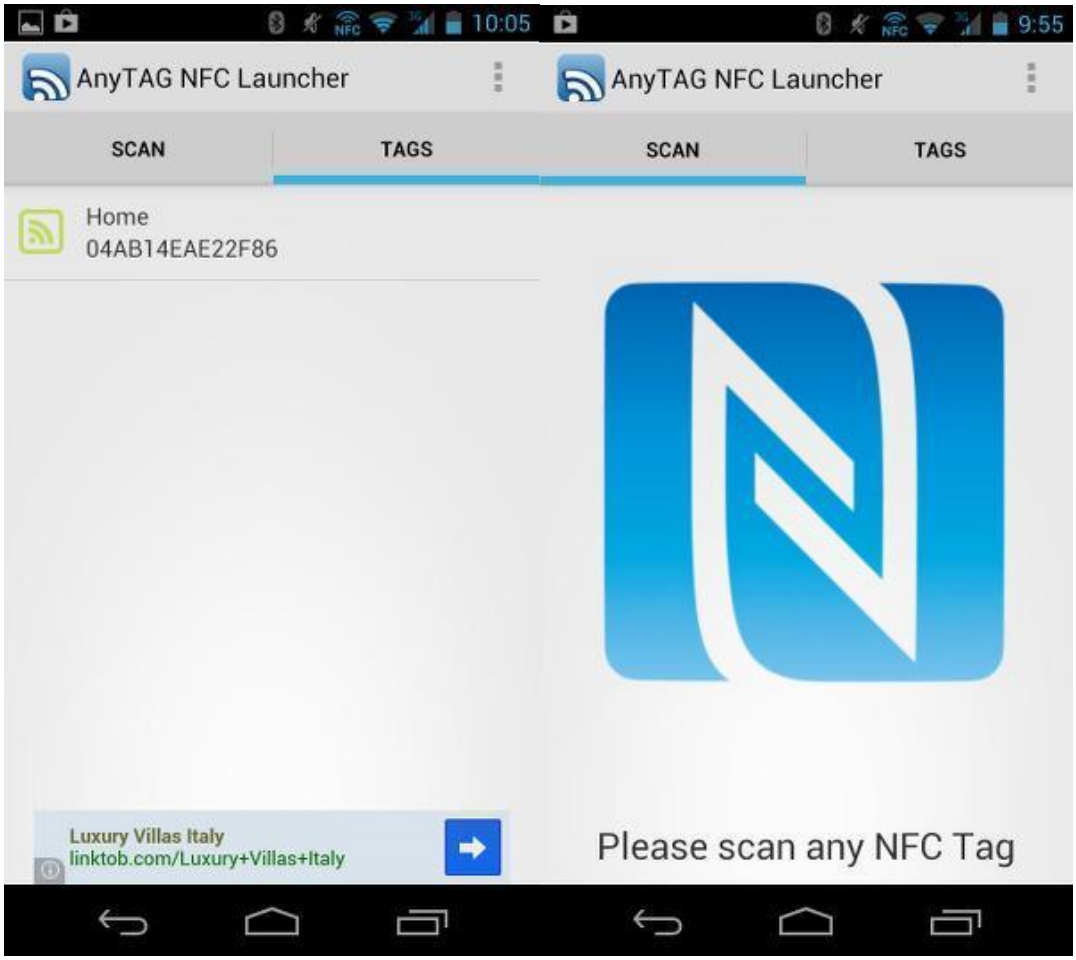
Як умову можна використовувати впізнання мітки або підключення пристрою, додатково можна обмежити час роботи схеми. Набір дій в програмі має обширний спектр, до нього входять: запуск деяких програми, відкриття посилання в браузері, дзвінок, запуск музики, регулювання режиму і гучності, підключення аудіо пристрою Bluetooth, відправка SMS, управління бездротовими інтерфейсами, регулювання яскравості на телефоні і інші дії. Їх також можна призначити і на вихід з даного режиму, який здійснюється за повторним розпізнаванням мітки.

Крім фірмових міток Sony - можна застосовувути і готові мітки, що не допускає зміни та перезапису інформації. Наприклад, це можуть бути різні використані або не використані транспортні карти. Справа в тому, що кожна з них має власний унікальний ідентифікатор, який можна прив'язати до певних дій спеціальними програмами. В якості можливої реакції

можуть виступати такі операції: включення / вимикання інтерфейсів, зміна профілю і безліч інших.

4.3 Програми для роботи с NFC мітками

AnyTAG NFC Launcher ця програма працює з усіма мітками, управління бездротовими інтерфейсами, музичним плеєром та фотокамерою, запуск додатків, регулювання гучності і параметрів екрану.



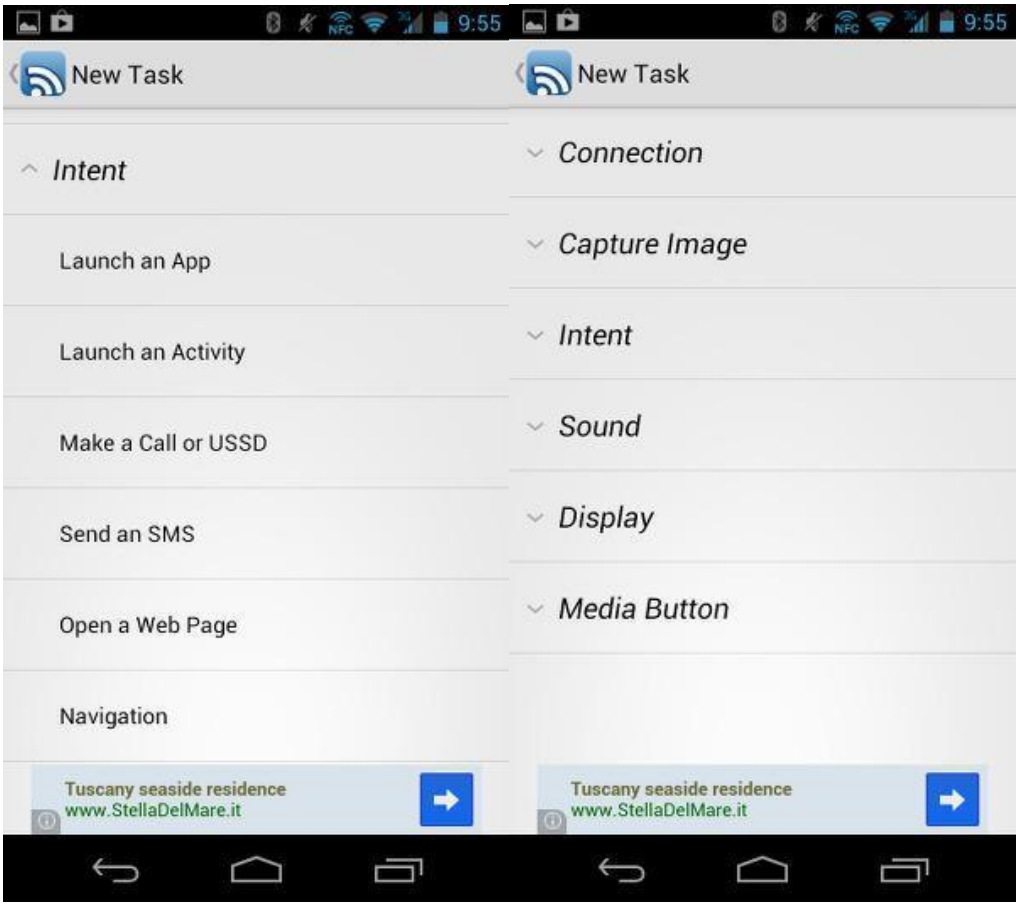


Рисунок 4.6 – AnyTAG NFC Launcher під час роботи

NFC ReTAG Free ця програма працює з будь-якими мітками, звуком і екраном, управління інтерфейсами, запуск програм, події календаря та установка будильника.

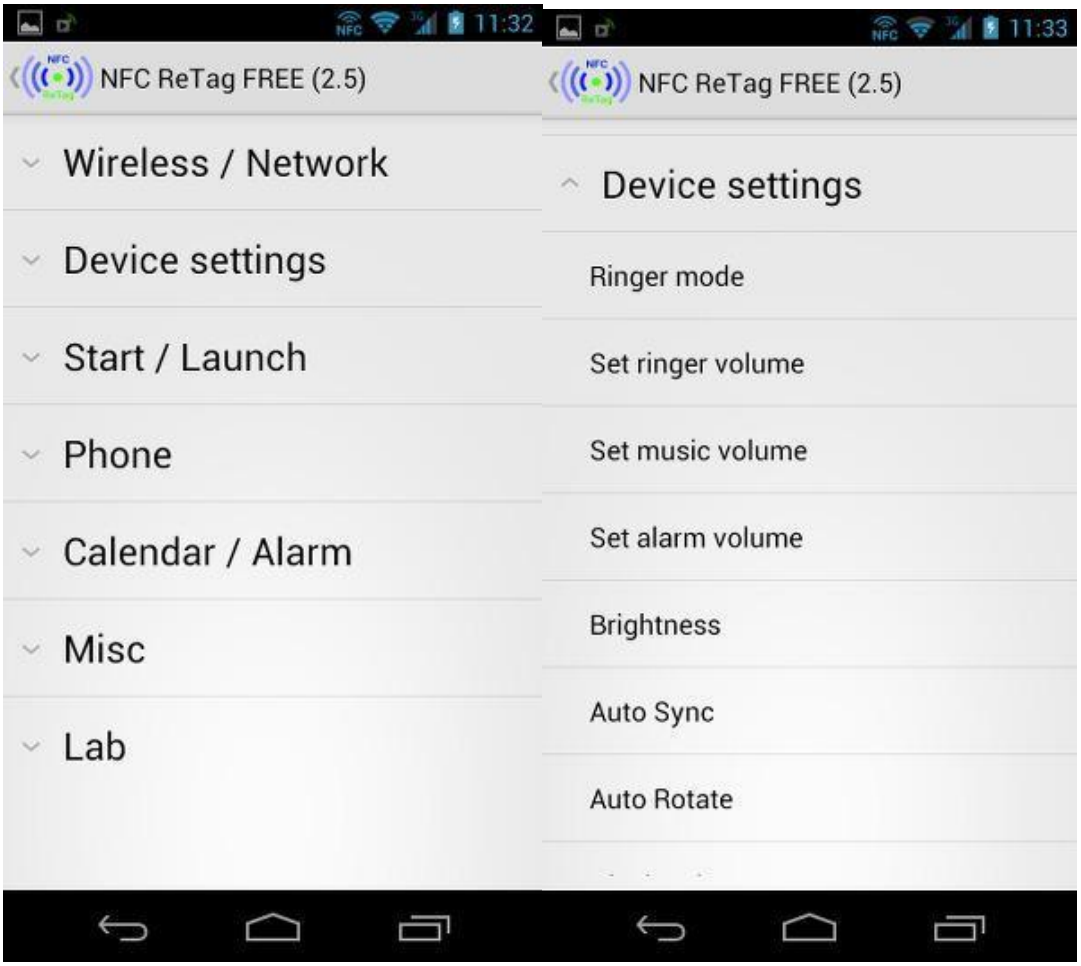


Рисунок 4.7 – Приклад роботи NFC ReTAG Free

NFC Task Launcher може крім міток NFC активувати настройки по підключенню до Bluetooth або Wi-Fi, серед дій є: гучності і налаштувань екрану, перемикання режимів, інтерфейсів, запуск додатків, публікації в соціальних мережах, відправка e-mail і SMS, настройка будильника, відкриття сторінок в браузері, управління медіаплеєром, телефонний дзвінок.

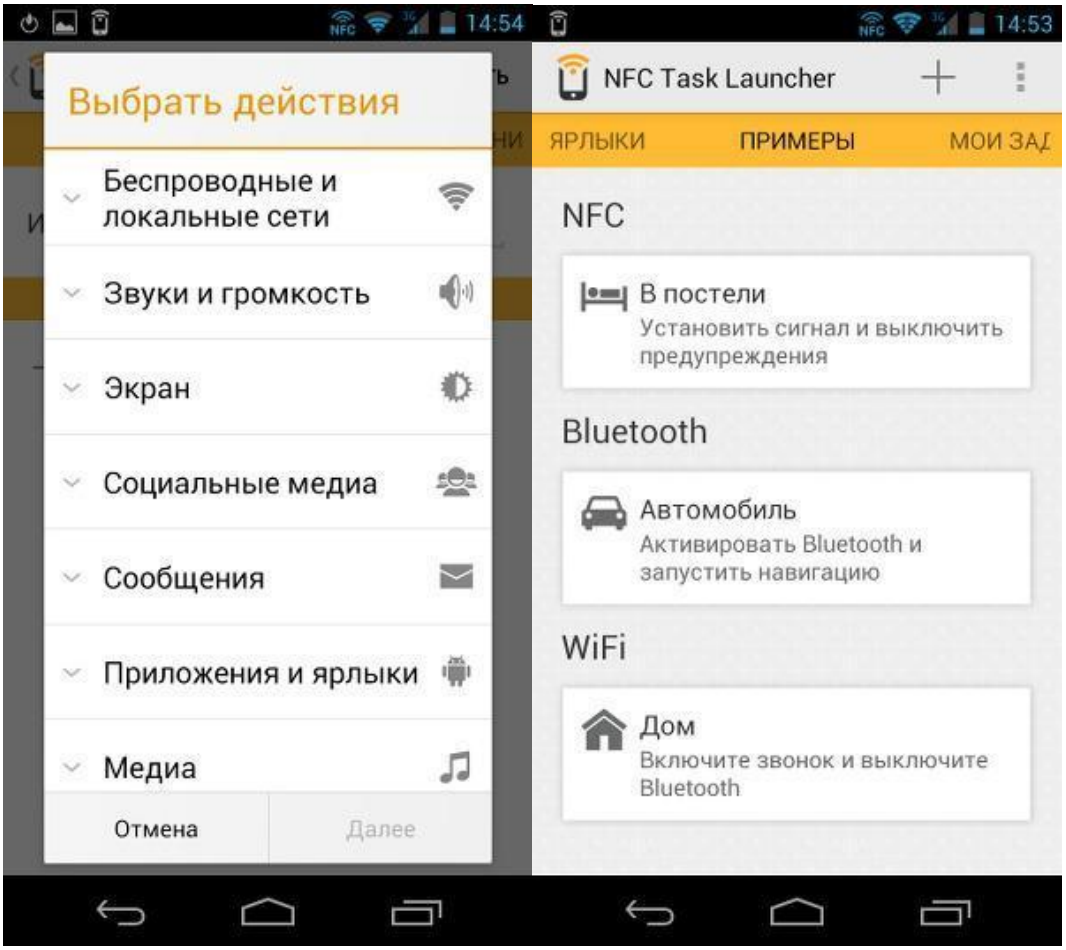


Рисунок 4.8 – Приклад роботи NFC Task Launcher

Не варто встановлювати відразу декілька програм які працюють з NFC мітками. Зручності від такого не додасться, оскільки при виявленні мітки на екрані телефону буде виникати діалогове вікно з вибором програми для її обробки. При цьому набір можливих дій в одній програмі, майже, не відрізняється набором дій в іншій.

4.4 Обмін інформацією між пристроями

Якщо ж говорити про прямий зв'язок апаратів між собою, то основне питання тут сумісність. Звісно, у разі продуктів одного виробника, особливо великого, той має можливість просто встановити у прошивку відповідну програму. Але якщо апарати випущені різними виробниками,

доведеться всім використовувати однакові утиліти. І зовсім не факт, що у вашого партнера буде встановлена така ж програма, як у вас.

Враховуючи, що власна швидкість NFC дуже мала, для швидкої передачі файлів зазвичай використовується Bluetooth або Wi-Fi, а NFC працює лише на етапі узгодження параметрів підключення та встановлення зв'язку.

Send! File Transfer (NFC) у безкоштовній версії дозволяє обмінюватися файлами фотографій, музики та відео. Для встановлення зв'язку можна використовувати NFC або QR-коди. Передача здійснюється через Bluetooth або Wi-Fi (у випадку, якщо обидва пристрої мають підтримку Wi-Fi Direct). У результаті тестування програма видає швидкість на рівні 65 КБ/с, що, звісно, замало навіть для фотографій.

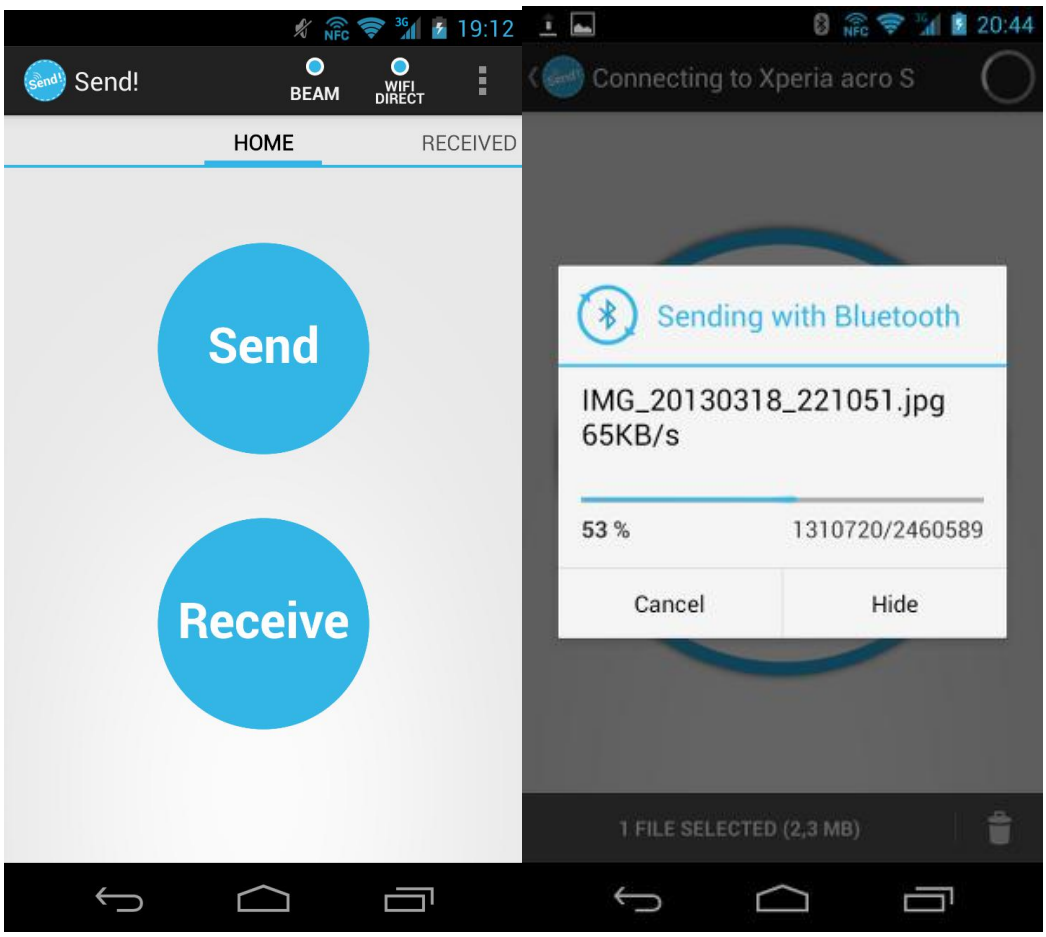


Рисунок 4.9 – Приклад роботи програми Send!

Blue NFC, як відомо з назви, також спрощує обмін файлами по Bluetooth, замінюючи етапи включення, пошуку та сполучення на дотик з обміном інформацією NFC. Швидкість роботи не дуже велика — на рівні згаданої вище програми.

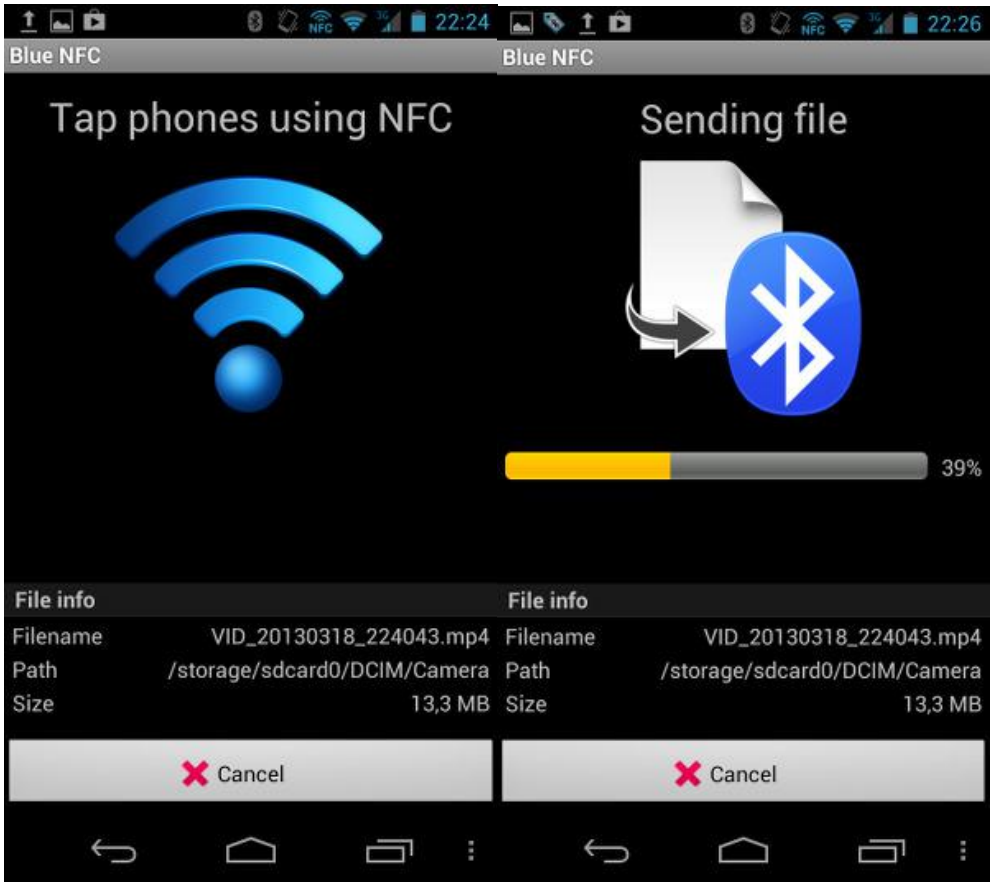


Рисунок 4.10 – Приклад роботи програми Blue NFC

File Expert HD також використовує Bluetooth, але швидкість становить 100-200 КБ/с. Правда, задля справедливості варто зауважити, що в цій програмі є і багато інших режимів обміну файлами.

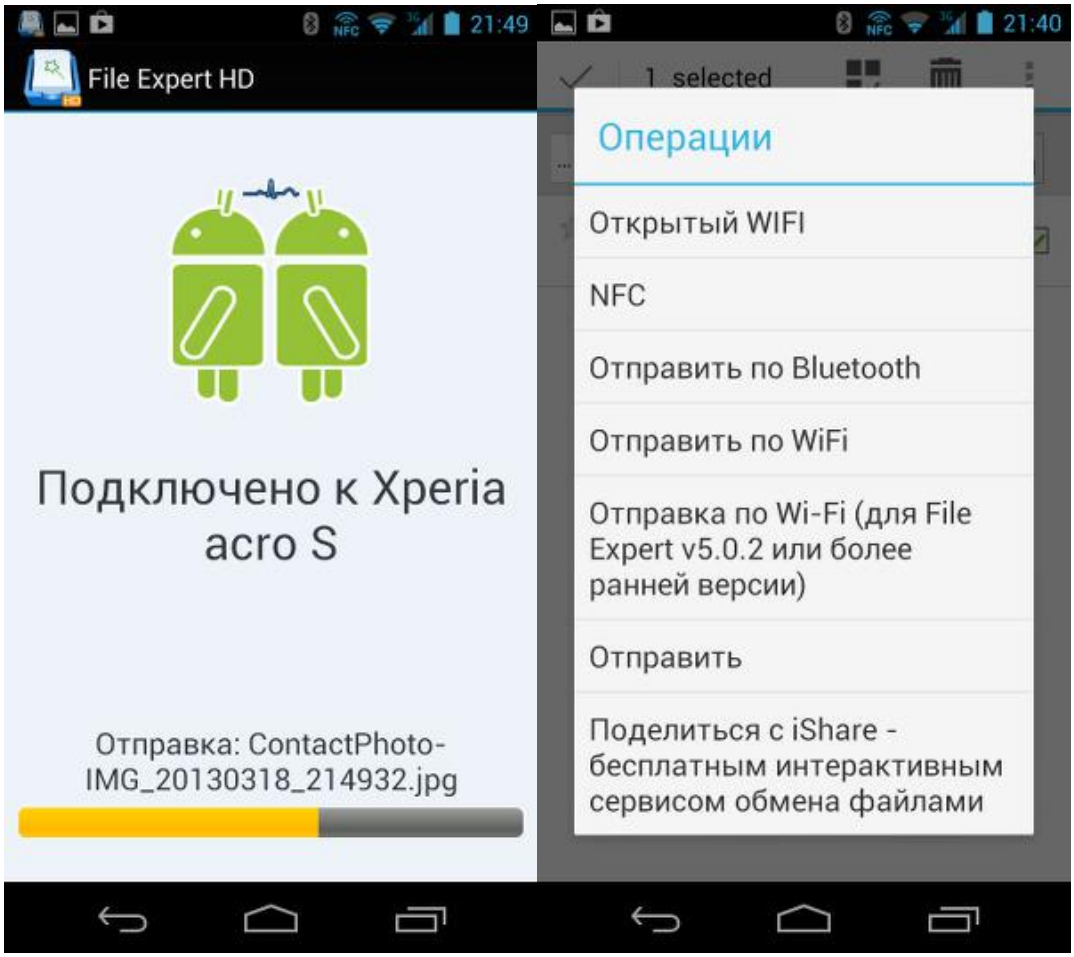


Рисунок 4.11 – File Expert HD

Більш високу швидкість показує утиліта SuperBeam WiFi Direct Share. Вона менш універсальна, ніж File Expert HD, проте здатна забезпечити з'єднання Wi-Fi, навіть якщо у пристроїв немає підтримки Wi-Fi Direct. А швидкість передачі становить близько 2 МБ/с, що дуже непогано. Таким чином, навіть відеоролики в кілька десятків мегабайт можна буде перенести за розумний час. Як і раніше, NFC використовується тут лише для початкового налаштування з'єднання пристроїв. Підтримується передача будь-якого типу файлів. Утиліта вбудовується у стандартне меню програм «Поділитись».

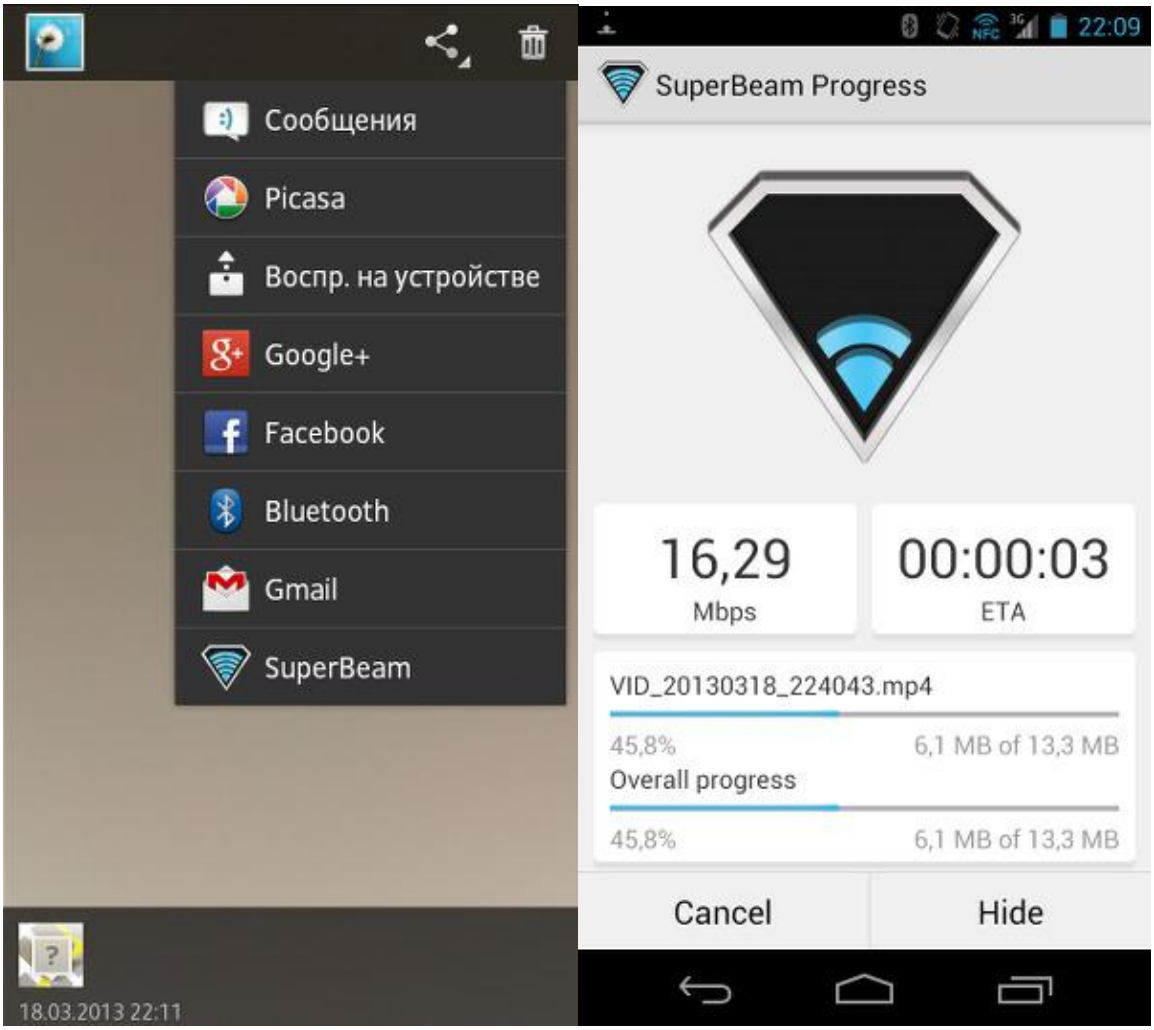


Рисунок 3.12 – SuperBeam

4.5 IoT

IoT чи Internet of things чи інтернет речи, це окрема глобальна тенденція. Це не просто праска з вайфаєм або чайник з блютузом, це не окрема технологія чи алгоритм, це міське середовище чи розумний будинок, це безліч технологій, алгоритмів та протоколів, які роблять життя людини кращим, екологічним та безпечним.

Рисунок 3.13 – NFC у світі IoT

Більшість таких розумних інфраструктур для дома цілком «юзерфрендлі», не потрібно купувати спеціальні виробничі контроллери, програмувати їх, писати код або робити що-то ще подібне.

У системах IoT використовуються різні прилади та датчики, які мають різні інтерфейси та різні механізми підключення. Наприклад, bluetooth вимагає підключення двох пристроїв, для підключення пристрою через Wi-Fi до мережі ethernet потрібно ввести пароль або вхідні дані мережі. А деякі датчики взагалі не мають інтерфейсу. Протокол NFC був розроблений, як протокол tap-and-go (нажми та працюй), що обіцяє легкість підключення пристроїв між собою.

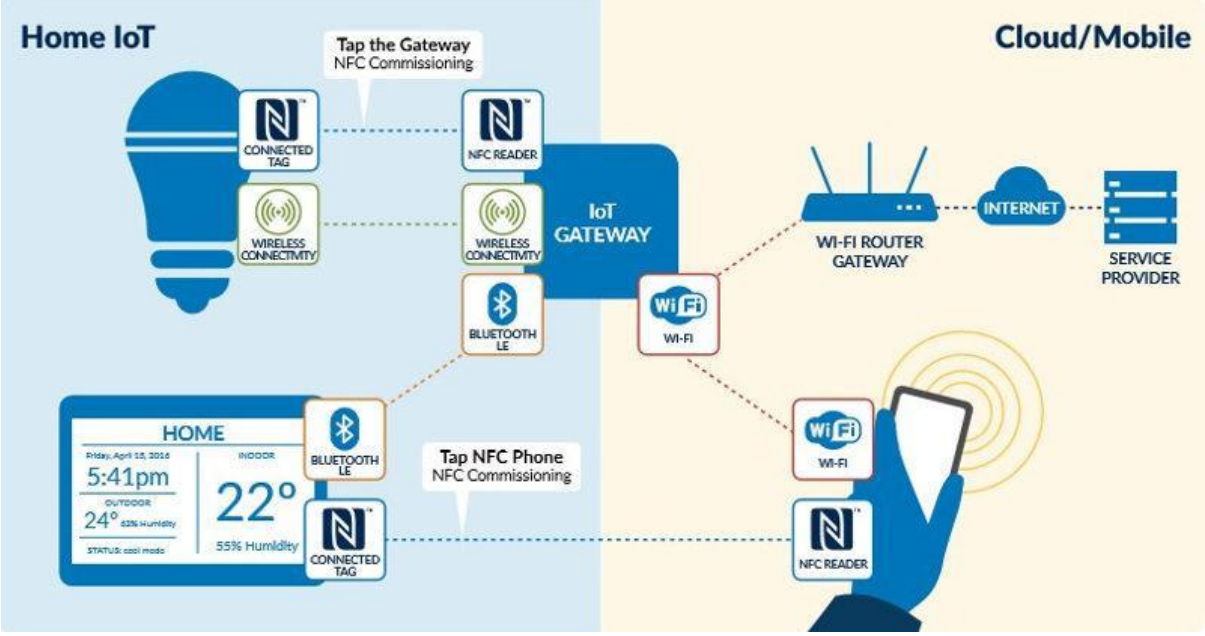


Рисунок 3.14 – Підключення пристроїв IoT.

Інтеграція інтерфейсу NFC в шлюз IoT (по суті це мікрокомп'ютер, який в першу чергу працює як агрегатор усіх пристроїв та інформації від них, розуміє різні протоколи зв'язку, має інтерфейс для віддаленого керування смартфоном) дозволяє безперешкодно підключати всі пристрої до шлюзу – незалежно від базової технології бездротового зв'язку.

Смартфон з підтримкою NFC, зареєстрований у шлюзі, можна використовувати як «чарівну паличку» для передачі настройок пристроям, ще пристрій може бути скинуто до заводських налаштувань або може бути виведено з мережі дотиком мобільного телефону, конфігурація одного пристрою може бути скопійована на інше, що дозволяє легко замінити старий пристрій на новий. NFC надає стандартизовані механізми, що забезпечують усі ці сценарії введення в експлуатацію.

Особливо це спрощує інтеграцію в систему пристроїв, які не мають інтерфейсу і дисплея для програмування налаштувань, наприклад, лампочки, датчики безпеки і присутності, електричні розетки і т.д.

5 АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ ТЕХНОЛОГІЇ NFC

5.1 Прослуховування

Оскільки NFC є стандартом бездротового зв'язку, захист від прослуховування є важливим завданням. Коли два пристрої взаємодіють за допомогою NFC, вони використовують радіочастотні хвилі, щоб обмінюватися повідомленнями або даними. Зловмисник може використовувати антену, щоб приймати сигнали, що передаються. Зловмиснику необхідно обладнання, необхідне для радіочастотного сигналу, а також обладнання для декодування радіочастотного сигналу. Передача даних по інтерфейсу NFC зазвичай відбувається між двома пристроями, що знаходяться безпосередній близькості один від одного. Зазвичай ця відстань не більше 10 см. Головне питання в тому, як близько зловмисник повинен бути, щоб мати можливість отримати корисну інформацію з радіосигналу. Точної відповіді на це питання немає, тому що відстань необхідна для атаки залежить від багатьох факторів, таких як:

Характеристика радіочастотного поля, що посилає сигнал пристрою (геометрія антени, екранування, навколишнє середовище);

1. Характеристика антени зловмисника;
2. Якість приймача зловмисника;
3. Якість декодера зловмисника;
4. Потужність сигналу NFC-пристрою;
5. Бар'єри на місцевості (стіни, метал, рівень шуму).

Таким чином, будь-яке точне число, відповідне відстані, яке необхідно зловмиснику, матиме сенс тільки для певного набору значень, наведених вище характеристик. Крім того, має значення, в якому режимі

пристрій відправляє дані - в активному або пасивному. Це означає, що відправник генерує власне поле (активний режим) або відправник використовує радіочастотне поле, породжене іншим пристроєм (пасивний режим). У різних режимах використовуються різні способи передачі даних. І прослуховувати пасивні пристрої набагато важче. Наприклад, коли пристрій посилає дані в активному режимі, зловмисник може перебувати на відстані близько 10 метрів. Якщо пристрій знаходиться в пасивному режимі, ця відстань зменшується до 1 метра.

Технологія NFC сама по собі не може захиститися від прослуховування. Важливо відзначити, що дані, що передаються в пасивному режимі, значно важче буде підслухати, але передавати дані лише за допомогою пасивного режиму, практично неможливо і одного лише пасивного режиму недостатньо для повноцінного використання технології NFC.

Єдиним реальним рішенням проти прослуховування є захист каналу передачі за допомогою шифрування.

5.2 Пошкодження даних

Замість того, щоб просто слухати трафік, зловмисник може спробувати змінити дані, які передаються через інтерфейс NFC. У найпростішому випадку зловмисник може просто порушити зв'язок, таким чином, що приймач не в змозі буде зрозуміти дані, що посилаються іншим пристроєм. Пошкодження даних може бути досягнуто шляхом передачі дійсних частот спектра даних у потрібний час. Правильний час може бути обчислено, якщо зловмисник добре розуміє схеми модуляції і кодування, що використовуються.

Пристрої з підтримкою технології NFC можуть протистояти цьому нападу, тому що вони можуть перевіряти радіочастотні поля на наявність

обурень, під час передачі даних. Якщо NFC сумісний пристрій робить це, він зможе виявити атаку.

Потужність, яка необхідна для пошкодження даних значно більша, ніж потужність, необхідна для виявлення пристроєм NFC. Таким чином, кожна така атака може бути виявлена.

5.3 Модифікація даних

При модифікації даних зловмисник хоче не пошкодити дані, а замінити їх непомітно від користувача. Можливість такої атаки сильно залежить від сили амплітуди модуляції. Це тому, що декодування сигналу відрізняється на 100% і 10% модуляції.

При 100% модуляції декодер переважно перевіряє дві половини бітів для радіочастотного сигналу (пауза чи не пауза). Для того, щоб декодер розумів всі одиниці як нуль, і навпаки, зловмисник повинен зробити дві речі. По-перше, пауза в модуляції має бути заповнена з несучою частотою. Це можливо, але, по-друге, зловмисник повинен створити паузу радіочастотного сигналу, який приймається законним приймачем. Це означає, що зловмисник повинен відправити деякий радіочастотний сигнал таким чином, що цей сигнал ідеально перекривається з оригінальним сигналом на антені приймача, щоб дати нульовий сигнал у приймачі. Це практично неможливо.

Тим не менш, через модифікований код Міллера у випадку з двох наступних одиниць, зловмисник може змінити другу одиницю на нуль, заповнивши паузу, яка кодує другою одиницею. Декодер не буде, бачити паузи в другому биті і декодуватиме це як нуль, тому що він передує одиниці.

У 100% модуляції зловмисник не може змінити біт значенням 0 в біт значення 1, але зловмисник може змінити біт значенням 1 в біт значення 0, якщо цей біт передує перед бітом значення 1 (тобто з ймовірністю 0,5).

У 10% модуляції декодера обидва рівні сигналу вирівнює їх. У випадку, якщо вони знаходяться в правильному діапазоні сигналу є дійсним, і виходить його декодувати.

Можливість атаки багато в чому залежить від динамічного діапазону вхідного сигналу приймача. Це дуже ймовірно, що високий рівень модифікованого сигналу перевищуватиме можливий діапазон вхідного сигналу.

Висновок такий, що для модифікованого кодування Міллера з 100% ASK ця атака є допустимою для деяких бітів і неможливо для інших бітів, але Манчестерського кодування з 10% ASK ця атака можлива для всіх бітів. Але слід зазначити, що на практиці досягти такої зміни бітів при передачі дуже важко.

Захист від модифікації даних можна досягти різними способами. За допомогою швидкості передачі 106 кбіт/с в активному режимі зловмисника практично неможливо змінити всі дані, які передаються по радіочастоті. Це означає, що для захисту необхідно, щоб обидва пристрої працювали в активному режимі. Хоча це можливо, існує серйозний недолік - активний режим є найбільш вразливим до прослуховування. Крім того, такий захист від модифікації не є ідеальним, тому що навіть прискорення 106 кбіт/с деякі біти можуть бути змінені .

Пристрої NFC може перевіряти радіочастотне поле під час відправлення. Це означає, що передавальний пристрій може безперервно перевіряти наявність такого нападу і може зупинити передачу даних, при виявленні атаки.

Третій і, ймовірно, найкращим рішенням було б забезпечення захисту каналу за допомогою хешування повідомлень.

5.4 Людина посередині

Необхідно визначити, чи потрібна автентифікація пристроїв в режимі точки. Якщо є можливість прослуховування трафіку, за певних обставин є можливість зміни трафіку, то чи можлива атака людина посередині і чи потрібний захист від цієї атаки.

У класичній схемі атаки «Людина посередині» є дві сторони, які хочуть спілкуватися один з одним - це Аліса і Боб, і третя сторона зловмисник - Єва. Це показано на рисунку 5.1.

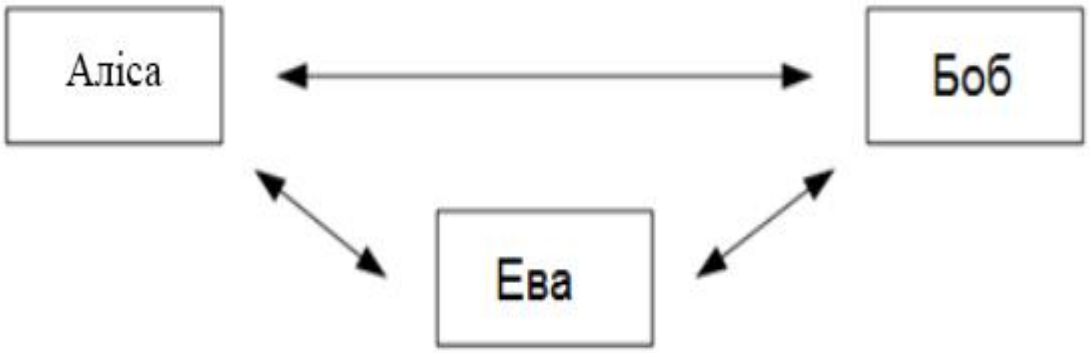


Рисунок 5.1 – Схема атаки "Людина посередині"

Аліса і Боб не повинні бути проінформовані про те, що вони не розмовляють один з одним, і про те, що вони приймають і передають дані третій стороні Єві. Це класична загроза при аутентифікації в протоколах подібних до протоколу Діффі-Хеллмана: Аліса і Боб хочуть домовитися про секретний ключ, який вони потім будуть використовувати для безпечного каналу. Але Єва, перебуваючи посередині, може встановити свій ключ з Алісою і ще один ключ з Бобом. І коли Аліса і Боб пізніше будуть використовувати свої ключі для захисту даних, Єва легко може прослухати передані дані, а також модифікувати їх.

Тепер розглянемо цю атаку в рамках NFC-спілкування.

Припустимо, що Аліса використовує активний режим, а Боб пасивний. Схема такої атаки наведена рисунку 5.2.

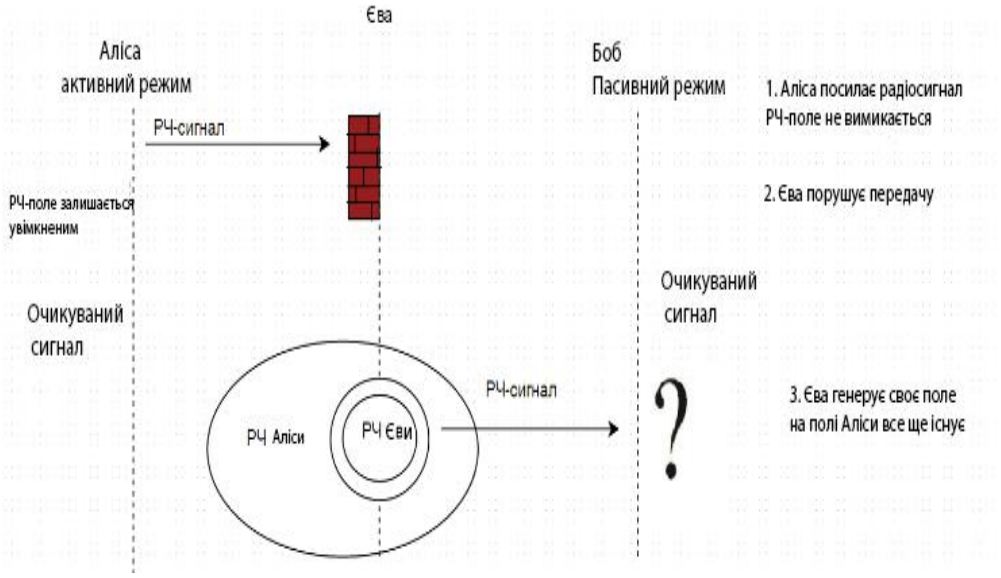


Рисунок 5.2 – Схема атаки людина посередині у разі активного та пасивного NFC-пристрою

Має місце така ситуація: Аліса генерує радіочастотний сигнал і надсилає дані Бобу. Якщо Єва досить близько, вона може підслухати дані, надіслані Алісою. Крім того, вона повинна активно порушити передачу Аліса, щоб переконатися, що Боб не отримує дані, передані Алісою. Маючи необхідні знання та обладнання, Єва може це зробити, але її дії можуть бути виявлені Алісою. У випадку, якщо Аліса виявляє порушення, Аліса може зупинити протокол погодження ключа. Припустимо, що Аліса не перевіряє обурення радіочастотного поля і протокол може бути продовжено. На наступному етапі Єві необхідно надіслати дані Бобу. Ось тут і починається проблема, тому що радіочастотне поле породжене Алісою ще є, але Єва повинна генерувати друге радіочастотне поле. Виходить, що два радіочастотні поля будуть активними в один і той же час. При цьому практично неможливо ідеально поєднати ці два радіочастотних поля. Таким чином, для Боба практично неможливо зрозуміти дані,

надіслані Євою. З цієї причини через можливість Аліси виявити атаку раніше можна зробити висновок, що атака Людина-посередині практично неможлива, якщо одностріл знаходиться в активному стані, а інше в пасивному.

Розглянемо наступний варіант, який полягає в тому, що Аліса і Боб використовують активний режим. Схема атаки показано на рисунку 5.3.

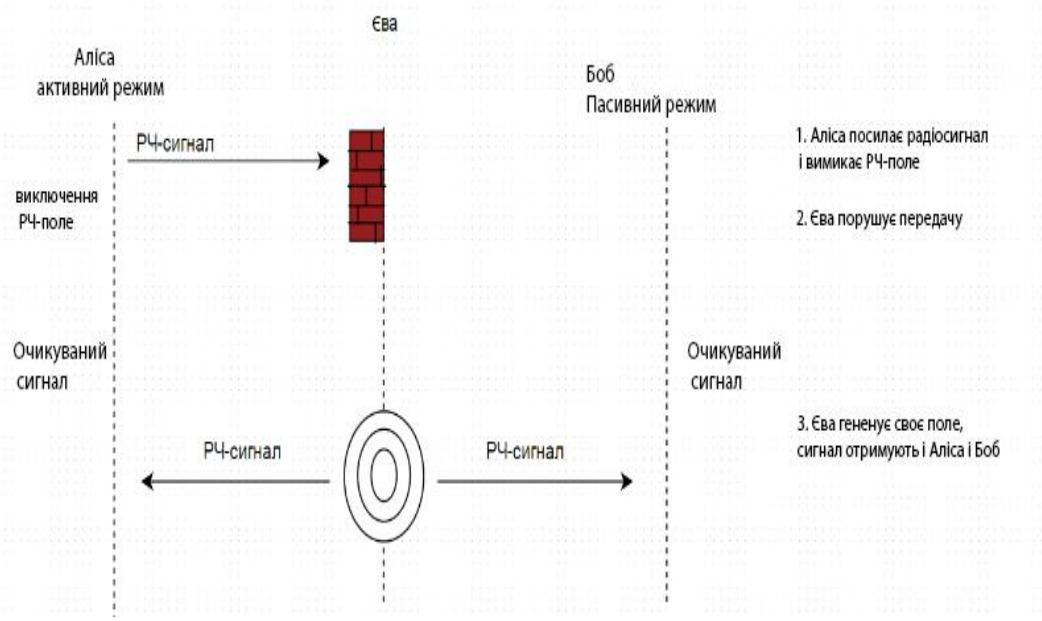


Рисунок 5.3 – Схема атаки людина посередині у разі двох активних NFC пристроїв

В цьому випадку Аліса надсилає деякі дані Бобу. Єва повинна перехопити ці дані і повинна порушити передачу Аліси, щоб переконатися, що Боб не отримав дані Аліси. При цьому Аліса вже може виявити обурення радіочастотного поля, виконані Євою і зупинити протокол. Але знову припустимо, що Аліса не робить цю перевірку і протокол продовжується. Наступним кроком Єви має бути відправлення даних Бобу. На погляд ситуація складається краще, ніж у прикладі коли є активний і пасивний пристрій. Адже зараз, коли взаємодіють два активні пристрої Аліса вимкнула своє радіочастотне поле, щоб Боб міг згенерувати своє

поле. Тепер Єва замість Боба може включити своє поле РФ і надсилати дані. Існує наступна проблема для зловмисника: Аліса прослуховує всі радіочастотні сигнали, поки вона очікує відповіді від Боба. Отже, Аліса отримуватиме дані, що передаються Євою і може знову виявити проблему в протоколі і зупинити протокол. Значить Єване може відправити дані тільки Алісі або тільки Бобу, так як дані, що відправляються, отримають обидва, а значить атака Людина-посередині неможлива.

Підіб'ємо підсумок атаку людина-посередині практично неможливо зробити в контексті NFC. Але для більшої впевненості, рекомендується використовувати активно-пасивний режим зв'язку, так щоб радіочастотне поле постійно генерувалося одним із дійсних учасників.

Крім того, активні учасники повинні слухати радіочастотне поле, створене під час відправлення даних, щоб мати можливість виявити будь-які вторгнення в поле, викликані зловмисником.

5.5 Розробка захисту каналу під час передачі за інтерфейсом NFC

Створення захищеного каналу між двома NFC пристроями найкращий підхід до захисту від прослуховування і модифікації та спотворення даних.

Через властиву технологію NFC особливостей, що дозволяють захиститися від атаки людина-посередині, можливе використання стандартного протоколу розподілу ключів Діффі-Хеллмана на основі RSA або на основі еліптичних кривих. Так як загрози людина-посередині немає, то оригінальна версія протоколу Діффі-Хеллмана чудово підійде для обміну ключами між двома пристроями.

Отриманий ключ може бути використаний для отримання симетричного ключа для алгоритмів 3DES або AES, який потім буде використовуватися для безпечного каналу, для забезпечення

конфіденційності, цілісності та справжності даних, що передаються. Для такого захищеного каналу можуть бути використані різні режими роботи 3DES та AES.

У цьому розділі розглядається стек протоколів, що використовується для захищеного каналу та передачі зашифрованих повідомлення, а також криптографічні протоколи та алгоритми, що використовуються для створення захищеного каналу.

5.5.1 Стек протоколів NFC

NFC має свій стек протоколів. Важливо розуміти, що спілкування до пристроїв з використанням інтерфейсу NFC, може бути здійснено, тільки якщо повідомлення, що передаються, мають певний формат - NDEF повідомлення. Отже, ми можемо шифрувати передане повідомлення повністю — і тіло і заголовок, тобто необхідно, щоб формат переданих повідомлень залишався правильним з точки зору NFC контролера.

Тому стек протоколів виглядатиме, як показано на рисунку 5.4.

Рисунок 5.4 – Стек протоколів NFC

При передачі даних відбувається таке:

1. На вершині стека на рівні додатків знаходяться крипто-протоколи. Вибираються дані, які потрібно надіслати і шифруються;

2. На наступному кроці дані підготовляються до відправки - формуються спеціальні блоки APDU або NDEF повідомлення, що містять зашифровані дані;

3. При зближенні пристроїв пристрої індуктивно з'єднуються за допомогою змінного магнітного поля одного з пристроїв;

4. після зближення запускається протокол активації сполуки та антиколізій;

5. Після встановлення з'єднання запускається протокол передачі даних. Відбувається передача зашифрованих/підписаних даних у форматі NDEF.

5.5.2 Загальна схема встановлення захищеного каналу

Установка та створення захищеного каналу визначається криптографічними механізмами, які використовують протокол Діффі-Хелмана для обміну ключами ключів та алгоритм AES для шифрування. За допомогою протоколу створюється захищений канал між двома пристроями NFC, які бажають обмінятися даними. Захищений канал розпадається, коли пристрої віддаляються один від одного на відстані недоступной для зв'язку NFC.

Загальна схема установки захищеного каналу показана на рисунку 5.5:

1. Обмін ключами.
2. Формування ключа для шифрування.
3. Обмін зашифрованими повідомленнями.
4. Завершення сеансу зв'язку.

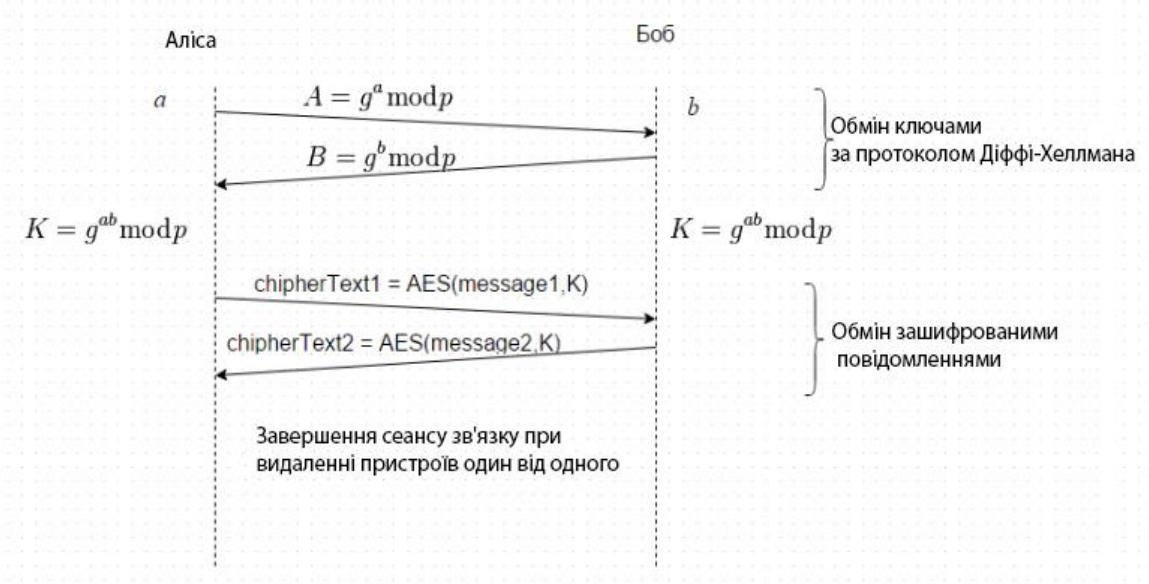


Рисунок 5.5 – Схема встановлення захищеного каналу

5.5.3 Обмін ключами

Для обміну ключами пропонується використати протокол Діффі-Хелмана. Для встановлення захищеного зв'язку два користувача Аліса і Боб спільно вибирають два числа g і p, які не є секретними і можуть бути відомі також іншим зацікавленим особам.

Для того, щоб створити невідомий більш нікому секретний ключ, обидва абоненти генерують великі випадкові числа: Аліса - число a, Боб - число b. Потім Аліса обчислює значення A= g^a mod p і пересилає його Бобу. А Боб вважає B= g^bmod p і передає Алісі.

Передбачається, що зловмисник може отримати ці значення, але не модифікувати їх.

На наступному етапі Аліса на основі наявного у неї числа a та отриманого по мережі B обчислює значення B^a= g^{ab} mod p. Аналогічно Боб на основі наявного у нього b та отриманого по мережі A обчислює значення: A^b= g^{ab}mod p.

В результаті і у Аліси і у Боба вийшло одне й те саме число: K = $g^{ab} \bmod p$

5.5.4 Шифрування

Дані шифруються алгоритмом AES в режим зчеплення блоків шифру (Cipher Block Chaining - CBC). AES був обраний як алгоритм шифрування, так як він є одним з найстійкіших алгоритмів.

AES є алгоритм шифрування 128-бітних блоків даних ключами по 128, 192 і 256 біт.

У режимі CBC до кожного блоку відкритого тексту перед шифруванням додається результат шифрування попереднього блоку за допомогою побітової операції XOR. До першого блоку відкритого тексту додається вектор ініціалізації, який генерується випадковим чином і зазвичай передається разом із зашифрованими даними, щоб їх можна було дешифрувати. Шифрування та дешифрування в режимі CBC показані на Рис.5.6 та Рис. 5.7.

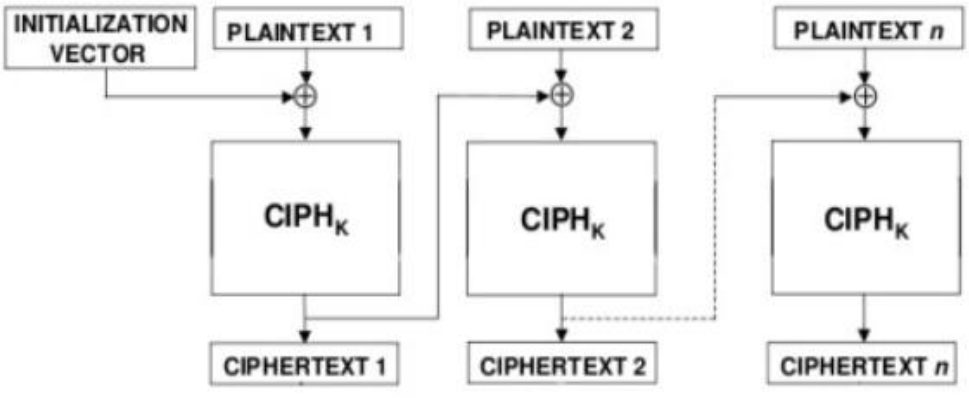


Рисунок 5.6 – Шифрування в режимі CBC

У режимі CBC для шифрування кожного наступного блоку потрібно мати результат шифрування попереднього блоку, тому шифрувати кілька

блоків одночасно не можна. Але можна робити дешифрування декількох блоків паралельно, оскільки для дешифрування кожного блоку потрібно мати тільки цей блок і попередній.

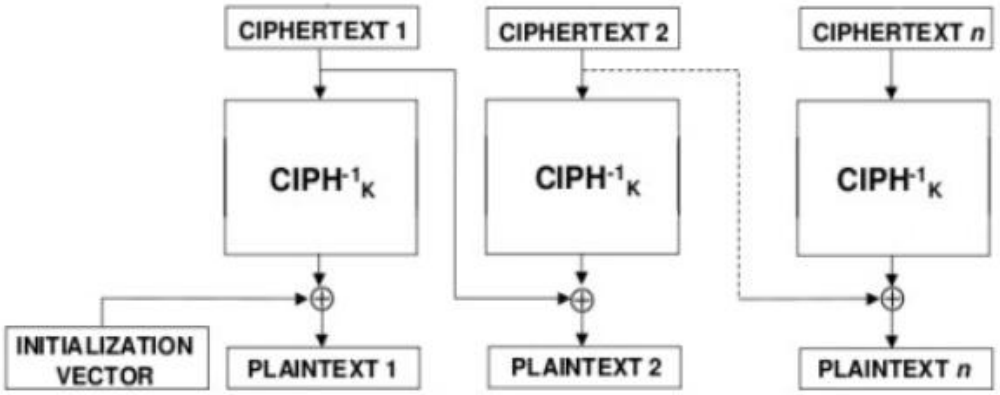


Рисунок 5.7 – Дешифрування в режимі CBC

Алгоритми блочного шифру шифрують за один раз дані в блоці, а не в одному байті. Найпоширеніший розмір блоку – 8 байт. Оскільки кожен блок піддається серйозній обробці, блокові шифри забезпечують більш високий рівень безпеки порівняно з потоковими шифрами. Однак алгоритми блокового шифрування виконуються повільніше, ніж потокові шифри.

Блокові шифри використовують один і той же алгоритм шифрування для всіх блоків. Внаслідок цього при шифруванні блоку відкритого тексту завжди буде виходити той самий зашифрований текст, якщо для шифрування використовувався один і той же ключ і алгоритм. Оскільки є можливість використовувати цю властивість для злому шифру, що представлені режими шифрів змінюють процес шифрування на основі зворотного зв'язку з раніше зашифрованими блоками. Отриманий в результаті шифр забезпечує більш високий рівень безпеки порівняно з звичайним блоковим шифруванням.

ВИСНОВОК

В даний час інтерес до технології NFC з'являється не тільки у розробників, а й простих користувачів смартфонами. І це не дивно, адже можливості використання технології обмежені лише уявою користувача. Однак, через недостатню увагу до питань захисту інформації при використанні сторонніх додатків, що підтримують NFC, існує проблема безпеки персональних даних.

Технологія NFC сама по собі не захищає користувачів від прослуховування трафіку, тобто. всі дані передаються у відкритому вигляді. Відсутні стандарти та протоколи для захисту даних, що передаються.

Цей недолік можна пояснити уявною неможливістю прослуховування трафіку через те, що передача даних між пристроями відбувається на відстані не більше 10 см. Проте, останнім часом з'явилося безліч практичних доказів можливості перехоплення відкритого трафіку за допомогою спеціальних антен. Компанії Microsoft і Google рекомендують розробникам не використовувати NFCAPI для передачі конфіденційних даних. Все це обумовлює необхідність розробки методів захисту даних, що передаються за інтерфейсом NFC, додатків, що підтримують створення захищеного каналу для передачі даних за інтерфейсом NFC.

У роботі досліджено існуючі стандарти, що стосуються технології NFC. Побудований стек протоколів, у якому на необхідний рівень вбудовані криптографічні протоколи, які забезпечують обмін ключами і шифрування трафіку під час передачі за інтерфейсом NFC. Була розроблена модель правопорушника та модель загроз.

Крім цього, розроблені були рекомендації з використання криптографічних засобів, для обміну даними в режимі точка-точка інтерфейсу NFC, обмін даними між пристроями можливий без аутентифікації, для шифрування можна використовувати симетричні алгоритми, а для обміну ключами - різні варіанти протоколу Діффі - Хеллмана.

ПЕРЕЛІК ДЖЕРЕЛ ТА ПОСИЛАННЯ

1. VedatCoskun, KeremOk, BusraOzdenizci, ― Near Field Communication From Theoryto Practice‖, NFCLabIstanbul, ISIKUniversity, Turkey, 2012.

2. NFC controller PN544 for mobile phones and portable equipment [Електронний ресурс]. - Режимдоступу до ресурсу : http//www.nxp.com/documents/leaflet/75016890.pdf

3. Rankl Wolfgang. Smart card handbook. Chichester: Wiley, 2003, 1088 с.

4. Security Concerns with NFC Technology [Електронний ресурс]. - Режим доступу до ресурсу: http://www.nearfieldcommunication.org

5. Finkenzeller Klaus. RFID handbook: Fundamentals and applications incontactless smart cards, radio frequency identification and near-fieldcommunication. Chichester: Wiley, 2010, 462 с

6. Near Field Communication Technology Standards [Електронний ресурс]. - Режим доступу до ресурсу: http://www.nearfieldcommunication.org

7. Про технологію NFC [Електронний ресурс]. - Режим доступу до ресурсу :http://www.nfcexpert.ru/ru/glossary/nfc

8. NFC security: 3 ways to avoid being hacked [Електронний ресурс]. - Режим доступу до ресурсу: http://www.pcworld.com

9. Технология NFC - связь на близких расстоянии [Електронний ресурс]. - Режим доступу до ресурсу: http://www.russianelectronics.ru

10. Warakagoda Narada. Презентация: Near Field Communication (NFC):Opportunities & Standards. [Електронний ресурс]. - Режим доступу до ресурсу: http://www.umts.no/files/081028%20nfc_standards_payments%20Narada.p

11. Yeager C. Douglas. Systems and methods for authorizing a transaction. [Електронний ресурс]. - Режим доступу до ресурсу: http://www.google.com/ patents/WO2012170895A1

12. ECMA-340. Near Field Communication Interface and Protocol (NFCIP-1).

13. Information technology - Telecommunications and information exchange; between systems — Near Field Communication — Interface and Protocol (NFCIP- 1). 2004.URL:http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnu m ber=56692.

14. ISO/IEC 14443-2. Identification cards — Contactless integrated circuit(s) cards— Proximity cards: Part 2: Radio frequency power and signal interface.

15. ISO/IEC 14443-3. Identification cards — Contactless integrated circuit(s) cards- Proximity cards: Part 3: Initialization and anticollision

16. ISO/IEC 14443-4. Identification cards - Contactless integrated circuit(s) cards -Proximity cards: Part 4: Transmission protocol.

17. R.Kilani, K.Jensen. Mobile Authentication with NFC enabled Smartphones. 2012. URL:http://ojs.statsbiblioteket.dk/index.php/ece/article/download/21229/18718

18. ECMA-352. Near Field Communication Interface and Protocol - 2 (NFCIP-2).

19. Максим Власов. RFID: 1 технология – 1000 решений: Практические примеры использования RFID в различных областях. — М.: Альпина Паблишер, 2014. — 218 с.

20. Стандарти NFC Forum [Електронний ресурс]. - Режим доступу до ресурсу: http://nfc-forum.org/

21. Технічна специфікація NFCForum-TS-NDEF-1.0. NFC Data ExchangeFormat (NDEF).

22. ECMA-373. Near Field Communication Wired Interface (NFC-WI). [Електронний ресурс]. - Режим доступу до ресурсу: https://www.ecma-international.org/publications-and-standards/standards/ecma-373/

23. TS 102 613. Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part1: Physical and data link layer characteristics.

24. ISO/IEC 7816-4. Identification cards — Integrated circuit cards: Part 4:Organization, security and commands for interchange.

25. Rancl Wolfgang. Smart card handbook. Chichester: Wiley, 2003, 1088 c.

26. Ernst Haselsteiner, Klemens Breitfub. Security in Near Field Communication(NFC) .

27. К.С. Пан, М.Л. Цымблер— Алгоритм блочного симметричного шифрования Advanced Encryption Standard (AES) Технический отчетCELLAES-01, 20 [Електронний ресурс]. - Режим доступу до ресурсу :http://pcs.susu.ru/projects/3/aes.pdf