# RFID


oyster
Transport for London


metapay
festivalcard
fesztiválkártya
12345 6789


citi

# Какво е RFID?

- Radio-frequency identification

- Комуникация между четец и карта/таг
- Чрез радио вълни
- Целяща трансфер на данни

# Приложения

# Идентификация на предмети

- Стоки
- Товарни контейнери
- Автомобили
- Животни
- Биометрични паспорти
- Хора

# Извършване на разплащания

- Транспортни услуги
- Малки суми
- Кредитни карти

# Устройства

# Четец

- Антена за комуникация
- Трябва да получи определена информация от картата
- Понякога може да изпраща данни към тага

# Таг

- Често с форма на карта
- Антена за комуникация с четеца
- Микрочип
- Съдържа информация, която трябва да се прочете

# Честоти

- Ниско честотни устройства – 125-134.2 kHz
- Високочестотни устройства – 13.56 MHz
- Други - 868–928 MHz; 433 MHz; 2.4 GHz;

# Стандарти

- ISO/IEC 18000 – описва радио комуникация за различни честоти
- ISO/IEC 14443/15693 – стандарти за 13.56 MHz безконтактни карти
- NFC – технология базирана на ISO 14443

# Тагове

# Пасивен таг

- Захранва се от полето на четеца
- Комуникация на къси разстояния – теоретично до няколко метра
- Най-често срещаните тагове

# Активен таг

- Захранва се самостоятелно
- Комуникация на по-дълги разстояния – теоретично десетки метри
- По-рядко срещани

# Функционалност на таговете

- Уникални данни за идентификация

- Криптография
- Специални протоколи за комуникация
- Възможност за запис на информация

# Прости тагове

- Използвани за контрол на достъп
- Ниско честотни – 125 kHz
- При захранване изпращат уникален за тага сигнал, записан от производителя
- Лесни за прочитане
- Лесни за симулиране
- Използват цифрова модулация – ASK/FSK/PSK

# Умни тагове

- Високочестотни – 13.56 MHz
- Използват се масово в услуги за обществен транспорт и малки разплащания
- Използват протокол за комуникация
- Имат реализирана криптография
- Разполагат с памет
- Зле защитени в миналото

# Четци

# Четец от производителя

- Работи с всички функции на картите
- За точно определени тагове
- Proprietary

# NFC устройства

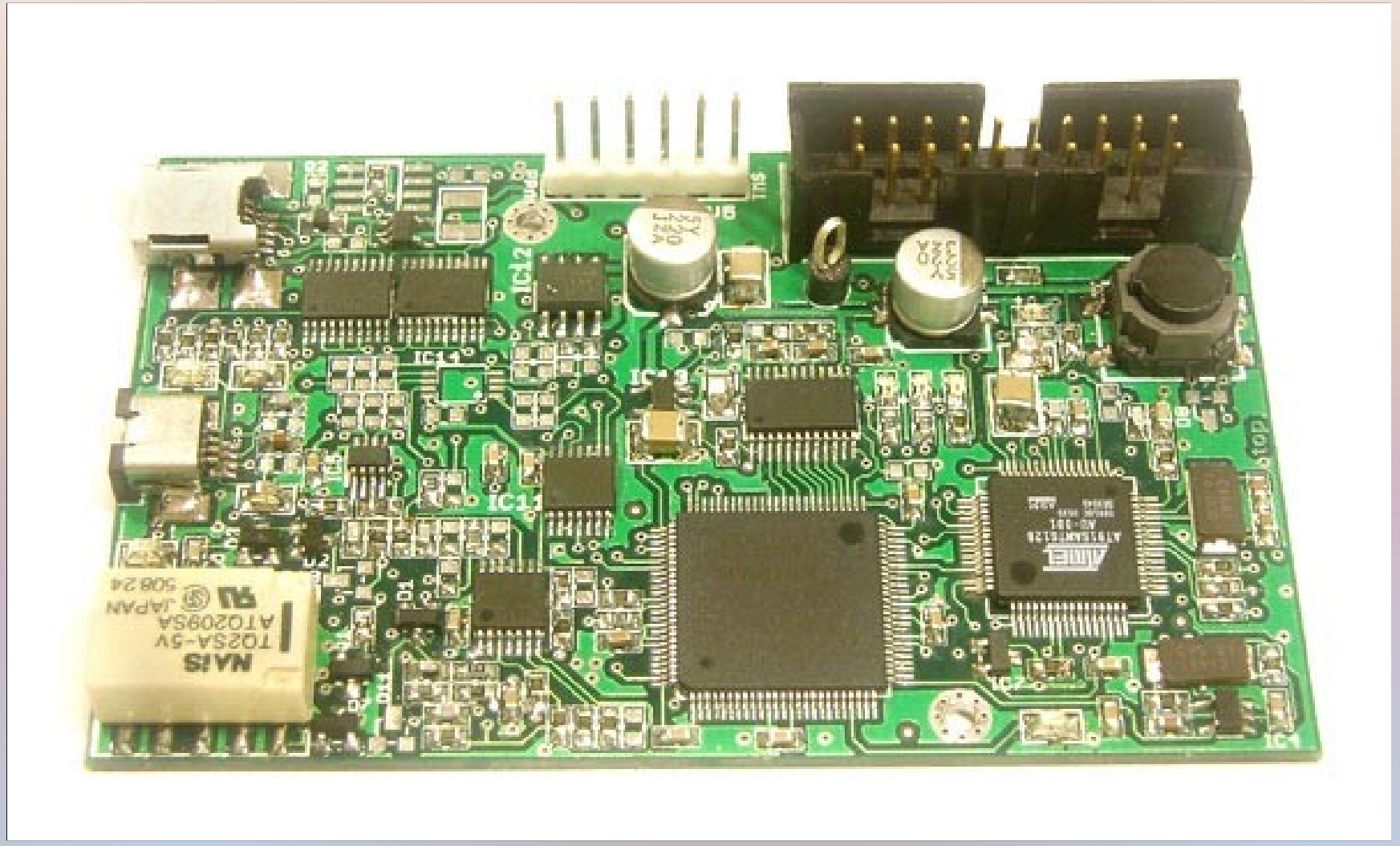
- Хардуер: Множество смартфони
- Софтуер: libnfc

# OpenPCD

# OpenPCD

- Само за тагове на честота 13.56 MHz
- Изцяло отворена платформа базирана на RFID чип
- Малко възможности в хардуера и в софтуера

# Proxmark3



# Proxmark 3

- Може да се използва за 125/134 kHz, 13.56 MHz
- Разполага с FPGA и ARM MCU
- Изцяло отворена платформа
- Подходящ за всякакви изследвания в областта
- Нестабилен софтуер

# Популярни тагове

# Обикновени тагове

- Прочитането на информацията става за секунда
- С устройство като Proxmark3 без проблем може да бъде възпроизведен отговора на картата
- Поради това, система разчитаща само на обикновени ниско честотни тагове, не може да се счита за надеждна

# Proxmark 3 – LF Четене

- lf read – захранва тага
- data samples 2000 – записва 2000 семпъла
- data askdemod / fskdemod / mandemod – демодулира семплите и ги превръща в цифров вид
- lf sim – повтаря прочетените данни

# NXP MIFARE Classic

- Създадени в далечната 1994
- Ограничена и уязвима криптография
- Масово използвани в различни системи
- 1, 4 или 8 kb данни

# Сектори и блокове

- Блокове от 0 до 64+
- Всеки 4 блока образуват сектор
- Блок 0,1,2 от сектор се използват за данни
- Блок 3 от сектор се използва за ключове и права за достъп
- Блок 0 (в сектор 0) съдържа уникална информация и не може да бъде записван

# ISO 14443A

- Таг->Четец – Manchester Encoding
- Четец->Таг – Modified Miller Encoding
- Използва се за предаване на команди
- Команди за първоначална идентификация на тага
- Parity бит на всеки 8 бита

# MIFARE Classic's CRYPTO1

- Създаден с идеята за security through obscurity
- Изцяло reverse engineer-нат през 2007
- Прекалено уязвим
- Stream шифър
- 48 битов LFSR за генериране на битове за криптиране
- 16 битов LFSR за генериране на случаен nonce
- libcrapto1

# MIFARE Classic Challange

- Tag->Reader: 4byte random tag nonce
- Reader->Tag: 4byte reader nonce
- Reader->Tag: 4byte reader reply
- Tag->Reader: 4byte tag reply

# MIFARE Classic - Darkside attack

- Слабости в crypto1
- Слабост в псевдо генератора на случайни числа
- Не всички битове се използват за криптиране
- Parrity битовете се смятат върху некриптираните данни
- Възстановяване на произволен ключ за време от 1-2 до 30-40 минути

# MIFARE Classic - Nested attack

- Възползва се от уязвимост в алгоритъма
- При използване на ключ, се постига конкретно състояние
- При това, познаването на отговор за nonce, става много по-предвидимо
- Така ако е известен поне един ключ, възстановяването на останалите е въпрос на около 30 минути

# Битове с права за достъп

| C1 | C2 | C3 | AR | AW | ACR | ACW | BR | BW | R | W | Inc | Dec |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | - | A | A | - | A | A | A/B | A/B | A/B | A/B |
| 0 | 1 | 0 | - | - | A | - | A | - | A/B | - | - | - |
| 1 | 0 | 0 | - | B | A/B | - | - | B | A/B | B | - | - |
| 1 | 1 | 0 | - | - | A/B | - | - | - | A/B | B | B | A/B |
| 0 | 0 | 1 | - | A | A | A | A | A | A/B | - | - | A/B |
| 0 | 1 | 1 | - | B | A/B | B | - | B | B | B | - | - |
| 1 | 0 | 1 | - | - | A/B | B | - | - | B | - | - | - |
| 1 | 1 | 1 | - | - | A/B | - | - | - | - | - | - | - |

# Proxmark 3 – MIFARE Classic

- hf mf mifare – възстановява ключ на MIFARE карта
- hf mf nested – възстановява останалите ключове използвайки възстановения
- hf mf rdbl – прочита информацията в блок
- hf mf wrbl – записва информация в блок

# Примерен сектор #1

- 00 00 00 97 00 00 00 97 00 00 00 04 13 fa b3 24
- 00 00 00 00 ff ff ff ff 00 00 00 00 07 f5 23 a4
- 00 00 00 00 ff ff ff ff 00 00 00 00 0e e2 0e b3
- 00 00 00 00 00 00 68 77 89 00 00 00 00 00 00 00

- 0x97 = 151; сума налична в картата
- байтове с права за достъп

# Примерен сектор #2

- 31 30 32 33 38 35 33 31 39 31 32 35 32 33 30 34
- 33 34 35 33 30 31 30 35 34 32 36 00 00 00 00 00
- 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
- 00 00 00 00 00 00 78 77 88 00 00 00 00 00 00 00

- номера отпечатан върху картата
- байтове с права за достъп

# Примерен сектор #3

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05 08 0b 0a 14 21 0c 01 04 01 20 20 20 20 20 20
17 2b e3 ac 01 00 06 08 0b 07 0b 0b 00 52 88 00
00 00 00 00 00 00 08 77 8f 00 00 00 00 00 00 00
```

- дата и час на последната комуникация
- ID на устройство
- ID записано на обратно
- валидност

# NXP MIFARE DESFire

- Създадени 2002
- Използват Tripple-DES или AES
- Известен протокол
- Използват се в системи за заместване на Classic
- Наскоро разбита защита на DES варианта

# HID iClass

- ISO 14443B и ISO 15693
- 13.56 MHz
- Използва 3DES
- Разполагат с памет 256 / 2k / 4k bytes
- 64 битови ключове
- Отново разбита защита

# Бъдеще

# NFC базирани устройства

- Смартфоните с NFC
- Специални устройства с NFC (PayPass)

# Въпроси?