
UNIVERSITÁ DEGLI STUDI DI SALERNO

Dipartimento di Informatica

Laurea Magistrale in Sicurezza Informatica

Tesina in Sicurezza dei Dati

# Carte di credito contactless e tecnologia HCE

Hilary De Gregorio 0522500401
Antonio Mazzarelli 0522500394
Francesco Silvano 0522500435

# Sommario

- Introduzione
- RFID
- NFC
- Le nostre app
- Attacchi
- Conclusioni

# Introduzione

Negli ultimi decenni l'uso delle tecnologie RFID ha subito una forte espansione.
Ad oggi, infatti, viene usata in molteplici applicazioni tra le quali:

- Controllo presenze
- Passaporto
- Tracciatura merci
- Pagamenti contactless


Una domanda sorge spontanea:

Questa tecnologia è realmente sicura?

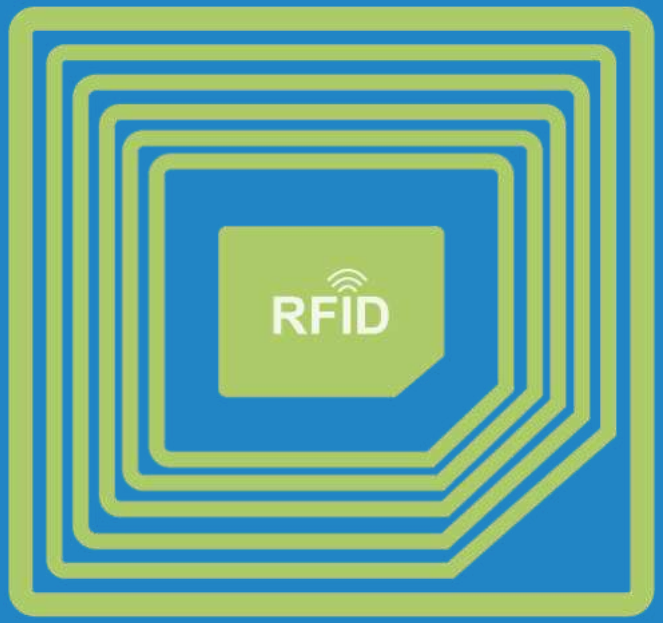
# Il nostro lavoro

Avendo in mente di analizzare la sicurezza della tecnologia sono state sviluppate 3 applicazioni:

- **CardInfo App:** lettura delle informazioni da una carta di credito contactless
- **CardEmulator App:** emulare una carta tramite un cellulare Android
- **CardReader App:** simulare un sistema pos

Inoltre sono stati analizzati due attacchi che sfruttano l'NFC:

- Distributed Guessing Attack
- Relay Attack




# La tecnologia RFID

# RFID

Radio Frequency Identification nasce negli anni ’60 per scopi militari e si basa sull’uso di onde elettro-magnetiche.
Gli usi principali sono:

- Identificazione di oggetti,animali e persone
- Memorizzazione di informazioni


Per l’uso servono:

- Tag: chip dove sono memorizzate le informazioni
- Reader: dispositivo in grado di leggere/scrivere i tag

# Perchè RFID?

RFID ha introdotto numerosi vantaggi rispetto allo standard precedentemente utilizzato ovvero la banda magnetica, tra i più importanti troviamo:

- Non deve essere a contatto per essere letto
- Non deve essere visibile per essere letto
- Si possono anche aggiungere informazioni sui chip in funzione della tipologia del chip
- L'identificazione e la verifica avvengono in 1/10 di secondo
- Possibilità di cifrare la comunicazione

# NFC

# NFC

Il *Near Field Communication* che significa comunicazione di prossimità è l'evoluzione più recente della tecnologia  RFID.

Le caratteristiche principali sono:

- Frequenza di 13.56 MHz
- Distanza massima di 10 cm
- Velocità di trasmissione dat. fino a 424 kbit/s

# La nascita di NFC

La tecnologia NFC nasce come naturale evoluzione dei sistemi RFID. La sua diffusione è dovuta anche alla sempre maggiore diffusione delle nuove tecnologie, in particolare di smartphone.

L'NFC è in grado di semplificare molte operazioni comuni quali ad esempio il pagamento di piccole somme di denaro o la tracciatura di oggetti e persone.

# La tecnologia Nfc ha 3 funzioni

**1**
Lo scambio di informazioni tra due dispositivi accostandoli tramite il *Peer-to-Peer*

**2**
Effettuare pagamenti rapidi e con il proprio cellulare, tramite il protocollo *HCE*(Host Card Emulation)

**3**
Leggere e scrivere i Tag NFC

# Carte di credito contactless ed EMV

*I soldi non danno la felicità per questo hanno inventato le carte di credito.*

# Carte di credito contactless

L’evoluzione delle carte di credito è la carta di credito “contactless” cioè senza contatto, non richiedono l’inserimento fisico della carta nel lettore ma è sufficiente l’avvicinamento, i POS sono dotati di un apparato supplementare che si aggiunge alla base principale oppure al PIN PAD e le carte sono dotate di Chip NFC.

# EMV

EMV (Europay  Mastercard VISA) è uno standard, nato nel 1994, per l'utilizzo delle smart card, terminali POS, sportelli ATM e per l'autenticazione di transizioni.

Le schede EMV sono conosciute anche come schede chip o schede IC che memorizzano i dati in circuiti integrati, nello standard sono incluse sia schede contactless che normali.

# APDU (1)

APDU, acronimo di *Application Protocol Data Units*, è una sequenza di byte che possono essere inviati da un'applicazione software del lettore alla smart card, le specifiche sono definite da ISO/IEC 7816.

Lo standard permette di comunicare con una smartcard e di effettuare transazioni.

# APDU (2)

Esistono due categorie di APDU:

- ***Comandi APDU***: inviato dal lettore smart card alla carta che contiene obbligatoriamente 4 byte di header (CLA, INS, P1, P2)  e di seguito da 0 a 255 byte dati.4

| CLA | INS | P1 | P2 | Lc | Data | Le |
|---|---|---|---|---|---|---|
| Header | | | | Body | | |

- ***Risposte APDU***: inviata dalla carta al lettore che contiene da 0a 65536 byte di dati e  2 byte riguardanti lo stato (SW1, SW2)

| Data | SW1 | SW2 |
|---|---|---|
| ← Body → | ← Trailer → | |

# Vulnerabilità (1)


**Clonazione bande magnetiche**

Se il lettore EMV è compromesso, viene intercettata la comunicazione tra la scheda e il terminale l'attaccante potrebbe recuperare entrambi i dati binari e il PIN costruendo una nuova banda magnetica.

Nel 2006 nei terminali Shell si è verificato l'attacco rubando più di 1 milione di sterline.

# Vulnerabilità (2)


## Disattivazione Pin

L'11 febbraio 2010 la squadra di Murdoch e Drimer alla Cambridge University ha annunciato di aver trovato "un difetto nel circuito integrato e nel PIN" . Una carta rubata è collegata ad un circuito elettronico e ad una carta falsa viene inserita nel terminale ("man-in-the-middle").

Tutte le quattro cifre sono digitate e accettate come PIN validi.

Una squadra ha visitato la caffetteria dell'Università di Cambridge (con permesso) con il sistema e sono stati in grado di pagare utilizzando le proprie carte  collegato al circuito, inserendo una carta falsa e digitando " 0000 "come PIN

# Le nostre app

# L'idea

Per poter studiare la sicurezza dei sistemi di pagamento NFC attuali sono state sviluppate 3 applicazioni:

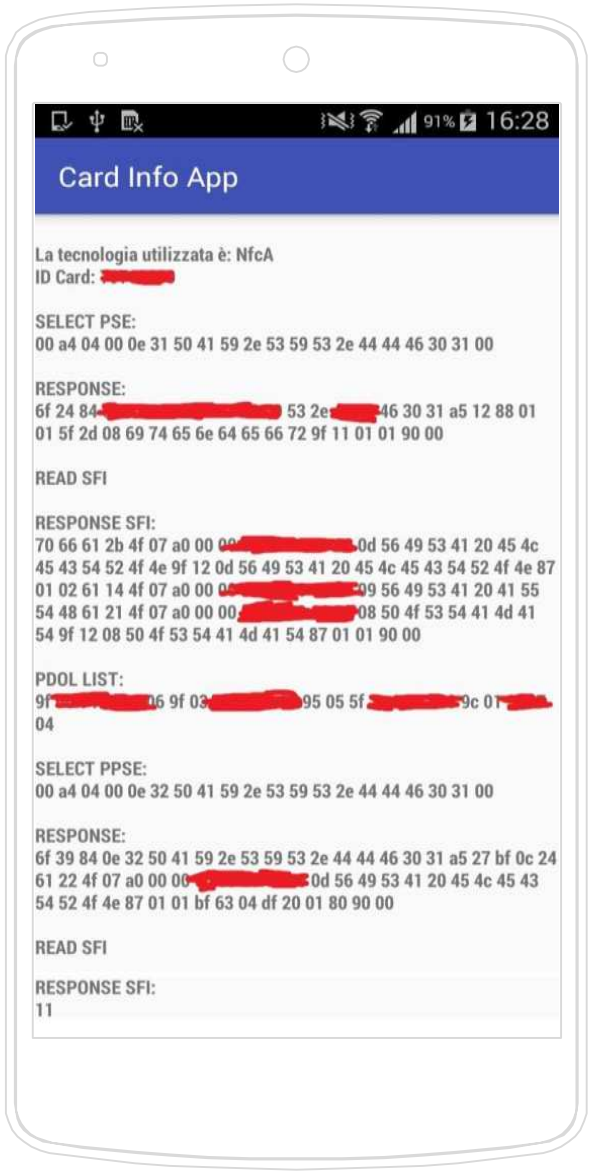
- **CardInfo App:** leggere le informazioni
- **CardEmulator App:** emulare la carta con un device Android
- **CardReader App:** simulare il comportamento di un POS

# CardInfo app

L’app ha lo scopo di raccogliere i dati interrogando direttamente la carta.

Le fasi dell’acquisizione sono:

- Scansione di nuovi tag
- Identificazione del tipo di carta
- Lettura dei dati, in particolare PAN e data di scadenza



# CardReader app

L’app è stata sviluppata come app tester per verificare l’emulazione.

L’esecuzione prevede:

- Lettura della tecnologia e dell’UID del tag
- Invio di comandi APDU simulando il comportamento di un POS

# CardEmulator app

L’app si occupa di emulare una carta EMV reale.

Per il corretto funzionamento l’app deve ricevere:

- Il comando SELECT AID per iniziare la comunicazione
- Comandi in formato APDU.

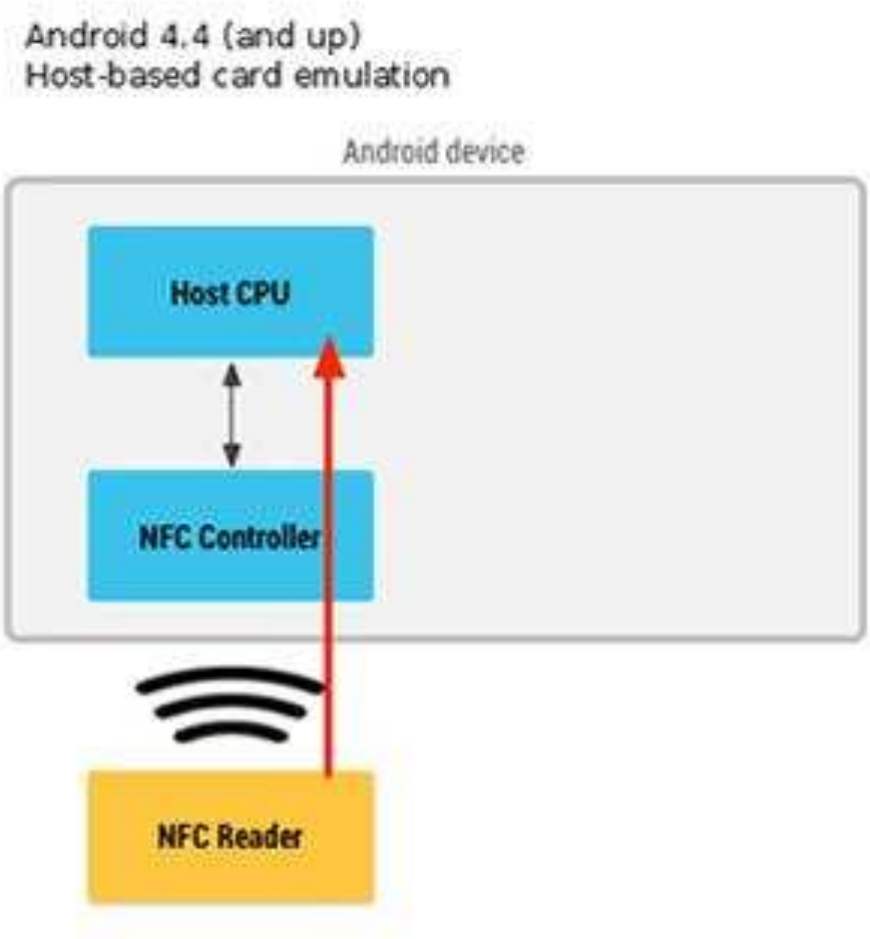
Nel caso in cui non sia disponibile la risposta ad uno specifico comando l’app risponde con un codice di errore predefinito.

# Host Card Emulation Service

Il servizio HCE di Android è la componente fondamentale per l'emulazione di una carta EMV sui dispositivi Android grazie al servizio HCE.

L'Host Card Emulation permette di instaurare una comunicazione tra un lettore e la nostra app.

Il servizio HCE è disponibile a partire dalla versione 4.4 di Android.



# Possibili usi delle app

L’app CardEmulation potrebbe essere usata per impedire la lettura dei dati da parte di uno scanner.

Effettuando qualche modifica è possibile fare in modo che l’app risponda con dati casuali o comunque non reali, proteggendo l’utente da eventuali furti di dati, trasformandola di fatto in un HoneyPot NFC.

# Attacchi

# Attacchi

Sono stati analizzati attacchi che sfruttano l'NFC per la raccolta di informazioni.

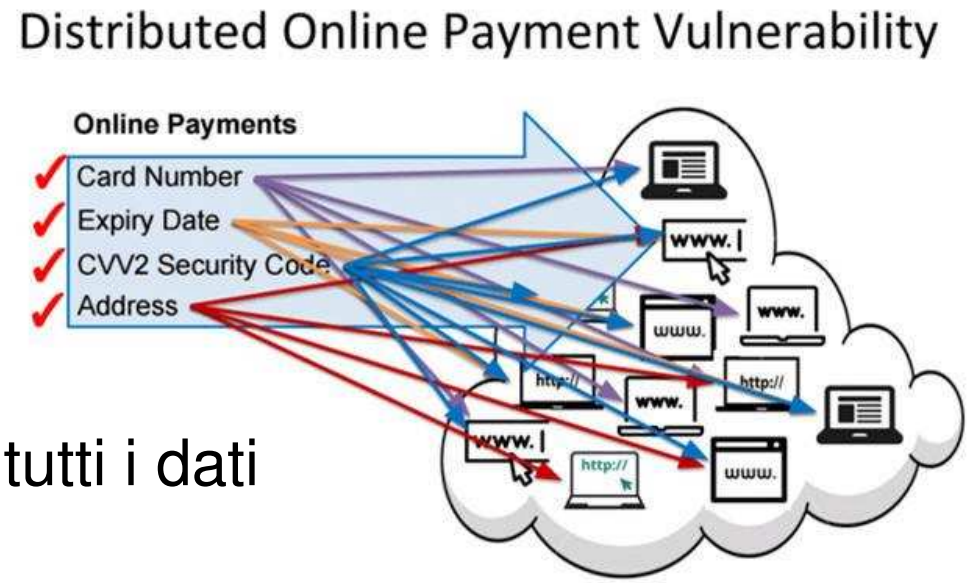
In particolare gli attacchi presentati sono:

- Distributed Guessing Attack
- Relay Attack

# Distributed Guessing Attack (1)

Pagamenti online

- PAN
- Data di scadenza
- CVV2
- Intestatario




Problema:

Non tutti i siti utilizzano tutti i dati

Quindi si possono sfruttare i siti web per ricavare i dati di una carta di credito.

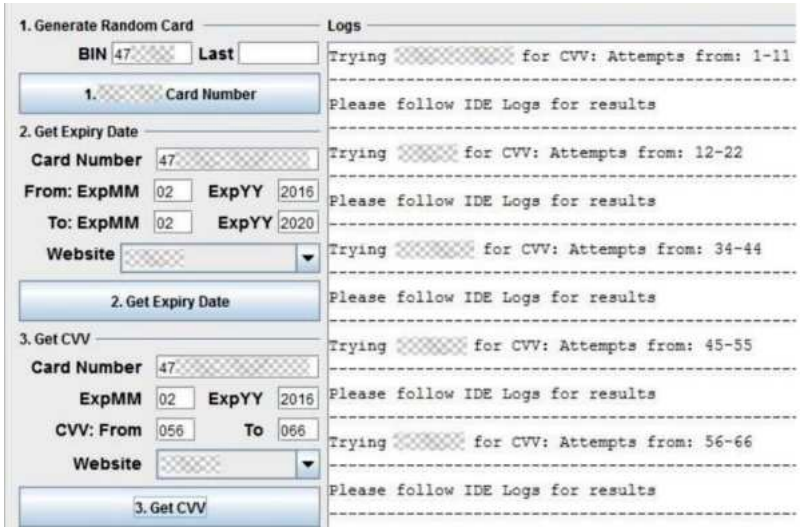
L'attacco è stato presentato dai ricercatori dell'università di NewCastle nel 2016

# Distributed Guessing Attack (2)

Sfruttando adeguatamente i vari siti è possibile ricavare

- La data di scadenza in 60 tentativi
- Il codice CVV2 in 1000 tentativi

Quindi si ottengono i dati in soli 1060 tentativi invece di 60000




Il browser bot realizzato dai ricercatori di NewCastle impiega circa 6 secondi per trovare tutti i dati.

# Relay Attack (1)

Immaginiamo di sfidare due campioni di scacchi a distanza, potremmo ingannarli e farli giocare uno contro l'altro mentre loro pensano di giocare contro di noi.

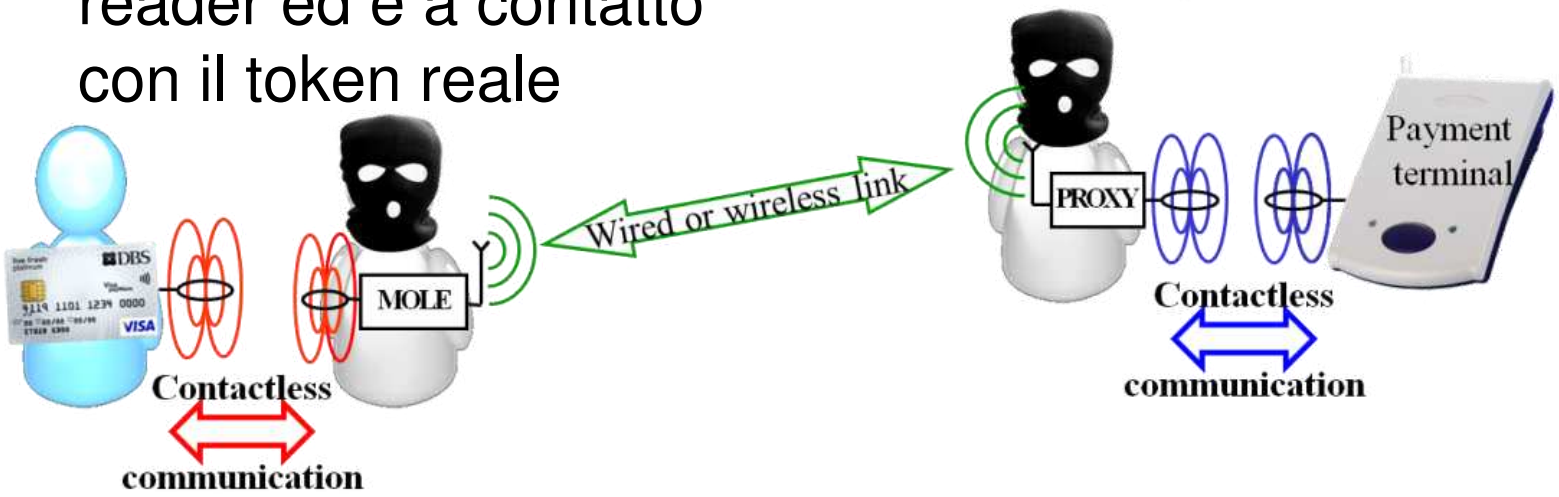
Questa è l'idea alla base del Relay Attack per le carte di credito NFC

# Relay Attack (2)

L'attacco è noto da tempo ed è stato implementato su diversi device mobili.

L'occorrente necessario è:

- *Proxy-Token*: simula il token reale ed è a contatto con il reader
- *Proxy-Reader*: simula il reader ed è a contatto con il token reale




L'attacco permette così di aggirare qualunque sistema di protezione anche non conoscendone i dettagli.

# Relay Attack (3)

L’uso dei device token aggiunge del ritardo alla comunicazione tra carta e reader.
Nonostante l’aumento dei tempi di esecuzione di una transazione il tempo totale necessario è inferiore al tempo di timeout del reader.

Quindi l’attacco descritto, per quanto non di immediata realizzazione, può realmente essere effettuato

# Conclusioni(1)

Il campo applicativo dei sistemi NFC è molteplice ed in via di forte sviluppo. Attualmente sono presenti sistemi di pagamento e di riconoscimento, non a caso esistono passaporti che integrano schede NFC.

Il lavoro svolto ha preso in considerazione unicamente i metodi di pagamenti e lo sviluppo delle app è stato effettuato su sistemi Android.

# Conclusioni(2)

Sarebbe interessante ampliare l'analisi sia su altri sistemi che usano la tecnologia NFC. Potrebbe essere utile anche verificare se è possibile implementare le app descritte su sistemi IOS.

Le app descritte, opportunamente modificate, potrebbero essere usate come protezione da possibili furti di dati da parte di un attaccante.

# GRAZIE PER L'ATTENZIONE