

Índice

Agradecimientos	7
Introducción	13
Capítulo I	
Introducción a pagos digitales	15
1. Introducción.....	15
2. El espectro RFID	16
¿Qué es la información de banda magnética?	16
¿Cómo funciona un lector de información de banda magnética?	17
¿Qué es el sistema de tokenización?	18
¿Qué son los Frameworks de Visa y MasterCard?.....	18
¿Qué es MSD?.....	19
¿Qué es un ataque estilo “downgrade”?.....	19
3. Diferentes Protocolos.....	20
El Protocolo APDU	20
¿Qué es NFC?	21
¿Qué es MST?	21
Elemento Seguro y Emulación de Tarjetas	22
4. Diferentes métodos de Pagos	22
Tarjetas de pago NFC	22
Apple Pay	22
Samsung Pay	23
Google Pay	23
¿Qué es una transacción?	23
Capítulo II	
Herramientas.....	35
1. Hardware	35

MagSpooF.....	35
BlueSpooF.....	37
NFCopy.....	39
TokenGet.....	41
Tarjeta PN532.....	43
Arduino.....	43
Raspberry Pi.....	44
Raspberry Pi y PN532.....	45
Instalando el cliente para la Proxmark3 RDV4.....	49
La consola de Proxmark3.....	51
Centinelas.....	58
NFCtoChip.....	58
2. Software.....	60
SwipeYours.....	60
EMVemulator.....	60
EMV Reader.....	60
Librería Adafruit PN532.....	61
Librería RFIDIot.....	61

Capítulo III

Ataques de Repetición: Información de banda magnética y MST.....63

1. Introducción.....	63
Información de Banda Magnética (mag-stripe).....	63
2. Ataques de Repetición: MST.....	64
MST vs banda magnética tradicional.....	65
Introducción a los ataques de repetición MST.....	66
3. Clonación de tarjetas físicas y de tokens MST.....	69
Usando el lector y escritor MSR.....	69
4. Spoofiendo información de banda magnética con MagSpooF.....	71
Implementar tokens MST con MagSpooF.....	72
Algunas limitantes de MagSpooF.....	74
5. Clonando información de banda magnética con BlueSpooF.....	74
Moviendo datos de banda magnética a ondas de sonido.....	75
6. Usar tokens MST en otros países.....	77

Capítulo IV

Ataques de Repetición: NFC.....79

1. Introducción.....	79
Analizando un ataque de repetición.....	79

2. Emulación con Acr122	80
3. Raspberry Pi y Acr122u.....	85
Pyscard.....	85
Comunicando Acr122 y Pyscard.....	86
Analizando el PDOL y generando un reto simple con Python	88
Generando un reto más complejo con Python.....	97
4. Ataque de repetición con Raspberry Pi y Acr122.....	101
5. Arduino y PN532	104
6. Android y SwipeYours.....	108
7. NFCopy85: ATtiny85 y PN532	112

Capítulo V

Ataques de Retransmisión o Relay.....	117
1. Introducción.....	117
Proceso de un relay	118
2. Relay Local: Acr122 y RFIDIot	119
3. Relay en WiFi: ESP32 y PN532.....	120
Servidor WiFi ESP32	120
Cliente WiFi ESP32	124
4. Relay en internet: Heltec ESP32 & LoRa y PN532.....	128
Dispositivo A.....	128
Dispositivo B.....	133
Servidor.....	137
5. Relay SDR: CC1101 y Teensy.....	139
Dispositivo A.....	140
Dispositivo B.....	144
6. NFCGate: Usando sistema Android como Relay.....	148
Clonación	149
Relay o retransmisión.....	150
Alterando el nivel monetario de una transacción.....	154
Modo Captura.....	163
Recomendaciones para NFCGate	164

Capítulo VI

Relay Inteligentes y Analizando Datos de Chips EMV.....	169
1. Introducción.....	169

2. Ataque inteligente	169
Transacción de Fitbit Ionic.....	170
3. Datos de Chips EMV	176
Cardpeek	176
Pyscard	183
ChipToNFC	187
Simtrace 2.....	195
Firmware para Simtrace V2	197
Cliente para la máquina Host.....	197
Simulación o emulación de tarjetas EMV.....	202
MiTM con Simtrace v2	208
 Índice alfabético	 215
 Índice de imágenes	 217