

Digitalización, riesgos y mejores prácticas en medios de pago en la actualidad

Salvador Mendoza

- Samsung Pay, Google Pay, Wells Fargo
- NFC Payments: The Art of Relay & Replay
- Ocelot Offensive Security Team
- Adafruit and Proxmark3 Contributor
- Hardware Enthusiast



Salvador Mendoza

Director of Research and
Development

Agenda

- 01 Riesgos actuales
- 02 Nuevas tecnologías y nuevos ataques
- 03 Consideraciones en el área de fraude
- 04 De contacto EMV a NFC
- 05 Conclusiones

Riesgos actuales

- Ransomware
- Familia de malwares
 - Robo de información
- Phishing
- Implementaciones inadecuadas

Problemas actuales en los sistemas de pagos

- Nuevas tecnologías y una inadecuada implementación
- Conocemos parcialmente el comportamiento de nuestros clientes, de ataques y de los atacantes
- Tendencias en “relays”: mas allá de NFC
- Poca colaboración proactiva
- Falta de talento o pocas oportunidades de entrenamiento para nuestros equipos

Últimos ataques registrados

- Bypass en el límite transaccional de NFC
- Emulación de tecnología de contacto EMV
- Ataque de repetición en transacciones
- Biométricos audio y rostro
- Cambio en el tipo de criptograma generado
- Cambio en el tipo de moneda utilizada

Banda Magnética:

Pista 1: %B4716042088430250^MR.P/GREEN^210820100000000000000000222000000?

Pista 2: ;4716042088430250=21082010000002220000?

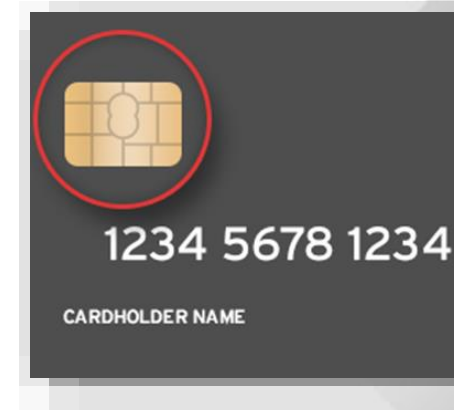
Chip EMV:

Pista 1: 4716042088430250^2108201000100000000000387000000

Pista 2: 4716042088430250D21082010000013870000F

NFC:

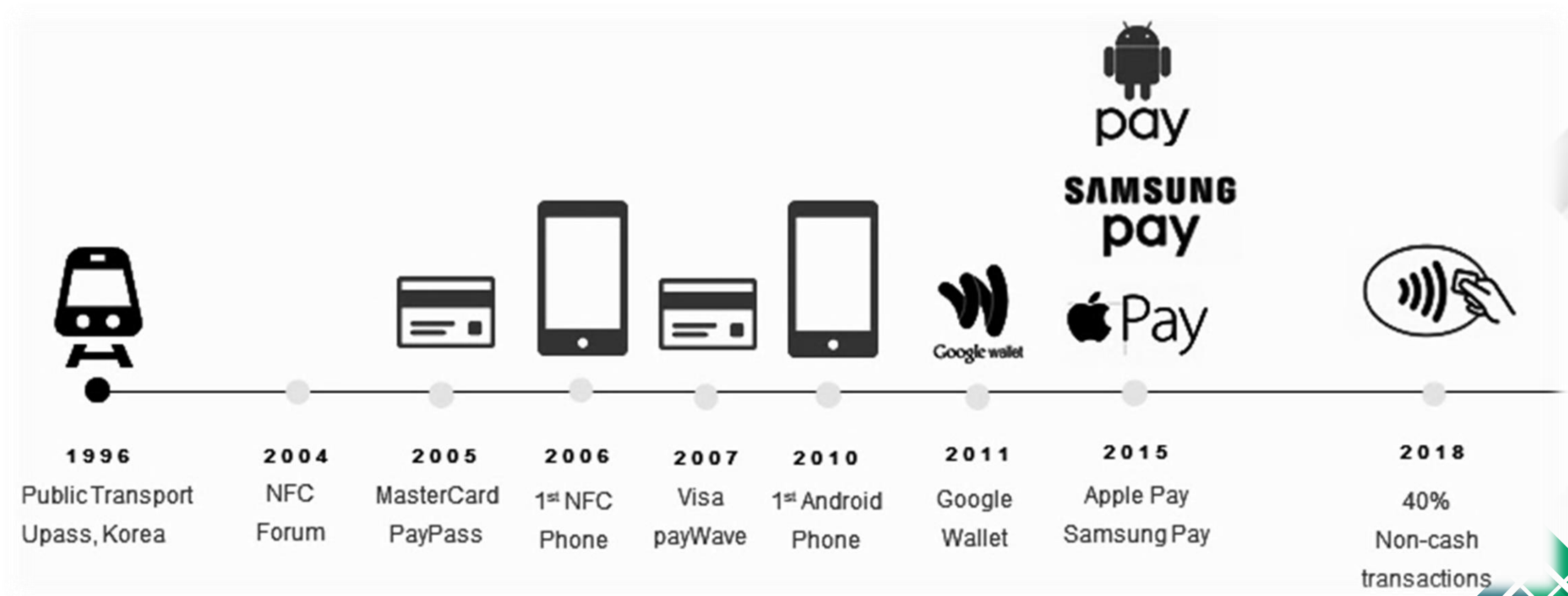
Pista 1: 4716042088430250D21082010000013870000F



Modificación Especial:

Pista 1: %B4716042088430250^MR.P/GREEN^210820100000000000000000387000000?

Tecnología NFC



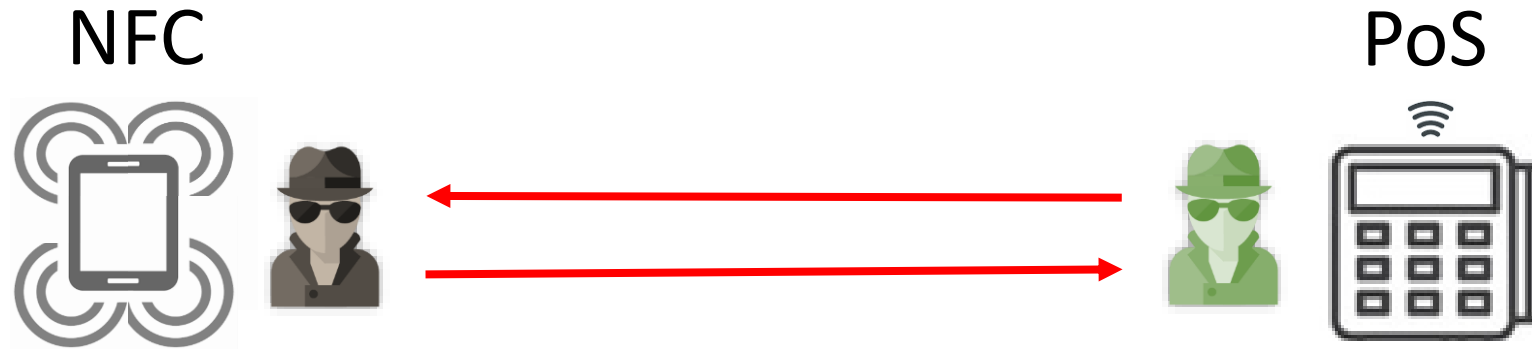
Tecnologías en transacciones



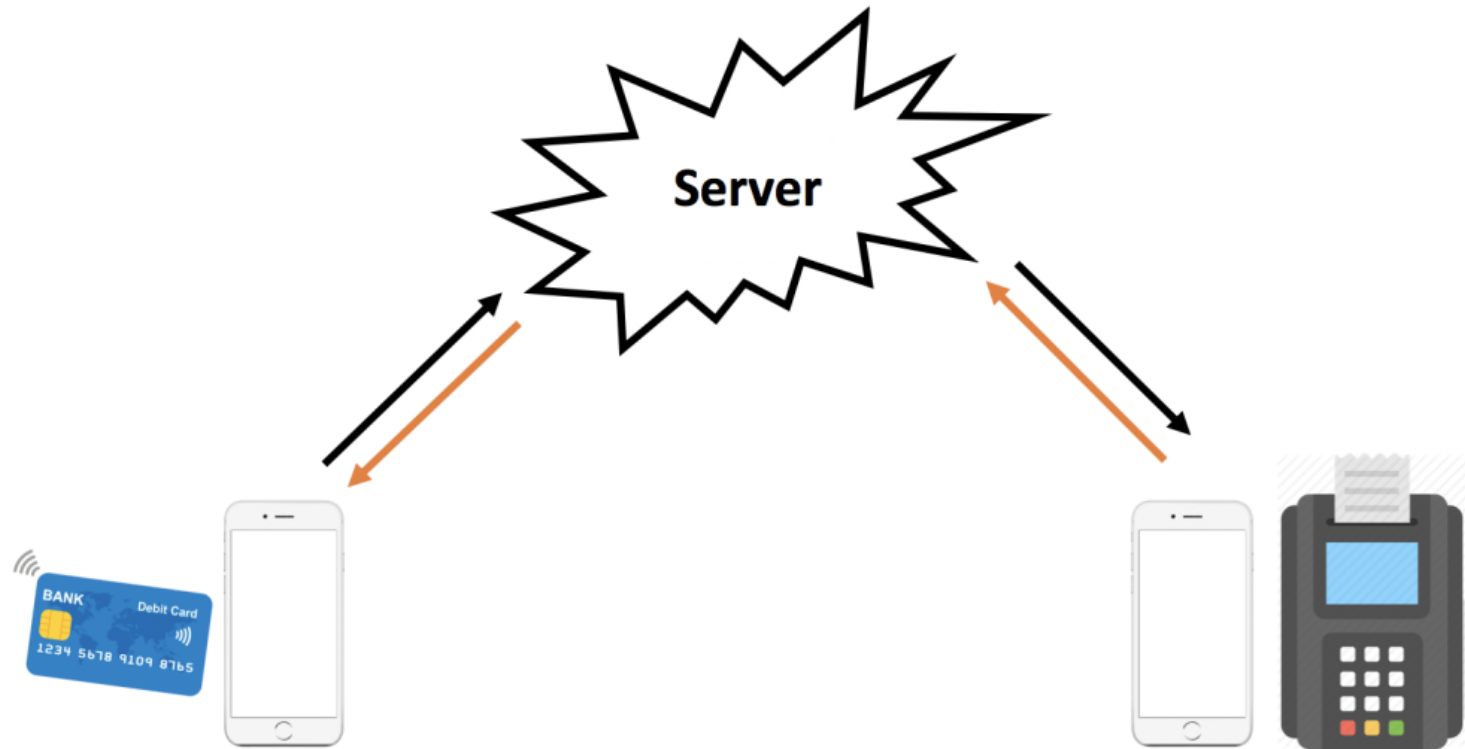
Sistemas de tokenización

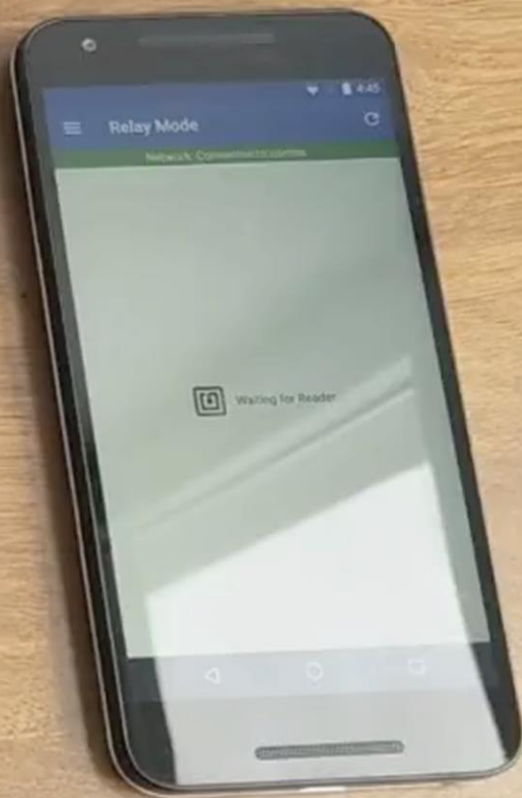
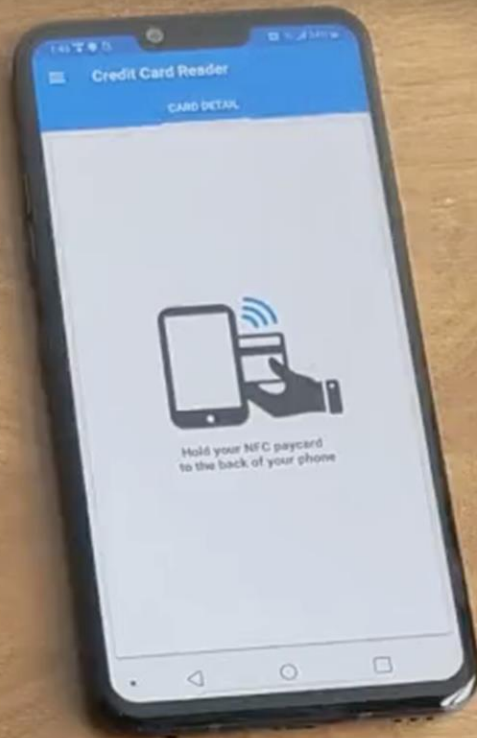


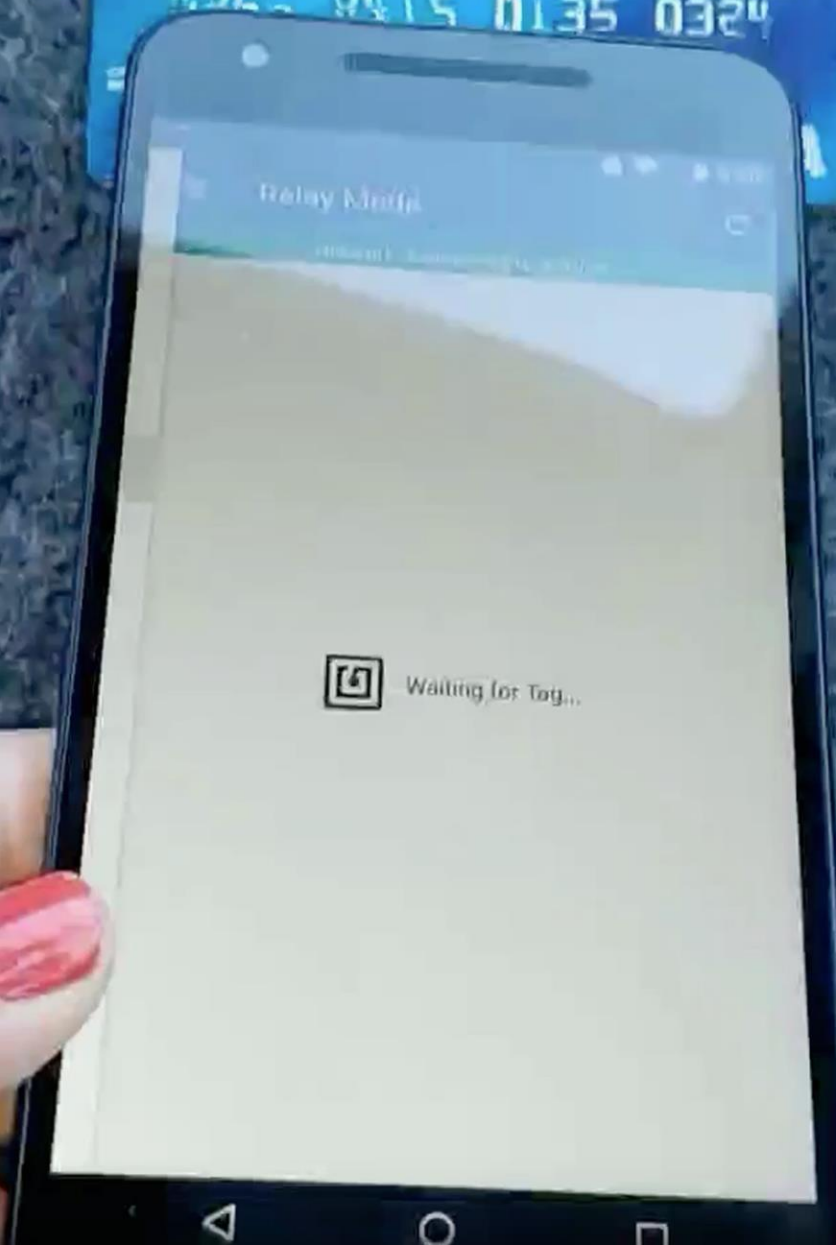
Relays en tecnologías NFC



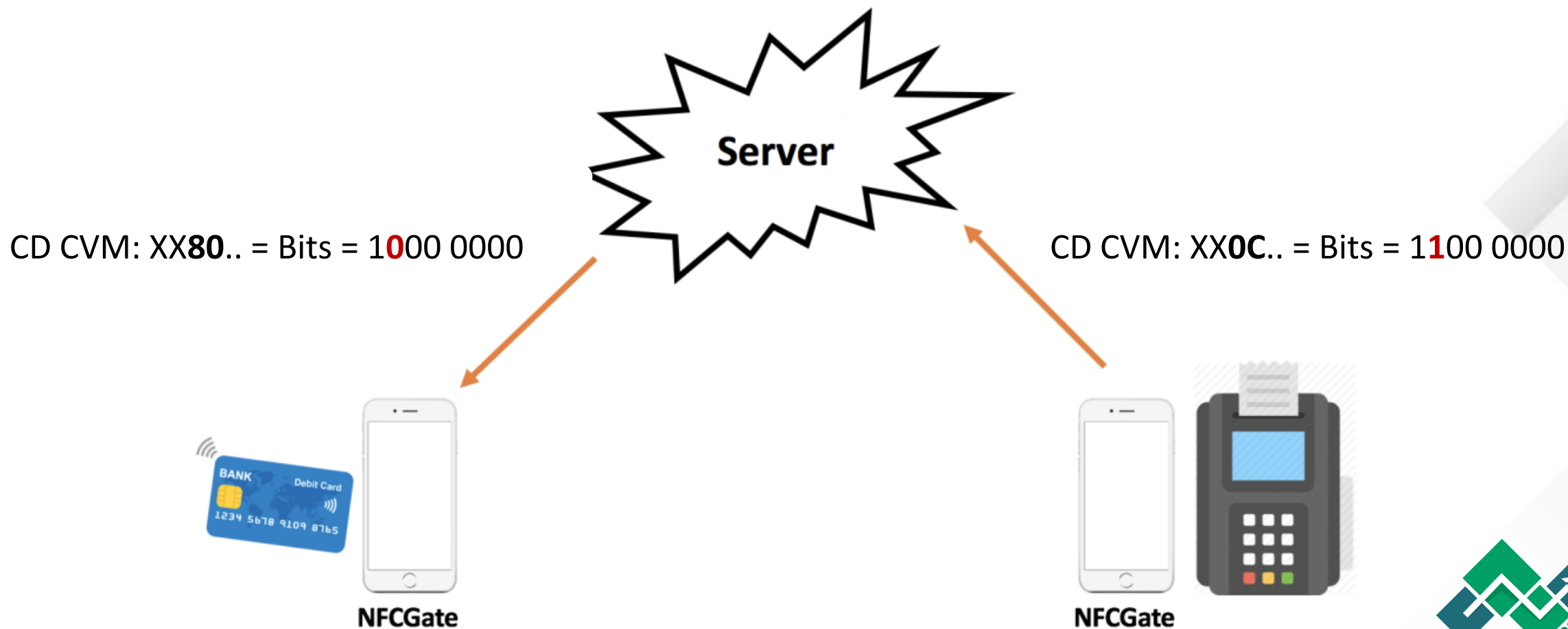
Relays en tecnologías NFC





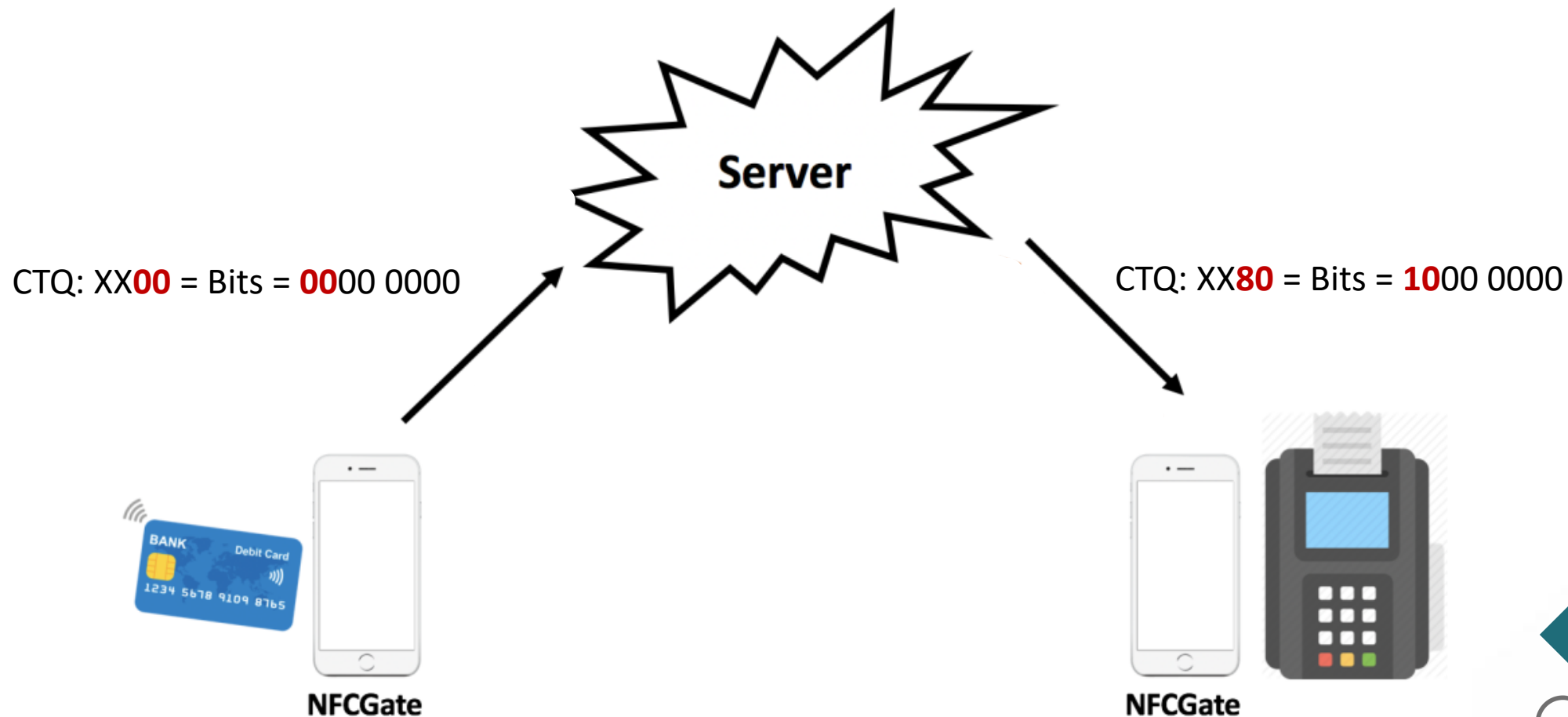


Bypass en el limite de la transacción



Bypassiando el limite de la transacción

Modificar la etiqueta CTQ(9F6C) byte 2 bit 8 de “0” a “1”

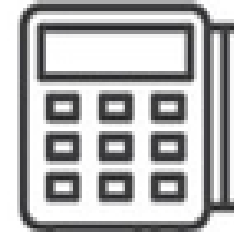


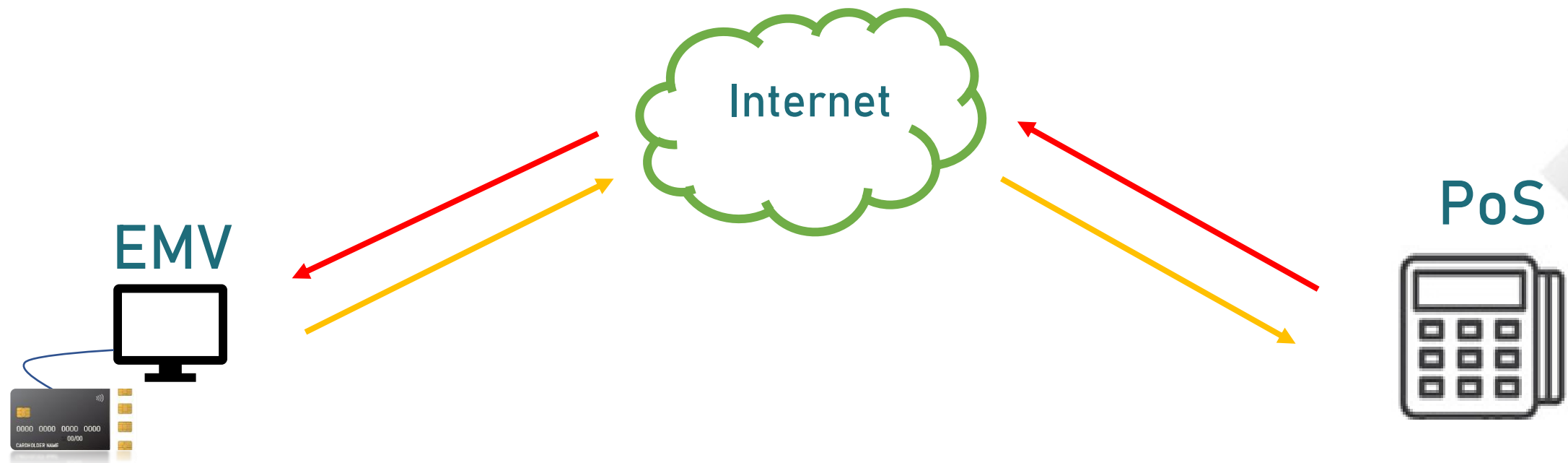


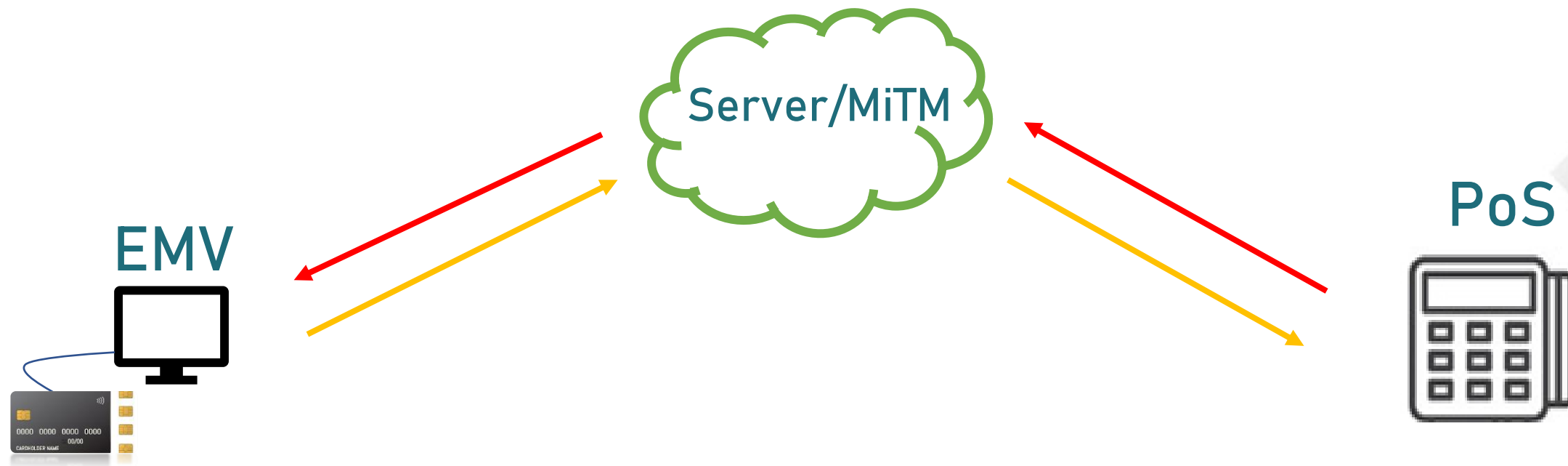
EMV

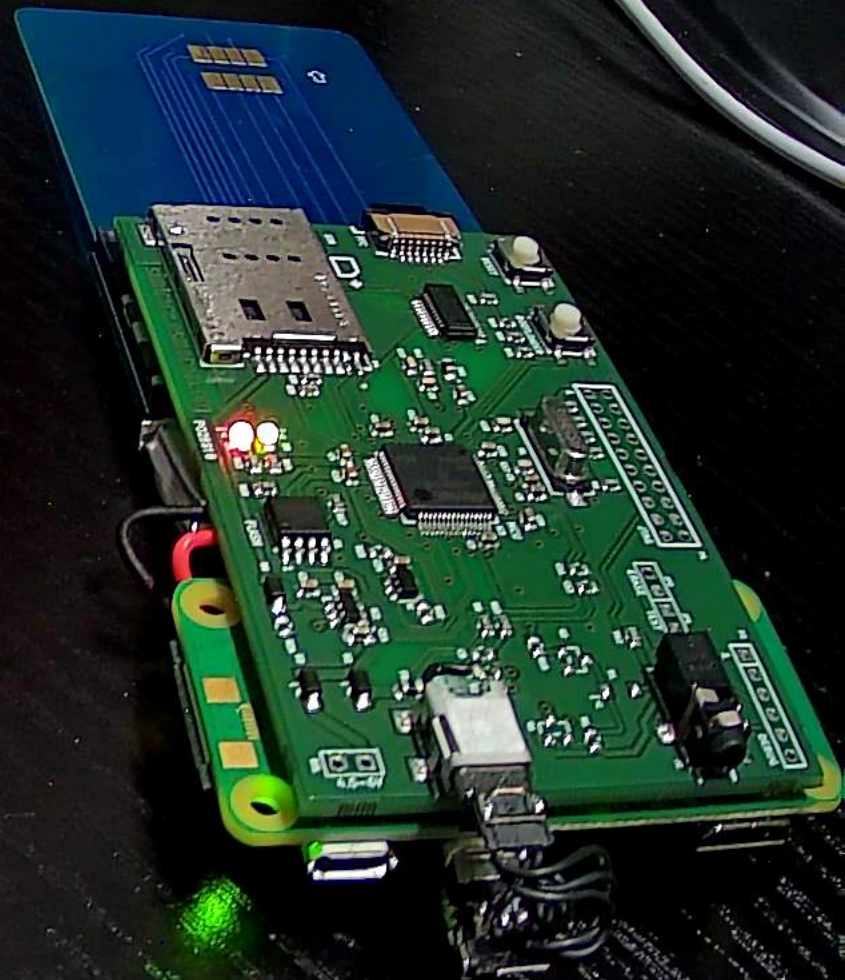


PoS









ISSUER	TERMINAL	CARD	EMV COMMAND	PROTOCOL PHASE
--------	----------	------	-------------	----------------

select file 1PAY.SYS.DOF01

available applications (e.g Credit/Debit/ATM)

SELECT/READ RECORD

select application/start/ transaction

SELECT/
GET PROCESSING OPTIONS

Card authentication

signed records. Sig(signed records)

READ RECORD...

unsigned records

PIN retry counter

GET DATA

PIN: xxxx

VERIFY

Cardholder verification

PIN OK/Not OK

T= (amount, currency, date, TVR, nonce,...)

GENERATE AC

ARQC= (ATC, AID, MAC(T,ATC,IAD))

T, ARQC

Transaction authorization

ARPC. ARC

ARPC. auth code

EXTERNAL AUTHENTICATE/
GENERATE AC

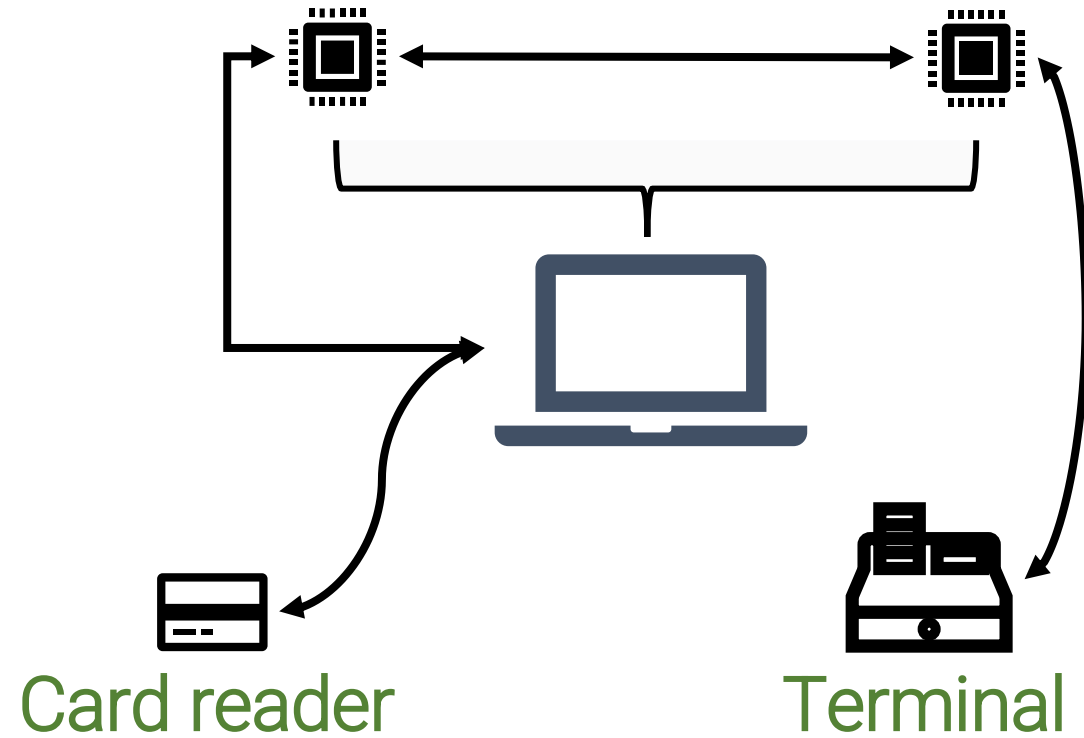
TC= (ATC, AID, MAC(ARC,T,ATC,IAD))

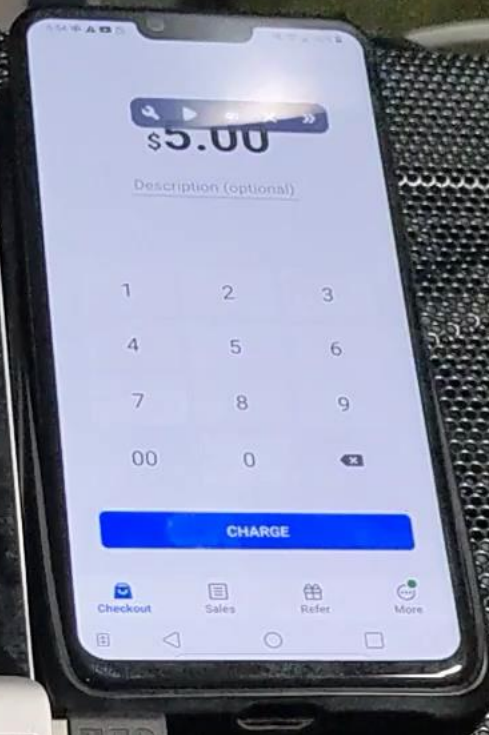
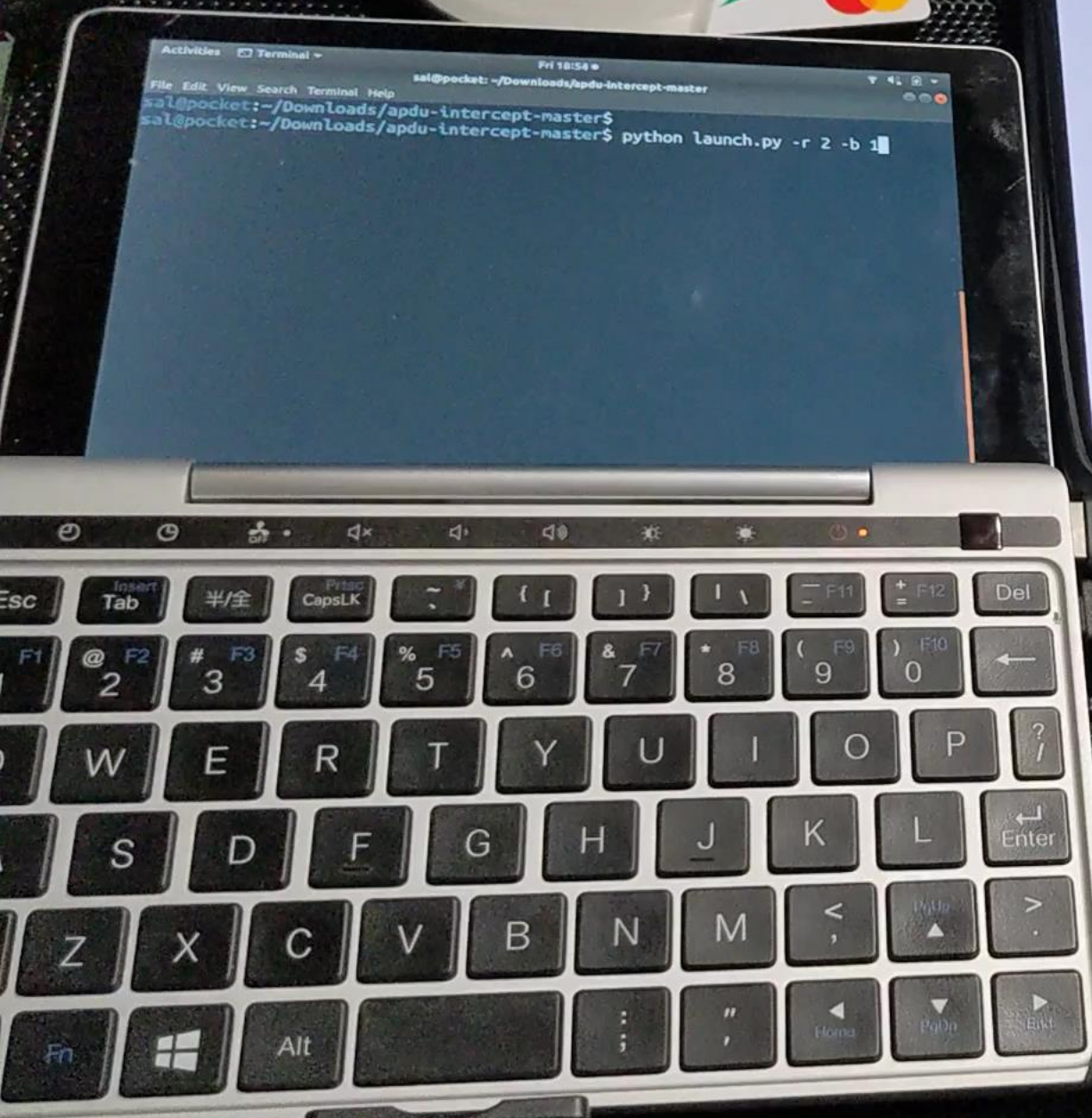
TC

Source: Chip and PIN is Broken

Virtual card reader

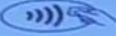
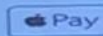
Emulator





Verifone

Tap/Swipe/Insert Payment



SAMSUNG pay



Como podemos mejorar en conjunto

- Entender los ataques actuales y a los atacantes
- Perfilar el comportamiento de nuestros clientes
- Implementaciones correctas desde un inicio
- Verificar lo implementado
- Colaboración nacional e internacional
- Inteligencia de amenazas

Conclusiones

- Las nuevas tecnologías nos ayudan en gran medida a crecer, innovar y proteger datos personales en el mundo transaccional, un adecuado plan de riesgos es elemental en la planeación para el futuro de las empresas.
- Los sistemas de pagos siguen y seguirán siendo un ambiente áspero y difícil de proteger para toda compañía. Una buena planeación, entrenamiento y prevención suelen ser las armas mas adecuadas para evitar abusos de manera proficiente.
- El usar nuevas tecnologías no conlleva a tener menores riesgos si estas no han sido implementadas correctamente. Entender el comportamiento de nuestros clientes y atacantes en ambos lados de las transacciones suele ser primordial en las mejoras detecciones de malas practicas.

Salvador Mendoza

Director of Research and Development
Metabase Q

contact@metabaseq.com
+52 55 2211 0920

// Better Base, Better Future





CLAR

7° Congreso Latinoamericano de Riesgos
SANTA CRUZ DE LA SIERRA – BOLIVIA