IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

Ataques a sistemas de pago: pasado, presente, y… ¿futuro?

CENTRO CRIPTOLÓGICO NACIONAL

ESCUELA DE CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y EVALUACIÓN

Dr. Ricardo J. Rodríguez

Universidad de Zaragoza

e: rjrodriguez@unizar.es

tw: @RicardoJRdez

w: http://www.ricardojrodriguez.es

Índice

1. Introducción (I)

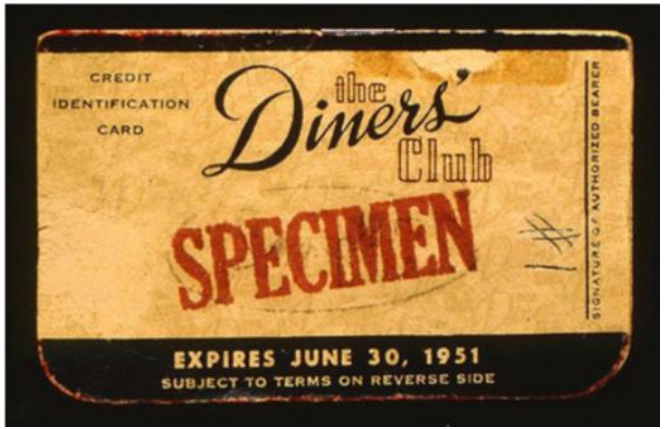
Pagos de “plástico”: *trending topic*

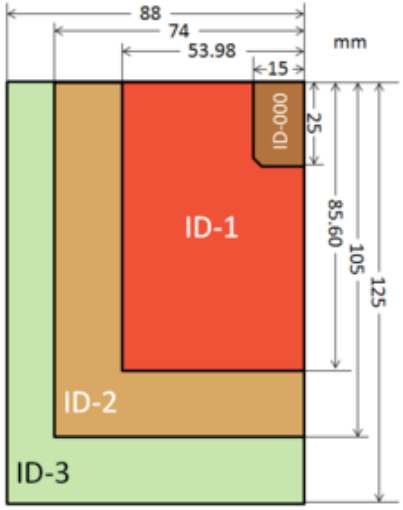
- **Primer método de pago para compras**
  - Cada vez menos gente paga en efectivo
  - Algunos países pretenden eliminar moneda física (e.g., Singapur)
    - Mejorar control de dinero negro
  - **TOP 5** (http://www.totalpayments.org/2013/07/08/top-5-cashless-countries/)
    1. Suecia
    2. República de Somalilandia
    3. Kenya
    4. Canadá
    5. South Korea
  - http://www.cnbc.com/2015/05/15/this-country-is-trying-to-go-cash-free.html
  - http://qz.com/525111/sweden-is-on-its-way-to-becoming-the-first-cashless-society-on-earth/

1. Introducción (II)

Everything happens for a reason

- Forma de tarjeta de crédito/débito: estándar
  - ISO/IEC 7810
    - Dimensiones físicas
    - Resistencia (doblado, fuego, químicos, temp. y humedad)
    - Toxicidad

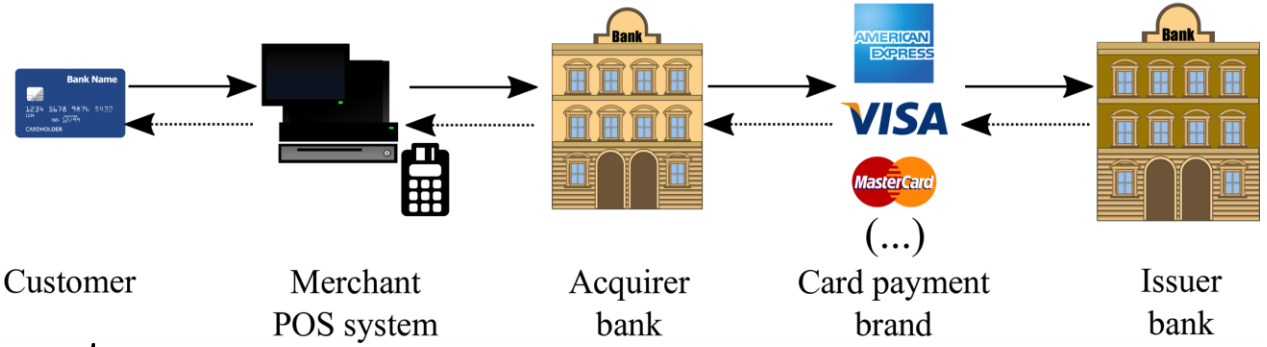




- Tarjetas bancarias:
  - ID-1, 85.60 × 53.98 mm, grosor 0.76 mm

1. Introducción (III)

Flujo (simplificado) de una transacción bancaria



- Diferentes actores
- La información del cliente puede estar en diferentes lugares:
  - En memoria
  - En almacenamiento temporal
  - En tránsito
- Aplicaciones de los sistemas

1. Introducción (III)

Un poquito más de estándares…

- **Payment Card Industry (PCI)**: *garantiza* la seguridad de los sistemas de pago electrónicos
- Dos estándares importantes:
  - **PCI Data Security Standard (PCI DSS)**: determina cómo la información confidencial del cliente se debe proteger por el comerciante y los proveedores de servicio (bancos)
  - **Payment Application Data Security Standard (PA-DSS)**: determina los requisitos software que deben de cumplir las aplicaciones de pago, para cumplir con PCI DSS

1. Introducción (IV)

Interés de los criminales en las tarjetas bancarias

- **Información de tarjeta de crédito/débito**: **++interés++**
  - Ejemplo
    - Tarjetas US: de US$1.50 a US$5.0, según tipo (fuente: Symantec)
      - Se aplican descuentos en compras al por mayor ☺
    - Tarjetas EU: más caras, de $5 a $8
  - *Fullz card*: Información de tarjetas +información adicional del propietario
    - Ejemplos: fechas de cumpleaños, PIN, otros…
    - Permite robo de identidad
    - Precio mayor: hasta US$20 (tarjetas US, fuente Symantec)

1. Introducción (V)

Cyber-ataques en US (2014)

- Ataques ocurridos a empresas norteamericanas en 2014
  - 36% son robo de información de tarjetas de crédito de clientes
    - Mayormente retailers y restaurantes
- **Caso más conocido**: TXJ Companies, Inc., en 2008 (con wardriving)
  - Cifrado WEP en algunas tiendas permitió acceder a su sistema (tienda)
  - Desde ahí, salto hasta los servidores (se almacenaban datos de clientes)
  - 40M de datos relativos a las tarjetas de pago de clientes
  - Albert González, sentenciado a 20 años por estos actos en 2010
- Sniffers de red: actualmente no son una amenaza

1. Introducc

Cyber-ataques

- Ataques oc 4
  - 36% so entes
    - May
- **Caso más** on wardriving)
  - Cifrado stema (tienda)
  - Desde a tos de clientes
  - 40M de
  - Albert G n 2010
- Sniffers de

2. Ataques a tarjetas de pago de banda magnética (I)

Tarjetas de banda magnética: el inicio

- **1969, IBM Information Records Division** (IRD)
- ¿Sabías que…?
  - En realidad, la banda magnética es un código de barras ☺
- MagSpoof: http://samy.pl/magspoof/

2. Ataques a tarjetas de pago de banda magnética (II)

Contenido de la banda magnética

- **Dividido en bandas** (horizontalmente)
- 3 bandas de información (tracks)
  - **Track 1 y track 2**:
    - ISO/IEC 7813
    - Información similar, pero con diferente formato
  - **Track 3**:
    - ISO/IEC 4909
    - THRIFT
    - NO SE USA (¿¿seguro??)
      - Inicialmente, se empezó a usar en Alemania para autorizar las transacciones de débito…

2. Ataques a tarjetas de pago de banda magnética (III)

Contenido de la banda magnética: Track 1

- Establecido por la **International Air Transport Association (IATA)**

SS	FC	PAN	FS	CN	FS	ED	SC	DD	ES	LRC

(tamaño de campos no escalado)

- SS: Start Sentinel (%)
- FC: Format Code
  - carácter [B|b] identifica tarjeta bancaria
- PAN: Primary Account Number (número de tarjeta)
- FS: Field Separator (^)
- CN: Cardholder name
  - Nombre y apellidos del propietario, separados por /
- ED: Expiration Date
  - Formato americano YYMM
- SC: Service Code (3 dígitos)
- DD: Discretionary Data (número de tarjeta)
  - Reservado para el proveedor de la tarjeta
  - Ejemplo: PIN Verification Value (requerido por VISA)
- ES: End Sentinel (?)
- LRC: Longitude Redundancy Check

2. Ataques a tarjetas de pago de banda magnética (IV)

Contenido de la banda magnética: Track 2

- Establecido por la **American Bankers Association (ABA)**

(tamaño de campos no escalado)

- SS: Start Sentinel (;)
- FC: Format Code
  - carácter [B|b] identifica tarjeta bancaria
- PAN: Primary Account Number (número de tarjeta)
- FS: Field Separator (=)
- ED: Expiration Date
  - Formato americano YYMM
- SC: Service Code (3 dígitos)
- DD: Discretionary Data (número de tarjeta)
  - Reservado para el proveedor de la tarjeta
  - Ejemplo: PIN Verification Value (requerido por VISA)
- ES: End Sentinel (?)
- LRC: Longitude Redundancy Check

2. Ataques a tarjetas de pago de banda magnética (V)

Ejemplo de lectura

2. Atac

Ejemplo

Frequently

i These item

This ite

MSR605

TMS® 7

MSR Utility Program (for HID & Bluetooth) v3.01

Message

Read Card <1> OK!

Track1 7 BPC Odd Parity 78

%B49[redacted]940^RODRIGUEZ FERNANDEZ/R. J.
^1811[redacted]135428?

Track2 5 BPC Odd Parity 39

;49[redacted]940=1811[redacted]400000?

Track3 5 BPC Odd Parity 106

;0149[redacted]940=724978[redacted]040
[redacted]18110=2085[redacted]1341==1=0000000000000
000?

Connect Device

HID

R/W: REVH2.39

Card

Lo

H

READ CARD

Please Swipe Card
Swipe Counter ->

2

Cancel

W

W

From File | To File

Seq. Write | Compare

Erase | Copy

Config... Device | Config... Bluetooth

Set Password

Exit

2. Ataques a tarjetas de pago de banda magnética (VI)

Desde terminales o cajeros

- **Skimming**
  - Micro cámara + MSR
  - Micro cámara + pad skimming

2. Ataques a tarjetas de pago de banda magnética (VII)

Desde sistemas POS

- **88% de sistemas de venta usan algún tipo de Windows**
  - A. Bodhani, "*Turn on, log in, checkout*," Engineering Technology, vol. 8, no. 3, pp. 60–63, April 2013
- **Fácil "reconvertir" conocimiento de desarrollo de malware**
  - POS RAM Scraping malware
  - Funcionamiento (abstracción):
    1. Leer procesos activos en la máquina comprometida
       - APIs: *CreateToolhelp32Snapshot, EnumProcesses, ZwQuerySystemInformation*
    2. Abrir proceso
       - *OpenProcess*
    3. Leer zonas de memoria del proceso, buscando patrón de Track 1/Track 2
       - *ReadRemoteProcessMemory*
       - Expresiones regulares, o comparación byte a byte

2. Ataques a tarjetas de pago de banda magnética (VIII)

Taxonomía de POS RAM scraping malware (1)

- **Protección del binario**
  - Protegido / no protegido
- **Persistencia en el equipo**
  - Basada en el registro (claves autorun)
  - Servicio de Windows
    - Ejecución transparente, dificulta la detección
  - Sin persistencia
- **Funcionalidad**
  - Tipo botnet (recibe comandos y actúa) / aislado

2. Ataques a tarjetas de pago de banda magnética (IX)

Taxonomía de POS RAM scraping malware (2)

- **Búsqueda de procesos**
  - Tipo de búsqueda: selectiva (whitelist / blacklist) / no selectiva
  - Funciones de búsqueda: APIs / ad-hoc
- **Información sensible**
  - Tipo de información buscada: Track 1 / Track 2 / ambas
  - Método de búsqueda: regex / algoritmo propio

2. Ataques a tarjetas de pago de banda magnética (X)

Taxonomía de POS RAM scraping malware (3)

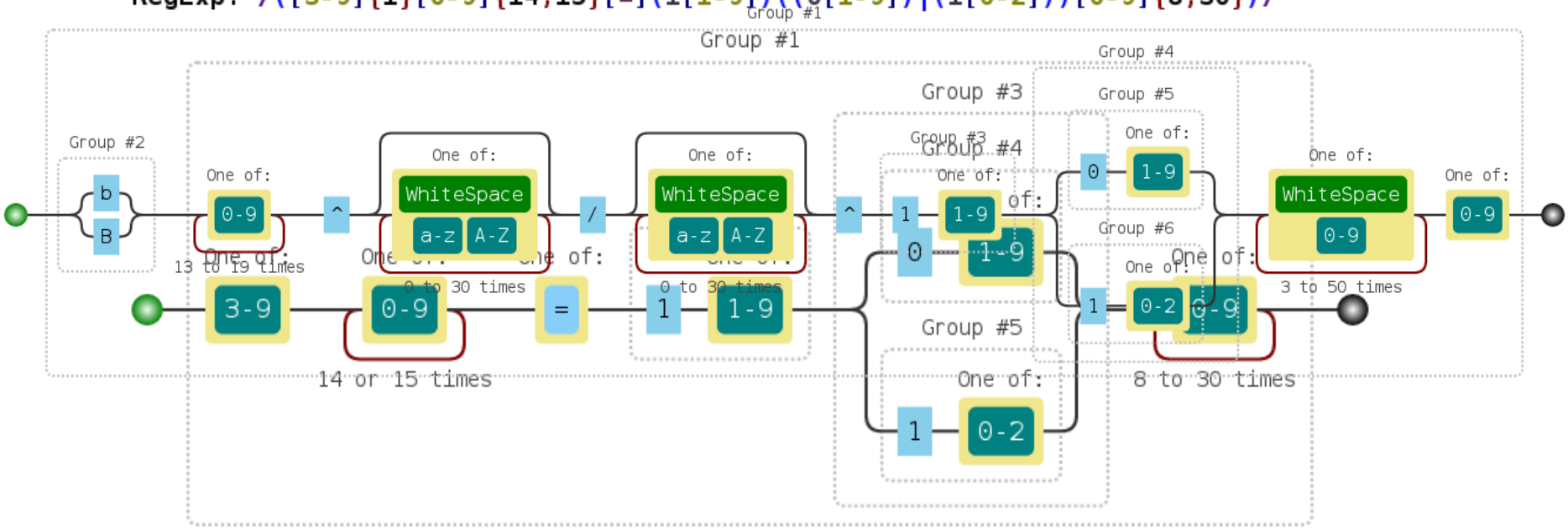
- **Exfiltración de información**
  - En plano / codificada / cifrada
- **Método de exfiltración**
  - Basado en la máquina: ficheros / USB
  - Basados en Internet: HTTP(S) GET/POST / DNS / FTP / correo / otros
- **Conexión para la exfiltración**
  - Ninguna
  - Anónima (e.g., TOR)
  - No anónima

2. Ataques a tarjetas de pago de banda magnética (XI)

Ejemplos de expresiones regulares

RegExp: /((b|B)[0-9]{13,19}\^[A-Za-z\s]{0,30}\/[A-Za-z\s]{0,30}\^(1[1-9])((0[1-9])|(1[0-2]))[0-9\s]{3,50}[0-9]{1})/

RegExp: /([3-9]{1}[0-9]{14,15}[=](1[1-9])((0[1-9])|(1[0-2]))[0-9]{8,30})/



2. Ataques a tarjetas de pago de banda magnética (XII)

Algunas conclusiones… (1)

- **Rápido incremento de familias maliciosas contra sistemas POS**
- Curiosamente, **muy pocas protegidas (!!)**
  - Sólo 5 con UPX ☺
  - Lenguajes de programación: destacan C++ y Delphi
- Únicamente **dos familias sin persistencia**
  - ¿Lanzadas por otro malware?
  - **13 familias usan claves de registro**
  - **NitlovePOS: usa NTFS ADS para ocultarse** (método anti-forense)
- **La mitad de ellas presentan características de botnet**

2. Ataques a tarjetas de pago de banda magnética (XIII)

Algunas conclusiones… (2)

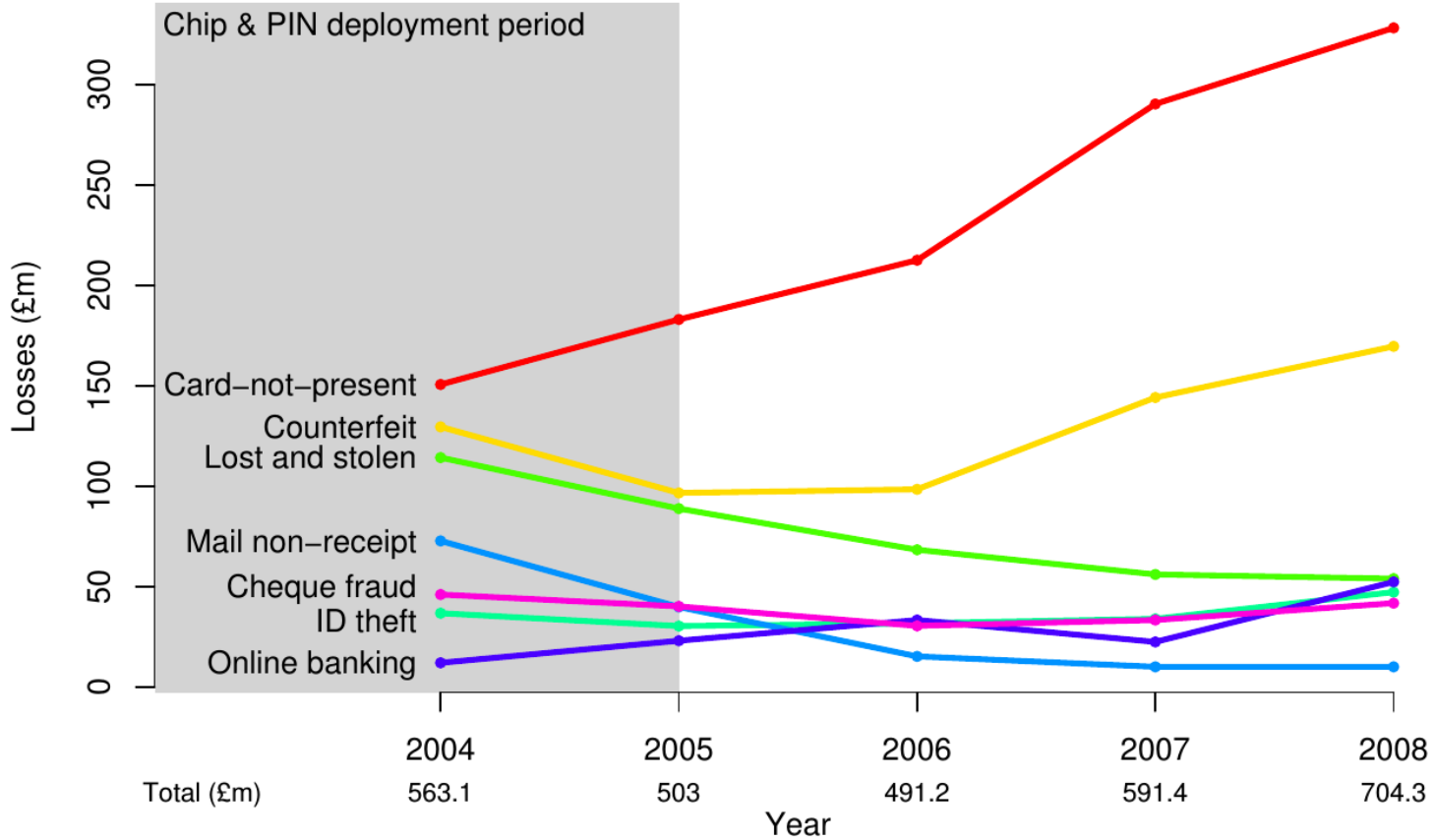
- **Tres de ellas hacen búsqueda de procesos específicos**
  - Conocimiento previo del sistema a atacar
  - Muchas familias implementan el algoritmo Luhn (ISO/IEC 7812-1)
- **Todas las familias usan APIs**
  - Para evitarlo sería necesario un malware tipo rootkit
- **Interesadas en Track 2, o ambas**
- **Muy pocas usan regex**
  - Fácil de detectar… (strings)
- **Destaca el método HTTP POST, algunas pocas usan DNS**
- **Sólo dos familias usan TOR**

3. Ataques a tarjetas de pago de chip (I)

Tarjetas EMV, o "chip & pin"

- **Objetivo**: reducir el fraude de tarjetas
  - Estándar de 1993/1994, fechas de despliegue varían (e.g., 2003 en UK)
- **Cambio de la responsabilidad ante fraude**:
  - *Del comerciante, si no se usa una tarjeta EMV*
  - *Del cliente, si se usa el PIN*

3. Ataques a tarjetas de pago de chip (II)



3. Ataques a tarjetas de pago de chip (III)

Resumen rápido del protocolo EMV (1)

- **Estándar dividido en 4 libros (700 páginas aprox.)**
- **4 métodos de autenticación de la tarjeta**
  - **Online**: la transacción se autoriza en la red del banco
  - **Offline**: SDA / DDA / CDA
- **6 métodos de verificación del propietario**
- **2 tipos de transacciones**: **online / offline**

Method
Fail CVM processing
Plaintext PIN verification
Enciphered online PIN verification
Plaintext PIN verification and Signature verification
Enciphered offline PIN verification
Encipher PIN verification and Signature verification
Signature verification
No CVM needed

TODO configurable por el cliente final…

¡ALTA COMPLEJIDAD!

3. Ataques a tarjetas de pago de chip (IV)

Resumen rápido del protocolo EMV (2)

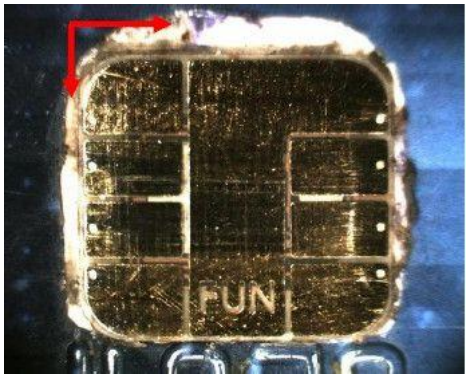
- **Pasos del protocolo**
  1. Inicialización
  2. Autenticación de la tarjeta
  3. Verificación del propietario de la tarjeta
  4. Transacción

¿Falta algo?

3. Ataques a tarjetas de pago de chip (V)

Breve resumen de ataques

- **Skimming**
  - La información de la banda magnética también está en el chip
- **Clonado de tarjetas SDA**
  - YES-cards
  - SDA no permitido en tarjetas con transacciones offline
- **DDA Man-in-the-middle**
- **Ataque rollback**
  - Forzar a autentificar con PIN en texto plano
- **Ataque preplay**
  - Números aleatorios con baja entropía, o consecutivos!



4. Ataques a tarjetas de pago sin contacto (I)

Protocolo EMV para pago sin contacto

- Estándar **dividido en cuatro libros**
- **Siete variantes del C** (Kernel Specification)
  - **Cada distribuidor de tarjetas diferente, alguno hasta varios…**
- NFC: basado en el protocolo **ISO/IEC 14443**
- **NFC no es más que una interfaz de acceso al chip**
  - **Más "rápido"**
  - **Más interactivo**: no hay PIN (para compras menores de 20€)

- **Problemas de EMV (tarjetas de chip) + problemas de NFC!!**

4. Ataques a tarjetas de pago sin contacto (II)

Vulnerabilidades de NFC (1)

- **Eavesdropping**
  - Primary Account Number (PAN)
  - Nombre del propietario
  - Fecha de expiración
  - Historial de transacciones

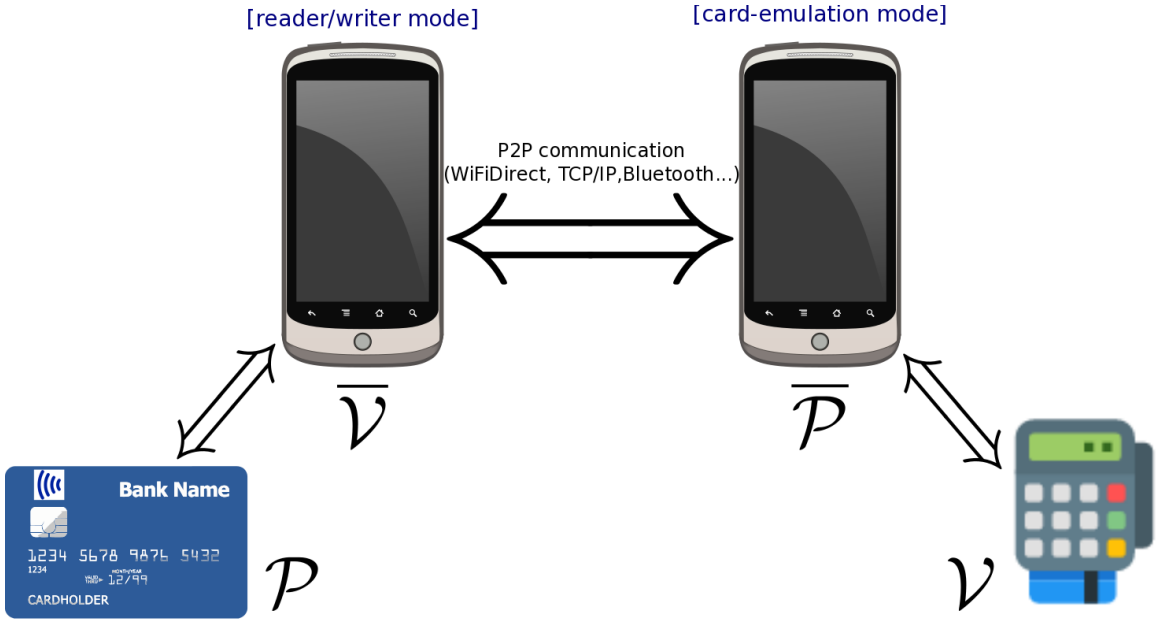
- **Últimas versiones de tarjetas ya no devuelven nombre ni historial**
  - Accesible mediante otros comandos EMV

DEMO TIME!

4. Ataques a tarjetas de pago sin contacto (III)

Vulnerabilidades de NFC (2)

- **Ataques de retransmisión**



(Os lo contamos en la pasada edición de STIC CCN-CERT ;))

5. Conclusiones y referencias (I)

Algunas conclusiones…

- **Evolución de las tarjetas bancarias:**
  - **Banda magnética ➔ Chip&PIN ➔ NFC**
- **Ataques a sistemas de pago**
  - Cada sistema tiene sus propias vulnerabilidades
  - Skimming
  - Malware: POS RAM scraping malware
- **¿Qué vamos a ver en el futuro?**
  - **Nuevos (y sofisticados) métodos de skimming**
  - **Malware de móviles con NFC para robar datos de tarjetas NFC**
  - **….** [TO BE FILLED IN BY CRIMINALS]

5. Conclusiones y referencias (II)

Referencias (1)

- Bond, M. et al.; **Be Prepared: The EMV Preplay Attack**. In *IEEE Security & Privacy*, 2015, 13, 56–64
- Murdoch, S. et al.; **Chip and PIN is Broken**. In *IEEE Symposium on Security and Privacy*, 2010, 433–446
- Bond, M. et al.; **Chip and Skim: Cloning EMV Cards with the Pre-play Attack**. In *IEEE Symposium on Security and Privacy*, 2014, 49–64
- Anderson, R. & Murdoch, S. J.; **EMV: Why Payment Systems Fail**. In *Commun. ACM*, ACM, 2014, 57, 24–28
- de Ruiter, J. & Poll, E.; **Formal Analysis of the EMV Protocol Suite**. In *Theory of Security and Applications*, Springer Berlin Heidelberg, 2012, 6993, 113–129
- Adida, B. et al.; **Phish and Chips**. In *Proceedings of the 14th Int. Workshop on Security Protocols*, Springer, 2009, 5087, 40–48
- Gomzin, S.; **Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions**. John Wiley & Sons Inc., 2014
- Rantos, K. & Markantonakis, K.; **Analysis of Potential Vulnerabilities in Payment Terminals Secure Smart Embedded Devices**. In *Platforms and Applications*, Springer New York, 2014, 311–333
- Frisby, W. et al.; **Security Analysis of Smartphone Point-of-sale Systems**. In *Proceedings of the 6th USENIX Conference on Offensive Technologies*, USENIX Association, 2012, 1–12

5. Conclusiones y referencias (III)

Referencias (2)

- Haselsteiner, E. & Breitfuß, K.; **Security in Near Field Communication (NFC) – Strengths and Weaknesses**. In *Proceedings of the Workshop on RFID Security and Privacy (RFIDSec)*, 2006
- Emms, M. et al.; **Risks of Offline Verify PIN on Contactless Cards**. In *Financial Cryptography and Data Security*, Springer Berlin Heidelberg, 2013, 7859, 313–321
- Chothia, T. et al.; **Relay Cost Bounding for Contactless EMV Payments**. In *Proceedings of the 19th International Conference on Financial Cryptography and Data Security (FC)*, 2015
- Sanders, R.; **From EMV to NFC: the contactless trail?**. *Card Technology Today*, 2008, 20, 12-13

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en Linked in