XXVI Congreso de Seguridad Bancaria
CELAES 2011

Fortificación Lógica de Cajeros

Alfonso del Castillo
15 de Septiembre 2011
acastillo@s21sec.com

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

FLORIDA INTERNATIONAL
FIBA
BANKERS ASSOCIATION

Indice

- Riesgos en autoservicios
- Securización de cajeros
  - Protección por capas
- Riesgos TPV-PC
- ¿Qué podemos hacer?
- ¿Quiénes somos?

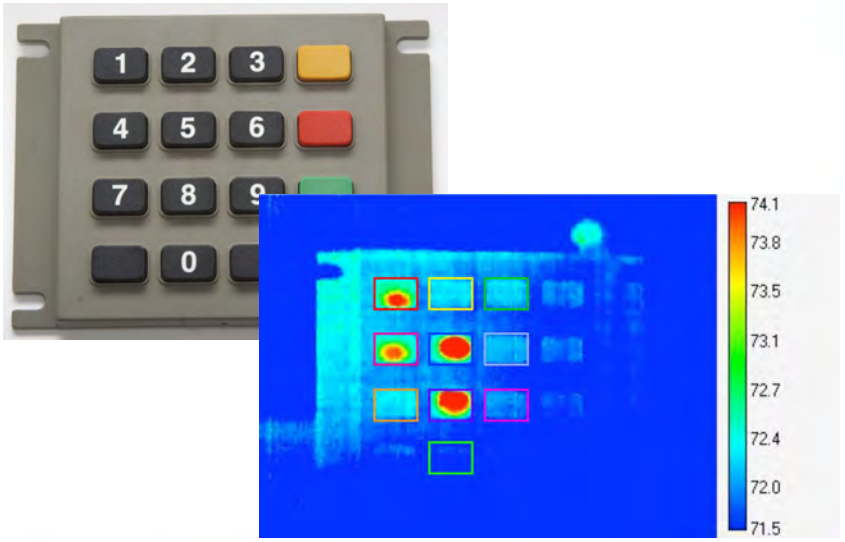
Riesgos en autoservicios

1.1 Algunos datos

- Pérdidas en cajeros cercanas a 500 millones de €
- + de 400.000 incidentes de seguridad en cajeros en 2010 en Europa:
  - Obtención de PIN por el medio que sea
  - Shoulder surfing
  - Cámaras
  - Skimming
  - PINPAD falso
  - Robo al usuario
  - Engaño
- Ataques tradicionales / soluciones tradicionales

Riesgos en autoservicios

1.1 Algunos datos



1.2 Ataques lógicos: Otro problema, otra solución

- Redes de ATM cada mes más conectadas como el resto de redes (IP, Windows, etc.)
- Las redes de cajeros se enfrentan así a los mismos problemas que cualquier PC:
  - MALWARE (troyanos especialmente diseñados) introducido vía red o dispositivos USB
  - Ataques de red: ARP-poisoning
  - Ataques de PIN cash-out : localización de la BBDD en la infraestructura del banco y copiado de detalles de tarjeta y PIN …. **No es nuevo, *USA 2008: OmniAmerican Credit Union y Global Cash Card***
- STUXNET: ¿La próxima amenaza?

Securización de Cajeros
Aproximación por capas

- Protección en varios niveles:
  - Sistema Operativo
  - Aplicación
  - Procesos
  - Red
  - Ficheros
- Monitorización de la actividad en remoto
- Generación de alertas

2.1 Sistema Operativo

- Importancia del nivel de actualizaciones de seguridad del Sistema Operativo
- Posibilidad de actualizar en remoto el Sistema.
- Restricciones de software vulnerable instalado
- Proteger de claves del registro
- Control de introducción de sistemas removibles (USB, CD-ROM,…)
- Control de introducción/extracción de teclado USB

2.2 Sistemas Operativo
Detección Malware

- ¿Soluciones basadas en antivirus? ¿Si o no?
  - Evitar carga de la máquina, esencial en entorno ATM con pocos recursos
  - Firmas: Son dependientes del reconocimiento unívoco del malware
    Solo el año 2010 alrededor de 20 millones de nuevos virus
  - Patrones de comportamiento del malware
  - Análisis del disco duro lo menos intrusivo posible en operativa, cuando no se esté utilizando.
  - Análisis de Procesos, Memoria, Ficheros y registro

2.2 Aplicación

- Parametrización de alertas de periféricos del cajero dependiendo de la plataforma.
- Verificación de PID que accede a drivers del cajero
- Acceso a periféricos solo desde la aplicación del cajero
- Control de conexión/desconexión del dispensador y PINPAD
- Protección de contraseñas modo supervisor
- Listas blancas de aplicaciones que pueden ejecutarse en el cajero
- Alarmas en base a sensores antivandalismo (Dispensador/ EPP/ Lector Tarjetas/ Ingresador/ Giróscopos) (dependiente modelo ATM)

2.3 Procesos y ficheros

- Es necesario controlar los procesos que corren el en sistema y los ficheros mas críticos, creando firmas.
- Es necesario monitorizar/impedir cambios en DLLs del sistema (creación de ocultas)
- Es necesario proteger ficheros críticos (no envío excepto a direcciones autorizadas, nunca permitir extracción a USB
- Recolección de logs de Seguridad y envío de alertas

2.4 Red

- Ataques en la capa de red pueden llevar a cambios en la configuración de red del Sistema Operativo con el objeto de que el cajero apunte hacia direcciones IP no permitidas
- Monitorización del archivo /etc/hosts
- Filtrado con reglas de acceso a/desde direcciones IP concretas y desde binarios concretos.
- Evaluación de la conectividad con distintos dispositivos (router por ARP, HOST por IP) incluyendo verificación de modificación de ARP (ARP poisoning) del router por defecto y cambios DNS si es pertinente.
- Alerta por modificación de configuración de red.
- Protección física del router (robos)

Riesgos TPV-PC

Múltiples riesgos encontrados a raíz de distintos análisis forenses

- TPVs-PC residentes en los mismos segmentos de red que cualquier otro equipo informático del comercio, con el consiguiente riesgo de intrusión.
- Routers ADSL incluyen WiFi con cifrado WEP, siendo altamente vulnerables.
- Políticas de contraseñas débiles.
- No hay registros de auditoría, no se guardan logs.
- No hay antivirus instalados.
- Lectura de banda magnética a través de dispositivo USB que se comporta como un teclado, abriendo la puerta a usar *keylogger* o troyanos.
- Aplicaciones de TPV-PC guardan datos de la banda magnética.
- TPVs-PC utilizados para otros fines tales como navegación por Internet.

¿Qué podemos hacer?

- Actuaciones
  - Adopción completa de EMV
  - Análisis de malware
  - Recuperación información robada
  - Procesamiento información - RAPIDEZ
  - Compartir información sobre Puntos de Compromiso
- Monitorización de fraude
  - Herramientas comerciales
  - Análisis manual
  - Monitorización comercios alto riesgo / localizaciones riesgo
  - Creación y revisión de patrones de fraude
- Cooperación con fuerzas de seguridad
- “Educación a nuestros clientes”

¿Qué podemos hacer?

Existentes en tarjetas Visa - hasta julio de 2011

1. **Chip opcional –** La información almacenada en un chip está protegida por encriptación. El chip funciona junto con la firma del titular de la tarjeta o número PIN para que el pago sea más seguro.
2. **Número de tarjeta en relieve o impreso –** Los números de tarjeta son de hasta 16 dígitos, comienzan con un 4 y se agrupan en cuatro grupos de cuatro números. Las tarjetas cuyo número está impreso no se muestra completo, aparece parcialmente.
3. **Elemento ultravioleta "paloma" –** Cuando se coloca bajo una luz ultravioleta, una paloma impresa con tinta ultravioleta será visible en el centro de la tarjeta.
4. **Holograma Visa paloma 3D –** Cuadro de holograma 3D contiene una paloma, que se mueve cuando se inclina la tarjeta.
5. **Logotipo de Visa –** Bandera: franja azul - logotipo de Visa sobre fondo blanco y franja dorada – aparece en la esquina derecha, superior o inferior. Tiene un borde con microtexto de seguridad de puntos, utilizado para fines de seguridad forense.
6. **Carácter de seguridad en relieve "V" –** Aparece junto a la fecha de caducidad en las tarjetas en relieve.
7. **Fecha de vencimiento –** Cada tarjeta debe tener una fecha de vencimiento como mínimo.
8. **Nombre del titular o nombre de identificador –** Nombre del titular de la tarjeta o la descripción como "Club de miembros", "Tarjeta de regalo", etc ... son opcionales y pueden aparecer en la parte frontal de la tarjeta.
9. **Impresos los cuatro primeros dígitos del número de tarjeta –** debajo del número de tarjeta. Estos cuatro dígitos aparecen impresos en el recibo del minorista.
10. **Valor de verificación de la tarjeta (CVV2) –** Puede aparecer ya sea en el panel de firma o al lado.

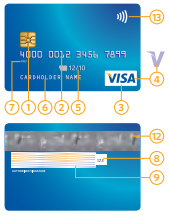
V PAY Cards

11. **El panel de firma –** El panel de la firma debe figurar en el reverso de la tarjeta. Sobre el fondo del panel tiene el logo "Visa".
12. **Chip obligatorio –** Las tarjetas V PAY siempre tienen un chip que contiene información cifrada. El chip funciona junto con el número PIN del titular de la tarjeta para hacer que el pago sea más seguro.
13. **Logo V-PAY –** letra "V" en color azul y oro sobre fondo blanco, leyenda "PAY" en blanco sobre fondo azul. Son posibles diferentes opciones de ubicación del logotipo y la orientación vertical de la tarjeta.
14. **Elemento ultravioleta "V" –** Cuando se coloca bajo una luz ultravioleta, la letra "V" impresa en tinta ultravioleta será visible sobre el logotipo V PAY.

Nota: Estos, junto con la banda magnética en la parte posterior, son las únicas características obligatorias de una tarjeta V PAY. Todo lo demás son opcionales, incluyendo el panel de firma, número de tarjeta, fecha de vencimiento y el nombre del titular.

Nueva Tarjeta Visa

XXXX-XXXX-X-XXXX-XX-XX



1. **Chip opcional –** La información almacenada en un chip está protegida por encriptación. El chip funciona junto con la firma del titular de la tarjeta o número PIN para crear un pago más seguro.
2. **En relieve o impresos número de cuenta –** Los números de tarjeta son de hasta 16 dígitos, comienzan con un 4 y se agrupan en cuatro grupos de cuatro números. Las tarjetas cuyo número está impreso no se muestra completo, aparece parcialmente.
3. **Logo Visa –** logotipo azul y oro sobre un fondo blanco. Más opciones de ubicación del logotipo y la orientación vertical de la tarjeta y el logotipo son ahora posibles.
4. **Elemento ultravioleta "V" –** Cuando se coloca bajo una luz ultravioleta, una "V" impresa en tinta ultravioleta será visible sobre el logotipo de Visa.
5. **La fecha de vencimiento –** Cada tarjeta debe tener una fecha de vencimiento, como mínimo.
6. **Titular de la tarjeta el nombre o identificador –** Nombre del titular o la descripción como "Club de miembros", "Tarjeta de Regalo", etc son opcionales y pueden aparecer en la parte frontal de la tarjeta.
7. **Impresos los cuatro primeros dígitos del número de tarjeta –** aparecen bajo el número de tarjeta. Estos cuatro dígitos aparecen impresos en el recibo del minorista.
8. **Valor de verificación de la tarjeta (CVV2) –** Puede aparecer ya sea en el panel de firma o al lado.
9. **El panel de firma –** El patrón visible en el panel de firma se puede personalizar, pero siempre lleva el logo "Visa", repetido en tinta ultravioleta y visible bajo esta luz. La longitud del panel de firma variará dependiendo del tipo de tarjeta.
10. **Holograma Visa paloma 3D –** Contiene una paloma, que se mueve al inclinar la tarjeta. En lugar del holograma de la paloma que está en el frente puede tener un holograma de la paloma de menor tamaño en la parte posterior.
11. **Un mini holograma Visa paloma 3D –** Puede aparecer en el reverso de la tarjeta y puede ser ubicado en cualquier lugar dentro del área indicada. El holograma paloma Visa que aparece en la parte posterior de la tarjeta no es de tamaño estándar.
12. **Holograma Visa en banda magnética –** La banda magnética holográfica Visa con las palomas en vuelo reemplaza el holograma cuadrado 3D en la parte frontal de la tarjeta.
13. **Indicador de contacto –** Cuando este símbolo aparece en un producto Visa, indica que es compatible con las transacciones sin contacto físico de la tarjeta.

Nueva Tarjeta Visa variaciones – desde Marzo de 2006

GUARDIA CIVIL

VISA

Guía para la lucha contra el fraude y falsificación de medios de pago

Este tríptico ha sido diseñado con la finalidad de servir de apoyo a los Agentes de las Fuerzas y Cuerpos de Seguridad de Estado, en la detección de medios de pago falsificados, así como para identificar los sistemas utilizados para la obtención de los datos que se incluyen en las bandas magnéticas de las tarjetas bancarias junto con sus números PIN.

¿Qué podemos hacer?

¿Qué podemos hacer?

¿Quiénes somos?

Mikel F.

Mikel Fernández preparó el terreno en el año 2000

270

El equipo de especialistas en seguridad más grande de España. 270 personas con el objetivo y la pasión por la seguridad.

Labs

S21sec labs: El primer Centro Europeo I+D+i en Seguridad.

eCrime

Especialistas en eCrime.
90% España
85% UK
Otros
Una de las 4 mejores compañías en el mundo según Gartner, 2011.

24/7

Protección y prevención 24/7/365

Bitacora

Plataforma Integral de Gestión de la Seguridad.

Cert®

International

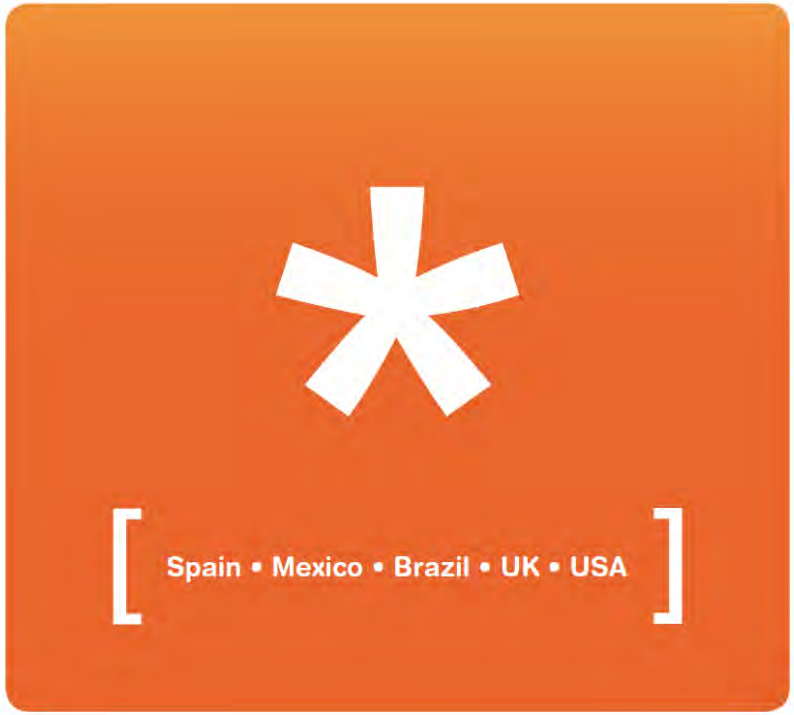
S21sec presencia mundial: España (8), Brasil, Mexico (2), UK, Panamá y USA.

Mensualmente se generan trabajos para 27 países

SOC

Primer centro de operaciones de seguridad en España

*[Gracias]



S21sec