Aplicaciones para Smart Cards

Realización de un sistema de ticket inteligentes para la entrada a eventos (partidos de fútbol, conciertos, ferias...etc).

BAJO NINGÚN CONCEPTO ESCRIBIR EN LOS Lock bytes ni en los OTP DE LA TARJETA

Se trata de realizar la simulación de un sistema de entradas o tickets inteligentes para eventos, utilizando la tarjeta mifare ultralight.
Utilizaremos la mifare ultralight C, pero sin hacer uso de sus características avanzadas (autenticación, protección de lectura y escritura...etc).
Es decir el proyecto que hagamos deberá funcionar en una ultralight sin necesidad de hacer cambios, aunque nosotros para probarlo usemos una ultralight C.

Para simular el sistema de smart ticket realizaremos dos scripts que llamaremos: **expedicion** y **puerta**.

expedicion: es el script que simula la creación del billete al usuario, quién lo abonará por el medio dispuesto al efecto. El billete será una tarjeta mifare ultralight, con una serie de campos escritos según la siguiente especificación:

> Página 04: FYES (en ASCII) (4 octetos indica billete válido) ó 0NOT (en ASCII) (4 octetos indica billete inválido)

Página 05: Código del evento (4 octetos con ún código que indica el evento al que pertenece el billete). Se pone por ejemplo a F001 en ASCII.
Página 06: Día y mes del evento en ASCII --> Ej. 26 de Febrero --> 32363032H
Página 07: Año del evento en ASCII --> Ej.- 1025 --> 31303235H
Página 08: Número de grada (4 dígitos en ASCII) --> Ej.- 1048 --> 31303438H
Página 09: Número de asiento (2 dígitos en ASCII, se escribe duplicado) -->Ej.- asiento 62 --> 36323632H
Página 0A: Código del vendedor (4 dígitos en ASCII) Ej.- Se pone a V001 en ASCII.
Página 0B: MAC (4 bytes). Calculado según lo siguiente:

El terminal del vendedor dispone de una clave maestra 3DES: KML = 0011223344556677, KMR = 8899AABBCCDDEEFF

El terminal de expedicion pide el número de serie a la tarjeta que son 7 bytes, lo rellena con FFH a la derecha para que sean 8 bytes y lo cifra con 3DES y ECB así obtendrá la clave por tarjeta.
Para calcular el MAC concatena las páginas 04|05|06|07|08|09|0A , y rellena a ceros para múltiplo de 8 con el método 2 (80 seguido del número de ceros necesarios). Utilizando como vector de inicialización la propia clave por tarjeta, cifra la concatenacion de páginas 04 a 0A con la clave por tarjeta. El MAC serán los cuatro bytes más a la izquierda de los últimos 8 bytes.

El terminal expedicion escribe en la tarjeta, en claro, las páginas 04H a 0BH, donde la última es el MAC.

puerta: es el script que simula la función del lector de billetes en la puerta de entrada.

El terminal de puerta dispone de la clave maestra 3DES: KML =

0011223344556677, KMR = 8899AABBCCDDEEFF
El terminal le pide el número de serie a la tarjeta la rellena por la derecha con FFH y calcula la clave de la tarjeta cifrándolo con 3DES.

Lee la página 04 y si es FYES entonces lee la página 0B de la tarjeta, y la compara con el MAC calculado por él (de la misma forma que lo calculó el vendedor) y si no coinciden, da un mensaje de error (en forma de luz roja parpadeante y un pitido adecuado... je je) y no abre.
Si lee la página 04 y lleva escrito 0NOT directamente da un mensaje de error (en forma de luz roja parpadeante y un pitido adecuado... je je).
Para cualquier otro valor leído de la página 04 dará un error.

Si lee la página 04 y tiene FYES, calcula el MAC de las páginas 04 a 0A y le coincide con el MAC que tiene la tarjeta en 0B entonces escribe 0NOT en la página 04 recalcula el MAC, lo escribe en página 0Bh y abre la puerta. Esto anula el billete y evita la utilización de billetes más de una vez.

Este sistema evita el clonado de billetes pues al no conocer la clave maestra es imposible de realizar.

Si este diseño se hiciera para producción (real) la expedición del billete no utilizaría el mecanismo de FLAG de billete válido o inválido (que aquí hemos escrito en la página 04). Este flag no sería nececesario pues podría usar un bit del contador OTP. Si ese bit está a "0" el billete sería válido, cuando pasa por la entrada el terminal de puerta lo pone a "1" y ya no se puede alterar después en la tarjeta, convirtiéndola en un billete inválido.
Igualmente el terminal expendedor bloquearía la escritura en las páginas 05 a 0B con los bits de lock correspondientes para que nadie pudiera sobreescribir esas páginas.

Subir al servidor web los script expedición y puerta.

Disponible en: sábado, 28 de febrero de 2015, 12:00
Fecha límite de entrega: domingo, 8 de marzo de 2015, 20:00

Borrador del envío

Aún no se han enviado archivos

Subir un archivo (Tamaño máximo: 10Mb)

Choose File No file chosen
Subir este archivo

Ud. está en el sistema como Lizandro José Ramirez Difo. (Salir)

ASC-2015