

MIFARE : las preguntas sobre el problema de los ID duplicados

Un poco de historia

Los elementos MIFARE fueron desarrollados por Mikron antes de 1994 (MIFARE es un acrónimo por “**MI**kron **FA**RE”). Mikron fue adquirida por Philips Semiconductors en 1998, la cual se convirtió en NXP Semiconductors en 2006. En la primera versión (MIFARE Classic) se definió un espacio de 4 Bytes para contener un ID único (número de identificación en ocasiones llamado CSN o Chip Serial Number y, más habitualmente, UID o Unique IDentifier) para cada elemento fabricado. Tal espacio daría cabida a más de cuatro mil millones de elementos perfectamente diferenciables, lo que hacía presuponer una muy larga vida para esta arquitectura, pero el éxito mundial de utilización masiva ha hecho que tal cantidad haya sido ya superada.

El principio del fin

A mediados de 2010, muchos usuarios de elementos MIFARE es probable que recibieran con estupor la noticia de que a finales de 2010 la numeración irrepitable basada en 4 Bytes habría llegado a su fin.

Esta noticia llegaba después de la conmoción que se produjo en 2008 cuando varios grupos de trabajo Universitarios consiguieron vulnerar el protocolo de encriptación CRYPTO1 y, como consecuencia, generar clónicos, por lo que la percepción del mercado sobre la seguridad de MIFARE cambió radicalmente, de manera que NXP decidió adaptar su arquitectura MX (la utilizada en los elementos MIFARE DESFire entre otros) para superar el problema de vulnerabilidad de MIFARE Classic (hay que recordar que éstos elementos son de lógica cableada, mientras que la arquitectura MX es microprocesada y aporta un esquema de seguridad radicalmente distinto y muy superior). Como consecuencia nació MIFARE Plus, la cual, al operar en Nivel 1 (utiliza CRYPTO1 bajo simulación), resulta por completo compatible con MIFARE Classic y permite que, cuando las aplicaciones hayan sido modificadas y los Cabezales lectores adaptados (o cambiados en la mayoría de los casos) pasar a trabajar en Nivel 2 ó 3 (máxima securización, entre otras características).

Pero mientras NXP afrontaba el problema, algún que otro fabricante decidió asumir los riesgos y comenzó a fabricar clónicos de las MIFARE Classic, inundando el mercado de tarjetas a menor coste aunque, en muchas ocasiones, con limitaciones de funcionamiento (debidas, por ejemplo, al uso de diferentes frecuencias de resonancia sobre la teórica portadora a 13,56 MHz).

El desastre está servido

Al existir otro fabricante además de NXP, los ID dejaban de ser únicos, cosa que no hizo más que empeorar cuando otros fabricantes también empezaron a distribuir clónicos a bajo precio y sin los controles de calidad de NXP.

Podría parecer que a NXP no le quedaba más opción que pleitear contra tales fabricantes, pero tal cosa cuesta mucho dinero, requiere mucho tiempo (en estos mercados el tiempo es oro) y, además, se hubiera tratado de defender la originalidad de un producto que había sido vulnerado, por lo que optaron por seguir la máxima de “si no puedes vencerlos, únete a ellos”, y así se convirtieron en vulneradores de su propio producto al implantar el NUID o Non-Unique Identifier, lo cual rompe definitivamente con el anterior paradigma del UID o Unique Identifier.

En resumen

Aquellas Instalaciones existentes que utilicen aplicaciones basadas en el uso de elementos MIFARE que dependan de un valor único de ID para la identificación de cada elemento, se enfrentan a un problema.

La manera en la que tal problema vaya a afectar a tales Instalaciones y como se supone que deberían reaccionar es lo que pretende resumir este documento en forma de preguntas y respuestas.

¿ Esto afecta a todos los elementos MIFARE ?

No, sólo afecta a aquellos dotados con un UID de 4 Bytes, por lo que están incluidos los elementos MIFARE Classic y MIFARE Plus en Nivel 1 (UID de 4 Bytes), mientras que no afecta a los elementos MIFARE Ultraligh, MIFARE Ultraligh C, MIFARE Plus en Niveles 2 ó 3, MIFARE Desfire ni MIFARE Desfire EV1, dado que tales elementos disponen de un UID de 7 Bytes.

En el informe de julio de 2010, NXP aportaba no sólo la idea del final cercano del ciclo de vida para los UID de 4 Bytes sino también la propuesta de repetir algunos UID antiguos (pasando a ser NUID) en nuevos lotes de fabricación pero sólo para necesidades muy concretas y contrastables, insistiendo con gran énfasis en que los implementadores de sistemas y aplicaciones se prepararan para migrar a elementos MIFARE con UID de 7 Bytes. Tal cosa es más fácil de decir que de hacer dada la infraestructura de Cabezales lectores instalados y los programas de aplicación existentes.

¿Cuál es el problema cuando los ID no son únicos ?

Para muchos sistemas existentes, el riesgo de disponer de dos elementos RFID con el mismo ID no es importante, por lo que no vale la pena preocuparse. Sin embargo, si los elementos se utilizan como parte de un sistema de pago (por ejemplo, en peajes, en venta de entradas, etc.) o en entornos de seguridad crítica (como en el caso de la mayoría de Controles de Accesos físicos), entonces el peligro de que existan dos elementos que presenten el mismo valor de ID es realmente grave, por lo que el riesgo de vulnerabilidad no debe ser ignorado. A mayor abundamiento, no hay que olvidar que aunque todos los Cabezales lectores reciben de los elementos MIFARE los 32 bits (4 Bytes) del UID, la inmensa mayoría de tales Cabezales lectores sólo transmiten al controlador (CPU, UCA, etc.) 24 bits; tal es el caso de aquellos Cabezales que utilicen la interfaz Wiegand 26 (así llamada por transmitir 24 bits de datos y dos de paridad), de manera que ante una resolución de 24 bits sobre 32 la posibilidad de duplicado es de 1 entre 16.777.215, pero al existir ahora los NUID de NXP más los de los clónicos, la posibilidad de duplicado puede llegar a ser de 1 entre 4.194.303 (asumiendo la existencia de dos fabricantes de clónicos, aunque parece ser que hay o habrá alguno más).

¿Qué está haciendo NXP al respecto?

NXP insiste mucho en que los implementadores pasen a utilizar la opción de UID de 7 Bytes, aunque anuncia que seguirá fabricando elementos MIFARE Classic con el NUID de 4 Bytes. Realmente pocas cosas puede hacer, dado que las decisiones estratégicas son competencia de los desarrolladores de sistemas.

¿Funcionarán los Cabezales lectores existentes con los UID de 7 Bytes?

Es difícil dar una respuesta categórica a esta pregunta. Algunos Cabezales lectores compatibles con la norma ISO/IEC 14443-3 Type A (la utilizada por MIFARE) son capaces de leer ID de 4 Bytes y también UID de 7 Bytes, pero otros no son capaces por ser de diseño anterior a la aparición de los UID de 7 Bytes. De todos modos hay que tener en cuenta que los Cabezales lectores se comportan de manera distinta en la parte de comunicación con los elementos MIFARE dado que por ese lado obtienen los ID al completo (sean de 4 o de 7 Bytes), pero por el otro lado sólo transmiten los bits para los que su interfaz de comunicación esté preparada (por ejemplo, para RS-232 o para Clock/Data será completo, pero para Wiegand normalmente no lo será). Finalmente, y aunque los Cabezales lectores acepten UID de 7 Bytes, los programas de aplicación también deben hacerlo, por lo que en caso contrario deberán ser modificados.

¿Mis aplicaciones actuales necesitan ser modificadas?

Aquellas Instalaciones actuales que pretendan mantener operativa la infraestructura actual de 4 Bytes necesitarán la modificación de las oportunas aplicaciones para implementar el necesario control sobre los duplicados que puedan surgir al mezclar UID de 4 Bytes con NUID y/o con UID de 7 Bytes. De todos modos, si se utiliza un esquema de 'Lista Blanca' formada por los ID de los elementos MIFARE, ahora existe la posibilidad de que aparezcan elementos (que pueden ser MIFARE y/o ser clónicos) no pertenecientes a la Instalación pero que presenten un ID igual que uno de los que estén en la 'Lista Blanca', por lo que el peligro de que se produzcan usos fraudulentos es muy real.

¿Cuáles son las opciones disponibles para los actuales sistemas afectados?

Para los actuales sistemas de cualquier fabricante basados directamente en el uso de elementos MIFARE con UID de 4 Bytes sólo hay dos opciones posibles:

1 - Continuar con los 4 Bytes de los ID, que ya nunca más podrán ser únicos, asumiendo los riesgos implícitos.

2 - Cambiar a la utilización de elementos con UID de 7 Bytes tal y como recomienda NXP, pero considerando que tal cosa presenta costes directos e indirectos que pueden ser muy elevados para las Instalaciones actuales (nuevas tarjetas, quizá nuevos Cabezales lectores y, muy probablemente, modificación de los programas de aplicación).

Una tercera opción podría ser cambiar el planteamiento básico y pasar a utilizar un sistema de abstracción del UID (como el llamado formato 'fS=4' de Qontinuum), que permite utilizar ahora y para siempre los actuales y futuros elementos MIFARE, pero tal cosa presenta costes directos e indirectos que pueden ser muy elevados para las Instalaciones actuales dado que habría que incorporar nuevas CPU, nuevos Cabezales lectores-grabadores y nuevos programas de aplicación (aquellas Instalaciones que actualmente estén utilizando material de Qontinuum se verían favorecidas por unos costes de migración notablemente inferiores).

¿Qué papel puede jugar Qontinuum al respecto?

Históricamente hablando, disponemos de dos líneas de productos para operar con elementos MIFARE.

En términos generales, los productos de la primera línea (a los que llamamos formato 'fS=3') se comportan como muchos otros productos existentes en el mercado, de manera que nuestros Cabezales de la Clase "F" de la Familia SEP leen ID de 4 Bytes y lo transmiten al completo, no siendo problema la posible existencia de ID duplicados dado que nuestros programas de aplicación evitan que más de un elemento MIFARE con ID coincidente sea dado de alta en el sistema, pero no evitan (porque no es posible hacerlo) que un elemento (que puede ser MIFARE y/o ser clónico) no perteneciente a la Instalación se presente en un Cabezal lector y que tal cosa produzca un acceso permitido al ser su ID igual que uno de los que estén en la 'Lista Blanca'.

Para la segunda línea Qontinuum dispone, desde el año 2001, de la estructura 'fS=4' (o formato 'fS=4'), la cual aporta, además de muchas prestaciones de alto nivel, la mejor abstracción posible sobre los ID (no importa que sean UID o NUID de 4 Bytes o UID de 7 Bytes) dado que, simplemente, no los tiene en cuenta al utilizar como ID un concepto propio al que llamamos NIS (Número Identificativo Serializado) y que se encuentra dentro de la información contenida en las estructuras 'fS=4'.