Sobre los UUID y los OID

UUID son las siglas en inglés del Identificador Universalmente Único, se trata de un código identificador estándar que se utiliza, fundamentalmente, en el proceso de construcción de un software o sistema informatizado.

El objetivo de los UUID es habilitar un código de identificación único sin que se requiera una gestión o coordinación central para su generación. Es decir que cualquier persona o institución puede generar un UUID sin tener la necesidad de estar subordinado a un servicio central que asigne dichos códigos.

El código UUID está conformado por una cadena compuesta por 32 dígitos hexadecimales (del 0 al 9 y las primeras 6 letras del alfabeto), es decir que se trata de una cadena de 16 octetos (128 bits), mostrados en 5 grupos separados por guiones de la forma (8 – 4 – 4 – 4 – 12). De esta forma se obtienen UUID como el siguiente ejemplo:

560a8451-a29c-41d4-a716-544676554400

La ITU nos refiere de la siguiente manera a la relación de los UUID y los OID:

Un UUID puede ser interpretado como una codificación de entero sin signo, y el valor entero resultante se puede utilizar como un arco o rama posterior del árbol internacional de OID {joint-iso-UIT-T UUID (25)} (Ver http://oid-info.com/get/2.25) en dicho árbol. (Fuente: http://www.itu.int/ITU-T/asn1/uuid.html). Es de recordar que la UNAOID ocupa su designación en la rama 2.16.

Atento a lo que nos ilustra la ITU, en consecuencia a la conversión decimal de UUID y su uso como parte de un OID, permitiría a los usuarios generar OID sin ningún procedimiento de registro o gestión centralizada.

Ejemplo: f81d4fae-7dec-11D0-A765-00a0c91e6bf6 es la notación hexadecimal que indica el mismo UUID como 329800735698586629295641978511506172918 en notación decimal.

Si un UUID se genera utilizando los mecanismos definidos en la norma Rec. UIT-T X.667 | ISO / IEC 9834-8 y SHA-1, se puede asegurar que será único y diferente a todos los demás UUID generados antes del año 3603.

La ITU advierte que es posible que se generen valores iguales de UUID, aunque la probabilidad es muy pequeña, si se obtienen a partir del Message-Digest Algorithm (MD5) o números pseudo-aleatorios, en lugar del Secure Hash Algorithm (SHA-1). Esto puede causar confusión para los usuarios de OID donde se embeban los UUID, y podría ser el desencadenante de un uso malintencionado, como por ejemplo la suplantación de identidad para instituciones, personas, transacciones, etc. (Ver: http://www.itu.int/ITU-T/asn1/uuid.html).

Recordemos también que el SHA-1 ha sido atacado a lo largo de su existencia con resultados que siembran dudas sobre su seguridad, si bien no se logró identificar ninguno de los ataques como efectivos.

Ejemplos de estos ataques a su cifrado son:

En febrero del 2005, Bruce Schneier, publica que ha logrado romper el SHA-1 (Ver http://www.schneier.com/blog/archives/2005/02/sha1_broken.html)

En julio del 2007, un equipo de investigadores chinos, compuesto por Xiaoyun Wang, Yiqun Lisa Yin y Hongbo Yu (principalmente de la Shandong University en China), demuestra que son capaces de romper el SHA-1 en al menos 2^{69} operaciones, unas 2000 veces más rápido que un ataque de fuerza bruta (que requeriría 2^{80} operaciones). Los últimos ataques contra SHA-1 han logrado debilitarlo hasta 2^{63}.

Según el Instituto Nacional de Normas y Tecnología de Estados Unidos (NIST por sus siglas en inglés), este ataque es de particular importancia para las aplicaciones que usan firmas digitales tales como marcas de tiempo y notarías. Sin embargo, muchas aplicaciones que usan firmas digitales incluyen información sobre el contexto, lo que hace este ataque difícil de llevarse a cabo en la práctica. (Ver http://www.theepochtimes.com/news/7-1-11/50336.html)

Generar los UUID

Basados en las normas citadas en este documento, es posible embeber en los sistemas informáticos y software específicos, las rutinas apropiadas para generar los UUID.

Atento a ello, cualquier organización puede hacer la correspondencia entre un OID y un UUID, en este caso, no embebiendo uno en el otro.

Por otro lado es posible convertir un UUID a su valor entero decimal, y embeber el mismo como parte de un OID, por ejemplo para la identificación de objetos. No obstante, la longitud de los UUID como entero decimal, incrementa la extensión de los OID resultantes de manera significativa, lo cual complejiza su utilización en los sistemas informáticos, tanto para su gestión, representación en pantallas e impresos, así como haría prácticamente imposible su recordación por persona alguna. Una particularidad de los OID, es que a pesar de su extensión, y gracias a sus especificaciones técnicas para la construcción de los mismos, mantiene como posibilidad real la recordación por parte de todo usuario.