Keyed Hash

Este documento no pretende ser un curso exhaustivo, en el mejor de los casos, únicamente puede considerarse como un conjunto de notas complementarias en alguna asignatura. Por supuesto, todo documento es susceptible de mejora, cualquier sugerencia o comunicación de error u omisión será bienvenida.

La posibilidad de integrar en herramientas de comprobación de la integridad de una clave permite obtener *códigos de autenticación de mensajes* (MAC del acrónimo en inglés). Estos son generados por dos partes que comparten un secreto para validar la información que se transmite. Las funciones resumen proporcionan una herramienta para la verificación que cuando se combina con la introducción de la clave mencionada proporciona las conocidas como HMAC, propuestas inicialmente por Bellare, Canetti y Krawczyk.

HMAC

La propuesta de estandar se describe en RFC-2104 y considera un mismo esquema aunque permite el uso de distintas funciones resumen: SHA-1, MD5 y RIPEMD-128/160, a las que suele denotarse como HMAC-SHA1, HMAC-MD5 y HMAC-RIPEMD respectivamente. El documento de propuesta del estandar se hace eco de la debilidad de MD5, sin embargo es suficientemente flexible en su descripción como para permitir adaptarse a las nuevas propuestas de funciones resumen.

La descripción considera una función resumen h que utiliza un *estado interno* de B bytes, una clave k y un mensaje x.

Inicialmente, la clave es procesada para ajustar su tamaño al de B, de modo que considera $h(k)$ si el tamaño de la clave supera B. A partir de la clave (resumida o no) se construyen dos nuevos bloques:

$$\begin{cases} innerkey = k \oplus ipad \\ outterkey = k \oplus opad \end{cases}$$

donde *ipad* y *opad* denotan dos secuencias constantes de tamaño B:

$$\begin{cases} ipad = (36_{HEX})^B \\ opad = (5C_{HEX})^B \end{cases}$$

los términos *inner* y *outer* utilizados (y mencionados en la documentación) son exclusivamente mnemotécnicos que hacen referencia al momento en que son utilizados en el esquema HMAC, que se define como:

$$HMAC(x) = h(\ outterkey \mid h(\ innerkey \mid x\ )\ )$$

Básicamente, la función consiste en anidar dos llamadas a la función resumen que considera la concatenación (denotada con '|' en la descripción) de una de las secuencias construidas a partir de la clave y bien el mensaje o el resultado del primer resumen.

Recomendaciones de implementación

La propuesta de estandar recomienda que la clave utilizada sea aleatoria o criptográficamente pseudoaleatoria y de tamaño B, indicando que claves mayores no proporcionan niveles de seguridad sustancialmente mejores. Se recomienda también la renovación frecuente de las claves utilizadas.

La definición permite la utilización directa de las funciones resumen. Dada la implementación habitual de estas, es posible reducir ligeramente el coste temporal considerando el estado inicial en el cálculo de las secuencias *ipad* y *opad*. En cualquier caso, esta modificación no afecta a la seguridad de la funciones catalogadas hasta la fecha (2018), pudiendo sustituirse una función determinada de la que se descubra alguna debilidad.

Se menciona como procesos de autenticación realizados en el pasado utilizando técnicas HMAC no pierden garantía en caso de detectar nuevas debilidades de la función resumen utilizada, que, obviamente, deberá ser sustituida desde ese momento.