educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 3

Códigos de autenticación de mensajes (MAC)

MAC

Un *código de autenticación de mensajes* (MAC, Message Authentication Code) es un *array* corto de bits, usados para autenticar un mensaje. Se conocen también como *etiquetas de autenticación*.

Características e implementación

- Para generarlo, el emisor necesita un **mensaje** y una **clave secreta**.
- Para verificar el MAC, el receptor necesita el mensaje y la misma clave secreta.

Los MAC difieren de la firma digital, que utiliza criptografía asimétrica para que el emisor y el receptor puedan verificarla. La firma digital, además de la autenticación, aporta no repudio.

Se utilizan en protocolos de red para establecer la integridad y la autenticidad de los datos transmitidos, para cifrado general y como base de las funciones derivadoras de clase, tales como *PBKDF*.

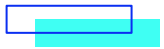
Existen muchas clases de **funciones *MAC*** diferentes, una de las más usadas en protocolos seguros de red son los ***HMAC*** (códigos de autenticación basados en *hash*).

Seguridad en MAC

Un MAC es seguro si puede resistir la lista de ataques siguientes:

- Ataque de **falsificación universal** (un atacante crea un MAC válido para cualquier mensaje).
- Ataque de **falsificación selectivo** (el atacante produce el MAC correcto para un mensaje particular, elegido previamente al ataque).
- Ataque de **falsificación existencial** (el atacante puede relacionar cualquier mensaje con su MAC) .
- Ataque de **falsificación existencial a un mensaje elegido** (el atacante puede enviar mensajes a un oráculo para que este genere un MAC, para poder analizarlo junto al comportamiento del oráculo.

El nivel de seguridad del MAC se mide en **bits**, pero depende de la seguridad de las funciones criptográficas y de la clave secreta que utilice.



Los códigos de autenticación de mensajes basados en *hash* (HMAC) utilizan **una función *hash* y una clave secreta**. La función no es compleja:

```
HMAC(K, message) = H(K' XOR opad || H(K' XOR ipad || message))
```

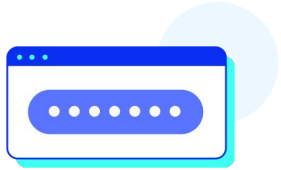
- **H** es la función *hash*. Por ejemplo: *SHA3-256*.
- **K** es la clave secreta.
- **K'** es la clave derivada de `K` del tamaño de bloque adecuado dependiendo del tamaño B del bloque interno de la función `H`.
- **ipad** es el *padding* interno, consiste en el *byte* `0x36` repetido B veces.
- **opad** es el *padding* externo, consiste en el byte `0x5C` repetido B veces.
- **||** representa una concatenación.

Si una HMAC usa una función *SHA-256*, se la denomina ***HMAC-SHA-256***. El nivel de seguridad es el mínimo valor entre la clave secreta y la longitud del *hash* medido en bits. *HMAC-SHA-256* con clave de 256 bits tiene **seguridad de 256 bits**.

Pero la fortaleza de la seguridad de una clave secreta descansa en su entropía. **Si una clave es creada mediante un generador aleatorio criptográficamente seguro, su seguridad es igual a su longitud**.

Si el generador aleatorio es sospechado de aleatoriedad débil, por ejemplo, cada 2 bits generados tiene solamente uno de entropía, se debería doblar el tamaño de la clave.

Si la clave se deriva a partir de una fuente de baja entropía tal como una contraseña, el nivel de seguridad de la función HMAC se degrada a la cantidad de entropía de la contraseña.



Esquemas de uso

Los esquemas más habituales de uso de los MAC con cifrado son:

- **EtM (*Encrypt-then-MAC*):** se cifra el texto claro, se calcula el MAC sobre el texto cifrado y se envían juntos MAC y criptograma.
- **E&M (*Encrypt-and-MAC*):** se cifra el texto plano y se calcula el MAC sobre el texto plano. Luego se envían juntos MAC y criptograma.
- **MtE (*MAC-then-Encrypt*):** se calcula el MAC cobre el texto plano, se concatenan y se cifran.

Investigadores en seguridad recomiendan **EtM** como el esquema más seguro.

Existen otros dos esquemas posibles, que están ganando en popularidad: **AES-GCM** y **ChaCha20-Poly1305** que son modos de cifrado autenticados y no necesitan HMAC.

¡Sigamos trabajando!