INTEGRIDADE DOS DADOS COM FUNÇÕES DE *HASH*

Os códigos de autenticação de mensagens de *hash* (HMAC) assinam pacotes para assegurar que as informações recebidas sejam exatamente as mesmas informações enviadas. Esse processo é chamado integridade.

Os HMACs asseguram a integridade através de um *hash* com chave, o resultado de um cálculo matemático em uma mensagem utilizando uma função de *hash* (algoritmo) combinada com uma chave secreta compartilhada.

Um *hash* normalmente é descrito como uma assinatura no pacote. No entanto, um *hash* difere de uma assinatura digital. Ele utiliza uma chave secreta compartilhada enquanto uma assinatura digital utiliza a tecnologia de chave pública e a chave particular do computador que está enviando os dados.

Uma assinatura digital fornece não-repúdio, o que não é assegurado pelo *hash*. O não-repúdio garante que a comunicação pode ter sido originada de uma pessoa específica cuja identidade pode ser verificada. Ele também garante que a comunicação ocorreu realmente.

As funções de *hash* também são chamadas de funções de mão única, pois é fácil determinar o *hash* a partir da mensagem, mas é matematicamente impossível determinar a mensagem a partir do *hash*. Em contrapartida, em funções bidirecionais, a mensagem original pode ser determinada a partir de sua forma convertida. Os esquemas de criptografia e descriptografia são exemplos de funções bidirecionais.

O *hash* é uma soma de verificação criptográfica ou um código de integridade de mensagem (MIC) que cada parte deve calcular para verificar a mensagem.

Por exemplo, o computador que está enviando os dados utiliza a função de *hash* e uma chave compartilhada para calcular a soma de verificação da mensagem, incluindo-a com o pacote. O computador que está recebendo os dados deve executar a mesma função de *hash* na mensagem recebida e na chave compartilhada e compará-la com a original (incluída no pacote do remetente). Se a mensagem tiver sido alterada quando estava em trânsito, os valores de *hash* serão diferentes e o pacote será rejeitado.

Para a integridade, você pode escolher entre duas funções de *hash* ao definir a diretiva:

- MD5
  O MD5 é baseado no RFC 1321. O MD5 passa quatro vezes pelos blocos de dados, usando uma constante numérica diferente para cada palavra contida na mensagem a cada vez que passa pelos dados. O número de constantes de 32 bits usadas durante o cálculo do MD5 produz, por fim, um *hash* de 128 bits que é usado para a verificação de integridade.
- SHA1
  O algoritmo de *hash* seguro (SHA1) foi desenvolvido pelo Instituto nacional de normas e tecnologia conforme descrito no padrão federal de processamento de informações (FIPS) PUB 180-1. O processo do SHA baseia-se em grande parte no MD5. O cálculo do SHA1 resulta em um *hash* de 160 bits que é usado para a verificação de integridade. Como quanto mais longo o *hash* maior a segurança, o SHA é mais seguro que o MD5.