1.HMAC

Para adicionar autenticação de origem e garantia de integridade, use um **Código de Autenticação de Mensagem Hash com Chave** (HMAC). HMACs usam uma chave secreta adicional como entrada à função hash. Outros métodos MAC (Message Authentication Code) também são usados. No entanto, o HMAC é usado em muitos sistemas, incluindo SSL, IPsec e SSH.

1.1 Algoritmo de hash HMAC

Um HMAC é calculado usando qualquer algoritmo criptográfico que combina uma função hash criptográfica com uma chave secreta. As funções de hash são a base do mecanismo de proteção dos HMACs. Somente o remetente e o destinatário têm conhecimento da chave secreta e agora a saída da função hash depende dos dados de entrada e da chave secreta. Apenas as partes que têm acesso a essa chave secreta podem calcular o digest de uma função HMAC.

Isso derrota os ataques do tipo Man-in-the-Middle e fornece autenticação da origem dos dados. Se duas partes compartilharem uma chave secreta e usarem as funções HMAC para autenticação, uma mensagem HMAC adequadamente construída, a parte recebeu indica que a outra parte foi a originadora da mensagem. Isso ocorre porque a outra parte possui a chave secreta.

1.3 Criação do valor HMAC

Dispositivo de envio insere dados no algoritmo de hash e calcula o HMAC Digest de comprimento fixo. Esse Digest autenticado é anexado à mensagem e enviado ao destinatário.

1.4 Verificação do valor de HMAC

O dispositivo receptor remove o Digest da mensagem e usa a mensagem de texto sem formatação com sua chave secreta como entrada na mesma função de hash. Se o Digest calculado pelo dispositivo receptor for igual ao resumo enviado, a mensagem não foi alterada. Adicionalmente, a origem da mensagem é autenticada porque apenas o remetente possui uma cópia da chave secreta compartilhada. A função HMAC garantiu a autenticidade da mensagem.