1.Autenticação

A autenticação verifica a identidade de um usuário para evitar acesso não autorizado. Os usuários provam sua identidade com um nome de usuário ou ID. Eles também podem precisar verificar sua identidade proporcionando uma das seguintes opções: Algo que saibam (senha), algo que tenham (toke/cartão) ou algo que sejam (impressão digital).

Em comunicações de rede, a autenticação pode ser realizada usando métodos criptográficos. Isso é especialmente importante para aplicativos ou protocolos, como e-mail ou IP, que não possuem mecanismos internos para evitar falsificação da fonte.

O **não-repúdio de dados** é um serviço similar que permite que o remetente de uma mensagem seja identificado exclusivamente. Com serviços de **não-receptação** no lugar, um remetente não pode negar ter sido a fonte dessa mensagem. Pode parecer que o serviço de autenticidade e o serviço de não-receptação estão cumprindo a mesma função. Embora ambos se dirijam à questão da identidade comprovada do remetente, há uma diferença entre os dois.

A parte mais importante da não-receptação é que um dispositivo não pode repudiar ou refutar a validade de uma mensagem enviada. O não repúdio depende do fato de que apenas o remetente possui as características ou a assinatura exclusivas de como essa mensagem é tratada. Nem mesmo o dispositivo de recepção pode saber como o remetente tratou esta mensagem para provar autenticidade porque o receptor poderia fingir ser a fonte.

Se a maior preocupação for para o dispositivo de recebimento validar a fonte e não há preocupação com o dispositivo de recebimento imitando a fonte, não importa se o remetente e o receptor sabem como tratar uma mensagem para fornecer autenticidade. Um exemplo de autenticidade versus não-repetição é uma troca de dados entre dois computadores da mesma empresa versus uma troca de dados entre um cliente e um site de e-commerce. Os dois computadores que trocam dados dentro de uma organização não precisam provar para o outro qual delas enviaram uma mensagem.

Esta prática não é aceitável em aplicativos de negócios, como ao comprar itens online. Se a loja on-line souber como uma mensagem de cliente foi criada para provar a autenticidade, ela pode facilmente falsificar pedidos "autênticos". Em tal cenário, o remetente deve ser a única parte com o conhecimento de como a mensagem foi criada. A loja online pode provar aos outros que a ordem foi, de fato, enviada pelo cliente, e o cliente não pode argumentar que o pedido é inválido.

2.Autorização

Os serviços de autorização determinam quais recursos os usuários podem acessar, juntamente com as operações que os usuários podem executar. Alguns sistemas conseguem isso através de uma ACL. Autorização também pode controlar quando um usuário tem acesso a um recurso específico.

3.Accounting

Accounting representa o controle sobre o que os usuários fazem, desde o que acessam até a quantidade de tempo que acessam os recursos disponíveis, observando as alterações feitas. Serviços de accounting de segurança cibernética funcionam da mesma maneira, com o sistema controlando cada transação de dados e fornecendo os resultados da auditoria.