Revisão para p1(10/04/2025) de Segurança da Informação 03/04/2025

Prof Ronny

1. Segurança de informação existe antes da informática, aumentou a velocidade no transporte da informação

E a quantidade de informação que trafega hoje.

Os três pilares são:

* Disponibilidade precisa de servidor, banda larga e banco de dados,
* Integridade (que ninguém altere a mensagem),
* Confidencialidade (chegar apenas ao destinatário).

Não é viável que a proteção seja mais cara que o produto. Ainda não existe proteção 100%. Por isso existe uma margem de risco aceitável, variando o tipo de negócio.

Até o código precisa de proteção, string de proteção, metodologias da propriedade intelectual. Por exemplo um app que não seja open source pode ser vendido sem a venda do código. Autenticação deve ser segura principalmente para assegurar proteção dos dados do cliente, podendo dar um processo caso haja perdas.

1. Programação segura

Proteção do código

Até o código precisa de proteção, string de proteção, metodologias da propriedade intelectual. Por exemplo um app que não seja open source pode ser vendido sem a venda do código.

Proteção do Aplicativo

Autenticação segura vai assegurar proteção dos dados do cliente, podendo dar um processo caso haja perdas.

Tecnologias de segurança: criptografia

1. Codificação

Criptografia – codificação ou emparelhamento em uma ponta e codificação ou embrulhamento em outra ponta.

Simétrica – usa a mesma chave para trancar e destrancar a mensagem. Deslocamento e transposição de bytes ou símbolo dentro da mensagem. É uma forma segura, pois para destrancar seria necessário usar todas as chaves possíveis, força bruta, seria quebrada pela escolha da chave. Técnica de segurança: validação com grau de dificuldade, maiúscula, caracteres especiais, números sem sequência, mínimo de 8 caracteres. Isso aumenta muito a quantidade de símbolos para destravar, demora para testar todas as senhas. Para proteger não é possível usando uma senha fixa. Vulnerabilidade: acesso de quem recebe a mensagem.

Assimétrica – NÃO É UMA ASSINATURA DIGITAL, ela é um processo que usa assinatura digital. Hashing serve para confirmar a integridade e guarda a informação de autenticação (senha), para comparar hashings.(MD5, SHA256 usam hashing)

Pois ela tem a função parcial dos pilares, integridade de envio ou recebimento.

O remetente usa chave privada e chave pública destranca, a chave que tranca é diferente da chave que destranca, ao contrário se trancar com a chave pública só destranca com a chave privada (Usando um modelo matemático). Isso torna apenas o emissor íntegro, pois se for aberto pela chave pública é visível que foi aberto, quem lê não pode trancar.

Para tornar confidencial o usuário A tranca com chave pública A chave privada B e o usuário B destranca com a chave pública A e a chave privada B, sendo necessário um par de chaves para cada usuário.

A assinatura digital aumenta muito o tamanho da informação, por isso não é utilizada em toda sessão, para isso se usa senha temporária com um algoritmo mais leve.

1. Ameaças – quem ou o que **pode** causar danos. Ex. Hacker

Vulnerabilidade = probabilidade. Acesso por exemplo, pode deletar dados; criar usuário fake;

Risco = dano. Impacto, dano moral; pode ser baixo, médio ou alto.

Não dá para eliminar ameaça e sim minimizar, mas precisa assumir o risco.

Métodos de controle, criptografia, autenticação (token), codificação, autorização (permissões).

Leiam o material de referência!

**Linux** tem poucos recursos, por isso é mais rápido

* Usuário dono
* Grupo associado
* Outros usuários

Permissões no Linux, leitura, escrita e execução.

ACL completo tem a lista de todos os recursos, o **Windows** tem muitas permissões e isso o torna lento.