Universidade Federal de Uberlândia

FEELT – Faculdade de Engenharia Elétrica

SISTEMAS EMBARCADOS 2

Segurança e Criptografia de Sistemas Linux

Professor Éder Alves de Moura

Engenharia de Controle e Automação

Aluna: Iohana Angélica Torres Cabral 11411EAU002

Novembro de 2021

1 Descreve o que é cyber segurança e os seis tipos apresentados no vídeo: https://www.youtube.com/watch?v=mo3R-LDTdos

Cyber Security é a prática de proteger os sistemas e networks de ataques digitais.

- Network Security é o processo que toma medidas para proteger os equipamentos de acessos não autorizados, modificação ou destruição.
- Information Security é o processo que assegura as informações de quaisquer tipos de violações na forma de roubo, abuso ou perda.
- Application Security é o processo que aumenta a segurança da web e aplicações mobile para proteger as informações de ataques.
- Cloud Security é um conglomerado de políticas e procedimentos que principalmente protege aplicações e sistemas baseados na nuvem.
- IOT Security é o processo que protege equipamentos IOT de vulnerabilidades.
- Mobile Security é a proteção de smartphones, tablets e vários outros equipamentos de vulnerabilidades.

2 Apresente um resumo das 6 dicas apresentadas no vídeo disponível em: https://www.youtube.com/watch?v=fKuqYQdqRIs explicando a razão assumida para cada uma delas.

- Desabilitar acesso com senha ao SSH: é recomendável pois cria mais uma barreira de segurança, dificultando o acesso do hacker ao sistema.
- Desabilitar o login SSH de Raiz Direta: impede que a senha seja reutilizada para o acesso ao root, dessa maneira evita a invasão.
- Mudar a porta SSH Padrão: ação não muito eficaz. Garante a proteção contra sistemas que buscam servidores por senhas básicas.
- Desativar IPv6 para SSH: o SSH é programado para listar somente IPv6.
- Configurar um Firewall Básico: abrir somente as portas necessárias para as ações bloqueando as demais.
- Atualização de servidor autônomo automática: atualizações de segurança são programadas para serem efetuadas de forma automática, porém o restante das atualizações não convém ser automática pois elas podem vir com alguma falha/erro que possa facilitar a invasão.

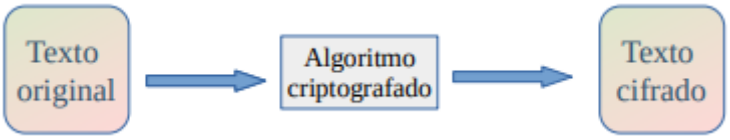
3 A partir dos vídeos disponíveis nos links:
https://www.youtube.com/watch?v=CcU5Kc_FN_4
https://www.youtube.com/watch?v=fCcMfu_Ni4E
Descreva como a segurança de um sistema de embarcado deve ser pensado. Nessa descrição, considere:

a) Qual o melhor método para armazenar um conjunto de senhas em um sistema embarcado, conectado à rede.

Para armazenar conjuntos de senhas o método indicado é o de criptografia unidirecional, pois nesse método o sistema embarcado vai salvar apenas o código e quando a senha for solicitada ela é inserida. Não é aconselhável a criação de senhas em modo de texto ou encriptadas. Para isso é utilizado o método Data Encryption.

b) Elabore um diagrama e uma breve explicação de como uma criptografia simétrica acontece.

A criptografia simétrica faz uso de uma única chave, que é compartilhada entre o emissor e o destinatário de um conteúdo. Essa chave é uma cadeia própria de bits, que vai definir a forma como o algoritmo vai cifrar um conteúdo.



c) Diferença entre um sistema de criptografia e um hash de validação.

A criptografia converte para a mensagem original após o processo, já o hash não.

d) Explique o que é STRIDE e 'Threat Model'.

Threat Model de um produto é o resultado do precesso de threat modeling onde potenciais ameaças podem ser identificadas, enumeradas e atenuadas.

Stride é uma metodologia que ajuda a identificar todas as ameaças no sistema.

e) Segurança de boot

É um sistema que protege a integridade e a autenticidade do código que roda no equipamento.

f) Criptografia de dados e de código.

É um sistema que protege a propriedade intelectual ou garante a confidencialidade das informações.

4 A partir dos vídeos disponíveis no link abaixo, explique:
https://www.youtube.com/watch?v=_qypi2NKCcg
https://www.youtube.com/watch?v=HCHqtpipwu4

a) A relação entre sistemas de criptografia e a geração de hashes do bitcoin.

A criptografia é necessária para proteger as transações. O hash é utilizado para que cada mineração concluída com sucesso tenha seu único algoritmo, o que é essencial para dificultar a resolução desse algoritmo e agregar rendimento ao bitcoin.

b) Explique como funciona a comunicação e infraestrutura dos siteshttpse a arquitetura de rede para a implementação do protocoloTSL/SSL.

O método TSL se difere na criptografia assimétrica pois ele utiliza a criptografia no começo da comunicação entre o cliente e o servidor. Já o protocolo TSL criptografa o

tráfego de internet. Quando ele é utilizado é possível ver na barra de endereço um cadeado e o https confirmando o uso desse protocolo.

c) Pesquise em outras fontes e explique o que é umcertificado digitale como funciona o sistema ICP-Brasil, do Instituto Nacional de Tecnologia da Informação (ITI).

Os certificados digitais são documentos eletrônicos que possuem mensagens, assinaturas e e verificações de identidade de forma criptografada. O responsável pela regulamentação e estabelecimento de critérios e políticas desses documentos é o ICP Brasil, Infraestrutura de Chaves Públicas Brasileira. Ele também viabiliza a identificação virtual do cidadão brasileiro. Para que isso ocorra de forma funcional e segura é necessário um ótimo sistema criptográfico.