Trabalho Semana12 – Sistemas embarcados

Nome: Augusto Perez de Andrade – 11611EMT009

1)

Dica 1: Desabilitar a utilização de senhas no protocolo SSH para efetuar login. Utilizar chaves de acesso no lugar. Isso se dá pelo fato de senhas podem conter padrões, tornando-as inseguras por natureza.

Dica 2: Desabilitar acesso ao SSH pela raiz. Utilizar um endereço no lugar. Se a raiz já entrega o endereço, não faz sentido em divulga-la.

Dica 3: Não utilizar portas padrões de acesso. Parte do princípio de que tudo pode ser hackeado, incluindo um protocolo SSH. A ação apenas diminuiria o risco.

Dica 4: Desabilitar Ipv6. Isso se dá pelo fato de que o endereço Ipv4 possui mais recursos de segurança.

Dica 5: Configurar um Firewall básico. Pode garantir um pequeno incremento na segurança pelo simples fato de restringir acessos estratégicos.

Dica 6: Fazer atualizações frequentes. Desta forma, o sistema de segurança pode ser alterado constantemente, prevenindo um ataque hacker que seja demorado (porém eficaz).

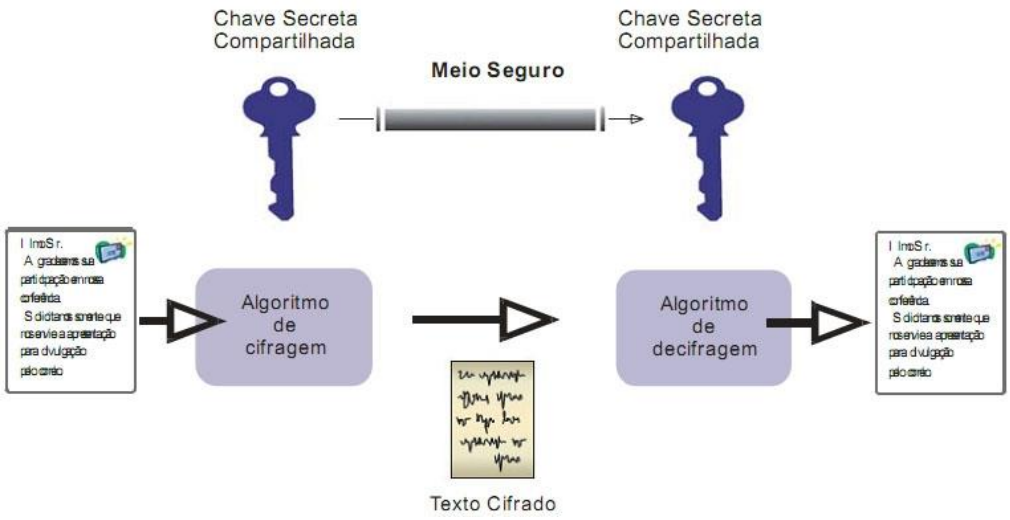
2)

a)

Um dos melhores métodos para garantir uma boa segurança em um sistema embarcado conectado à rede é utilizando criptografia. Os métodos podem ser simétricos ou assimétricos, e utilizarem segredos que podem ser básicos (Ex: Shift, Análise de frequência) ou avançados, dependendo da aplicação.

b)

A criptografia simétrica parte do princípio de criptografar utilizando uma entrada composta por um texto e um segredo, e uma saída referente ao texto “bagunçado”. Ao passar o texto encriptografado pelo mesmo algoritmo de decifragem de forma inversa, o resultado é o texto original.



c)

Funções Hash, diferentemente da criptografia simétrica, funcionam em uma mão única. Isso significa que recebem entradas de tamanhos variáveis e tem como saída um texto de tamanho fixo, dificultando a conversão reversa uma vez que cada elemento do texto de saída não está unicamente relacionado com o respectivo elemento do texto de entrada. Desta forma, esse tipo de função é utilizado em sistemas com alta demanda de segurança (Ex: Criptomoedas).

3)

a)

A geração de hashes do bitcoin está relacionado com sistemas de criptografia uma vez que as moedas são representadas por um texto finito escrito em hexadecimal que pode ter a saída completamente alterada com uma simples diferença na entrada. Isso explica a alta demanda por processamento em busca de obter pequenas faixas de código (mineração).

b)

O funcionamento se dá pelos algoritmos dos próprios navegadores (Chrome, Firefox, etc..) que utilizam os protocolos HTTPS (HTTP + SSL). Este algoritmo permite a criptografia/descriptografia apenas na saída e chegada de dados, permitindo que o usuário consulte contas bancárias, por exemplo.

c)

A ICP-Brasil disponibiliza a emissão de certificados digitais para a identificação virtual de um cidadão ou empresa. O modelo brasileiro tem como raiz única o Instituto de Tecnologia e informação que tem o papel de autoridade certificadora raiz, responsável por credenciar, supervisionar e auditar processos.

Fonte: https://www.gov.br/iti/pt-br/acesso-a-informacao/perguntas-frequentes/icp-brasil