



SEGURANÇA CIBERNÉTICA

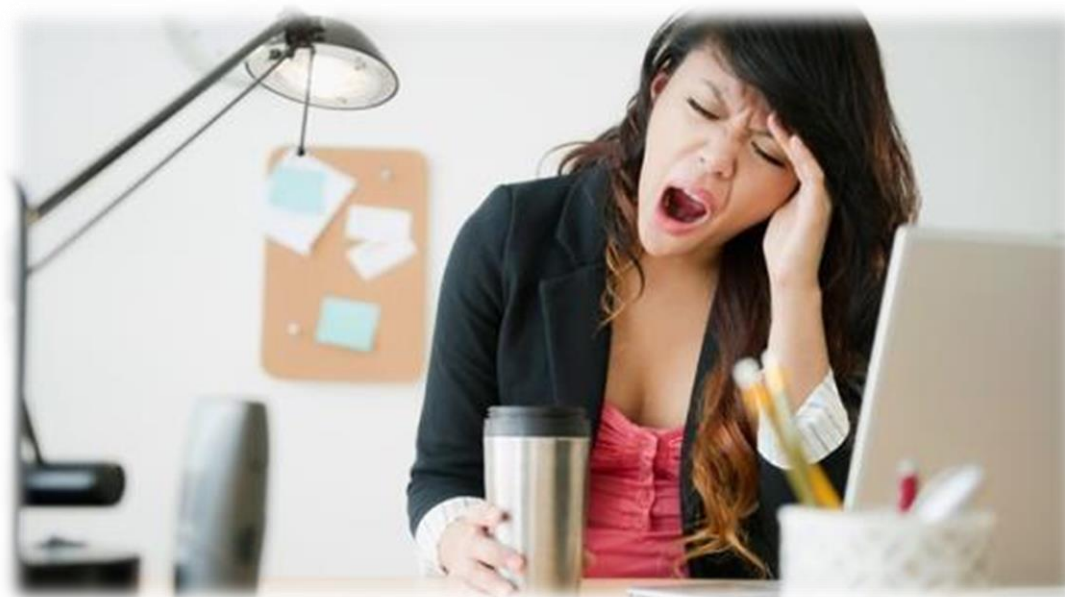
CONTRAMEDIDAS E HARDENING

Prof. Dr. Daniel Caetano

2022 - 1

Compreendendo o problema

- **Situação:** A cada ano que passa, crescem os ataques cibernéticos, tirando o sono de inúmeros analistas de segurança.



**Há algo que possa ser
feito?**

Compreendendo o problema

- **Situação:** existem diversas medidas relevantes para nos protegermos, as chamadas “contramedidas”. Dentre elas, existe um conjunto de ações denominado “hardening”.



**Você faz alguma ideia do que
seja Hardening?**

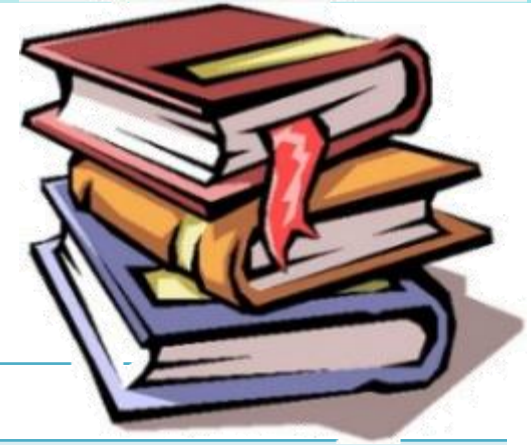
Objetivos

- Retomar os conceitos de criptografia e certificados digitais
- Compreender o conceito de Hardening
- Discutir alguns aspectos relativos à IoT

- **Atividade Avaliativa B**



Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	https://www.caetano.eng.br/aulas/2021b/ara0076.php (Segurança Cibernética – Aula 9)
Minha Biblioteca	<ul style="list-style-type: none">• Segurança de Computadores: Princípios e Práticas (ISBN: 978-85-352-6449-4). Págs 575 a 607.• Hackers Expostos: Segredos e Soluções para a Segurança de Redes. (ISBN: 978-0-07-178028-5). Págs 225 a 229.• Segurança de Redes sem Fio: Guia do Iniciante (ISBN: 978-0-07-178028-5). Pág. 128.• Redes de Computadores e Internet (ISBN: 978-0-13-358793-7). Págs 451, 452 e 498 a 500.
Material Adicional	<ol style="list-style-type: none">1) Criptografia. Disponível em: https://youtu.be/_Eeg1LxVWa82) Hardening: Base. Disponível em: https://youtu.be/FmB59AV4LSg3) Hardening. Disponível em: https://youtu.be/wPkYN5shNEg4) Segurança em IoT. Disponível em: https://youtu.be/JkzFkS5TsBE5) IoT - Privacidade e Seg.. Disponível em: https://youtu.be/zp0NOXv6THY



RECORDANDO:

CRIPTOGRAFIA E CERTIFICADOS

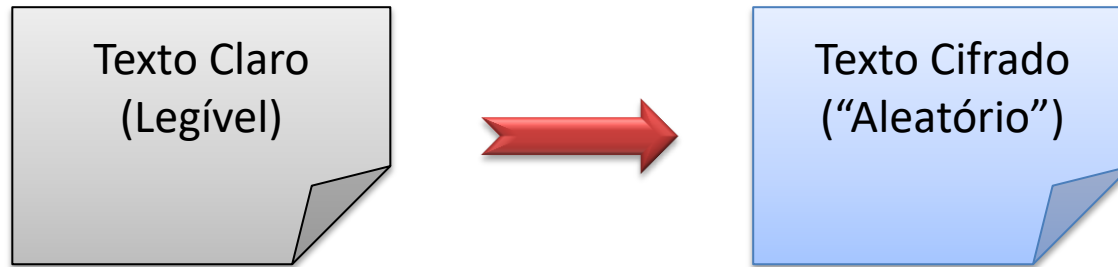
Mecanismos de Segurança

- Os mecanismos mais clássicos são:
 - Criptografia dos dados
 - Assinatura digital dos dados
- Focam em garantir
 - Sigilo: só quem pode acessar, acessará
 - Integridade: conferir se dado permanece “original”
 - Autenticação: de usuário, remetente, destinatário
 - Atualidade: a mensagem é nova, não um reenvio.



Criptografia

- Codificação dos dados
- Processo que transforma



- Algoritmo de criptografia
 - Cifragem: tornar o texto claro em cifrado
 - “Criptografar” ou “Encriptar”
 - Decifragem: tornar o texto cifrado em claro
 - “Decriptografar” ou “Decriptar”

Criptologia

Chave Criptográfica

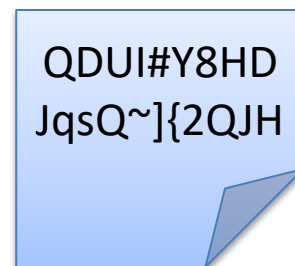


- Chave permite “trancar”...
 - ... e “destrancar”.
 - É o “segredo” de um criptografia
 - Similar a uma “senha”
- Tradicionalmente, remetente e destinatário...
 - Precisam ter uma cópia da chave

Mensagem Legível



Mensagem Cifrada



Mensagem Legível



Uso da Criptografia

- Assim, dados criptografados...
 - Armazenados ou transmitidos
 - Só serão legíveis por quem tiver a chave



Estarão mais seguros!

Algoritmos Comuns

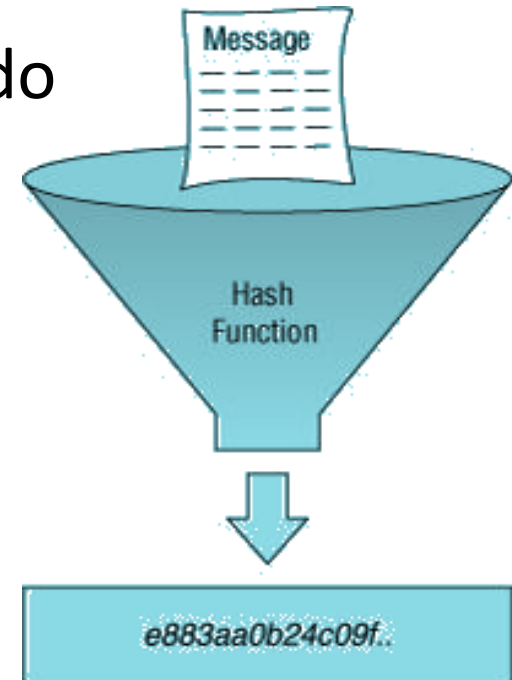


- Criptografia de chave simétrica (128, 256...)
 - AES - Rijndael
 - 3DES
 - IDEA
- Criptografia de chave assimétrica (1024...)
 - RSA
 - Diffie-Hellman
 - ECC
 - DSA



Hash ou Número Resumo

- Analisar arquivo ou mensagem:
 - Certificar-se de que não foi alterado
- Criptografia: “ida” e “volta”
 - Se eu codifiquei, eu decodifico
- Hash: só “ida”
 - Só codifico, nunca decodifico
 - Deve ser único para uma mensagem legível

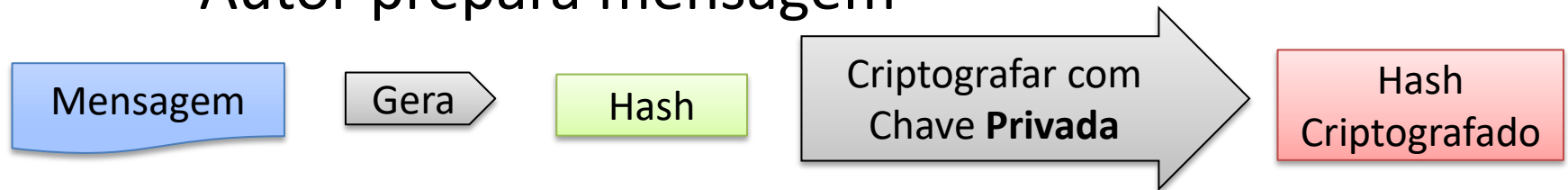


Assinaturas Digitais

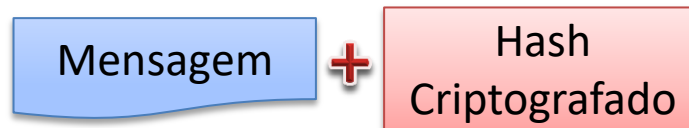


- Mecanismo

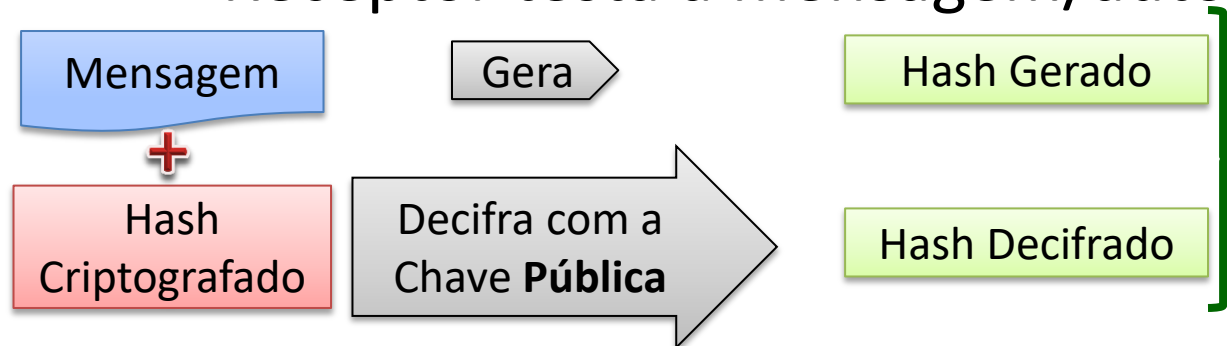
- Autor prepara mensagem



- Autor envia a mensagem



- Receptor testa a mensagem/autor



Devem ser iguais!

Chave Pública: Como Obter?

- Importante: ter acesso às chaves públicas
 - Para decifrar e verificar as mensagens
 - Para enviar mensagens secretas
- Como saber se a chave pública é realmente a da pessoa, e não de um bisbilhoteiro qualquer?
 - “Terceiro Confiável”: entidade certificadora
 - Certificados Digitais
 - Banco de chaves públicas
 - Domínios ou CPFs ou CNPJs



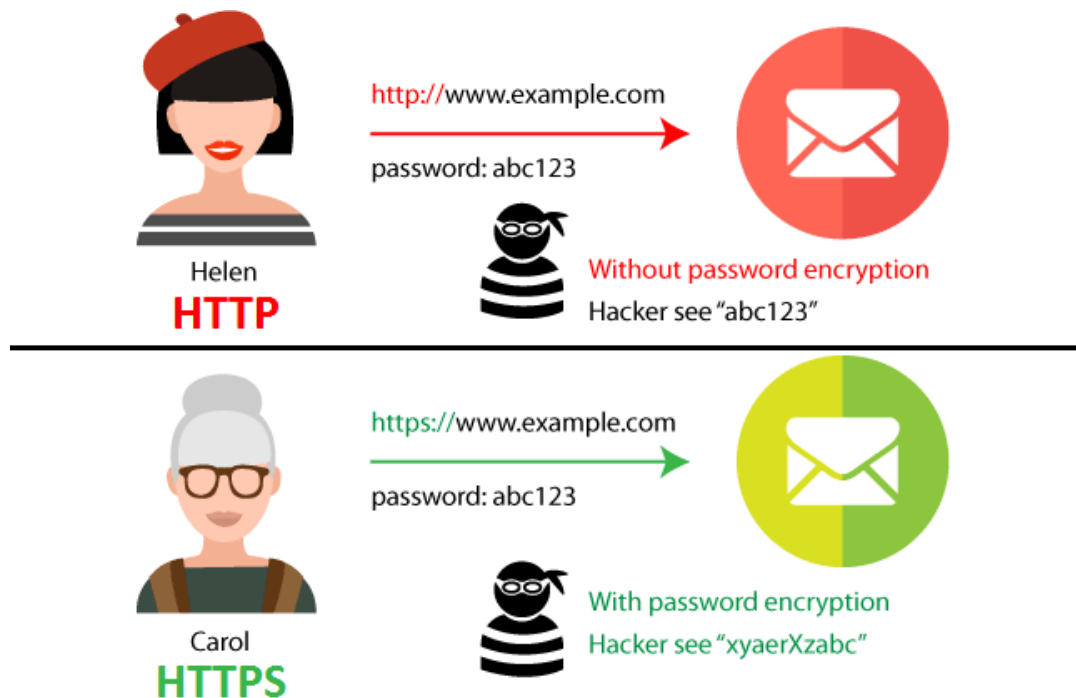
Negociação e Verificação de Chaves

- “Terceiro Confiável”
 - Fornece a chave pública de uma entidade
- Procedimento Simplificado (Navegador x Server)
 - Negociam algoritmos
 - Trocam chaves públicas
 - **Validam as chaves x domínios (autoridades)**
 - Geram chaves secretas de comunicação
 - Codificam com chave pública e enviam pra parte
 - Passam a trocar mensagens criptografadas

<https://www.davidsonsilva.com.br/seguranca-com-o-protocolo-https/>

Exemplos de Usos

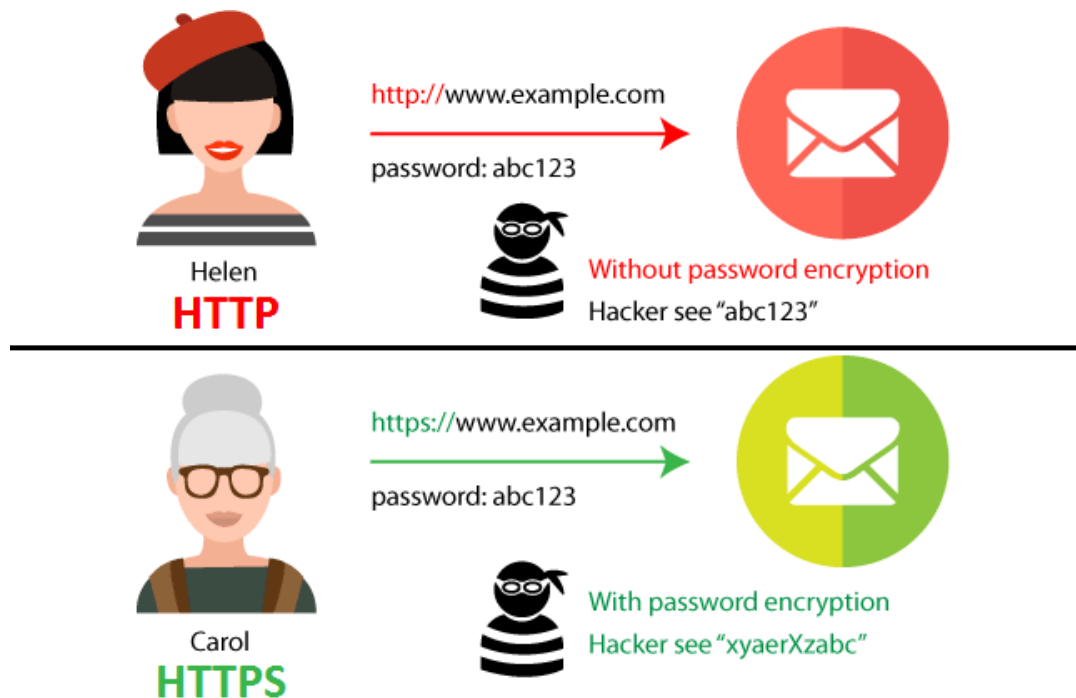
- HTTPS: Servidor Web x Navegador Web
 - Configuração de segurança do Apache
 - Avaliação de certificado no Firefox



Exemplo!

Exemplos de Usos

- HTTPS: Servidor Web x Navegador Web
 - Configuração de segurança do Apache
 - Avaliação de certificado no Firefox

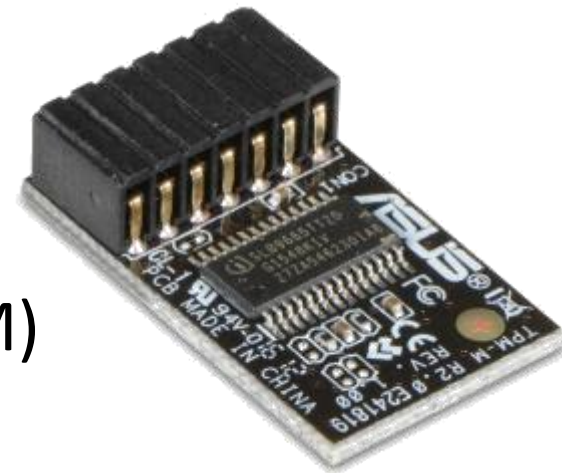


Exemplo!



Exemplos de Usos

- HTTPS: Servidor Web x Navegador Web
 - Configuração de segurança do Apache
 - Avaliação de certificado no Firefox
- Outros usos
 - SSH, VPN, WiFi (WPA x)
 - PGP
 - Trusted Platform Module (TPM)
 - ...





HARDENING

Hardening

- O que é?
 - “Blindagem”.
- Como se faz?
 - Configurar adequadamente o SO
 - Configurar adequadamente os serviços
 - Configurar adequadamente os programas.
- Propósito:
 - Diminuir riscos de invasão ou sucesso em ataques.



Hardening

- Procedimento para Atenuação de Riscos:
 - Mapear ameaças
 - Desativar serviços desnecessários
 - Retirar privilégios desnecessários
 - Atuar com atividades preventivas e corretivas.



Hardening - Exemplos

- Tarefas Básicas
 - Manter sistemas atualizados
 - apt-get update / apt-get upgrade
 - yum update / Windows Update

Exemplo!



Hardening - Exemplos

- Tarefas Básicas

- Manter sistemas atualizados

- `apt-get update / apt-get upgrade`
- `yum update / Windows Update`

- Limpar contas de usuários

- Manter privilégios adequados (`sudo`, grupos...)
- Ajustar a segurança no sistema de arquivos.

- Rever serviços necessários no sistema

- `Telnet`, `sshd`, `ftpd`, `identd`...

- Monitorar os logs de sistema

- `Syslog`, `access.log` etc....



Hardening - Exemplos



- Uso do Sudo

- visudo ou nano /etc/sudoers

- Privilégio de usuário

- maria ALL=/usr/bin/apt-get,/bin/nano /etc/passwd

- Privilégio de grupo

- %sudo ALL=(ALL:ALL) ALL

- Criando “grupos” de usuários

- User_Alias ADMINS = fulano,cicrano

- ADMINS ALL=(ALL:ALL) ALL

- Criando “grupos” de comandos

- Cmd_Alias UPDATE = /usr/bin/apt-get

Exemplo!

Hardening - Exemplos

- Configuração do SSHD
 - `nano /etc/ssh/sshd_config`
 - Não permitir login de root pelo SSH
`PermitRootLogin no`
 - Mudar a porta do SSH
`Port 7722` (valor qualquer, evite nmap com o firewall!)

Exemplo!

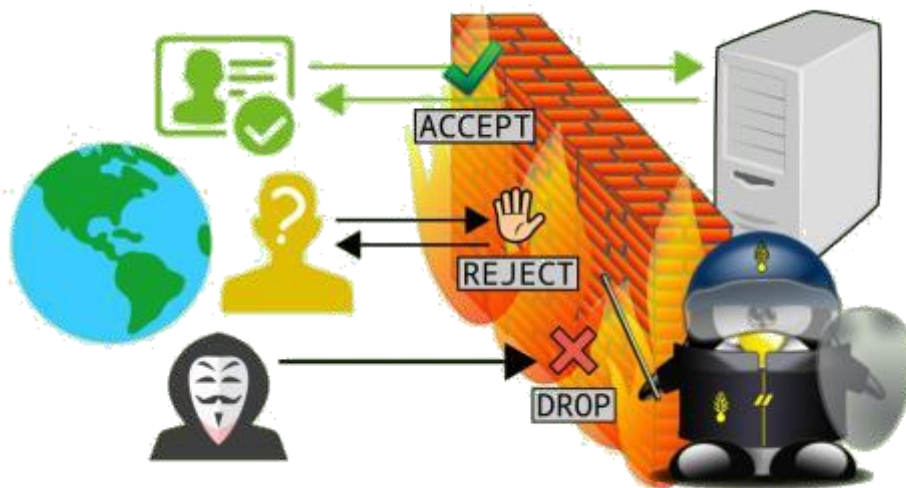
Hardening - Exemplos

- Configuração do SSHD
 - `nano /etc/ssh/sshd_config`
 - Não permitir login de root pelo SSH
`PermitRootLogin no`
 - Mudar a porta do SSH
`Port 7722` (valor qualquer, evite nmap com o firewall!)



Hardening - Exemplos

- Configurar Firewall
 - Liberar apenas o estritamente necessário...
 - Ou seja: Bloquear tudo que não é necessário
 - Endereços, portas, protocolos...
 - Não usar REJECT
 - Use DROP



Exemplo!

QUESTÕES DE IoT



Questões de IoT

- Maioria dos dispositivos: dados por WiFi
 - Segurança mais delicada
- Permitem controle/monitoramento
 - Da casa ou da empresa
- Podem possuir falhas que permitam...
 - Instalação de malwares, sniffers, etc.



Questões de IoT - Soluções

- Proteção das redes da casa
 - Firewall, criptografia, tudo que for possível
- Controle pela rede
 - Não rotear dados de equipamentos IoT <-> WAN
- Vídeos sugeridos
 - Técnicas já estudadas aplicadas em IoT





ATIVIDADE AVALIATIVA

Atividade Avaliativa B

- Vale: 2,5 na AV2
- Individual
 - Instalar o WireShark
 - Use google hacking para achar site sem criptografia
 - Capture pacotes abertos
 - Analise os pacotes em busca de algo interessante
 - Procure um site com criptografia (a maioria, hoje)
 - Capture pacotes
 - Analise e veja se consegue encontrar algo útil
 - Documente todo o processo (entrega).



ENCERRAMENTO

Resumo e Próximos Passos

- Várias técnicas de proteção
 - Criptografia
 - Hardening
 - Segurança em IoT
 - Atividade Avaliativa
 - **Pós Aula:** Saiba Mais, A Seguir... e Desafio!
 - No mural: <https://padlet.com/djcaetano/segciber>
-
- Ocorrência de incidentes...
 - Como reagir?



PERGUNTAS?