Aula 2

Segurança em Sistemas de Informação

Prof. Douglas Eduardo Basso

1

Conversa Inicial

2

Conversa Inicial

- Nessa aula, vamos apresentar alguns *frameworks* de gestão de apoio à segurança da informação, com destaque para o CIS Controls e o NIST CSF. Além disso, vamos falar sobre a criptografia e suas técnicas, as funções *hash*, a assinatura, a certificação digital e os algoritmos de criptografia simétrica e assimétrica. O objetivo dessa aula é conhecer os principais mecanismos de segurança na Internet

3

Frameworks de gestão e apoio à segurança da informação

4

Frameworks de gestão de apoio à SI

- Um *framework* de gestão e apoio à segurança da informação nada mais é que uma série de procedimentos e guias que são utilizados na definição de políticas e processos relacionados à segurança

5

CIS *Controls*

- Os controles CIS (*Center for Internet Security*) são basicamente conjuntos desenvolvidos de práticas recomendadas em segurança cibernética, ações defensivas que visam minimizar e evitar ataques cibernéticos

6

NIST CSF

- **O intuito desse framework é criar um aprimoramento nas capacidades de prevenção, detecção e resposta a diversos tipos de ataques cibernéticos. Nesse *framework*, os fatores relacionados ao negócio possuem um peso maior. Seu enfoque está sobre médias e grandes empresas, devido à complexidade de sua concepção**

7

MITRE ATT & CK

- **O MITRE (*Massachusetts Instituto of Technology Research & Engineering*) é uma grande instituição americana financiada pelo governo sem fins lucrativos. Esse instituto vai além da cibersegurança e possui uma série de inovações relacionadas a campos da área militar e computação**

8

Security ScoreCard

- **A *Security Scorecard* é uma empresa que atua no segmento de segurança da informação que busca avaliar a maneira que a segurança cibernética está sendo implementada e executada em organizações e entidades corporativas**

9

Introdução à criptografia

10

Introdução à criptografia

- **A segurança da informação teve que migrar para esse cenário de Internet, mensagens eletrônicas, aplicações baseadas na Internet, computação em nuvem, entre outros. Dentro desse cenário, a criptografia é essencial para a garantir a confidencialidade, integridade e autenticação**

11

Criptografia

- **Podemos dizer que criptografia é uma área que cria, desenvolve e estuda técnicas seguras de comunicação que permitam a leitura de mensagens apenas para os referidos emissores e receptores**

12

Criptografia clássica

- A chamada criptografia clássica surgiu com os povos antigos. Antes da Idade Média, os hebreus e romanos utilizavam formas simples de substituição, monoalfabéticas e monogâmicas, fazendo trocas de caracteres um pelo outro

13

Criptografia moderna

- Quando falamos de criptografia moderna, podemos dizer que foi iniciada juntamente com o surgimento da mecanização. Equipamentos foram desenvolvidos para acelerar alguns processos de cifragem e decifragem e métodos para criptoanálise

14

Algoritmos e protocolos de criptografia

- Os algoritmos e protocolos de criptografia podem ser agrupados em quatro áreas principais:

15

- Encriptação simétrica: utilizada para ocultar o conteúdo dos blocos ou fluxos contínuos de dados de qualquer tamanho, incluindo mensagens, arquivos, chaves de encriptação e senhas
- Encriptação assimétrica: usada para ocultar pequenos blocos de dados, como valores de função *hash* e chaves de encriptação, que são usados em assinaturas digitais

16

- Algoritmos de integridade de dados: usados para proteger blocos de dados, como mensagens, de possíveis alterações
- Protocolos de autenticação: são esquemas baseados no uso de algoritmos criptográficos projetados para autenticar a identidade de entidades

17

Padrões de segurança de redes sem fio

- Alguns padrões de criptografia foram criados para a redes *wireless.* Entre eles, podemos destacar:
  - WEP
  - WPA
  - WPA2
  - WPA3

18

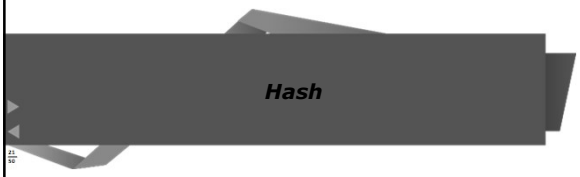
Mecanismos de segurança

- Existem alguns mecanismos e recursos de segurança que podem ser utilizados, entre os quais podemos destacar:
  - Controles físicos
  - Controles lógicos
  - Mecanismos de criptografia
  - Assinatura digital

19

- Mecanismos de garantia da integridade da informação
- Mecanismos de controle de acesso
- Mecanismos de certificação
- Integridade
- *Honeypot*

20



21

Hashs

- Os *hashs* são utilizados para fazer a identificação de funções criptográficas. As funcionalidades de codificação de dados concatenam caracteres de maneira exclusiva, gerando uma espécie de carimbo, para garantir a autenticidade de dados, armazenar senhas de segurança e assinar documentos de maneira digital

22

História das funções *hashs*

- A primeira função *hash,* criada em 1961, tinha o intuito de fazer uma verificação cíclica de redundância, isto é, foi gerada para fazer a checagem e correção de dados transmitidos pela rede, como a Internet. Isso desencadeou novas implementações de funções *hash*, entre as quais podemos elencar:

23

- MD2: uma das pioneiras funções *hash* criptográficas foi implementada em 1989 por Ronald Rivest. Era uma função muito utilizada na segurança da Internet, e a sua evolução levou à criação da MD5, padrão muito empregado atualmente
- RIPEMD: em 1992, o projeto europeu RIPE criou essa função, que foi implementada para substituir o então *hash* MD4. É considerada uma função extremamente segura

24

- **SHA: é um padrão atual de *hashes* criptográficos. Foi desenvolvido pela NSA em 1993, como componente de um projeto para autenticar documentos eletrônicos. O SHA e suas evoluções são considerados as funções *hashes* mais seguras na atualidade. A criptomoeda *Bitcoin* utiliza o SHA-256 como tecnologia de segurança**

25

Propriedades e requisitos do *hash*

- **Há três características que merecem destaque:**
  - **Resistência à pré-imagem**
  - **Resistência à segunda pré-imagem**
  - **Resistência à colisão**

26

Algoritmos *hash* criptografados

- **Entre as funções criptográficas mais comumente utilizadas atualmente, estão o MD5, Whirlpool, SHA-1, SHA-2 e o SHA-3. As funções *hash* devem garantir que as mensagens específicas sejam identificadas de uma maneira única e impossivelmente duplicável**

27

- **MD5 (*Message Digest Algorithm 5*): trata-se de uma função de dispersão criptográfica unidirecional de 128 *bits* criada pela RSA em 1991. É empregada em aplicações e *softwares* com protocolo de conexão ponto a ponto para checagem e verificação de integridade de autenticação e transferência de arquivos**
- ***Whirlpool*: é um dos algoritmos de criptografia que utiliza codificação livre, utilizado pela Organização Internacional de Padronização (ISO) e pela Comissão Eletrotécnica Internacional (IEC)**

28

- **SHA-1 (*Secure Hash Algorithm 1*): foi projetado e desenvolvido pela Agencia Nacional de Segurança (NSA) dos Estados Unidos. Publicado pela NIST, implementa um valor de dispersão de 160 *bits* (20 *bytes*). O SHA-1 integra uma série de aplicações e protocolos de segurança, incluindo o TLS e o SSL. O SHA-1 também é implementado em sistemas de controle de revisão distribuídos, como o *Git.* Através do SHA-1, é possível detectar alteração ou modificação de dados**

29

- **SHA-2 (*Secure Hash Algorithm 2*): foi implementado em 2001 pelo NIST, em uma composição *hash* de 224, 256, 384 ou 512 bits. É utilizado em procedimentos de autenticação de pacotes da distribuição Linux Debian e também em assinaturas de mensagens DKIM. Algumas criptomoedas utilizam o SHA-2 para checagem de transações**

30

- **SHA-3 (*Secure Hash Algorithm 3*): desenvolvido por Keccak, foi disponibilizado em 2015 para substituir o SHA-2 e o SHA-1. O SHA-3 é atualmente o algoritmo criptográfico mais seguro e eficiente do mundo, garantindo integridade de dados em transações digitais. Sua grande vantagem é poder ser implementado em uma grande variedade de dispositivos embarcados, móveis, entre outros, e permite a entrada e saída de dados com tamanhos variáveis. Para Stallings, a estrutura básica do SHA-3 é um esquema denominado por seus projetistas de construção em esponja. A construção em esponja tem a mesma estrutura geral de outras funções *hash* iterativas, isto é, recebe uma mensagem de entrada e divide em blocos de tamanho fixo**

31

Aplicações com *hash*

- **Autenticação de mensagens**
- **Assinatura digital**
- **Carteira de endereços**
- **Mineração de moedas virtuais**
- **Contratos inteligentes**

32

Chave simétrica e assimétrica

33

Chave simétrica e assimétrica

- **Para a segurança da informação, os algoritmos de criptografia são indispensáveis. As chaves de segurança possibilitam a verificação, a checagem e a validação de informações. Esses processos podem ser feitos utilizando duas técnicas de criptografia: a simétrica e a assimétrica**

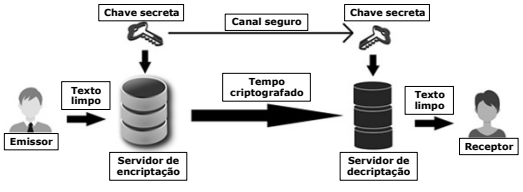
34

Algoritmos de criptografia simétrica

- **Os algoritmos de criptografia simétrica apresentam algumas vantagens. Entre elas, está a simplicidade, uma vez que estes algoritmos apresentam facilidade de utilização e rapidez para executar o processamento criptográfico**

35

Criptografia Simétrica



Ujjwal Swami/Shutterstock

36

- **Entre os algoritmos de criptografia simétrica, podemos destacar:**
  - **AES (*Advanced Encryption Standard*)**
  - **DES (*Data Encryption Standard*)**
  - **3DES (*Triple Data Encryption Standard*)**
  - **IDEA (*Internacional Encryption Algorithm*)**

37

- **Entre os algoritmos de criptografia simétrica, podemos destacar:**
  - ***Blowfish***
  - ***Twofish***
  - **RC (*Cifra Rivest*)**
  - **CAST (*Carlisle Adams and Stafford Tavares*)**

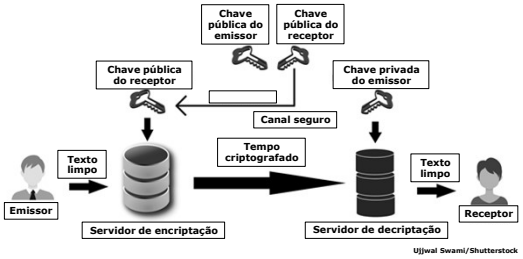
38

Algoritmos de criptografia assimétrica

- **As principais vantagens desse método é a segurança, pois não é necessário compartilhar nenhum tipo de chave. Entretanto, o tempo de processamento de mensagens dos algoritmos de criptografia assimétrica é mais elevado em relação aos algoritmos de segurança assimétrica**

39

Criptografia Assimétrica



40

- **Entre os algoritmos de criptografia assimétrica, podemos destacar:**
  - **RSA (*Rivest Shamir Adleman*)**
  - **ElGamal**
  - **Diffie-Hellman**
  - **Curvas Elípticas (ECC)**

41

Assinatura e certificação digital

42

Assinatura digital

- A assinatura digital é um código digital concatenado com uma mensagem transmitida de maneira eletrônica e que faz a identificação do emissor de modo único, com a garantia de integridade da mensagem. A assinatura garante que a mensagem não foi adulterada, ou seja, que a mensagem é íntegra, e o remetente atesta que realmente é quem diz ser. É uma prova de autenticidade do emissor, bem como um endosso da origem dos dados

43

- A assinatura digital deve cumprir algumas premissas, tais como:
  - Verificação de autoria, data e hora de assinatura
  - Validação e autenticação de todo o conteúdo da mensagem no ato da assinatura
  - Caso seja checado por terceiros, garantir a validade e integridade

44

Certificado digital

- O certificado digital é um processo de garantia de que uma chave pública pertence efetivamente a uma pessoa ou uma empresa. Essa garantia é alcançada a partir da combinação de assinatura digital com Autoridade Certificadora (CA). Os certificados digitais são arquivos que possuem a chave pública e as informações pessoais do seu proprietário, fazendo, assim, a associação da identidade do utilizador com a sua chave pública correspondente. São validados e assinados de maneira digital pela Autoridade Certificadora

45

- Em algumas situações, os certificados podem ser revogados para o mesmo autor:
  - Quando a sua validade, previamente definida, acaba expirando, logo deixam de produzir os seus efeitos
  - Quando ocorre algum problema de comprometimento de chaves, tornando-se, então, necessário proceder com a sua invalidação

46

Requisitos de assinaturas digitais

- A assinatura deve apresentar um padrão de *bits* que depende do fechamento e assinatura da mensagem
- A assinatura deve usar algumas informações exclusivas do emissor, para que, dessa maneira, possa ser impedida a falsificação e a negação

47

- É preciso ser relativamente fácil produzir a assinatura digital
- É preciso ser relativamente fácil reconhecer e verificar a assinatura digital

48

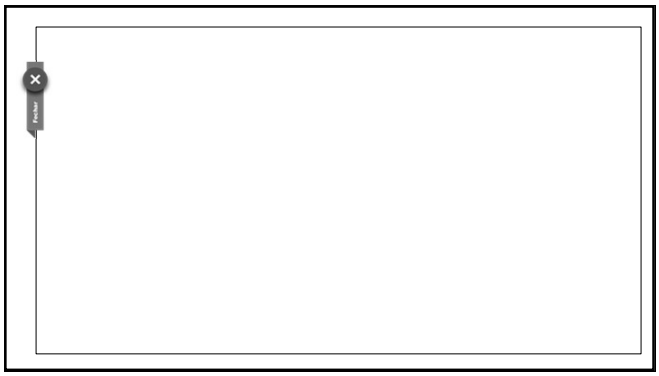
- **É preciso ser computacionalmente inviável falsificar uma assinatura digital, seja construindo uma nova mensagem para uma assinatura digital existente, seja uma assinatura digital fraudada para determinada mensagem**
- **É preciso ser prática a retenção de uma cópia de assinatura digital em termos de armazenamento**

49

Certificados X.509

- **A padronização X.509 apresenta algumas boas práticas em relação a serviços de diretório, que nada mais são que um servidor ou grupo de servidores (sistema distribuído) que mantêm disponível um banco de dados com todas as informações dos usuários**

50



51