MBA USP ESALQ

Fundamentos da Segurança da Informação

Rodolfo Ipolito Meneguette

*A responsabilidade pela idoneidade, originalidade e licitude dos conteúdos didáticos apresentados é do professor.

AGENDA

- Criptografia
- Exemplos
  - Porta scan
  - Homem no meio

APRESENTAÇÃO DO PROFESSOR

- Formação;
- Experiência com segurança;
- Linha de Pesquisa.

CRIPTOGRAFIA

(kriptos = oculto
+ graphos = grafia)

“Arte ou a ciência de escrever em cifras (código).”

VISÃO GERAL

O que a criptografia pode e não pode fazer?

A garantia de 100% de segurança é uma falácia, mas é possível trabalhar em direção a 100% de aceitação de riscos.

- “Um bom sistema criptográfico atinge o equilíbrio entre o que é possível e o que é aceitável.”

CRIPTOGRAFIA – FUNDAMENTOS

O QUE A CRIPTOGRAFIA PODE E NÃO PODE FAZER?

CRIPTOGRAFIA - Conjunto de técnicas que permitem tornar "incompreensível" uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinatário a decifre e a compreenda.

CRIPTOANÁLISE - do grego kryptos + análysis (decomposição) - ciência que estuda a decomposição do que está oculto ou a "quebra" do sistema criptográfico.

CRIPTOLOGIA - Criptografia + Criptoanálise.

CRIPTOGRAFIA – FUNDAMENTOS

PRÉ-REQUISITOS DA CRIPTOGRAFIA

- Teoria de Números;
- Matemática Discreta;
- Teoria da Informação;
- Teoria de Probabilidade;
- Complexidade Computacional;
- Processamento de Sinais.

CRIPTOGRAFIA – FUNDAMENTOS

TERMO	DESCRIÇÃO
Texto claro, simples	Mensagem original
Cifração ou criptografia	Processo de “embaralhar” a mensagem de forma a ocultar seu conteúdo de outrem
Texto cifrado ou criptograma	Mensagem cifrada
Decifração ou descriptografia	Processo inverso de recuperação da mensagem a partir do criptograma
Chave criptográfica	Parâmetro de controle. Segredo por meio do qual a mensagem pode ser cifrada ou decifrada

CRIPTOGRAFIA – FUNDAMENTOS

TERMO	DESCRIÇÃO
Algoritmo criptográfico	Transformação matemática - converte uma mensagem em claro em uma mensagem cifrada e vice-versa.
Alice	**Origem** - Cifra uma mensagem.
Bob	**Destino** - Decifra uma mensagem.
Eva	**Intruso** – tenta interceptar e decifrar a mensagem.

CRIPTOGRAFIA – FUNDAMENTOS

DIVISÕES DA CRIPTOGRAFIA

- Criptografia fraca;
- Criptografia forte.

CRIPTOGRAFIA – FUNDAMENTOS

CRIPTOGRAFIA FRACA:

Maneira banal de tentar ocultar informações de pessoas leigas no assunto.

Exemplo: jogo criptograma, a pessoa deve chegar a identificar uma frase analisando certos símbolos.

CRIPTOGRAFIA – FUNDAMENTOS

CRIPTOGRAFIA FORTE:

De alta complexidade que visa manter as informações ocultas mesmo sob intensa verificação de supercomputadores.

- Pode ser feita de duas formas: em **chaves simétricas** ou em **chaves assimétricas**.

Exemplo: PGP (*Pretty Good Privacy*).

Geralmente, a maneira mais fácil de determinar se um algoritmo é forte ou fraco consiste em publicar sua descrição, fazendo com que várias pessoas possam discutir sobre a eficiência ou não dos métodos utilizados.

CRIPTOGRAFIA SIMÉTRICA X ASSIMÉTRICA

Número de chaves necessárias/número de participantes:

Nº de participantes	Criptografia Simétrica n(n-1)/2	Criptografia Assimétrica 2n
2	1	4
4	6	8
8	28	16
16	120	32

CRIPTOGRAFIA SIMÉTRICA X ASSIMÉTRICA

SIMÉTRICA	ASSIMÉTRICA
FUNCIONAMENTO • Utiliza um algoritmo e uma chave para cifrar e decifrar.	**FUNCIONAMENTO** • Utiliza um algoritmo e um par de chaves para cifrar e decifrar.
REQUISITO DE SEGURANÇA • A chave tem que ser mantida em segredo; • Tem que ser impossível decifrar a mensagem; • Algoritmo mais alguma parte do texto cifrado devem ser insuficientes para obter a chave.	**REQUISITO DE SEGURANÇA** • Uma chave é pública e a outra tem que ser mantida em segredo; • Algoritmo com alguma parte do texto cifrado com uma das chaves não devem ser suficientes para obter a outra chave.

CRIPTOGRAFIA SIMÉTRICA X ASSIMÉTRICA

PROBLEMAS

Criptografia Simétrica

- Como distribuir e armazenar as chaves secretas de forma segura?
- Quantas chaves são necessárias para uma comunicação segura entre *n* pessoas?

Criptografia Assimétrica

- Como garantir que o detentor da chave pública é realmente quem diz ser?
- Necessidade de ter uma infraestrutura para armazenar as chaves públicas.

CRIPTOGRAFIA – AUTENTICAÇÃO

Algumas vezes há a necessidade de se provar quem escreveu um documento e de manter as informações desse documento sem modificações.

SOLUÇÃO: serviços de autenticação e integridade de dados.

A autenticidade de muitos documentos é determinada pela presença de uma **ASSINATURA DIGITAL**.

CRIPTOGRAFIA – AUTENTICAÇÃO

ASSINATURA DIGITAL – item que acompanha um determinado dado e apresenta as seguintes funções:

1. Confirmar a origem do dado;
2. Certificar que o dado não foi modificado;
3. Impedir a negação de origem.

ASSINATURA DIGITAL

Vantagens provenientes do envio de mensagem "***assinada***":

1. O receptor poderá verificar a identidade alegada pelo transmissor;

2. Posteriormente, o transmissor não poderá repudiar o conteúdo da mensagem;

3. O receptor não terá a possibilidade de forjar ele mesmo a mensagem;

ASSINATURA DIGITAL

- Assinaturas de Chave Simétrica;
- Assinaturas de Chave Pública;
- Sumários de mensagens (*Message Digests*);
- Aplicações Práticas.

ASSINATURA DIGITAL

ASSINATURA DE CHAVE SIMÉTRICA

Estratégia – uso de uma autoridade central que saiba de tudo e na qual todos confiem (BB - Big Brother).

- Cada usuário escolhe uma chave secreta e a leva para o BB;
- Somente Alice e BB conhecem a chave secreta de Alice, KA, e assim por diante.

ASSINATURA DIGITAL

PROBLEMAS - ASSINATURAS DE CHAVE SIMÉTRICA

- Todos têm de confiar no BB;
- O BB tem de ler todas as mensagens assinadas.

ASSINATURAS DIGITAIS – Assimétrica

Transmissor (Bob) assina digitalmente o documento, atestando que ele é o dono/criador do documento.

Verificável, não falsificável e incontestável (irretratabilidade): destinatário (Alice) pode verificar que Bob, e ninguém mais, assinou o documento.

ASSINATURAS DIGITAIS

Assinatura digital simples para a mensagem *m*:

- Bob codifica **m** com a sua chave privada d_B, criando a mensagem assinada, $d_B(m)$;
- Bob envia **m** e $d_B(m)$ para Alice.

Dear Alice;

This is a message for Alice, This is a message for Alice, This is a message for Alice, This is a message for Alice.

Bob.

Chave privada de Bob

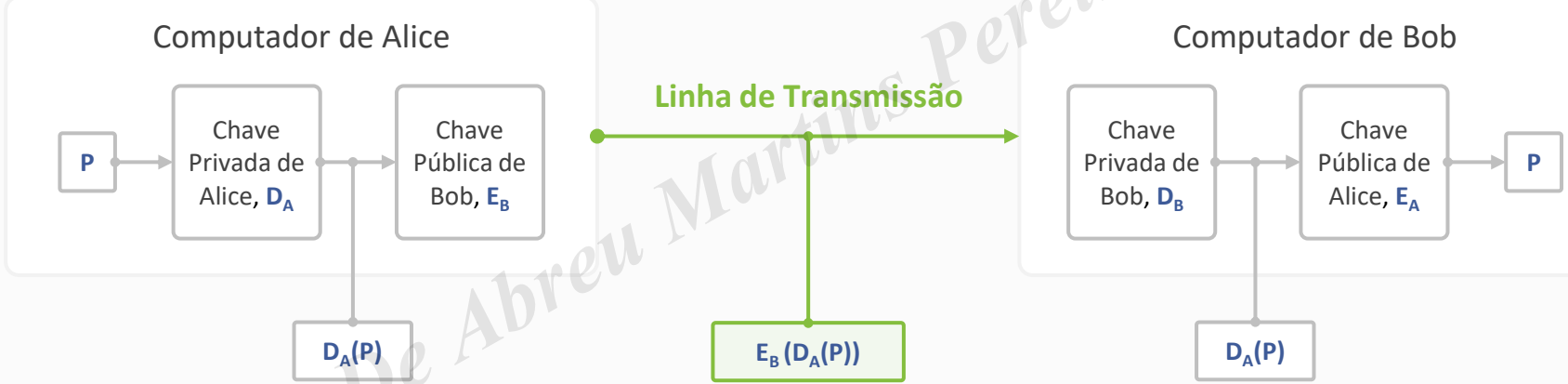
TEXTO

CRIPTOGRAFADO

Mensagem pronta para transmissão

ASSINATURA DIGITAI

Assinaturas de Chave Pública



Assinaturas digitais com o uso de **chave pública**.

ASSINATURA DIGITAL

ASSINATURAS DE CHAVE PÚBLICA - PROBLEMAS RELACIONADOS AO AMBIENTE NO QUAL OPERAM

Bob só poderá provar que uma mensagem foi enviada por Alice enquanto D_A permanecer secreta.

Se Alice revelar sua chave secreta, o argumento deixará de existir - qualquer um poderá ter enviado a mensagem.

- **O que acontecerá se Alice decidir alterar sua chave?**

ASSINATURA DIGITAL

CRIPTOGRAFIA ASSIMÉTRICA (CHAVE PÚBLICA) - CRÍTICAS

- Reúnem **SIGILO** e **AUTENTICAÇÃO**;
- Em geral, o sigilo não é necessário;
- Cifragem da mensagem inteira é lenta.

SOLUÇÃO: assinar a mensagem sem cifrá-la completamente.

SUMÁRIOS DE MENSAGENS.

ASSINATURA DIGITAL

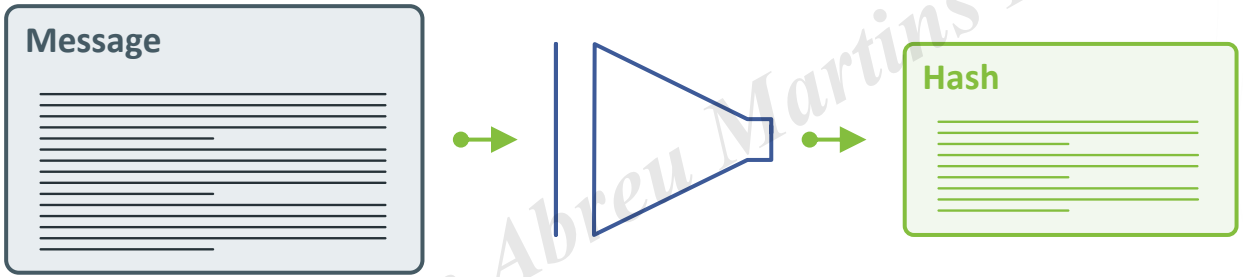
SUMÁRIOS DE MENSAGENS (*MESSAGE DIGESTS*)

- Uso de uma função *hash* unidirecional que extrai um trecho qualquer do texto simples e, a partir deste, calcula um *string* de bits de tamanho fixo.

- **Função *hash*** – geralmente denominada **sumário de mensagens** (MD).

ASSINATURA DIGITAL

HASH - Algoritmo que faz o mapeamento de uma sequência de bits de tamanho arbitrário para uma sequência de bits de tamanho fixo menor, de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash.



FUNÇÃO HASH - funciona como uma **impressão digital de uma mensagem** gerando, a partir de uma entrada de tamanho variável, um valor fixo pequeno: o **digest** ou **valor hash**.

ASSINATURA DIGITAL

MD - PROPRIEDADES IMPORTANTES

- Se *P* for fornecido, o cálculo de *MD(P)* será muito fácil;
- Se *MD(P)* for fornecido, será efetivamente impossível encontrar *P;*
- Dado *P*, não deve ser possível encontrar *P´* tal que *MD(P´) = MD(P);*
- Uma mudança na entrada de até mesmo 1 bit produz uma saída muito diferente.

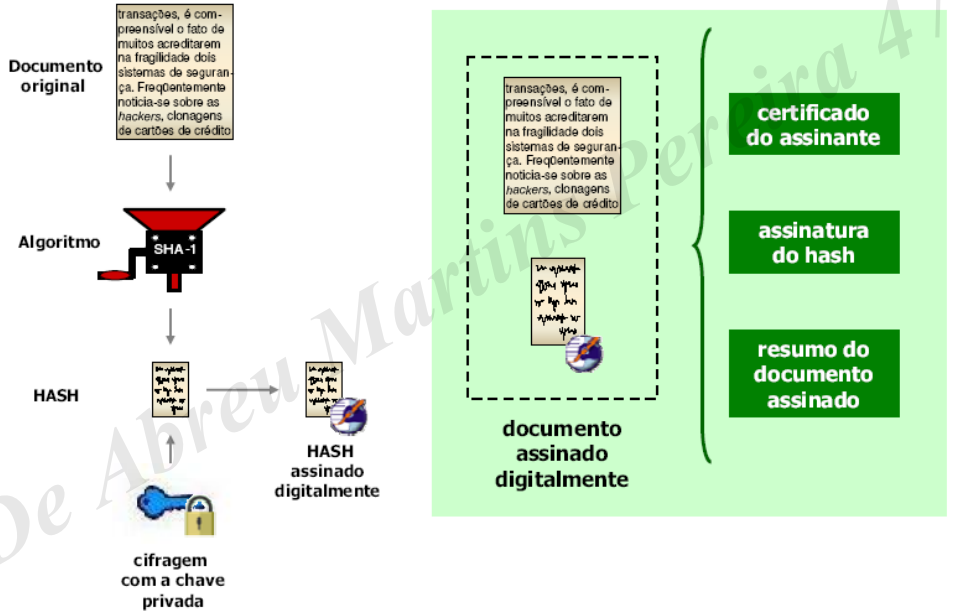
ASSINATURA DIGITAL

MESSAGE DIGESTS - PROPRIEDADES IMPORTANTES

- Gera um sumário de **tamanho fixo** para qualquer comprimento de mensagem;
- Efetivamente impossível **adivinhar** a **mensagem** a partir do sumário;
- Efetivamente impossível encontrar outra mensagem que gere o **mesmo sumário**;
- Uma pequena mudança na mensagem **altera** bastante o sumário.

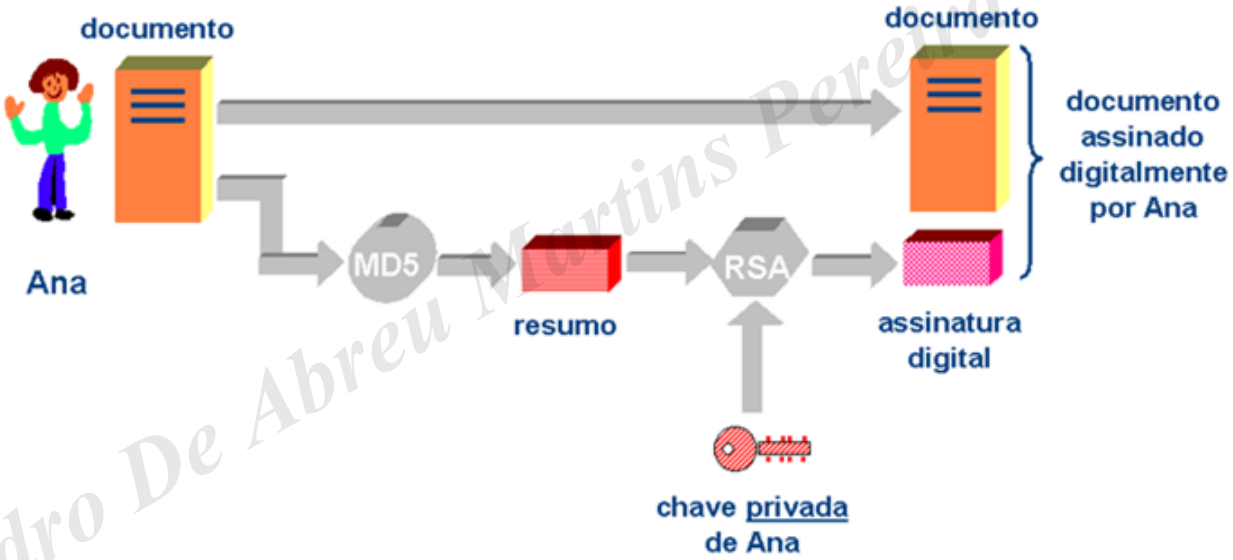
FUNÇÃO HASH – MESSAGE DIGESTS

ASSINATURA DIGITAL – GERAÇÃO



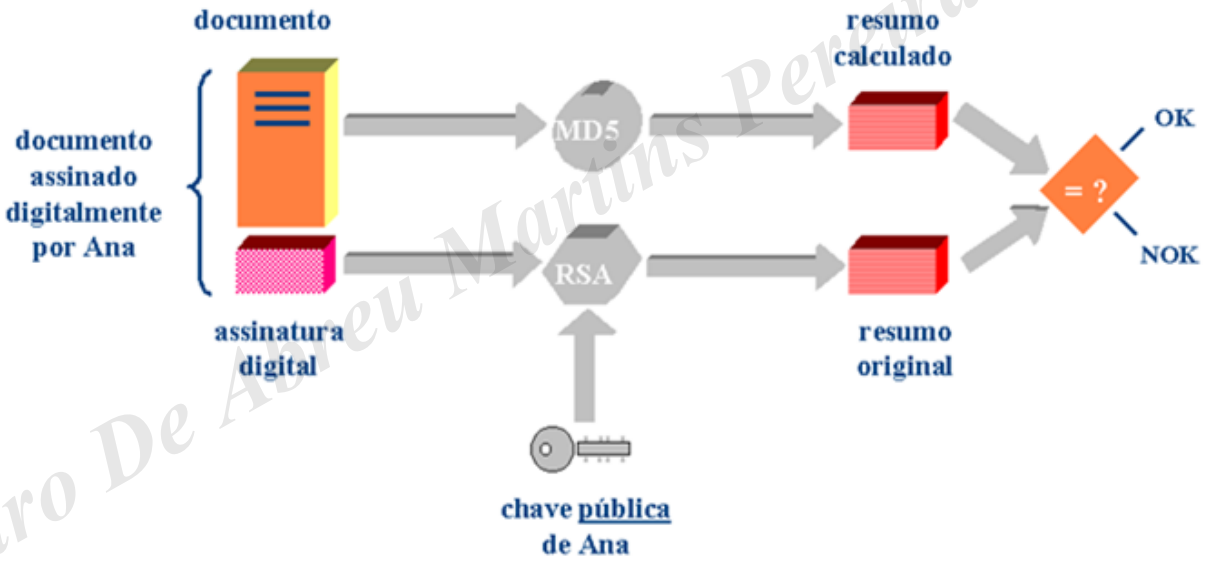
SEGURANÇA NA INTERNET

Função Hashing



SEGURANÇA NA INTERNET

Função Hashing



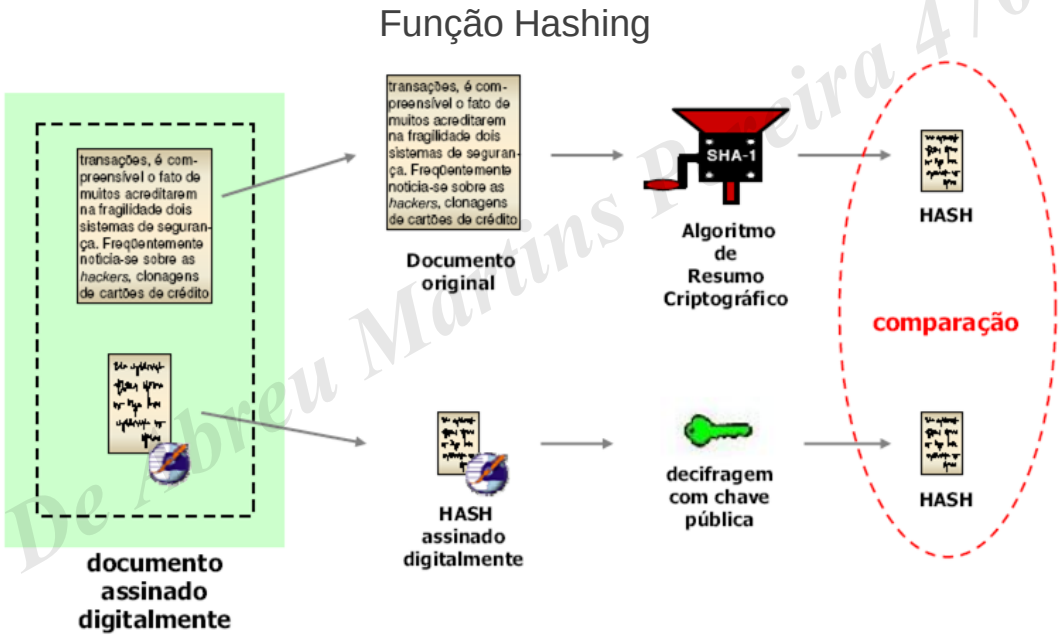
ASSINATURA DIGITAL – GERAÇÃO

GERAÇÃO DA ASSINATURA DIGITAL

1. Entra-se com os dados a serem "digeridos" e o algoritmo MD gera um *hash* de 128 ou 160 bits (dependendo do algoritmo).

2. Computada uma MD, criptografa-se o *hash* gerado com uma chave privada.

ASSINATURA DIGITAL – VERIFICAÇÃO



ASSINATURA DIGITAL – VERIFICAÇÃO

VERIFICAÇÃO DA ASSINATURA DIGITAL

1. Executa-se a função MD (usando o mesmo algoritmo MD que foi aplicado ao documento na origem), obtendo-se um *hash* para aquele documento, e posteriormente, decifra-se a assinatura digital com a chave pública do remetente;

2. A assinatura digital decifrada deve produzir o mesmo *hash* gerado pela função MD executada anteriormente;

3. Se estes valores são iguais é determinado que o documento não foi modificado após a assinatura do mesmo, caso contrário o documento ou a assinatura, ou ambos foram alterados.

ASSINATURA DIGITAL – informa apenas que o documento foi modificado, mas não o que foi modificado e o quanto foi modificado.

ASSINATURA DIGITAL

É IMPORTANTE PERCEBER: a assinatura digital, como descrita no exemplo anterior, não garante a confidencialidade da mensagem.

Qualquer um poderá acessá-la e verificá-la, mesmo um intruso (*Eva*), apenas **utilizando a chave pública** de Alice.

ASSINATURA DIGITAL

OBTENÇÃO DE CONFIDENCIALIDADE COM ASSINATURA DIGITAL

Alice

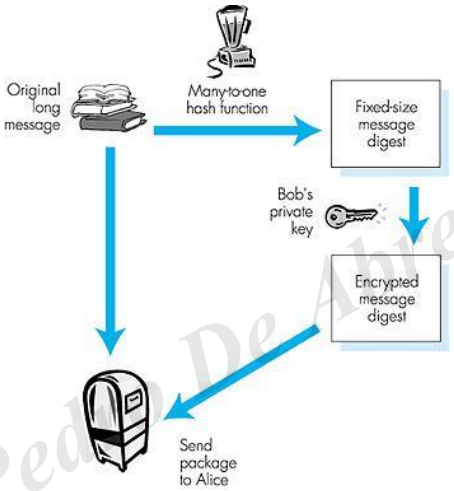
- Assina a mensagem, utilizando sua chave privada.
- Criptografa a mensagem novamente, junto com sua assinatura, utilizando a chave pública de Bob.

Bob

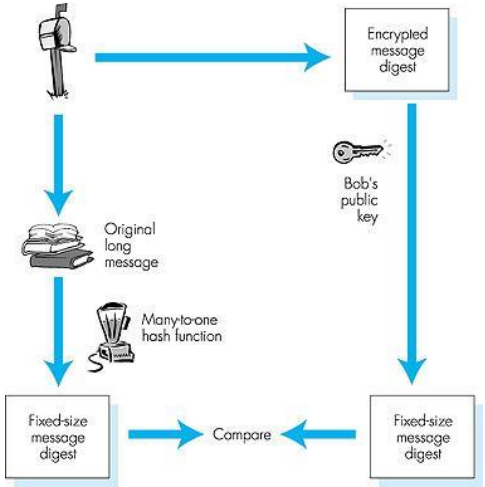
- Ao receber a mensagem, deve decifrá-la com sua chave privada, o que garante sua privacidade.
- “Decifrá-la" novamente, ou seja, verificar sua assinatura utilizando a chave pública de Alice, garantindo assim sua autenticidade.

ASSINATURA DIGITAL = Assinatura do resumo da mensagem

Bob envia mensagem assinada digitalmente



Alice verifica a assinatura e a integridade da mensagem assinada digitalmente



SEGURANÇA NA INTERNET

OBTENDO UMA ASSINATURA DIGITAL

Um certificado digital é um documento eletrônico que contém as informações da identificação de uma pessoa ou de uma instituição. Esse documento deve ser solicitado a uma **AC** ou ainda a uma **AR** (**A**utoridade de **R**egistro). Uma AR tem a função de solicitar certificados a uma AC.

Para que um certificado seja válido, é necessário que o interessado tenha a chave pública da AC para comprovar que aquele certificado foi, de fato, emitido por ela. A questão é que existem inúmeras ACs espalhadas pelo mundo e fica, portanto, inviável ter a chave pública de cada uma.

A solução encontrada para esse problema foi a criação de "ACs supremas" (ou "ACs-Raiz"), ou seja, instituições que autorizam as operações das ACs que emitem certificados a pessoas e empresas. Esse esquema é conhecido como **ICP** (**I**nfraestrutura de **C**haves **P**úblicas) ou, em inglês, PKI (Public Key Infrastructure).

SEGURANÇA NA INTERNET

OBTENDO UMA ASSINATURA DIGITAL

No Brasil, a **ICP-Brasil** controla seis ACs: a **Presidência da República**, a **Receita Federal**, o **SERPRO**, a **Caixa Econômica Federal**, a **Serasa** e a **CertiSign**. Isso significa que, para que tenha valor legal diante do governo brasileiro, uma dessas instituições deve prover o certificado. Porém, para que isso seja feito, cada instituição pode ter requisitos e custos diferentes para a emissão, uma vez que cada entidade pode emitir certificados para finalidades distintas. E isso se aplica a qualquer AC no mundo.

Agora, uma coisa que você deve saber é que qualquer instituição pode criar uma ICP, independente de seu porte. Por exemplo, se uma empresa criou uma política de uso de certificados digitais para a troca de informações entre a matriz e suas filiais, não vai ser necessário pedir tais certificados a uma AC controlada pela ICP-Brasil. A própria empresa pode criar sua ICP e fazer com que um departamento das filiais atue como AC ou AR, solicitando ou emitindo certificados para seus funcionários.

UM EXERCÍCIO ...

Duas pessoas (um remetente e um receptor) têm uma mensagem (documento).

A mensagem do receptor é cópia da mensagem do remetente.

QUESTÃO: a mensagem do receptor é realmente uma cópia ou a mensagem foi alterada durante o trânsito?

UM EXERCÍCIO ...

Para descobrir, eles **resumem as duas mensagens e as compara**.

Se os **resumos forem iguais**, ambos sabem que **as duas versões são correspondentes**. Se os resumos não corresponderem, algo saiu errado.

Como se pode saber **que o resumo do remetente não foi alterado**?

UM EXERCÍCIO ...

Pode-se saber disso **porque ele foi encriptado com a chave privada do remetente**.

Como se pode saber que **ele foi encriptado com a chave privada do remetente**?

Pode-se saber **porque a chave pública apropriada o decripta**.

ALGUMAS OUTRAS VERIFICAÇÕES ...

Um assinante encriptará um **bloco de dados**, consistindo de **um enchimento, o identificador do algoritmo de resumo e o resumo**.

O valor encriptado é a assinatura.

O **identificador do algoritmo** evita que um invasor substitua esse algoritmo, por **outro algoritmo de resumo** alternativo.

ALGUMAS OUTRAS VERIFICAÇÕES ...

Ao usar a chave pública apropriada, essa assinatura é decriptada com o valor do enchimento.

Neste caso, não apenas o **resumo**, mas o **identificador de algoritmo** de resumo *SHA-X* e também os **bytes de enchimento** são verificados.

A CRIPTOGRAFIA BENEFICIA...

A **criptografia de chave simétrica** fornece privacidade sobre os dados sigilosos.

A **criptografia de chave pública** resolve o problema da distribuição de chaves.

Resumo de mensagem - assegura integridade.

A CRIPTOGRAFIA BENEFICIA...

Uma **assinatura** oferece **autenticação**.

A entidade que envia dados deve revelar ser a entidade que afirma ser. Os dados são verificados para garantir que vieram dessa entidade.

Uma **assinatura** também fornece **não repúdio**: quem assina não pode mais tarde desautorizar qualquer conhecimento sobre a mensagem.

Exemplo
Porta SCAN

FOOTPRINTING

- Coleta de informações (footprinting) é a primeira etapa que deve ocorrer em um pentest.
- Consiste em obter todas as informações a respeito da rede: topologia, mapeamento, servidores, funcionários, etc.
- Quanto mais informações coletar do alvo, maior a chance de acesso ao sistema auditado.
- Informações tais como: servidores, roteadores, firewalls, hábitos dos funcionários e sua capacitação e setor de trabalho, pessoas relacionadas à empresa, empresas terceirizadas, e-mails, redes sociais (Facebook, Twitter), telefones, informação jogada no lixo, etc.

FOOTPRINTING – ENUMERAÇÃO DE DNS

- Realiza o mapeamento dos servidores DNS ativos ajudando na coleta de informações com base em DNS.
- Se o servidor DNS não estiver com a proteção de Transferência de Zona protegida e desativada, será transferido para cada registro do NS – Name Server (nsX1, nsX2, firewall) a numeração de todos os servidores. Esta falha permite que o atacante obtenha toda a topologia da rede, ou seja, todo o endereçamento IP que pertence àquele domínio e toda infraestrutura mapeada.
- A transferência de zona é recomendada somente entre os servidores DNS primário e DNS secundário.
- Montado todo o mapeamento da rede, será iniciado a busca por vulnerabilidades naquele domínio.

FOOTPRINTING – ENUMERAÇÃO DE DNS

- Este processo estando bloqueado, não garante que a rede não será invadida, mas evita que o atacante não obtenha, de maneira fácil, todo o mapeamento e infraestrutura.
- Uma outra opção é descobrir as máquinas de um domínio por meio de ataques de força bruta (brute force). Nesta opção é criada uma lista de palavras e testando-as uma a uma, até descobrir qual é o nome que combina com o domínio DNS.

ENUMERAÇÃO DE DNS (FERRAMENTAS)

DNSenum: permite pesquisar hosts, nomes de servidores, regisros MX, IPs e outros.

EXEMPLOS:

#dnsenum kali.com.br

- Com força bruta (*brute force*).

Criar um arquivo com uma lista de palavras contendo os nomes do domínio DNS (adm, firewall, pentest, auditoria, admin, srv etc).

#dnsenum -f /usr/share/dnsenum/dns.txt kali.com.br (*wordlist* própria).

ENUMERAÇÃO DE DNS (FERRAMENTAS)

DNSrecon: mais uma ferramenta para consulta de DNS e enumeração de domínios.

EXEMPLOS: (opção –d domínio).

#dnsrecon –d kali.com.br

OPÇÕES: (–D wordlist e –t tipo de registro a ser usado (brt, axfr)).

#dnsrecon –d kali.com.br –D /root/wordlist –t brt

#dnsrecon –d kali.com.br –D /root/wordlist –t axfr

FOOTPRINTING – ROTAS

Dados que trafegam da sua máquina (origem) até a máquina destino passam por roteadores, que determinarão a melhor rota entre origem e destino.

Algumas ferramentas auxiliam a ver quais são os lugares por onde o pacote passa até ao seu destino.

TRACEROUTE: ferramenta nativa do Linux que utiliza o protocolo ICMP e consegue determinar a rota dos dados.

FOOTPRINTING - ROTAS

PADRÃO:

#traceroute 92.168.1.100

Envia pacotes ICMP Echo Request:

#traceroute –I 192.168.1.100

Envia pacotes TCP SYN (burlar regras de firewall):

#traceroute –T 192.168.1.100

Envia pacotes UDP (burlar regras de firewall):

#traceroute –U 192.168.1.100

FINGERPRINTING

Ao coletarmos informações sobre a rede alvo (topologia, servidores DNS, rota e outros), através do método de *footprinting*, agora é necessário descobrir versões dos SO dos servidores desta rede.

Sendo assim, conseguimos determinar quais ferramentas iremos utilizar para explorar o alvo (*exploits*).

MÉTODOS DE FINGERPRINTING:

PASSIVO: varredura por tipo de escuta/espera de conexões de rede, ou seja, normalmente fica executando um serviço e esperando por tais conexões. Gera-se menos rastros e suspeitas.

ATIVO: varredura para a máquina alvo, ou seja, são enviados pacotes para esta máquina para descobrir a versão do SO.

FINGERPRINTING

PING: envia pacote ICMP Echo Request ao alvo. Campos importantes TTL (Time To Live). Junto com traceroute (Linux) ou tracert (Windows) é possível definir o tipo de SO do servidor alvo.

EXEMPLOS:

#ping www.ifsp.edu.br –c 1

c:\> ping www.ifsp.edu.br

#traceroute www.ifsp.edu.br

c:\> tracert www.ifsp.edu.br

SO	TTL
Linux	64
Windows	128
Unix	255

Através do TTL decrementado ou não, podemos definir o tipo de SO respondido pelo servidor alvo, conforme tabela acima.

FINGERPRINTING ATIVO

Hping3: gerador de pacotes. Possivelmente conseguimos detectar hosts ativos, regras de firewall, varrer portas, testar desempenho da rede, fragmentação de pacotes, TOS, *fingerprinting* e outros.

- Suporta vários protocolos: TCP, UDP, ICMP etc.

FINGERPRINTING ATIVO

EXEMPLOS:

Envia pacotes ICMP Echo Request:

#hping3 192.168.1.100 -1

Limitando o número de pacotes para 3:

#hping3 192.168.1.100 -c 3

Trabalhando com o ICMP (modificando):

#hping3 192.168.1.100 -1 –C 8 –K 0 > ICMP Echo Request.

#hping3 192.168.1.100 -1 –C 0 –K 0 > ICMP Echo Reply.

#hping3 192.168.1.100 -1 –C 13 –K 0 > ICMP Timestamp Request.

FINGERPRINTING ATIVO

Envia pacotes SYN para uma porta específica:

#hping3 192.168.1.100 –S –p 80 > Porta aberta <flags=SA>

#hping3 192.168.1.100 –S –p 81 > Porta fechada <flags=RA>

Pacotes UDP e com porta específica:

#hping3 192.168.1.100 -2

#hping3 192.168.1.100 -2 –p 80 > Porta aberta, não há resposta

#hping3 192.168.1.100 -2 –p 81 > Porta fechada, resposta <name=UNKNOW>

Trabalhando como Port Scanner:

#hping3 192.168.1.100 –c 3 –S **–p ++79** > Inicia varredura a partir da porta 79.

#hping3 192.168.1.100 –S **–-scan 77-81** > Realiza a varredura das portas 77 a 81.

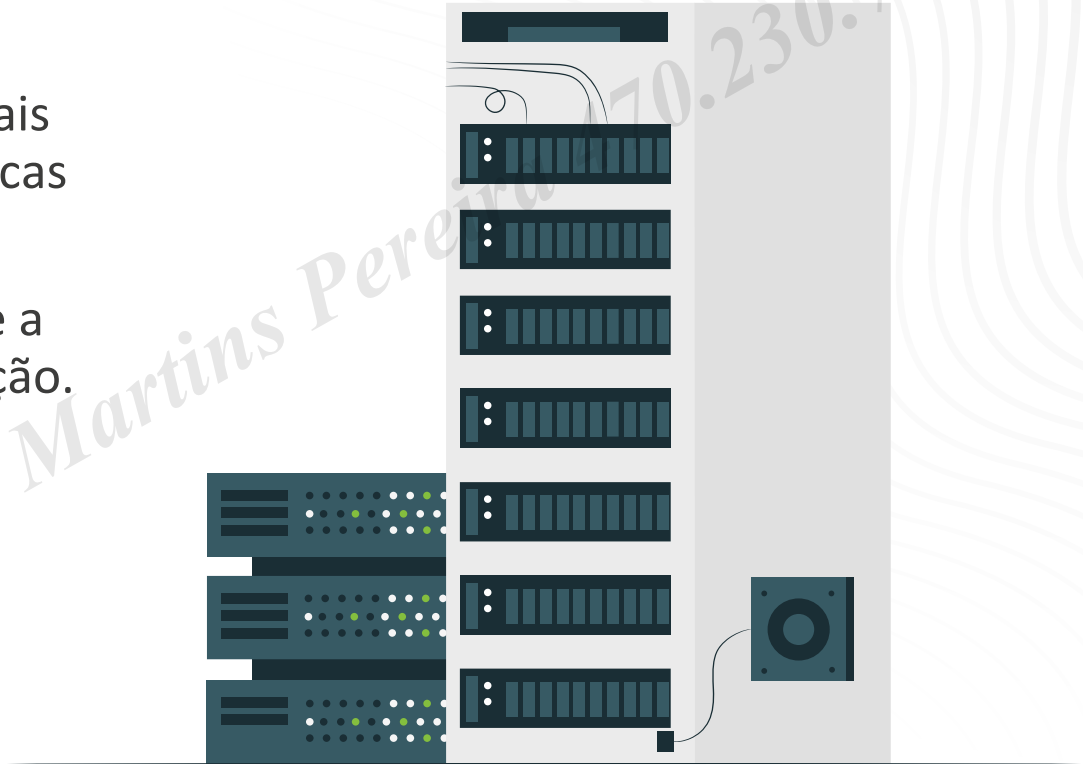
ENUMERAÇÃO

- Após as análise e coleta de dados realizadas pelos passos do ***Footprinting*** e ***Fingerprinting***.
- Tendo os hosts online, o processo de *pentest* deve ser "afunilado" através da etapa de enumeração.
- Etapa que consiste realizar um levantamento mais específico sobre determinada máquina.
- Considerando-se que uma máquina, específica daquela rede, esteja online e respondendo por pacotes e, mesmo assim, ainda é superficial o ataque, pois a mesma não é necessariamente vulnerável.

ENUMERAÇÃO

Sendo assim, para descobrir mais informações afundas e específicas devemos descobrir:

- Portas abertas e juntamente a versão do serviço em execução.
- Sistema Operacional.



PORT SCANNER

- Técnica de *scanning* ou varredura de portas (*port scan*).
- Muito comum e utilizada por atacantes para descobrir serviços vulneráveis em um sistema.
- Descobrir portas abertas, tipos de serviços, sistema operacional do servidor e outros.
- A resposta do *port scanner* varia com o tipo de conexão (TCP ou UDP).

PORT SCANNER

- Conexões TCP para descobrir uma porta aberta, o port scanner envia uma flag SYN para a porta. Resposta de flags: SYN+ACK > porta aberta, caso contrário, flags: RST+ACK > porta fechada.
- Port scanner receber a mensagem ICMP PORT UNRECHELE > porta filtrada pela regra REJECT do iptables, ou nenhuma resposta > regra DROP.
- Em UDP envia uma flag SYN e receber resposta ICMP PORT UNRECHELE > indica porta filtrada pela regra REJECT ou porta fechada. Sem respostas, filtrada pela regra DROP.

NMAP (FERRAMENTA)

Port scanner com muitas qualidades e muito utilizado. Possui versões Windows e Linux.

- Criada pelo hacker Fyodor em 1997 (gratuita).

Varredura simples:

#nmap 192.168.1.100

Varredura de uma rede inteira:

#nmap 192.168.1.0/24

Varredura 3-way handshake completa:

#nmap 192.168.10 -sT

Exemplo
Main in the middles

MITM

O ataque MITM é uma forma de interceptação de comunicação, onde um invasor se posiciona entre duas partes, interceptando e possivelmente alterando o tráfego de dados.

Objetivos do Ataque MITM

- Captura de informações confidenciais, como senhas, dados bancários, etc.
- Interceptação e alteração de comunicações.
- Injeção de código malicioso em comunicações.

MITM

MÉTODOS DE REALIZAÇÃO DO ATAQUE

- Redirecionamento de tráfego: O invasor redireciona o tráfego através de sua própria máquina.
- *Spoofing* de ARP: O invasor falsificar endereços MAC na tabela ARP do roteador ou dispositivo alvo.
- DNS *Spoofing*: O invasor falsifica respostas de DNS para redirecionar os usuários para sites maliciosos.

MITM

FERRAMENTAS COMUNS PARA REALIZAR UM ATAQUE MITM

- **WIRESHARK**: Para capturar e analisar o tráfego de rede.
- **ETTERCAP**: Uma suíte de ferramentas para interceptação de comunicações.
- **BETTERCAP**: Uma ferramenta de segurança de rede para ataques MITM.

MITM

MITIGAÇÃO DE ATAQUES MITM

- Uso de criptografia: Criptografar o tráfego de rede pode dificultar a interceptação.
- Verificação de certificados SSL/TLS: Certifique-se de que os certificados SSL/TLS são válidos e confiáveis.
- Monitoramento de tráfego: Esteja atento a padrões de tráfego suspeitos e anomalias.

OBRIGADO!

linkedin.com/in/rodolfo-meneguette-30287329