MECANISMOS DE SEGURANÇA EM REDES

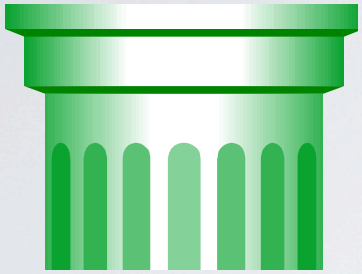
UCSAL - Graduação Tecnológica em Redes de Computadores

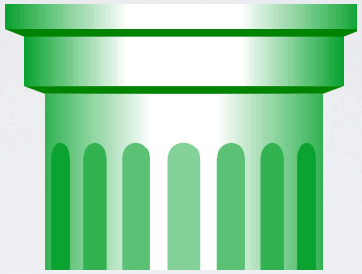
Professor Marco Câmara

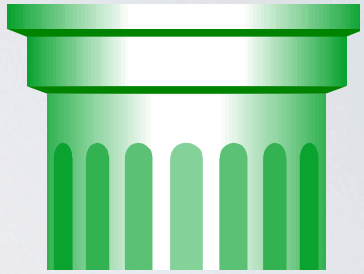
AGENDA

- Conceitos Básicos
- Política de Segurança
- Recursos, Controles e Pontos de Aplicação
- TI: Controles Aplicáveis
- Ocorrências de Segurança da Informação

OS 3 PILARES







- Integridade
  - Exatidão
  - Completude
- Confidencialidade
  - Acesso apenas para pessoas autorizadas
- Disponibilidade
  - Os dados estarão lá quando forem necessários

OUTROS PARÂMETROS

- Autenticidade
  - Certeza de que um objeto (em análise) provém das fontes anunciadas e que não foi alvo de mutações ao longo de um processo;
- Não repúdio
  - Também chamada de irretratabilidade, define a propriedade pela qual o emissor não pode negar a autenticidade de uma mensagem.

PONTOS DE APLICAÇÃO

- Usuário
  - Confidencialidade?
- Tráfego
  - Integridade
  - Confidencialidade
- Serviço
  - Disponibilidade

SEGURANÇA EM CAMADAS
DEFENSE IN DEPTH

- Princípio dos Castelos Medievais: primeiro o descampado expõe o atacante saindo da floresta; depois, o fosso, a ponte levadiça, a muralha, e, mesmo dentro, vielas para dificultar o acesso à edificação principal. Por fim, uma torre onde se entrincheirar se tudo desse errado;
- Em TI:
  - *Firewall*;
  - IDS (*Intrusion Prevention System*);
  - *Gateway*;
  - Servidores;
  - Estações de Trabalho;
  - Treinamento.

TI: CONTROLES APLICÁVEIS

- *Firewall*
- Controle de Conteúdo
- Detecção de Intrusão (IDS)
- Prevenção de Intrusão (IPS)
- Antivírus
- Criptografia
- Autenticação (Forte?)

TI: CONTROLES APLICÁVEIS

- *Firewall*
  - Fica na fronteira entre duas redes;
  - Controla o tráfego entre elas;
  - Política de Lista "branca" e "negra";
  - Pode tratar de forma diferenciada uma rede específica (DMZ).
- Controle de Conteúdo
- Detecção de Intrusão (IDS)
- Prevenção de Intrusão (IPS)
- Antivírus

TI: CONTROLES APLICÁVEIS

- *Firewall*
- Controle de Conteúdo
  - Determina o acesso ou bloqueio da WEB em função do conteúdo;
  - Pode estar associado a horário, usuário, computador etc;
  - Conteúdos podem ser identificados de diversas formas:
    - Lista "branca" ou "negra" de URLs;
    - Seqüências de texto;
    - Categorias.
- Detecção de Intrusão (IDS)
- Prevenção de Intrusão (IPS)

TI: CONTROLES APLICÁVEIS

- *Firewall*
- Controle de Conteúdo
- Detecção de Intrusão (IDS)
  - **Ferramenta tipicamente passiva;**
  - **Monitora e analisa eventos, registrando LOG e emitindo alertas;**
  - **Normalmente fica distribuído na rede em diversos pontos.**
- Prevenção de Intrusão (IPS)
- Antivírus
- Criptografia

TI: CONTROLES APLICÁVEIS

- *Firewall*
- Controle de Conteúdo
- Detecção de Intrusão (IDS)
- Prevenção de Intrusão (IPS)
  - **Ferramenta ativa;**
  - **Detecta eventos e toma ações visando proteger a rede.**
- Antivírus
- Criptografia
- Autenticação (Forte?)

TI: CONTROLES APLICÁVEIS

- *Firewall*
- Controle de Conteúdo
- Detecção de Intrusão (IDS)
- Prevenção de Intrusão (IPS)
- Antivírus
  - Identifica padrões de códigos maliciosos, bloqueando seus efeitos;
  - Pode ser instalado em 3 pontos: estação, servidor e *gateway*.
- Criptografia
- Autenticação (Forte?)

TI: CONTROLES APLICÁVEIS

- *Firewall*
- Controle de Conteúdo
- Detecção de Intrusão (IDS)
- Prevenção de Intrusão (IPS)
- Antivírus
- Criptografia
  - **Ferramenta típica para controle de integridade e confidencialidade;**
  - **Usada como tecnologia padrão para VPNs.**
- Autenticação (Forte?)

TI: CONTROLES APLICÁVEIS

- Controle de Conteúdo
- Detecção de Intrusão (IDS)
- Prevenção de Intrusão (IPS)
- Antivírus
- Criptografia
- Autenticação (Forte?)
  - Garante a autenticidade;
  - É considerada "forte" quando envolve mais de um dos elementos:

    O QUE VOCÊ ... É? SABE? TEM?

FIREWALL

- Um *firewall* é composto de *hardware*, *software*, ou uma combinação de ambos utilizada para controlar o acesso de uma rede por outra, seja por usuários ou por aplicações;
- O controle de acesso normalmente permite a liberação ou o bloqueio do tráfego com base em regras específicas:
  - A "lista branca" determina o que deve ser liberado, bloqueando todo o resto;
  - A "lista negra" determina o que deve ser bloqueado, liberando todo o resto.
- Tipicamente está classificado em três tipos:
  - Filtro de Pacotes
  - *Stateful Firewall*
  - *Proxy Firewall*

FIREWALL

- Um *firewall* que opera no modo "filtro de pacotes" determina a liberação ou bloqueio do tráfego com base em informações específicas de cada pacote analisado:
  - Endereço de Origem (camada 3);
  - Endereço de Destino (camada 3);
  - Portas de Origem (camada 4);
  - Portas de Destino (camada 4);
  - Bits de Controle TCP (camada 4);
  - Protocolo utilizado;
  - Direção;
  - Interface (física ou "lógica").

FIREWALL

TABELA DE PERMISSÕES (EXEMPLO)

Ação	Endereço de Origem	Endereço de Destino	Protocolo	Porta de Origem	Porta de Destino	Bit de Controle
Allow	Endereço Interno	Endereço Externo	TCP	Any	80	Any
Allow	Endereço Externo	Endereço Interno	TCP	80	>1023	Ack
Deny	All	All	All	All	All	All

Fonte: Counter Hack Realoaded, tabela 2.2, página 59

FIREWALL

- Um *firewall* que opera no modo "*stateful*" determina a liberação ou bloqueio do tráfego com base em informações históricas do tráfego de pacotes:
  - Ao contrário do "filtro de pacotes", que é estático, o "*stateful*" é dinâmico, construindo as informações a partir do tratamento do tráfeto que atravessa o dispositivo;
  - Permite detectar, por exemplo, ataques DOS (*Denial of Service*)
    - Pedidos de conexão não finalizados (*Three Way Handshake*).
  - Pode trabalhar fazendo a associação entre conexões de diferentes tipos para aplicações mais sofisticadas
    - Um exemplo é o tráfego FTP, que exige duas conexões: uma de controle e outra para conexões de dados. Conexões de dados podem ser condicionadas à existência de conexões de controle, por exemplo.
  - Para funcionar, o *firewall* estabelece uma tabela de estados que armazena informações sobre as conexões ativas;

FIREWALL

- Plataformas de Implantação
  - *Software*
    - Computador "Genérico" rodando SO "genérico"
    - Computador "Genérico" rodando SO proprietário
  - *Hardware*
    - Hardware proprietário rodando SO genérico (Ex. IOS da CISCO);
    - Hardware proprietário rodando SO proprietário (*appliance*),

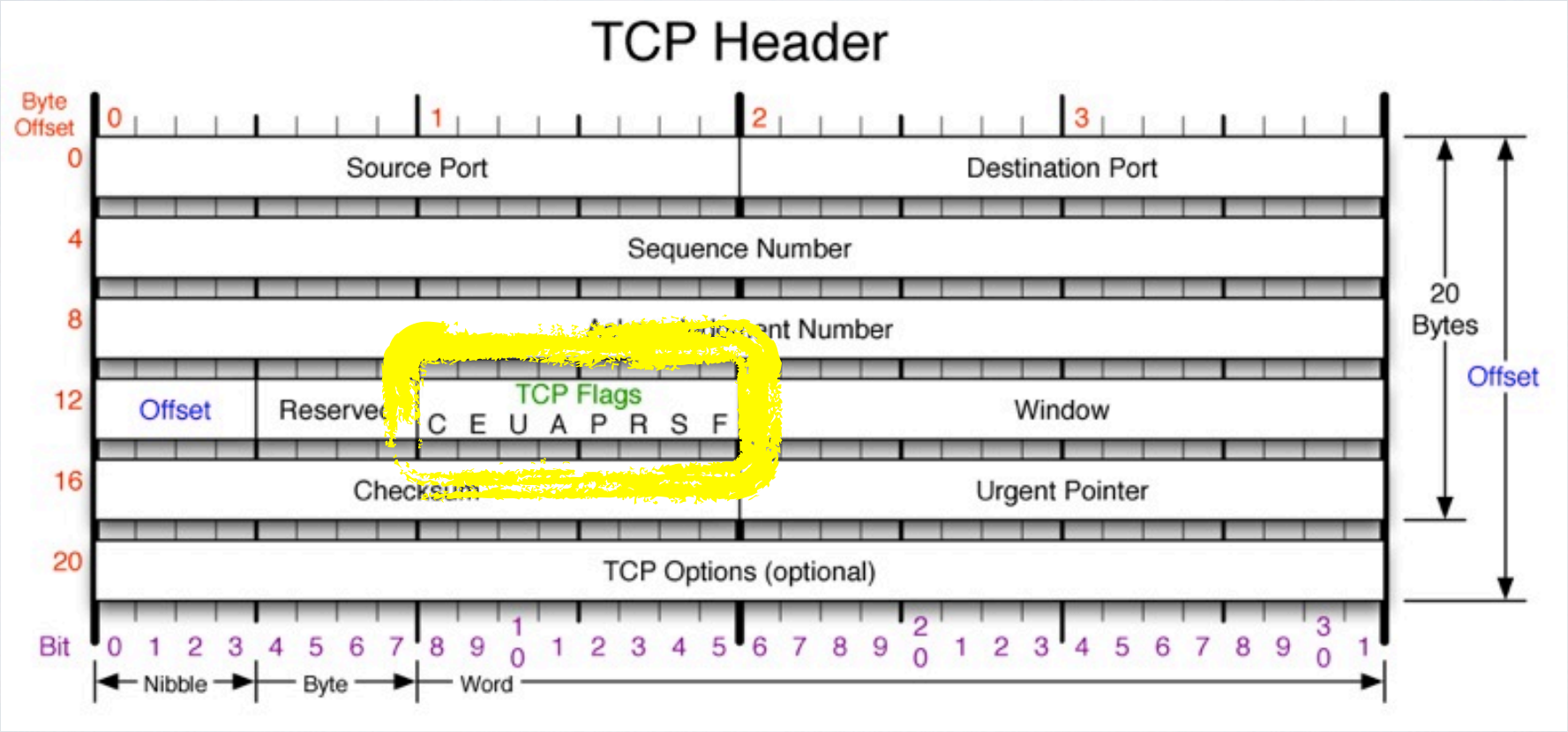
FIREWALL

- Trabalho proposto
  - Pesquisa e resumo técnico sobre *firewalls* de mercado;
  - Algumas marcas e produtos recomendados:
    - CheckPoint (Firewall 1);
    - CISCO (ASA);
    - Watch Guard;
    - Juniper;
    - Sonicwall;
    - BlueCoat;
  - Avaliar opções baseadas em software:
    - Microsoft (ISA Server);
    - IP Tables;
    - Outras (diversas !)

FIREWALL

- Parâmetros de Configuração
  - Camada 3 (revisar pacote IP e seus campos);
  - Camada 4 (idem para TCP e UDP)
    - 0 a 1023: Well Known Ports
      - TCP. Ex: 21 (FTP), 23 (Telnet), 25 (SMTP), 80 (HTTP);
      - UDP. Ex: 69 (TFTP), 161 (SNMP).
    - 1024 a 49151: Portas Registradas
      - TCP. Ex: 1433 (MS SQL Server), 1525 (Oracle Server);
      - UDP. Ex: 7070 (Real Player)
    - 49152 a 65535: Privadas

FIREWALL


TCP Header
Byte Offset
0
1
2
3
Source Port
Destination Port
4
Sequence Number
8
nt Number
12
Offset
Reserved
TCP Flags
C E U A P R S F
Window
16
Checksum
Urgent Pointer
20
TCP Options (optional)
20 Bytes
Offset
Bit
0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
Nibble
Byte
Word

FIREWALL

- **C**ongestion **W**indow **R**educed
  - Usado para controle de congestionamentos na rede.

FIREWALL

C	**E**	U	A	P	R	S	F
W	**C**	R	C	S	S	Y	I
R	**E**	G	K	H	T	N	N

- **E**xplicit **C**ongestion notification **E**cho
  - Também usado para controle de congestionamentos na rede.

FIREWALL

- **URG**ent

FIREWALL

- **ACK**nowledge
  - Utilizado no processo de conexão

FIREWALL

C	E	U	A	P	R	S	F
W	C	R	C	S	S	Y	I
R	E	G	K	H	T	N	N

FIREWALL

C	E	U	A	P	R	S	F
W	C	R	C	S	S	Y	I
R	E	G	K	H	T	N	N

FIREWALL

C	E	U	A	P	R	S	F
W	C	R	C	S	S	Y	I
R	E	G	K	H	T	N	N

CONTROLE DE CONTEÚDO

- Normalmente são estabelecidas políticas
  - Uma política normalmente está associada a usuários, grupos, computadores, domínios e faixas de endereçamento IP;
  - Usuários não listados estão sujeitos à uma "política padrão (default).
- A política pode determinar o acesso ou bloqueio de uma determinada categoria de conteúdos;
  - Número de categorias depende da especificação do sistema de Controle de Conteúdo;
  - Outra opção é a identificação individual dos conteúdos, através de URLs ou endereços IP;
  - Além do conteúdo, alguns sistemas têm comportamentos configuráveis por protocolo utilizado naquela conexão (MSN em um site, por exemplo, pode ser bloqueado) ou por dia e horário da conexão.
- Conteúdos podem ser identificados de diversas formas:
  - Endereço (Ex.URL) identificado por robô ou colaborador do fabricante;
  - Seqüências de texto

CRIPTOGRAFIA

- Histórico
- Cifras de Substituição
- Cifras de Transposição
- Cifra de Chave Única (inquebrável)
- Princípios Fundamentais
- Criptografia Simétrica e Assimétrica
- Chave Pública e Privada
- Algoritmo RSA

CIFRAS DE SUBSTITUIÇÃO

- Cifra de César (pula 3 letras);
- Deslocamento Genérico
- Substituição Monoalfabética

CIFRAS DE TRANSPOSIÇÃO

- Escolher palavra sem letras repetidas como chave
- Distribuir letras do texto horizontalmente, desprezando os espaços em branco;
- Transmitir por colunas, seguindo a ordem alfabética das letras da chave
- No destino, seguir o processo inverso

CIFRA DE CHAVE ÚNICA

- Operação OU-EXCLUSIVO do conteúdo a ser criptografado com sequência pseudo-aleatória conhecida por ambos os lados;
- No destino, repetir o processo para decriptografar

PRINCÍPIOS FUNDAMENTAIS

- Redundância
  - Sequências aleatórias não podem fazer sentido;
- Atualidade
  - Ataques de repetição precisam ser evitados
  - Uma das estratégias é a marcação de tempo nas mensagens.

SIMÉTRICA OU ASSIMÉTRICA

- Criptografia Simétrica
  - Emissor e Receptor compartilham a mesma chave, que precisa ser encaminhada em segredo;
- Criptografia Assimétrica
  - Chaves do emissor e receptor são diferentes, e não precisam ser trocadas.

CHAVE PÚBLICA E PRIVADA

- Bob e Alice: figuras típicas
- Para Bob enviar uma mensagem para Alice
  - Bob solicita a chave pública de Alice;
  - Alice fornece a chave pública;
  - Bob utiliza esta chave para criptografar o conteúdo;
  - Alice recebe a mensagem criptografada, e com sua chave privada, é capaz de decodificar a mensagem.

CRIPTOGRAFIA RSA

- Origem da sigla:
  - Rivest
  - Shamir
  - Adleman
- Criado em 1978, e até hoje não foi quebrada

CRIPTOGRAFIA RSA

- Dificuldade: fatorar o produto de dois números primos grandes;
- Passos:

1o.) Escolher 2 números primos grandes "p" e "q";

2o.) Calcular "n" e "z" da seguinte forma:

$n = p \cdot q$

$z = (p - 1) \cdot (q - 1)$

3o.) Escolha um número "d" tal que "d" e "z" sejam primos entre si;

4o.) Calcule "e", tal que:

$(e \cdot d)$ **mod**[*1] $z = 1$

*1 A operação "**mod**" retorna o resto da divisão entre seus operadores. Ex: 10 **mod** 4 = 2.

CRIPTOGRAFIA RSA

- De posse dos valores calculados, divida a mensagem em trechos "T" com valor binário inferior a "n". Para criptografar, transforme "T" em "C":

  $C = T^{\mathbf{e}} \bmod \mathbf{n}$, onde "e" e "n" formam a chave pública

- Para decriptografar, transforme "C" em "T":

  $T = C^{\mathbf{d}} \bmod \mathbf{n}$, onde "d" e "n" formam a chave privada

O PROBLEMA DA CONFIABILIDADE DAS CHAVES

- Um risco da criptografia por chave pública-privada é a possível interceptação da mensagem de Bob solicitando a chave pública de Alice;
- Um invasor poderia responder no lugar de Alice, receber a mensagem, e depois redirecioná-la para Alice;
- Para resolver, é importante associar a chave pública ao seu proprietário -> é aí que entram os certificados digitais
  - As entidades certificadoras (CA - Certification Authorities) associam o emissor à sua respectiva chave pública, e adicionam um conteúdo criptografado no certificado com a chave privada da CA, que pode ser checada pelo emissor antes do envio da mensagem.

INFRAESTRUTURA DE CHAVE PÚBLICA

- A infraestrutura de chave pública (PKI - *public-key infrastructure*) permite criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais;

- A PKI associa as chaves públicas com as identidades de usuário inequívocas através de uma autoridade certificadora (CA). A garantia de que esta associação está correta é dada pela Autoridade de Registro (RA), de forma que fica garantido o não-repúdio.

CONTEÚDO DE UM CERTIFICADO DIGITAL

- **Serial Number**: Identificação do certificado.
- **Subject**: Identificação da pessoa física ou jurídica.
- **Signature Algorithm**: Algoritmo usado para criação da assinatura.
- **Signature**: Assinatura do Emissor.
- **Issuer**: Órgão Emissor.
- **Valid-From**: Data de emissão.
- **Valid-To**: Data de Validade.
- **Key-Usage**: Objetivo da Chave (Ex. encriptação, assinatura etc).
- **Public Key**: Chave pública.