INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

105 ANOS
REDE FEDERAL
DE EDUCAÇÃO
PROFISSIONAL
E TECNOLÓGICA
1909-2014

Redes de Computadores

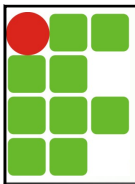
Segurança de Redes
Parte II

Prof. Thiago Dutra <thiago.dutra@ifrn.edu.br>

Agenda

- Parte I
  - Segurança da Informação
- Parte II
  - Segurança em Redes de Computadores

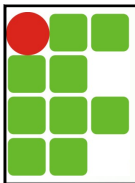
2



Agenda – Parte I

- Parte I
  - Introdução
  - Tendências
  - Incidentes
  - Arquitetura de Segurança
  - Ataque à Segurança
  - Serviço de Segurança
  - Mecanismo de Segurança
  - Modelo

3



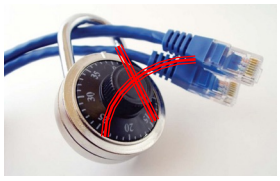
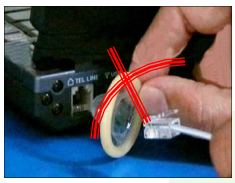
Agenda – Parte II

- Parte II
  - Comunicação Segura
  - Ataques
  - Criptografia
  - Chaves Simétricas e Públicas
  - Função de Resumo, Assinatura Digital
  - SSL
  - IPsec
  - Redes Privadas Virtuais (VPNs)
  - Firewall, IDS

4

Comunicação Segura

- Quando falamos de redes de computadores estamos nos referindo a comunicação
- Falar então sobre segurança em redes de computadores, significa falarmos sobre como realizar essa comunicação com segurança
- O que significa exatamente uma comunicação segura ?


5

Comunicação Segura

- A comunicação segura deve garantir que :
  - primeiramente, os recursos necessários para a comunicação não sejam negados
  - apenas o destinatário leia e entenda a mensagem
  - o emissor realmente foi o autor da mensagem
  - o destinatário realmente é quem de fato diz ser
  - a mensagem recebida é idêntica a original

6

Comunicação Segura

- Propriedades da Comunicação Segura
  - Confidencialidade
  - Autenticação do ponto final
  - Integridade da mensagem
  - Segurança operacional

Comunicação Segura

- Confidencialidade
  - Somente o remetente e o destinatário pretendido devem poder entender o conteúdo da mensagem
    - Ex.: mensagem cifrada
- Autenticação do ponto final
  - Remetente e destinatário precisam confirmar a identidade da outra parte envolvida na comunicação (confirmar que elas realmente são quem alegam ser)
    - Ex.: assinatura digital

Comunicação Segura

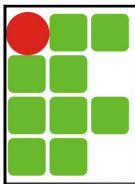
- Integridade da mensagem
  - Garantir que o conteúdo da mensagem não foi alterado, seja por acidente ou por má intenção, durante o processo de transmissão
    - Ex.: funções de hash
- Segurança operacional
  - Entidades internas e externas a rede não podem acessar informações não autorizadas; Utilização de mecanismos para deter ataques contra a rede
    - Ex.: firewall e sistemas de detecção de intrusão

9

Ataques

- Nem tudo são flores nas redes !
  - Existe um lado negro, onde "vilões" tentam danificar computadores, violar a privacidade e/ou tornar serviços inoperantes
- Esses vilões atuam principalmente :
  - Colocando "malwares" no hospedeiro
  - Atacando servidores e infraestrutura
  - Analisando pacotes
  - Fingindo ser alguém de sua confiança
  - Alterando ou excluindo mensagens

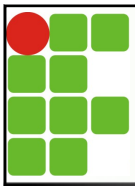
10



Ataques
Malware no Hospedeiro

- Malware = software mal intencionado
  - Apagar arquivos, coletar e repassar informações privadas (spyware), abrir brechas de segurança, ...
- Em sua maioria são autorreprodutivos
  - A partir do hospedeiro infectado buscam comunicação com outros hospedeiros para infectarem estes
- Se espalham na forma de :
  - Vírus : necessitam da interação do usuário (ex.: anexos de e-mails, arquivos em pen-drive)
  - Worm : sem interação do usuário; podem atacar programas frágeis (SOs desatualizados, softwares com falhas de segurança)
  - Cavalo de Tróia : parte de um programa funcional (ex.: software pirata, cracks)

11



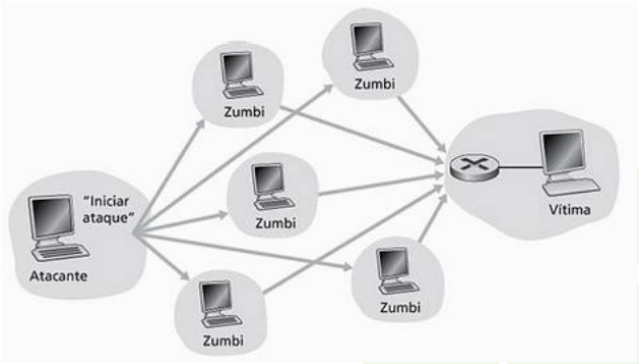
Ataques
Servidores e Infraestrutura

- DoS (Denial-of-Service)
  - Ataque de negação de serviço
  - Torna uma rede, hospedeiro ou parte da infraestrutura inutilizável por usuários verdadeiros
- Principais categorias de ataque DoS
  - Ataque de vulnerabilidade : envio de mensagens, em uma sequência específica, a uma aplicação vulnerável
  - Inundação na largura de banda : envio de um grande número de pacotes ao hospedeiro entupindo o enlace
  - Inundação da conexão : estabelecer um grande número de conexões com o hospedeiro -> recusa de novas

12

Ataques
Servidores e Infraestrutura

- DDoS (Distributed Denial-of-Service)
  - Uso de botnets



13

Ataques
Analise de Pacotes

- Analisador de pacotes (sniffer) = receptor passivo que grava uma cópia de cada pacote que passa
  - Podem atuar tanto em conexões cabeadas quanto em conexões sem fio
  - Existem diversos analisadores de pacotes gratuitos (ex.: Wireshark)
  - São difíceis de detectar, pois não realiza modificações ou introdução de pacotes no canal
  - Pode ser usado de forma legítima para analisar o tráfego e/ou comportamento da rede

14

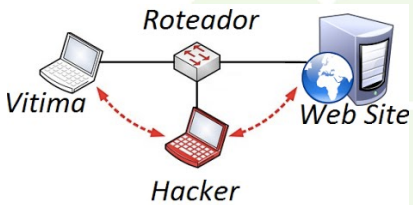
Ataques
Fingindo ser Alguém Confiável

- É extremamente fácil criar um pacote com um endereço fonte arbitrário, conteúdo de pacote e endereço de destino e transmiti-lo
- O receptor inocente recebe o pacote, acreditando ser de uma fonte confiável, e executa os comandos integrados ao conteúdo do pacote
  - Ex.: modificar tabela de roteamento
- IP spoofing
  - Introduzir pacotes na Internet com um endereço IP de origem falso

15

Ataques
Alterar ou Excluir Mensagens

- Man-in-the-middle (homem no meio)
  - O atacante fica infiltrado no percurso da comunicação entre duas entidades comunicantes
    - As entidades podem ser usuários finais ou dispositivos de rede (ex.: roteador, servidor)
    - Os atacantes podem ser, por exemplo, roteadores comprometidos ou softwares no hospedeiro
  - O atacante pode :
    - Analisar,
    - Introduzir,
    - Alterar,
    - Excluir pacotes



16

Criptografia

- Criptologia
  - kriptos = escondido, oculto; logia = estudo, ciência
  - Ciência que reúne a criptografia e a criptoanálise
- Criptografia
  - kriptos = escondido, oculto; grapho = grafia, escrita
  - Técnica que habilita a escrita em cifras, de forma que apenas o destinatário decifre e compreenda a mensagem;
- Criptoanálise
  - kriptos = escondido, oculto; analisis = decomposição, interpretação
  - Técnica que compreende a decomposição de uma senha ou interpretar mensagens cifradas sem o conhecimento da chave. Uma tentativa de criptoanálise é considerado um ataque

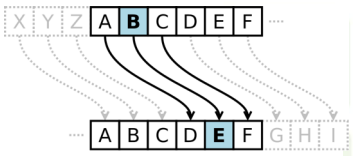
17

Criptografia

- A criptografia vem sendo utilizada pelos séculos
  - Gregos, Egípicios, Romanos, II Guerra Mundial, ...

Cítala

Enigma



Cifra de César (K=3)

ATACAR O INIMIGO
DWDFDU R LQLPLJR

18

Criptografia

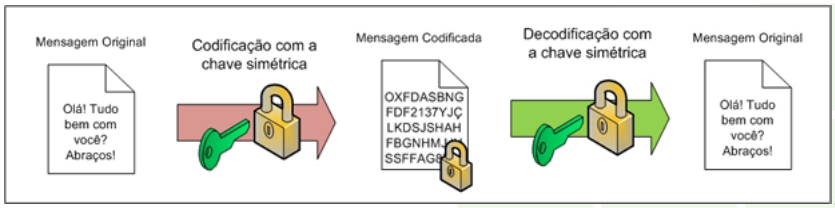
- Para que é utilizada a criptografia ?
  - A princípio, para garantir confidencialidade
  - Porém, incorporou-se mecanismos que também permitem garantir integridade, autenticidade, não repúdio, ...
- Termos comuns utilizados na criptografia :

Termo	Significado
Texto claro	Informação legível (original) que será protegida, ou seja, que será codificada
Texto codificado (cifrado)	Texto ilegível, gerado pela codificação de um texto claro
Codificar (cifrar)	Ato de transformar um texto claro em um texto codificado
Decodificar (decifrar)	Ato de transformar um texto codificado em um texto claro
Método criptográfico	Conjunto de programas responsável por codificar e decodificar informações
Chave	Similar a uma senha, é utilizada como elemento secreto pelos métodos criptográficos. Seu tamanho é geralmente medido em quantidade de *bits*

19

Chave Simétrica

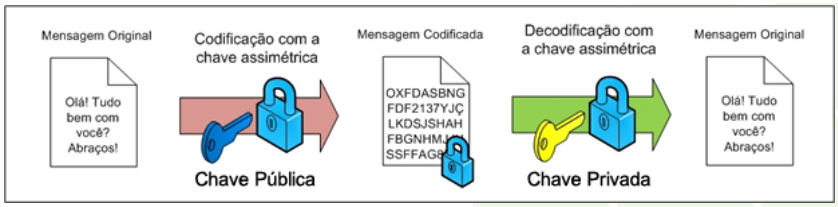
- Criptografia de chave simétrica
  - Utiliza a mesma chave tanto para codificar quanto para decodificar
  - A chave necessita ser previamente compartilhada, por um canal seguro, entre remetente e destinatário
  - Métodos criptográficos : AES, Blowfish, 3DES, IDEA, ...



20

Chave Pública

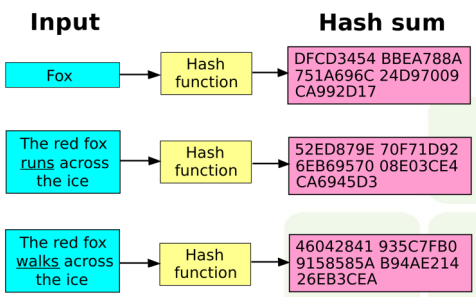
- Criptografia de chave pública ou chaves assimétricas
  - Utiliza duas chaves distintas:
    - uma pública (livremente divulgada)
    - uma privada (mantida em segredo pelo dono)
  - Uma informação codificada com uma das chaves só pode ser decodificada pelo seu par correspondente
  - Métodos criptográficos : Diffie-Hellman, RSA, DSA, ...



21

Função de Resumo

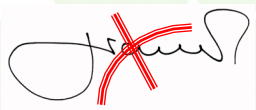
- Método criptográfico que aplicado sobre uma informação, independente do tamanho que ela tenha, gera um resultado "único" e de tamanho fixo, chamado hash
- Métodos criptográficos : MD5, SHA-1, SHA-256, ...



22

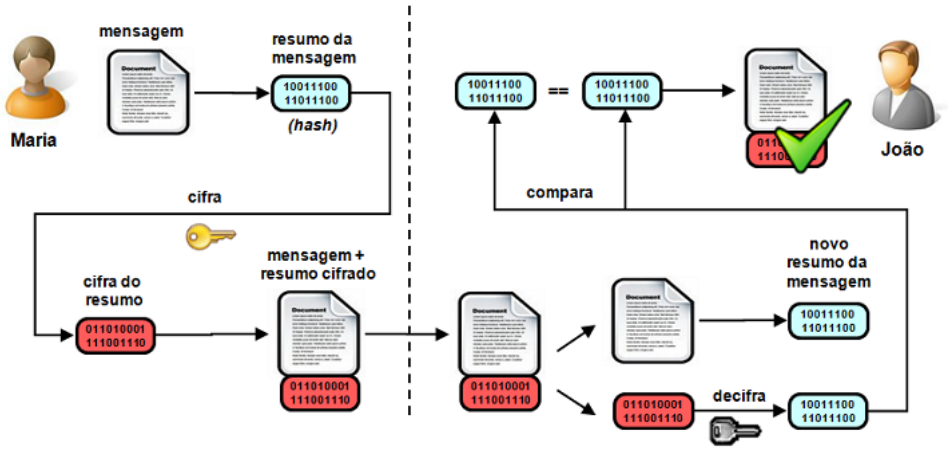
Assinatura Digital

- Permite comprovar a autenticidade e a integridade da informação
  - Baseia-se no fato de que apenas o dono conhece a chave privada, então a codificação com ela só pode ter sido feita pelo dono
  - A verificação da assinatura é feita com a chave pública correspondente
  - Utiliza função de hash na criação da assinatura, agilizando assim o processo de codificação



23

Assinatura Digital



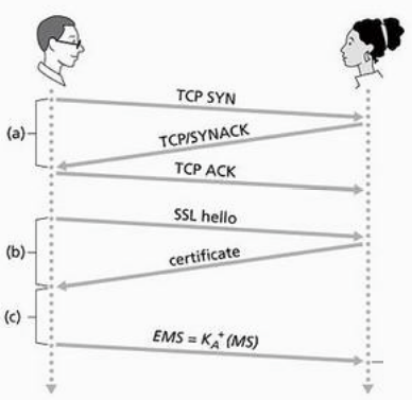
24

SSL

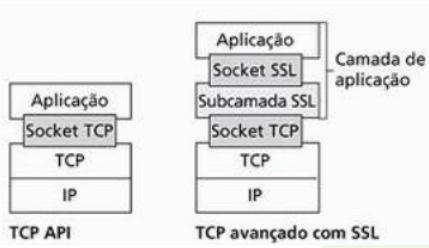
- Secure Socekts Layer
  - Camada segura de sockets
  - "Versão aprimorada" do TCP que inclui serviços de segurança (sigilo, integridade e autenticação)
  - Cria um canal de comunicação criptografado entre cliente e servidor
  - Em geral utilizado para prover transações segura no HTTP (https://), mas pode ser utilizado por qualquer aplicação que execute o TCP

25

SSL



(a) Conexão TCP
(b) Envio de certificado
(c) Criação de chave secreta mestre



Tecnicamente o SSL reside na camada de aplicação, mas na visão o desenvolvedor, ele é um protocolo de transporte que provê serviços do TCP aprimorados com serviços de segurança

26

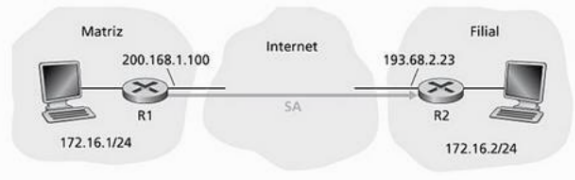
IPsec

- Internet Protocol Security
  - Protocolo de Segurança IP
  - É um framework (conjunto de protocolos) usado para prover serviços de segurança na camada IP
  - Possui dois protocolos principais:
    - AH (Cabeçalho de Autenticação)
      - Provê autenticação e integridade
    - ESP (Carga de Segurança de Encapsulamento)
      - Provê autenticação, integridade e confidencialidade

27

IPsec

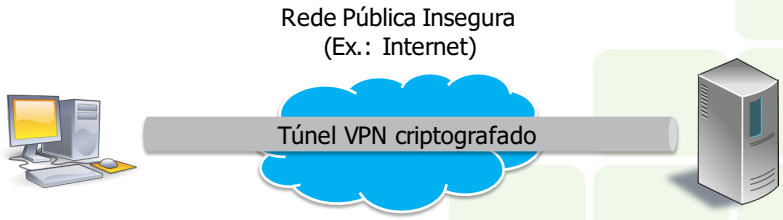
- Os datagramas IPsec são enviados entre pares de entidades de rede (roteadores, cliente-servidor, ...)
- É necessário que exista uma conexão lógica, denominada associação de segurança (SA).
  - Uma SA é simplex (comunicação unidirecional)
  - Comunicação bidirecional -> 2x SA



28

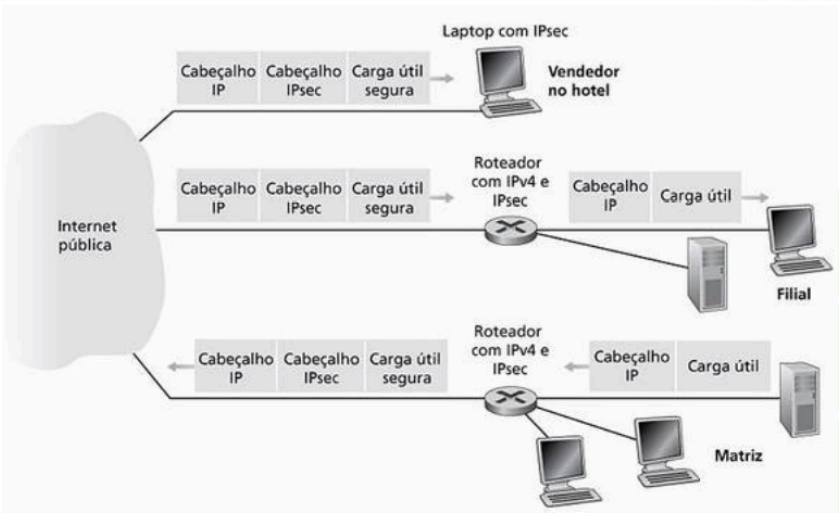
VPN

- Virtual Private Network
  - Rede Privada Virtual
  - Surge devido ao fato das instituições geograficamente separadas necessitarem ter sua própria rede IP, para que seus hospedeiros e servidores possam trocar dados de maneira segura e sigilosa



29

VPN



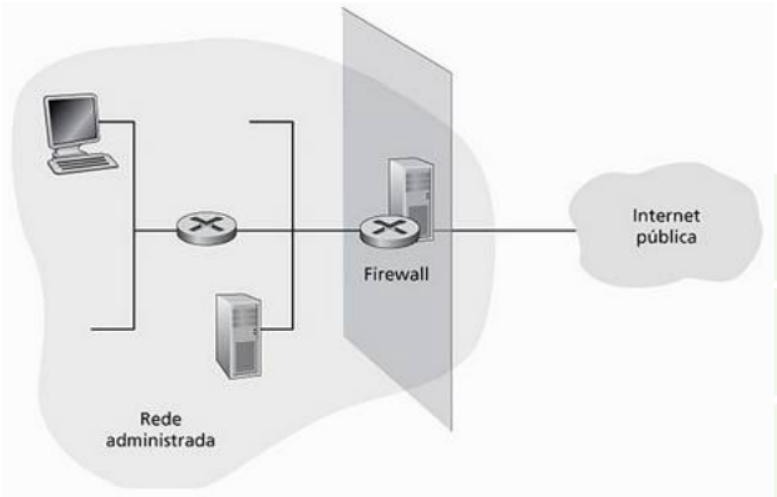
30

Firewall

- Um firewall é uma combinação hardware-software que isola a rede interna de uma instituição da Internet em geral
  - Permite que alguns pacotes passem e outros sejam bloqueados
- São objetivos do firewall
  - Todo tráfego, tanto de entrada quanto de saída, deve passar por um firewall
  - Somente tráfego autorizado poderá passar
  - O próprio firewall deve ser imune à penetração

31

Firewall



32

Firewall

- Podem ser classificados em três categorias:
  - Filtros de pacote tradicionais
  - Filtros de estado
  - Gateways de aplicação

33

Firewall

- Filtros de pacote tradicionais
  - Examina cada pacote individualmente e determina, baseado em uma lista de regras, se o pacote passa ou é barrado

Ação	Endereço de origem	Endereço de destino	Protocolo	Porta de origem	Porta de destino	Flag bit
Permitir	222.22/16	Fora de 222.22/16	TCP	>1023	80	Qualquer um
Permitir	Fora de 222.22/16	222.22/16	TCP	80	>1023	ACK
Permitir	222.22/16	Fora de 222.22/16	UDP	>1023	53	_
Permitir	Fora de 222.22/16	222.22/16	UDP	53	>1023	_
Negar	Todos	Todos	Todos	Todos	Todos	Todos

34

Firewall

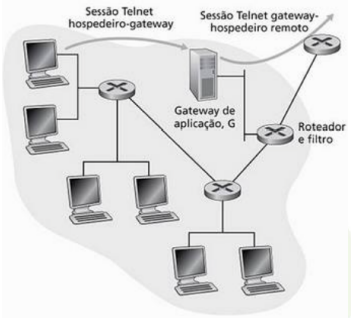
- Filtros de estado
  - Além de examinarem o pacote, verificam o estado da conexão para tomar decisões de filtragem

Ação	Endereço de origem	Endereço de destino	Protocolo	Porta de origem	Porta de destino	Flag bit	Conexão de checagem
Permitir	222.22/16	Fora de 222.22/16	TCP	>1023	80	Qualquer um	
Permitir	Fora de 222.22/16	222.22/16	TCP	80	>1023	ACK	X
Permitir	222.22/16	Fora de 222.22/16	UDP	>1023	53	_	
Permitir	Fora de 222.22/16	222.22/16	UDP	53	>1023	_	X
Negar	Todos	Todos	Todos	Todos	Todos	Todos	

Endereço de origem	Endereço de destino	Porta de origem	Porta de destino
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

Firewall

- Gateways de aplicação
  - Servidor específico de aplicação por onde todos os dados (entrada e saída) da aplicação passam ao se comunicarem com a rede externa
  - São usados para realizar a filtragem em um nível mais alto (ex.: nível de usuários)



IDS

- Intrusion Detection System
  - Sistema de detecção de intrusos
  - Um IDS realiza uma inspeção profunda dos pacotes, podendo então localizar atividades anormais e suspeitas na rede
    - Quando um tráfego diferente do padrão é verificado ações preventivas podem ser tomadas (ex.: geração de alertas, filtragem do tráfego, configuração de equipamentos)

37

IDS

- São classificados como:
  - Sistemas baseados em assinatura
    - Possuem um extenso banco de dados com conjuntos de regras relacionadas a uma atividade intrusa (assinatura)
    - As assinaturas podem ser referentes a características de um único pacote ou de uma série de pacotes
  - Sistemas baseados em anomalias
    - Criam um perfil de tráfego enquanto observa o tráfego da rede em operação normal
    - Com base nesse perfil, procura por cadeias de pacotes que são estatisticamente incomuns
    - Podem detectar novos ataques potenciais

38

Referências

- KUROSE, J. F. e ROSS, K. – Redes de Computadores e a Internet – 5a Ed., Pearson, 2010.
- STALLINGS, W. – Criptografia e segurança de redes, 4. Ed., São Paulo: Pearson Prentice Hall, 2008.
- CERT.br – Cartilha de Segurança para Internet. Disponível em: http://cartilha.cert.br . Acesso em: 08/2015.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

105 ANOS
REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
1909-2014

Redes de Computadores

Segurança de Redes
Parte II

Prof. Thiago Dutra <thiago.dutra@ifrn.edu.br>