PTC 3450 - Aula 04

1.6 Redes sob ataque: segurança

1.7 História

2.1 Princípios das aplicações de rede

(Kurose, p. 41 - 62)

(Peterson, p. 425 - 444)

17/03/2017

Capítulo 1: Conteúdo

1.1 O que é a Internet?

1.2 A borda da rede

- sistemas finais, redes de acesso, enlaces

1.3 Núcleo da rede

- Chaveamento de pacotes, chaveamento de circuitos, estrutura da rede

1.4 Atraso, perdas, vazão em redes

1.5 Camadas de protocolos, modelos de serviços

1.6 Redes sob ataque: segurança

1.7 História

Segurança de rede

- área de segurança de rede:
  - como pessoas mal-intencionadas podem atacar redes de computadores
  - como podemos defender redes contra ataques
  - como criar arquiteturas que são imunes a ataques
  - Tópico central na área de redes de computadores!
- Internet não foi projetada originalmente com (muita) segurança em mente
  - *visão original:* "um grupo de usuários que confiam mutualmente ligados a uma rede transparente" ☺
  - Projetistas de protocolos Internet apostando corrida com *hackers*
  - considerações de segurança em todas as camadas!

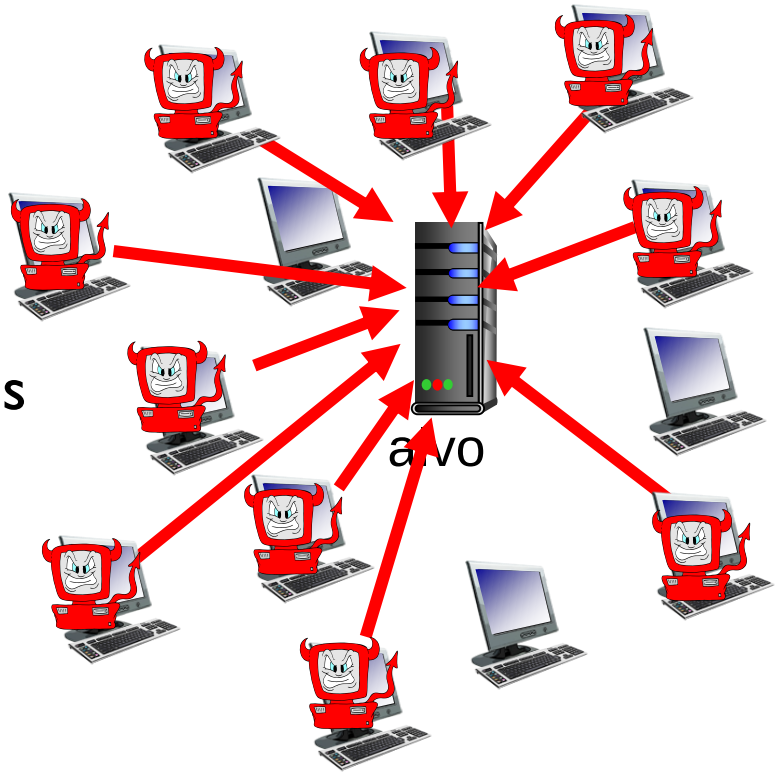
Bad guys: colocar *malware* em *hosts* via Internet

- *malware* pode chegar a *host* a partir de:
  - *vírus:* infecção autoreplicante pela recepção/execução de um objeto (e.g., anexo de e-*mail*)
  - *worm:* infecção autoreplicante devido a receber passivamente um objeto que se autoexecuta
- *spyware malware* pode gravar toques de teclado, visitas a *web sites*, *fazer upload* de infos para *site* coletor
- *host* infectado pode ser aliciado em *botnet*, usado para *spam* e ataques DDoS

Bad guys: ataque a servidor, estrutura de rede

Distributed Denial of Service (DDoS): atacantes fazem recursos (servidor, largura de banda) indisponível para tráfego legítimo esgotando os recursos com tráfego falso

1. seleciona um alvo
2. invade *hosts* na rede (veja *botnet*)
3. envia pacotes para o alvo a partir de *hosts* comprometidos

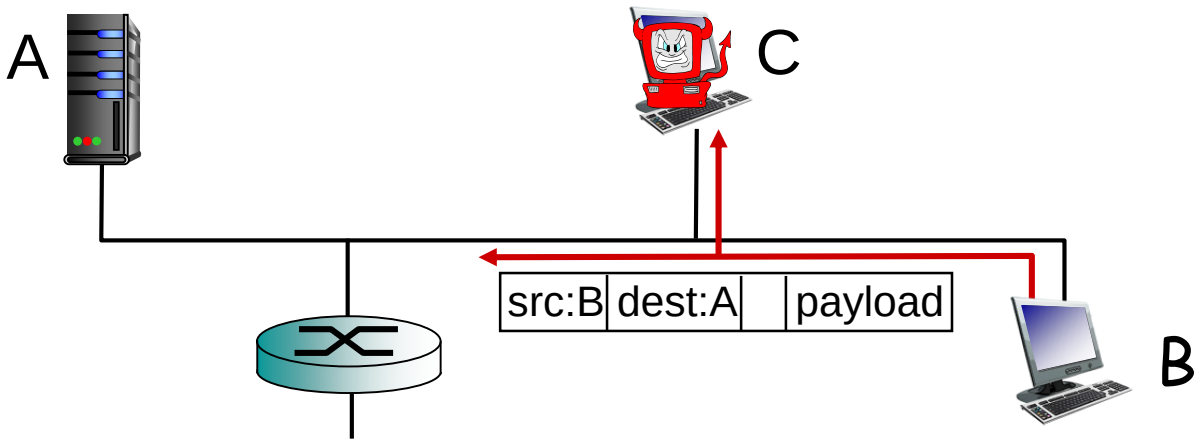


Milhares por ano!

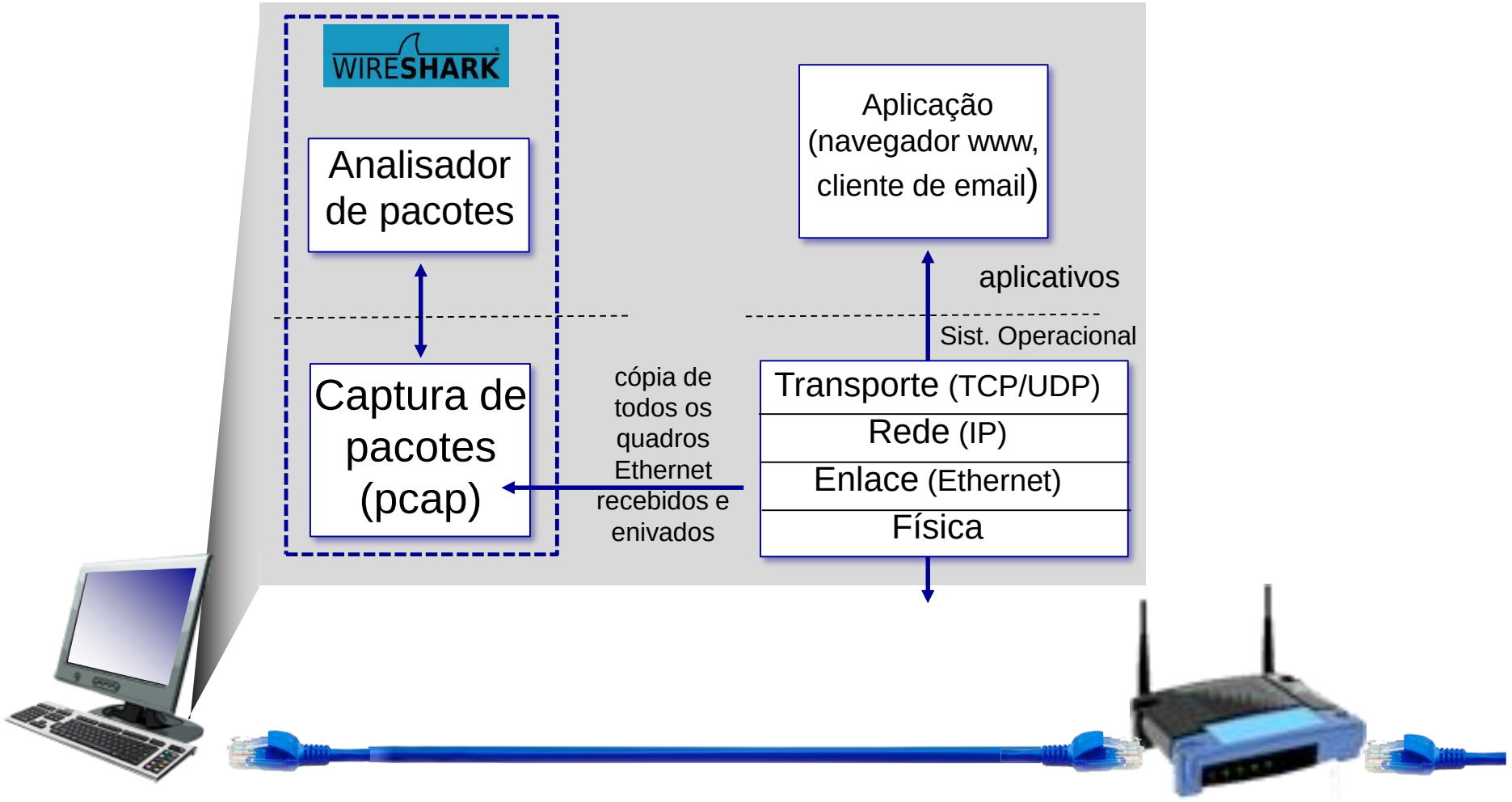
Bad guys podem farejar pacotes

"farejando" pacotes:

- meio *broadcast* (ethernet compartilhada, sem fio)
- interface de rede comprometida lê/grava todos os pacotes (e.g., incluindo senhas!) passando

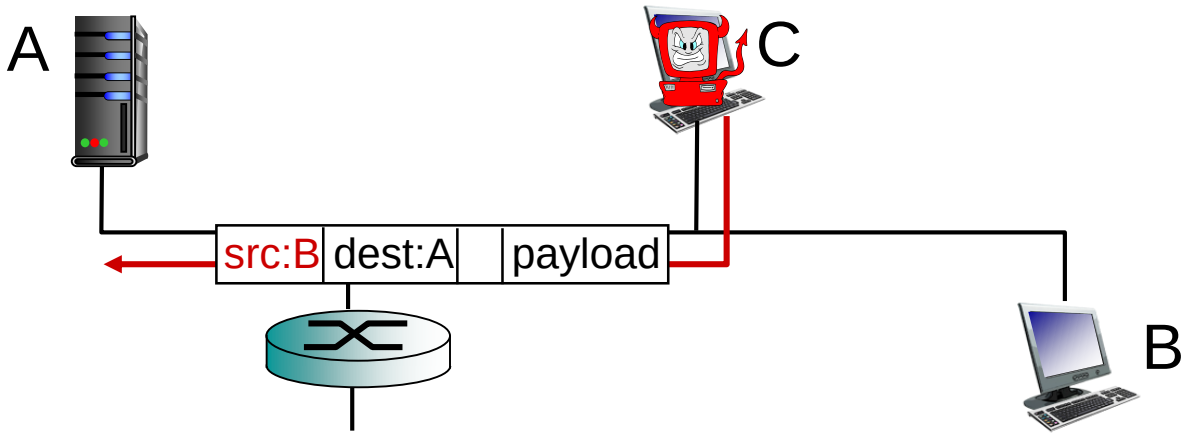


- programa *Wireshark* usado em EP é um farejador de pacotes (*packet-sniffer*) (gratuíto)


WIRESHARK
Analisador de pacotes
Captura de pacotes (pcap)
cópia de todos os quadros Ethernet recebidos e enivados
Aplicação (navegador www, cliente de email)
aplicativos
Sist. Operacional
Transporte (TCP/UDP)
Rede (IP)
Enlace (Ethernet)
Física

Bad guys podem falsificar endereço

IP enganoso: enviar pacote com falso endereço de fonte



Ao longo do curso, vamos sempre voltar a essas questões

Capítulo 1: Conteúdo

1.1 O que é a Internet?

1.2 A borda da rede

- sistemas finais, redes de acesso, enlaces

1.3 Núcleo da rede

- Chaveamento de pacotes, chaveamento de circuitos, estrutura da rede

1.4 Atraso, perdas, vazão em redes

1.5 Camadas de protocolos, modelos de serviços

1.6 Redes sob ataque: segurança

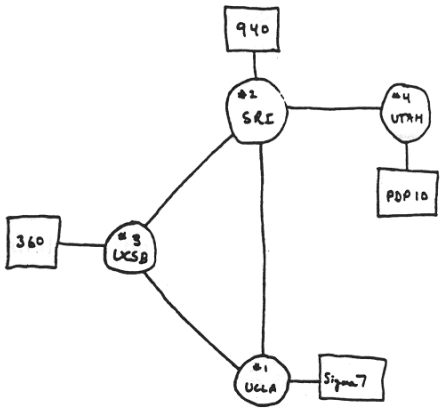
1.7 Histórico das redes e Internet

História da Internet

1961-1972: Primeiros princípios da comutação de pacotes

- 1961: Kleinrock (MIT)– teoria das filas mostra eficiência da comutação de pacotes
- 1964: Baran (Rand Institute) – comutação de pacotes em redes militares
- 1967: ARPAnet concebida pela *Advanced Research Projects Agency*
- 1969: primeiros nós ARPAnet operacionais (UCLA, Stanford (SRI), UC Santa Barbara e Utah)

- 1972:
  - demonstração pública da ARPAnet – 15 nós
  - RFC001 - NCP (*Network Control Protocol*) primeiro protocolo *host-host*
  - primeiro aplicativo de *e-mail*



THE ARPA NETWORK

História da Internet

1972-1980: Internetworking, redes novas e proprietárias

- 1970: ALOHAnet (rede sem fio no Hawaii) e muitas outras redes proprietárias surgem
- 1974: Cerf e Kahn (DARPA) – arquitetura para interconectar redes
- 1976: Ethernet na Xerox PARC
- fim dos anos 70's: arquiteturas proprietárias: DECnet, SNA, XNA
- fim dos anos 70's: comutação de pacotes de tamanho fixo (precursor do ATM)
- 1979: ARPAnet tem 200 nós

Princípios do *internetworking* de Cerf e Kahn:

- minimalista, autônomo – não são necessárias mudanças internas para interconectar redes
- modelo de serviço de melhor esforço
- roteadores sem estado
- controle descentralizado

define a arquitetura da Internet atual

História da Internet

1980-1990: novos protocolos, uma proliferação de redes

- 1983: desenvolvimento do TCP/IP
- 1982: definido protocolo SMTP para *e-mail*
- 1983: definido DNS para tradução nome-endereço IP
- 1985: definido protocolo FTP
- 1988: controle de congestionamento do TCP

- novas redes ligando universidades americanas: CSnet, BITnet, NSFnet
- Minitel (França - governo)
- 100 000 *hosts* conectados a confederações de redes

História da Internet

1990 - 2005: comercialização, a Web*, novos apps*

- início dos anos 1990: ARPAnet sai de serviço
- 1991: NSF retira restrições ao uso comercial da NSFnet (sai de serviço em 1995 – ISP comerciais assumem)
- inicío dos anos 1990: *WWW*
  - hipertexto [Bush 1945, Nelson 1960's]
  - HTML, HTTP, servidor web e navegador: Berners-Lee
  - 1993: 200 servidores web
  - 1994: Mosaic, depois Netscape
  - fim dos anos 1990: comercialização na *Web*

fim dos anos 1990 – início dos anos 2000:

- mais *apps* populares: webmail, mensagem instantânea (ICQ, MSN), compartilhamento de arquivos P2P (Napster)
- segurança da rede passa a ser importante
- est. 50 milhões de *host*, +100 milhões de *usuários*
- enlaces *backbone* rodando em Gbps

História da Internet

2005-presente

- ~1 bilhão de *hosts*
  - *Smartphones* e *tablets*
- Desenvolvimento maciço do acesso banda larga – popularização de aplicações com vídeo: Youtube, Netflix, Skype
- Crescimento onipresente do acesso sem fio de alta velocidade (conexão constante e aplicações com GPS)
- Emergência das redes sociais:
  - Facebook: 1,86 bilhões de usuários (dezembro 2016)
- Provedores de serviço (Google, Microsoft) criam suas próprias redes
  - Evitando a Internet, provendo acesso "instantâneo" a buscas, e-mail, etc.
- *E-commerce*, universidades, empresas, rodando seus serviços na "nuvem" (e.g., Amazon EC2)

Introdução: sumário

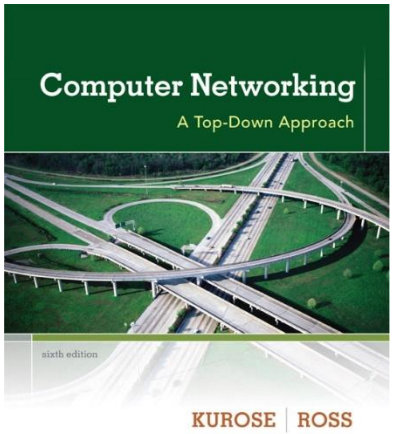
cobrimos muito material!

- Visão geral da Internet
- O que é um protocolo?
- Borda da rede, núcleo, redes de acesso
  - comutação de pacotes versus comutação de circuitos
  - Estrutura da Internet
- Desempenho: perdas, atraso, vazão
- Camadas, modelos de serviço
- Segurança
- História

agora você tem:

- contexto, visão geral, "ideia" de redes
- vamos agora aprofundar!

Capítulo 2
A Camada de Aplicação



Computer Networking: A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley
March 2012

Capítulo 2: conteúdo

2.1 Princípios de aplicativos de rede

2.2 *Web* e HTTP

2.3 Correio eletrônico

- SMTP, POP3, IMAP

2.4 DNS

2.5 Aplicativos P2P

2.6 *Streaming* de video e redes de distribuição de conteúdo

2.7 Programando *socket* com UDP e TCP

Capítulo 2: camada de aplicação

nossos objetivos:

- aspectos conceituais e de implementação de protocolos de aplicativos de rede
  - modelos de serviço da camada de transporte
  - paradigma cliente-servidor
  - paradigma *peer-to-peer*
- aprender sobre protocolos
  - examinando exemplos da camada de aplicação populares
    - HTTP
    - FTP
    - SMTP / POP3 / IMAP
    - DNS
  - criando aplicativos de rede
    - *socket* API

Alguns *apps* de rede

- *e-mail*
- *web*
- mensagens de texto
- *login* remoto
- compartilhamento de arquivos P2P
- jogos em rede multiusuários
- *streaming* de vídeo armazenado (YouTube, Hulu, Netflix)
- voz-sobre-IP (e.g., Skype)
- videoconferência em tempo real
- redes sociais
- busca
- …
- …

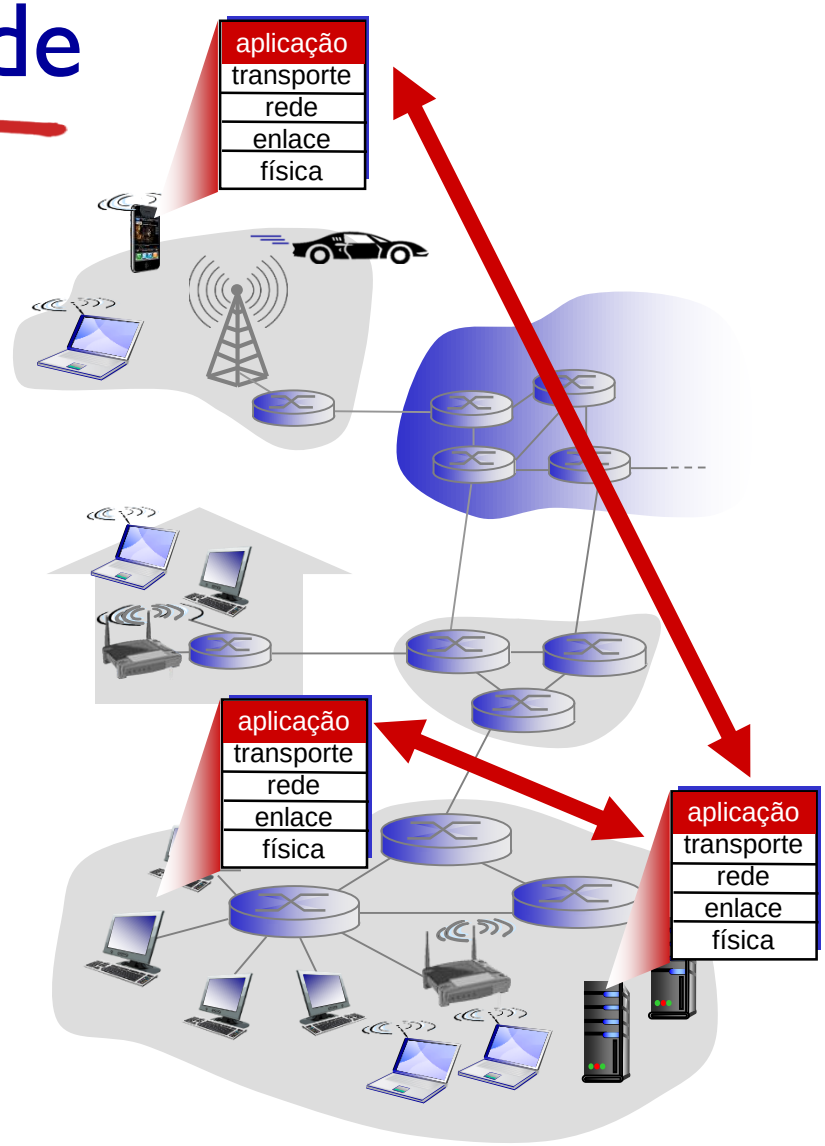
Criando um *app* de rede

escrever programas que:

- rodam em (diferentes) sistemas finais
- comunicam-se sobre a rede
- e.g., programa servidor *web* rodando em servidor comunica-se com navegador em host do usuário
- e.g., sistema de compartilhamento de arquivos P2P – programa em cada um dos hosts que participam da comunidade

não é necessário escrever programa para dispositivos do núcleo da rede

- dispositivos do núcleo da rede não rodam aplicativos de usuário
- aplicativos em usuários finais permite rápido desenvolvimento e propagação de *apps*



Arquiteturas de aplicativos

possíveis estruturas de aplicativos:

- cliente-servidor
- *peer-to-peer* (P2P)