Fundamentos de Sistemas Computacionias (IC/UFRJ)

Aula 11: Redes de Computadores e a Internet - Segurança na Rede

Prof. Silvana Rossetto (IC/CCMN/UFRJ)

Segurança na rede

O campo de **segurança na rede** aborda:

- como pessoas mal intencionadas podem atacar redes de computadores
- como podemos nos defender contra esses ataques
- como projetar arquiteturas que são imunes aos ataques

Segurança na rede

A Internet não foi projetada originalmente para lidar com ataques de segurança

- **visão original**: modelo de "confiança mútua"
- do ponto de vista atual, a capacidade de um usuário enviar um pacote para qualquer outro é uma falha de segurança: a identidade do usuário deveria ser — por princípio — confirmada
- **visão atual**: considerações de segurança em todas as camadas!

Malware - recursos maliciosos

"Infectam" sistemas computacionais conectados na Internet, podendo ocasionar:

- perda de arquivos
- instalação de programas (*spyware*) que coletam dados confidenciais
- instalação de bots que propagam spams e outros ataques

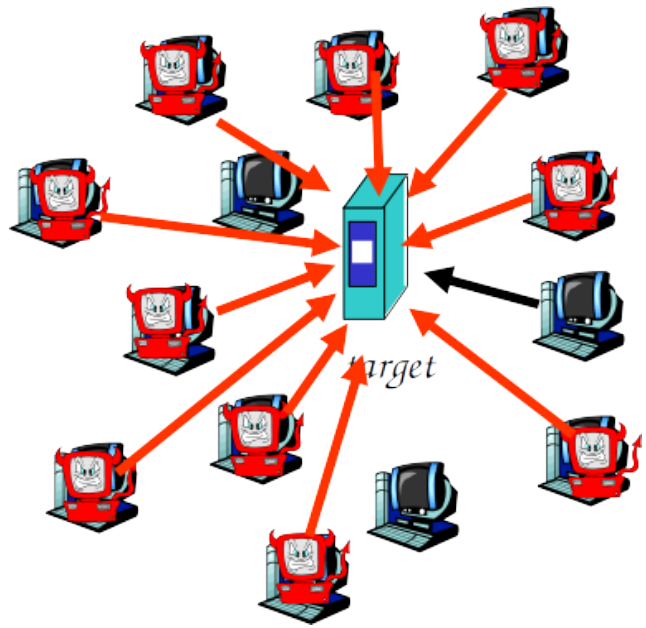
Malware - recursos maliciosos

Malware aparecem na forma de:

- Trojan horse: oculto dentro de outro software (ex., plugins)
- Virus: infecção por um objeto que é ativamente executado (ex., arquivo anexado em email)
- Worm: infecção por um objeto recebido passivamente que se auto executa (ex., aplicação de rede frágil)

Denial of Service (DoS): tornam os recursos indisponíveis para as requisições legítimas

- seleção do alvo
- formação de rede botnet de atacantes
- envio massivo de pacotes para o alvo



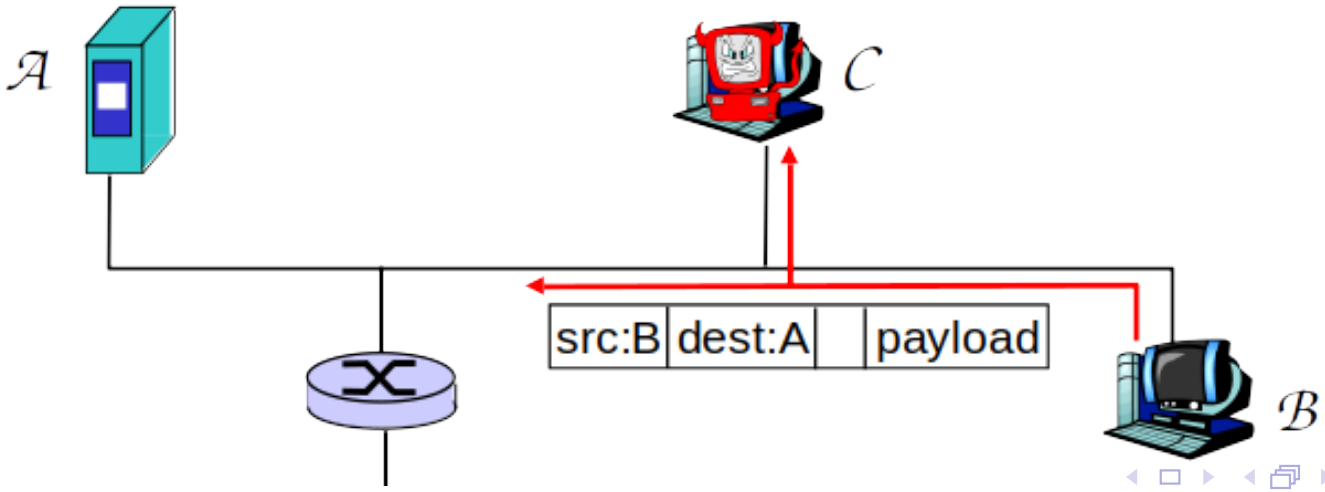
Ataques de DoS

Denial of Service (DoS) (negação de serviço) aparecem em três categorias comuns:

1. Ataque de vulnerabilidade: envio de mensagens corretas a uma aplicação vulnerável
2. Inundação da largura de banda: envio de grande número de pacotes ao sistema alvo, sobrecarregando o enlace de acesso
3. Inundação da conexão: estabelecimento de grande número de conexões TCP falsas que faz o sistema alvo parar de aceitar conexões válidas

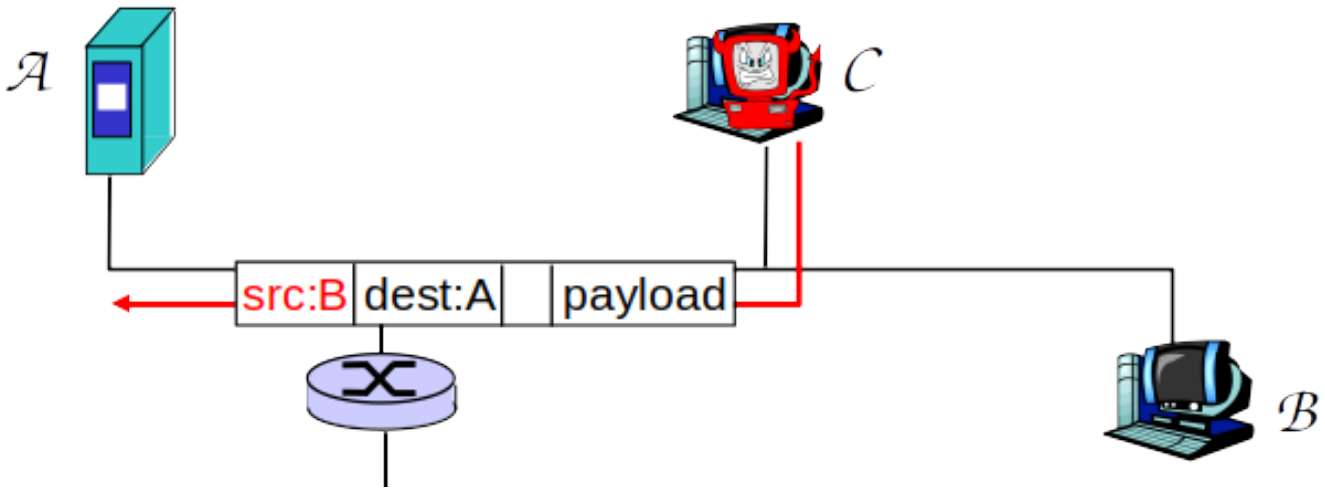
Analisadores de pacotes

- Receptor passivo que "escuta" (e grava cópias) de pacotes que trafegam pela rede
- Mais comum/fácil em redes sem fio (meio de acesso compartilhado)
- Difícil de detectar pois não causa dano "aparente"
- Mecanismos de defesa requerem uso de criptografia



Injeção de pacotes de fonte falsa (*IP spoofing*)

- O atacante cria um pacote com endereço da fonte arbitrário, conteúdo e endereço de destino alvo
- O receptor acredita que a fonte é verdadeira e executa o pacote
- Mecanismos de defesa requerem uso de confirmação da fonte



Ataques *man-in-the-middle*

- Atacante infiltrado no percurso da comunicação
- Capaz de observar todos os pacotes, introduzir, alterar ou excluir pacotes
- Pode ser um roteador comprometido ou um módulo de software no sistema final
- Compromete a integridade dos dados

Segurança na rede

Temos hoje muitos desafios relacionados à segurança das aplicações distribuídas que usam a Internet

A comunicação entre usuários de confiança mútua é mais **exceção** do que uma regra

Propriedades da comunicação segura

- Confidencialidade: conteúdo legível apenas para os comunicantes
- Autenticação: confirmação dos remetentes e destinatários
- Integridade: conteúdo não alterado
- Segurança operacional: redes das organizações não comprometidas

Referências bibliográficas

1. J. Kurose and K. Ross, **Computer Networking: A Top-Down Approach**, Addison-Wesley, 5^a ed., 2009