哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
立足航天，服务国防，面向国民经济主战场

计算机网络之危机四伏

主讲人：李全龙

本讲主题

网络安全威胁（1）

“坏蛋”们可能做什么？

Q: “坏蛋”们能做什么?

A: 很多！

- 窃听(eavesdrop): 窃听信息
- 插入(insert):主动在连接中插入信息
- 假冒(impersonation): 可以通过伪造(spoof)分组中的源地址(或者分组的任意其他字段）
- 劫持(hijacking): 通过移除/取代发送发或者接收方“接管”(take over)连接
- 拒绝服务DoS(denial of service): 阻止服务器为其他用户提供服务(e.g., 通过过载资源)

Internet安全威胁

映射(Mapping):

- 发起攻击前:“探路”(case the joint) – 找出网络上在运行什么服务
- 利用ping命令确定网络上主机的地址
- 端口扫描(Port-scanning): 依次尝试与每个端口建立TCP连接
- nmap (http://www.insecure.org/nmap/)，广为使用的国外端口扫描工具之一

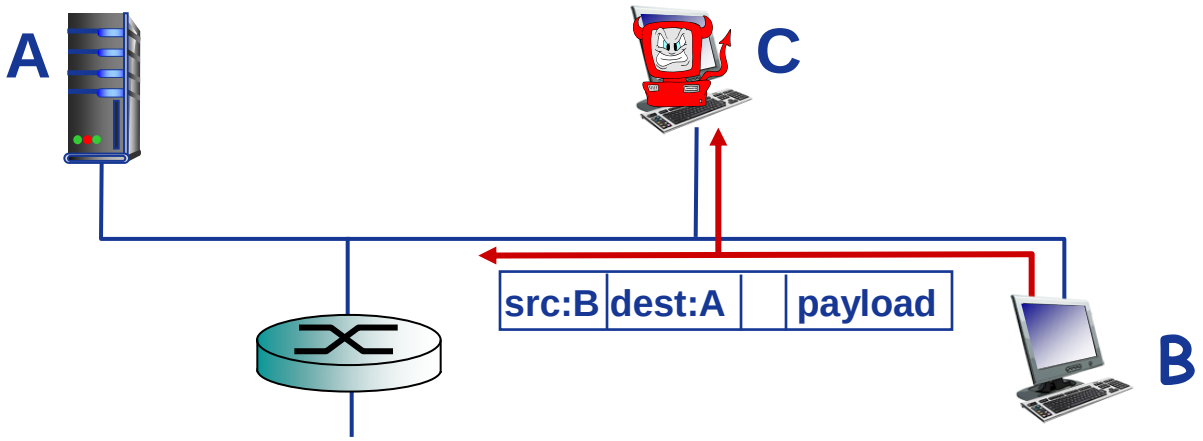
对策(Countermeasures)?

- 记录到达的网络流量
- 分析、识别出可疑活动(IP地址和端口被依次扫描)

Internet安全威胁

分组“嗅探”(sniffing):

- 广播介质(共享式以太网，无线网络)
- 混杂(promiscuous)模式网络接口可以接收/记录所有经过的分组/帧
- 可以读到所有未加密数据(e.g., 包括口令！)

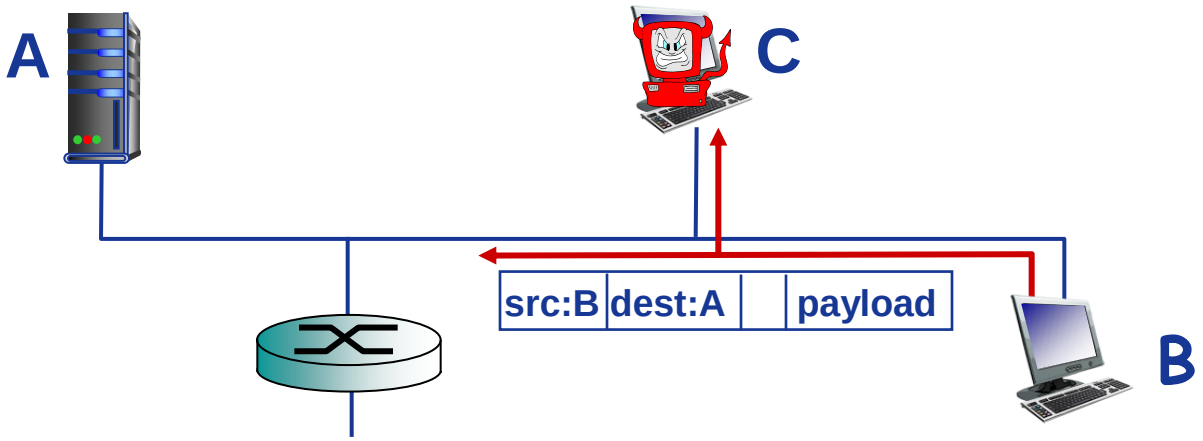


- Wireshark就是一个典型免费的分组嗅探软件

Internet安全威胁

分组嗅探: 对策

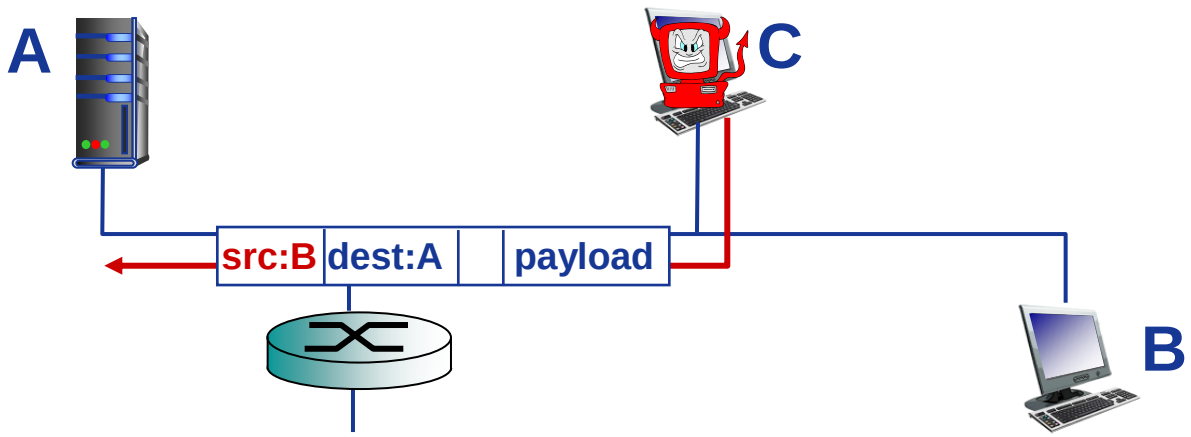
- 组织中的所有主机都运行软件，周期性监测网络接口是否工作在混杂模式
- 每段广播介质连接一台主机(如交换式以太网)



Internet安全威胁

IP欺骗(Spoofing):

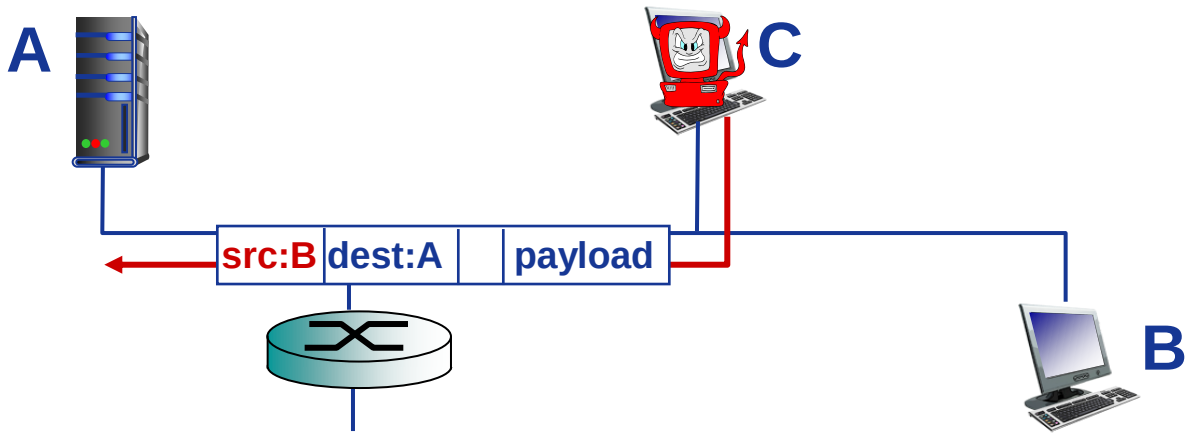
- 直接由应用生成“原始”IP分组，可以设置分组的源IP地址字段为任意值
- 接收方无法判断源地址是否被欺骗
- e.g.: C冒充B



Internet安全威胁

IP欺骗对策: 入口过滤(ingress filtering)

- 路由器不转发源IP地址无效的IP分组 (e.g., 源IP地址不属于所连接网络)
- 很有效！但是不能强制所有网络都执行入口过滤



哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场

谢 谢！