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

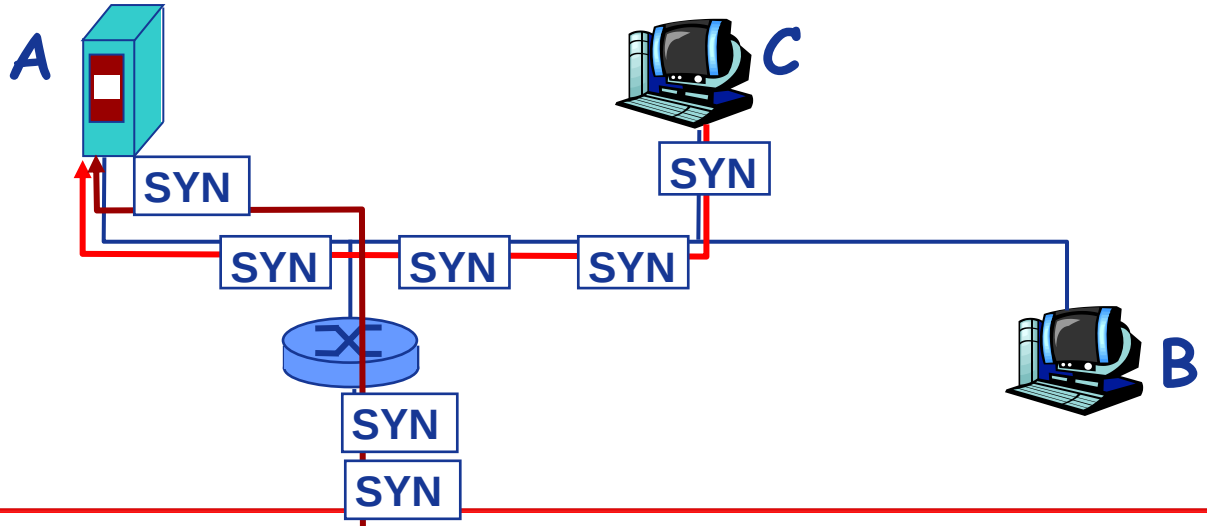
本讲主题

网络安全威胁（2）

Internet安全威胁

拒绝服务DOS(Denial of service):

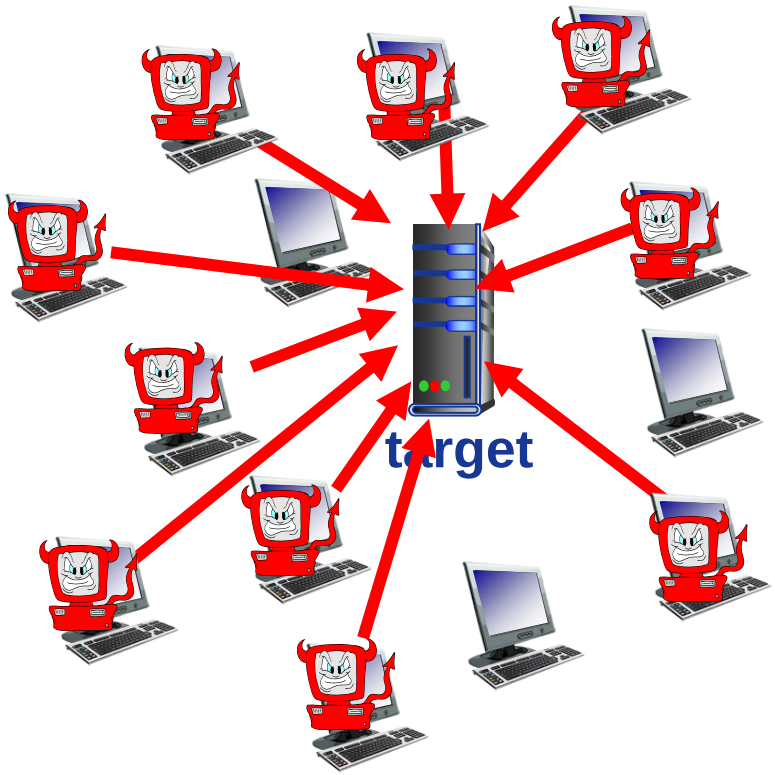
- 向接收方恶意泛洪(flood)分组，淹没(swamp)接收方
  - 带宽耗尽
  - 资源耗尽
- 分布式拒绝服务攻击 (DDOS): 多个源主机协同淹没接收方
- e.g., C与另一个远程主机协同对A进行SYN攻击



Internet安全威胁

DDoS攻击过程:

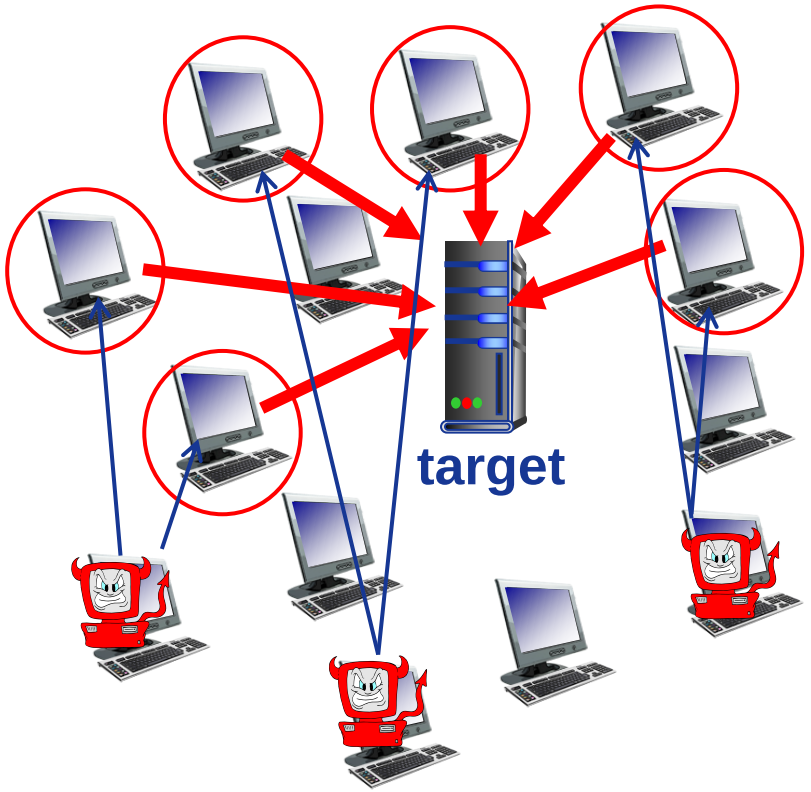
1. 选择目标
2. 入侵(break into)网络中主机（构建僵尸网络）
3. 控制僵尸主机向目标发送分组



Internet安全威胁

反射式DDoS攻击：

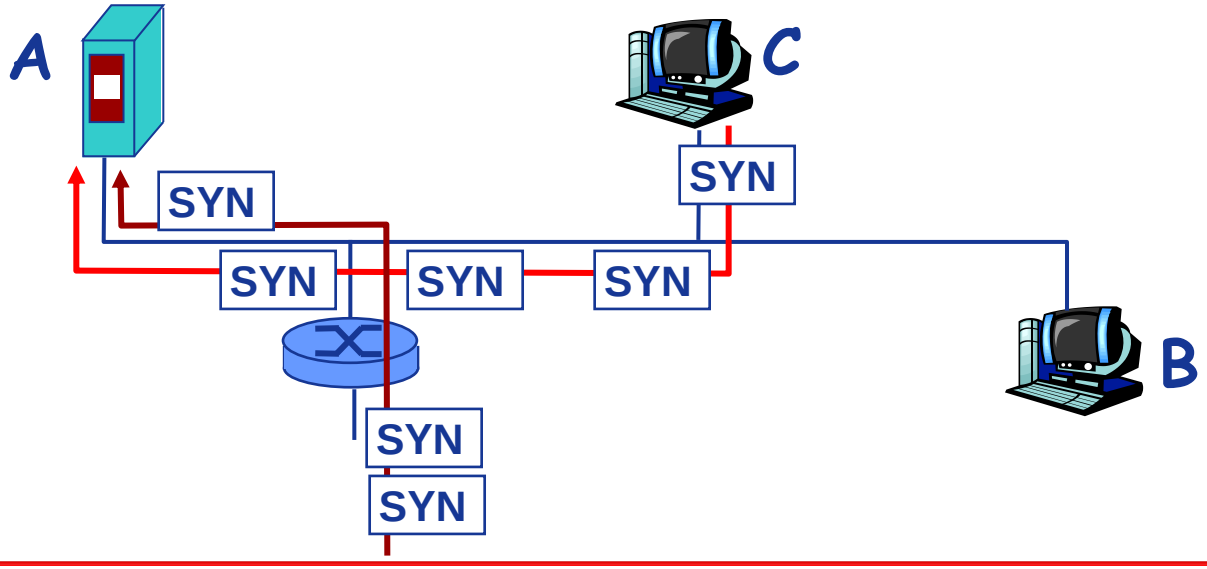
1. 选择目标
2. 入侵网络中主机（构建僵尸网络）
3. 选择反射服务器
4. 借助反射服务器向目标发起攻击



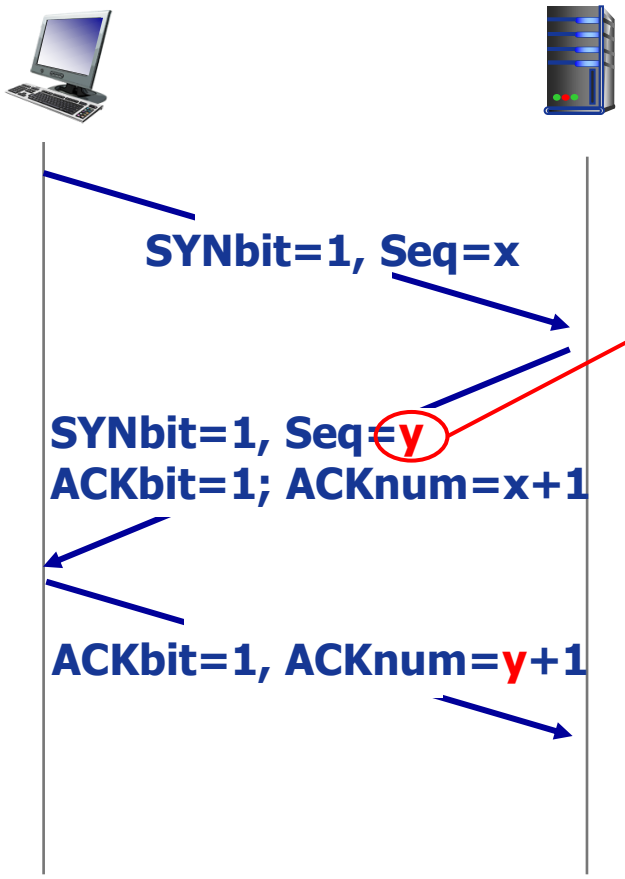
Internet安全威胁

DOS: 对策

- 在到达主机前过滤掉泛洪分组(e.g., SYN)
  - 可能好坏一起扔
- 追溯(traceback)攻击源
- SYN cookie[RFC 4987]



SYN cookie



SYN cookie：
y=Hash(源IP地址，目的IP地址，源端口号，目的端口号，R)

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！