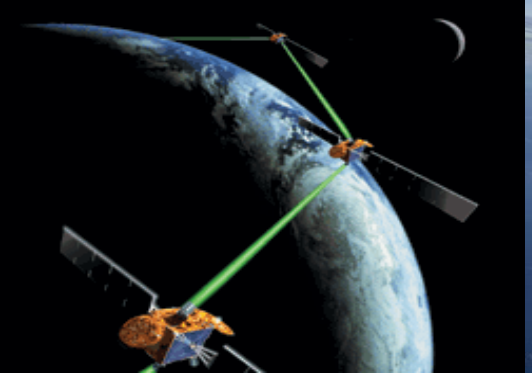
普通高等教育“十一五”国家级规划教材
教育部2011年精品教材

网络安全—技术与实践（第2版）

刘建伟 王育民 编著

清华大学出版社




课件制作人声明

- 本课件总共有17个文件，版权属于刘建伟所有，仅供选用此教材的教师和学生参考。
- 本课件严禁其他人员自行出版销售，或未经作者允许用作其他社会上的培训课程。
- 对于课件中出现的缺点和错误，欢迎读者提出宝贵意见，以便及时修订。

课件制作人：刘建伟

2016年3月21日

第2章 低层协议的安全性

一 基本协议

二 网络地址和域名管理

三 IPv6

四 网络地址转换

第2章 低层协议的安全性

一 基本协议

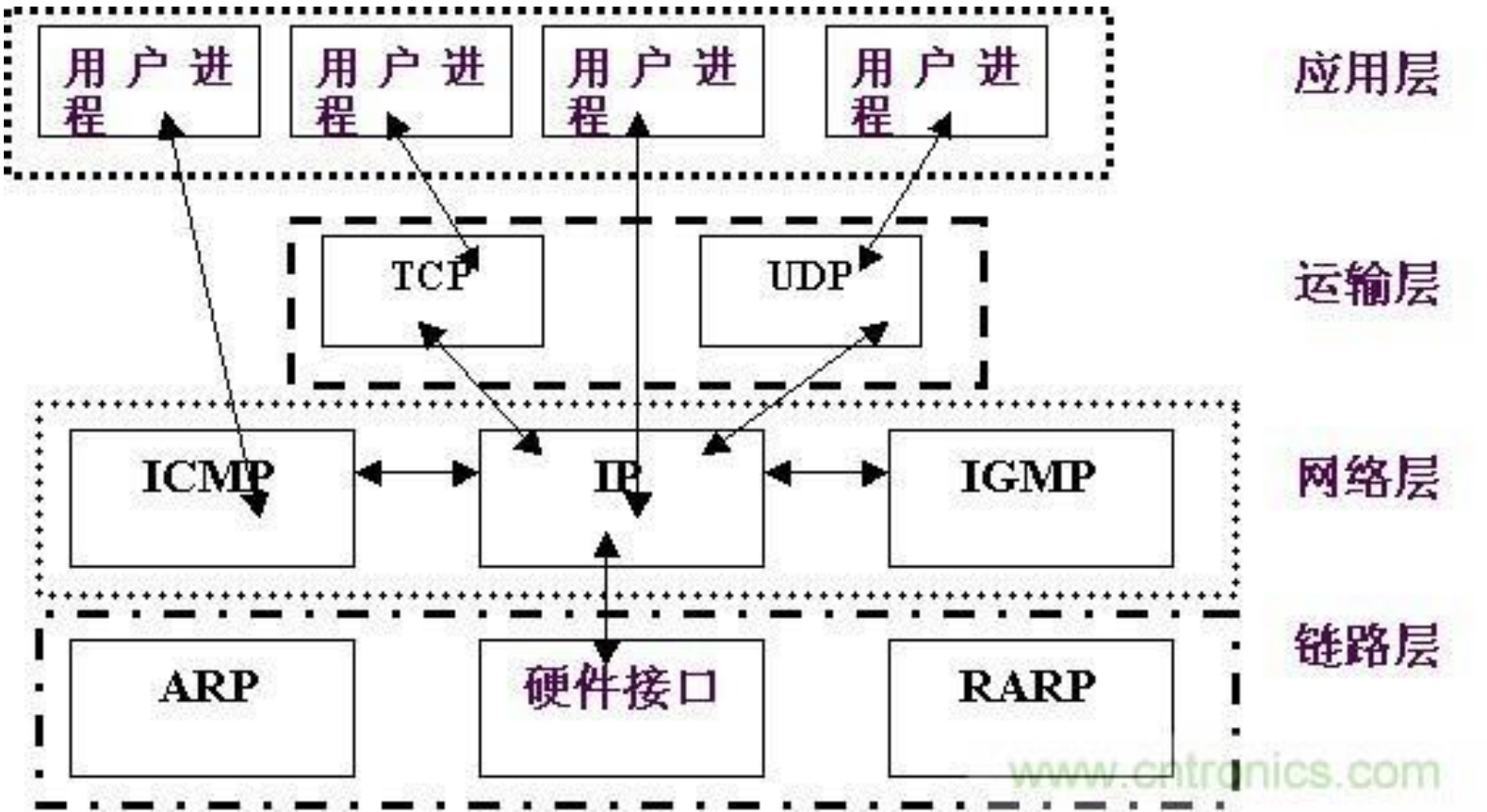
二 网络地址和域名管理

三 IPv6

四 网络地址转换

TCP/IP协议族

- Internet上的计算机和网络设备使用的是TCP/IP协议。
- TCP/IP协议不是TCP和IP这两个协议的合称，而是指因特网整个TCP/IP协议族。



网际协议—IP

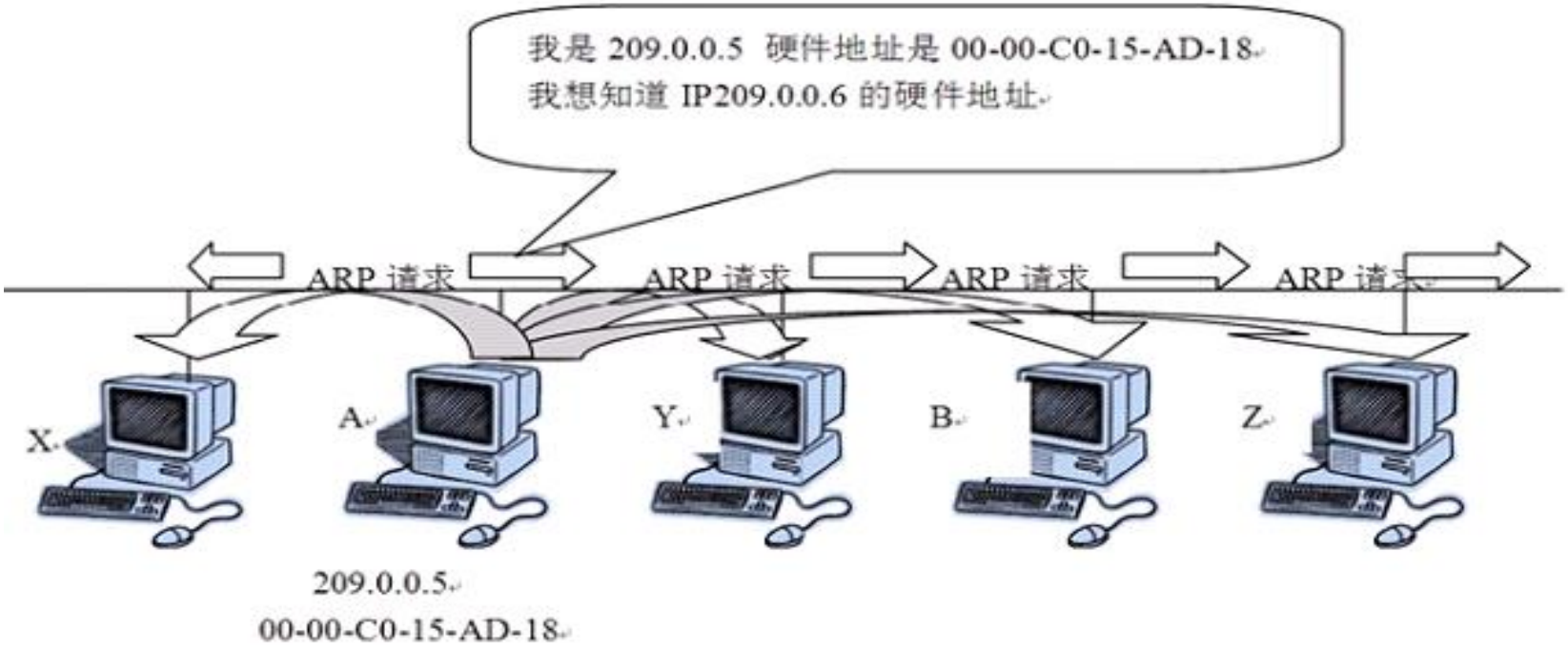
- IP协议是TCP/IP的心脏，也是网络层最重要的协议。
- 每个IP数据包是一组数据，包含有源地址和目的地址；
- IP数据包头部：包含一些比特位选项、头检验和数据净荷；
- 网络层MTU：数据包头部占20字节，MTU最长可达1480字节；
- 它可通过以太网/串行线/Sonet/分组无线电/ATM /Frame Relay等链路进行传输；
- 在IP层，不存在虚拟电路或“电话呼叫”的概念，每个数据包都是独立的；
- IP协议没有任何机制保证数据包一定能被发送、只发送一次，或以特定的次序发送；
- 路由器仅对IP头做检验，不能检验整个数据包的正确性。

IP协议的安全性

- IP协议不能保证数据就是从数据包中给定的源地址发出的，你绝对不能靠对源地址的有效性检验来判断数据包的好坏；
- 攻击者可以发送含有伪造地址的返回数据包，这种攻击叫做IP欺骗攻击；
- 当路由器遇到大数据流量的情况下，可能在没有任何提示的情况下丢掉一些数据包；
- 大数据包可能在中间节点上被分拆成小数据包。通过向包过滤器注入大量病态的小数据包，可以对包过滤器造成破坏。

地址解析协议—ARP

- 以太网发送的是48位以太地址的数据包；
- IP驱动程序必须将32位IP目标地址转换成48位地址；
- 两类地址存在静态或算法上的影射；
- ARP用来确定两者之间的影射关系；



ARP协议的安全

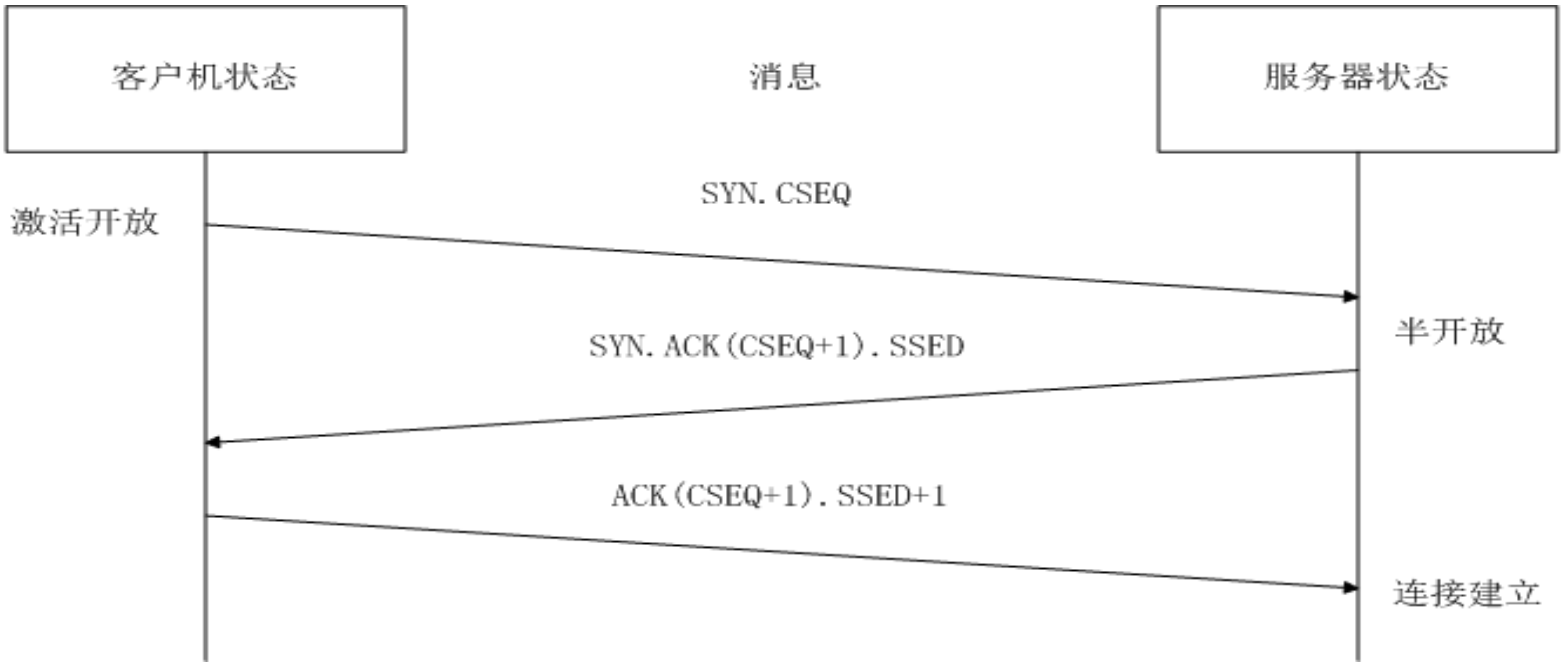
- 一台不可信赖的计算机会发出假冒的ARP查询或应答信息，并将所有流向它的数据流转移。这样，它就可以伪装成某台机器，或修改数据流。这种攻击叫做ARP欺骗攻击。
- 许多黑客软件均能实现这种攻击，如 Arpspoof。
- 在特别安全的网络上，ARP通过硬件实现静态的影射，并禁止使用自动协议以防干扰。如果我们不想让两台主机通信，只须确保它们之间不能相互进行ARP翻译。然而，要确保永远不能获得它们影射表是非常困难的。

传输控制协议—TCP

- 格式：<localhost, localport, remotehost, remoteport>
- UNIX系统规定：只有超级用户Root才能创建小于1024的端口，这些端口称为特权端口，目的是为了让远程系统可以信赖写入这些端口的信息的真实性。对于非UNIX操作系统，没有这一约定。
- 只有当你确定系统具有这样的约定，并得到正确实施和管理的时候，才能相信低端口号的特权性。
- 在实际工作中，人们通常认为具有这一特权端口约定的操作系统是安全的，但其实不然。

传输控制协议—TCP

1. TCP连接是一个3步握手过程。在服务器收到初始的SYN数据包后，该连接处于半开放状态。
2. 此后，服务器返回自己的序号，并等待确认。
3. 最后，客户机发送第3个数据包使TCP连接开放，在客户机和服务器之间建立连接。



TCP协议的安全性

- **SYN Flood攻击**：攻击者利用TCP连接的半开放状态发动攻击。攻击者使用第一个数据包对服务器进行大流量冲击，使服务器一直处于半开放连接状态，从而无法完成3步握手协议。
- 该协议易遭受**序号攻击**。如果攻击者能够预测目标主机选择的起始序号，他就可能欺骗该目标主机，使其相信它正与一台可信的主机会话。Morris已经证明，预测目标主机选择的起始序号确实是可行的。这样，攻击者会利用只靠IP源地址认证的协议攻入目标系统。
- 序号攻击的前提是必须要建立一条通往目标主机的合法连接。如果这些连接被防火墙阻挡，攻击将不会成功。

SYN-Flooding攻击

正常的三次握手建立通讯的过程

发起方

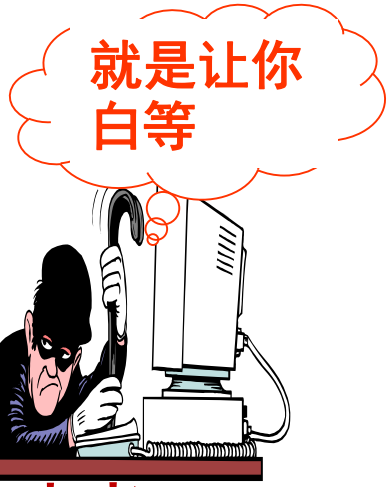
SYN （我可以和你连接吗？）

ACK | SYN（可以，请确认！）

ACK （确认连接）

应答方

攻击者伪造源地址进行SYN请求



攻击者

SYN （我可以和你连接吗？）

ACK | SYN（可以，请确认！）

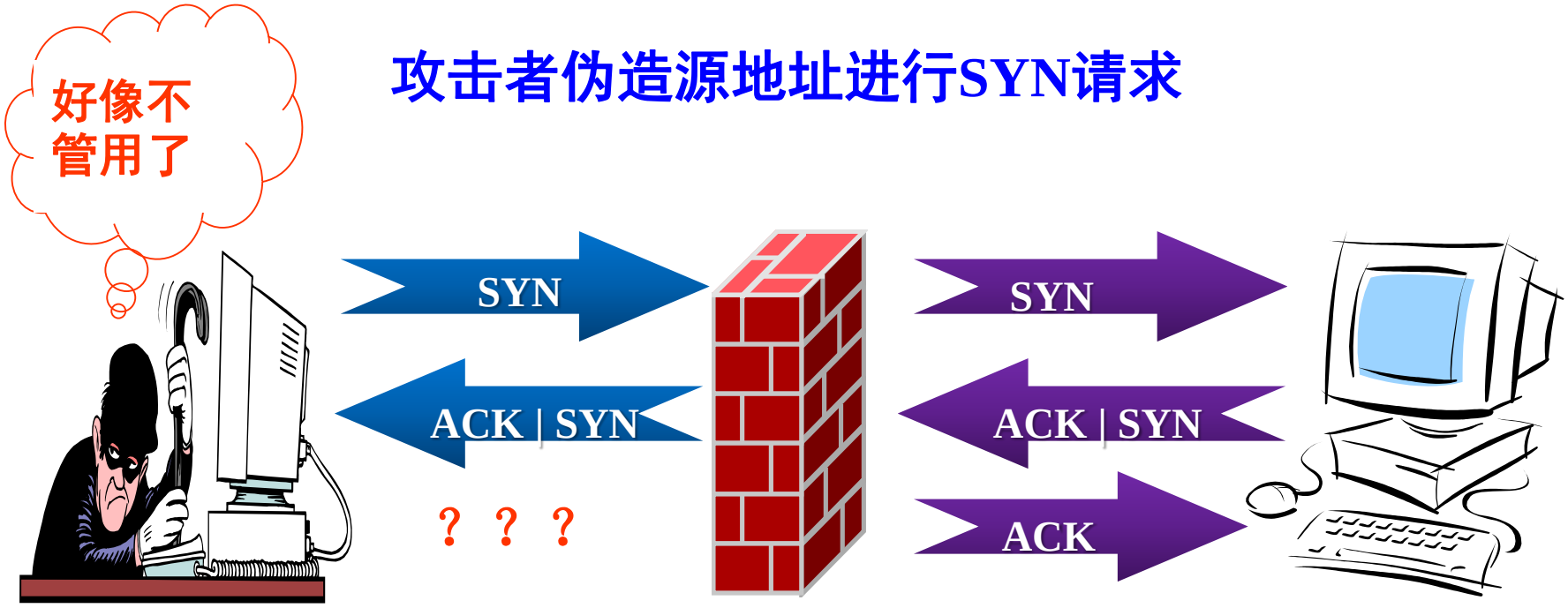
？ ？ ？

不能建立正常的连接
其它正常用户得不到响应

受害者

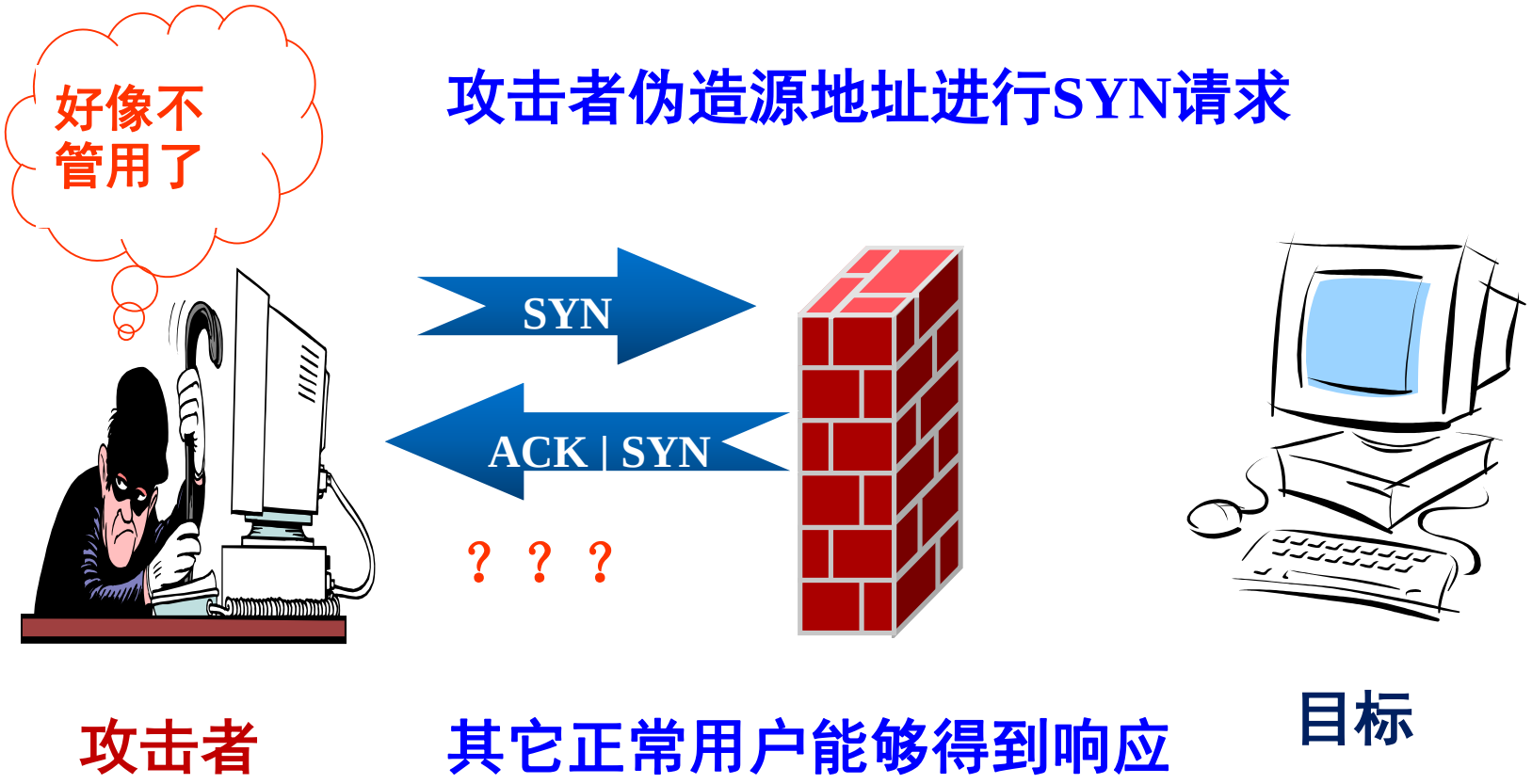
针对SYN-Flooding攻击的防范措施

1. SYN Defender



针对SYN-Flooding攻击的防范措施

2. SYN proxy



用户数据报协议——UDP

- UDP（User Datagram Protocol）数据传输过程中，没有纠错和重传机制，也没有检测丢包、复制或重新排序的机制，甚至误码检测也是可选项。
- 在数据的接收端，被分片的UDP数据包能够得以重组。
- UDP提供无连接通信，不用于那些使用虚电路的面向连接的服务；
- 由于UDP用于交换消息的开销要比TCP小得多，使得它非常适用于挑战/响应等类型的应用，如NFS、NTP、DNS等。

UDP协议的安全性

- 当UDP用于大量的数据传输时，协议自身缺少流控制特征，所以它能堵塞主机或路由器，并丢失大量的数据包。
- UDP没有虚电路的概念，忽略了源地址。在使用这些UDP数据包的源地址时，要特别小心。
- 由于UDP没有握手建立过程或序列号，所以它比TCP更加容易遭受欺骗攻击。
- 对于一些重要应用来说，必须要采用适当的认证措施。
- 针对UDP攻击的工具： udpflood.zip

Internet控制消息协议——ICMP

- ICMP是一低层机制，用来对TCP和UDP的连接行为产生影响。它可以用来通知主机到达目的地的最佳路由，报告路由故障，或者因网络故障中断某个连接。
- 它是网管员常使用的两个非常重要的监控工具—ping和traceroute（windows下为tracert）的重要组成部分。
- ICMP是一种差错和控制报文协议，不仅用于传输差错报文，还传输控制报文。

```
C:\Documents and Settings>ping www.163.com

Pinging www.cache.gslb.netease.com [61.135.253.12] with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 61.135.253.12:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

ICMP协议的安全性

- 一台主机所收到的ICMP消息都属于某些特定的连接。黑客会滥用ICMP来中断这些连接。例如，网上流行的nuke.c黑客程序。
- 更坏的情况是，黑客能够用ICMP对消息进行重定向。只要黑客能够篡改你到达目的地的正确路由，他就有可能攻破你的计算机。
- 一般来说，重定向消息应该仅由主机执行，而不是由路由器来执行。仅当消息直接来自路由器时，才由路由器执行重定向。
- 有时网管员有可能使用ICMP创建通往目的地址的新路由。这种不谨慎的行为最终会导致非常严重的网络安全问题。

第2章 低层协议的安全性

一 基本协议

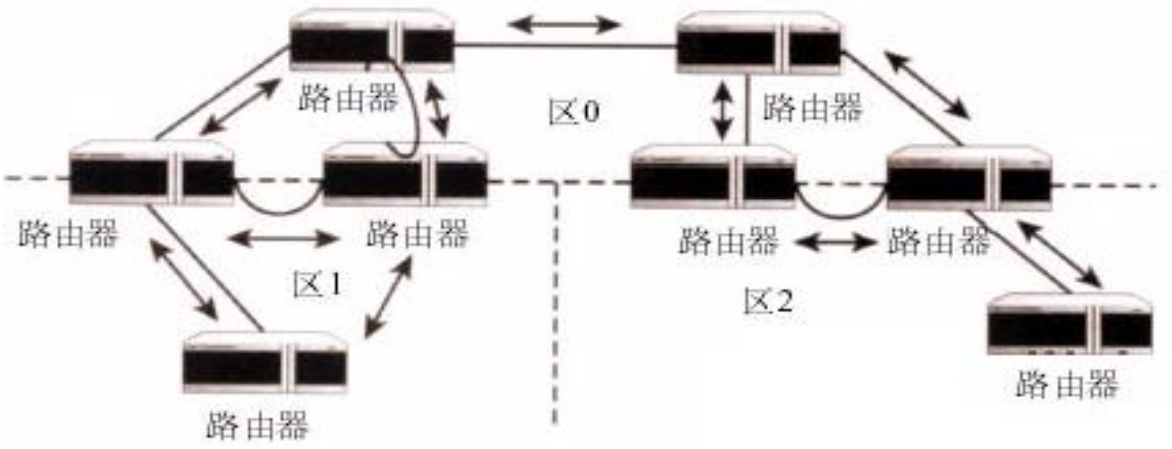
二 网络地址和域名管理

三 IPv6

四 网络地址转换

路由协议

- 路由协议是一种在因特网上动态寻找一条路径的机制。路由信息确立了两种通路：(1)主叫机器到目标主机；(2)目标主机返回到主叫机器。第2条通道可以是第1条的逆通道，也可以不是。当第2条通路不是第1条的逆通道时，就称做非对称路由。
- 路由分为静态路由和动态路由，其相应的路由表称为静态路由表和动态路由表。
- 常用的路由协议有RIP、OSPF、IS-IS、IGRP、EIGRP、BGP等



路由协议的安全性

- 攻击路由协议的常用办法是采用“IP loose source route”选项

采用这一选项，发起TCP连接的人能够指定一条到达目标主机的明确的路由，以覆盖正常的路由选择进程。因目标主机必须使用逆通道作为返回路由。这意味着攻击者可以通过控制路由而假冒任何主机以骗取被攻击的主机的信任。

- 黑客采用的另外一种途径是“戏弄”路由协议

将伪造的RIP数据包注入网络中非常容易，主机和路由器通常会相信它们。如果发起攻击的主机比真实的源主机离目标的距离更近，就容易改变数据流的方向。

对路由攻击的防护措施

- 对抗源路由欺骗攻击的最简单的办法是拒绝接收包含该选项的数据包。许多路由器都可以设置这种功能。
- 有些路由协议，如RIPv2和OSPF都规定了认证域，可以抵御某些攻击，但作用非常有限。
- 采用具有防火墙功能的路由器，以确保一条给定线路上的路由是合法的。
- 有些ISP在内部采用IS-IS路由协议来取代OSPF，使外部网络用户不能注入假的路由消息。由于IS-IS协议不是通过IP实现，所以对用户来说就没有连通性。

BGP及其安全性分析

- BGP（Border Gateway Protocol）是边界网关协议，用于为因特网上的核心路由器提供路由表。

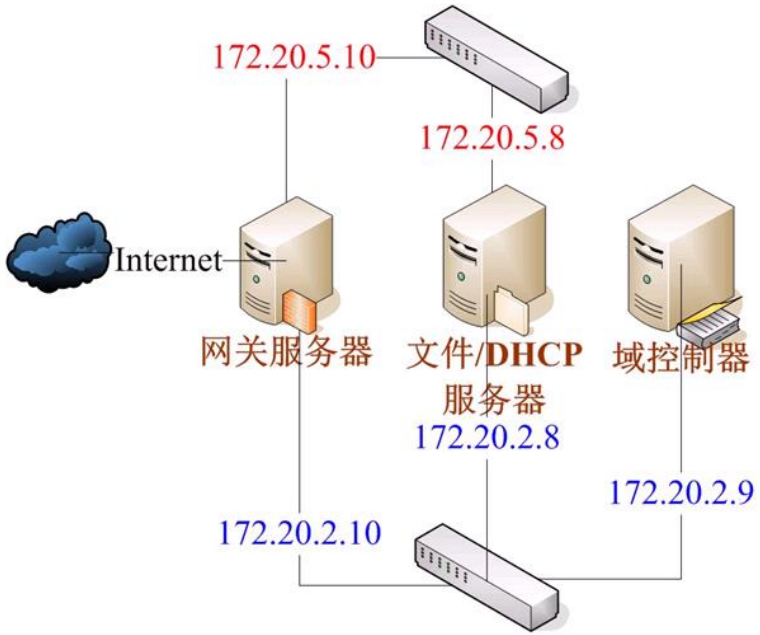
- 已经有黑客攻击BGP的报告，他们通过GRE隧道使数据流转向，并通过路由器窃听、截获或抑制正常的会话。

- 黑客有可能劫持BGP 的TCP会话。采用认证技术可以对付这一攻击。虽然该方法已成熟，但还未得到广泛应用。

动态主机配置协议——DHCP

- 域名DHCP用来分配IP地址，并提供启动计算机（或唤醒一个新网络）的其他信息。
- 此协议能够提供：域名服务器地址、默认的路由地址、默认的域名及客户机的IP地址，以及网络时间服务器的地址等。

DHCP对IP地址提供集中化的管理，简化了管理任务，可以很容易地为便携计算机分配IP地址。

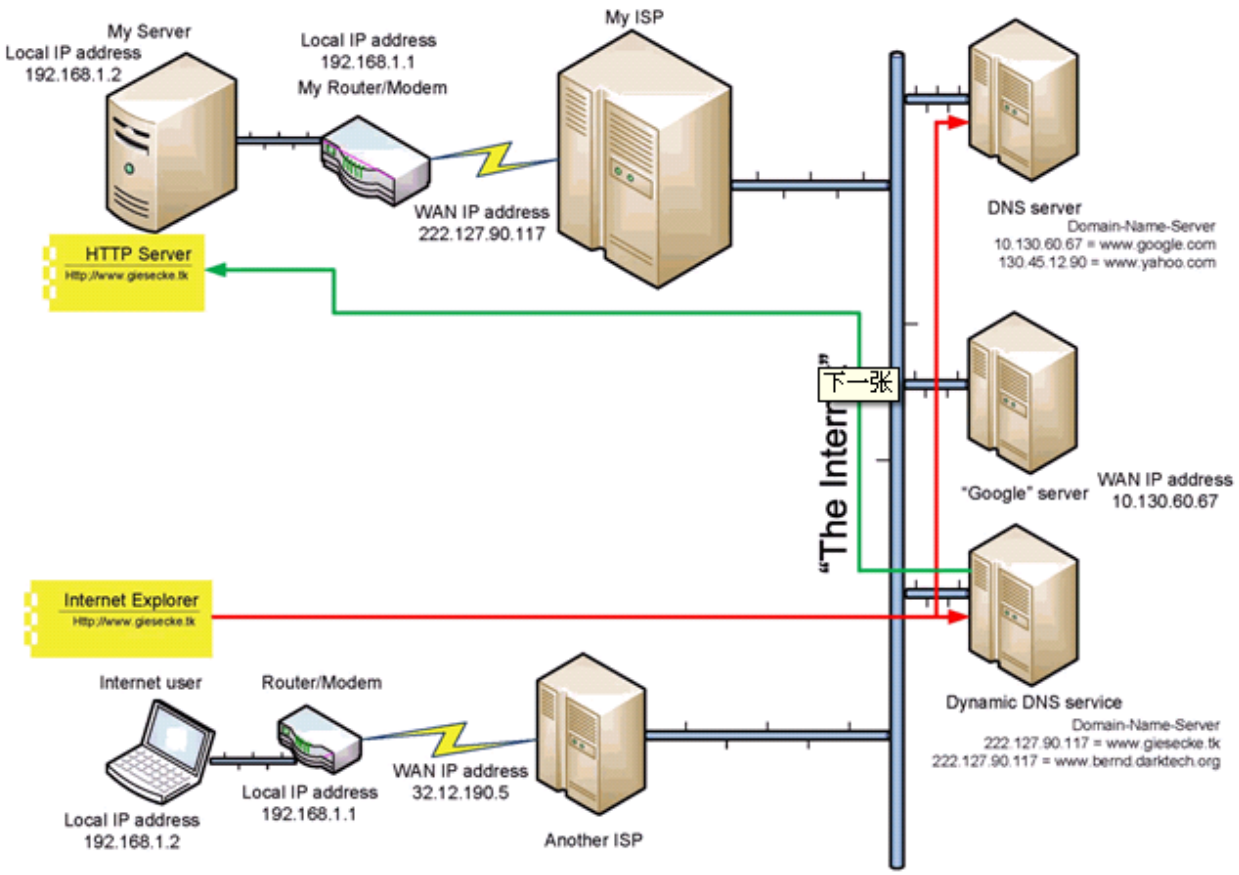


DHCP协议的安全性

- 此协议只能在本地网络上使用。由于处于启动状态的主机尚不知道其自身的IP地址，服务器的响应必须要传送它的MAC地址。由于远程攻击者无法做到对本地网络的直接访问，因此也不能发动远程攻击。
- 由于DHCP查询没有认证措施，所以查询响应容易遭受中间人攻击和DOS攻击。
- 如果攻击者已经接入到本地网络，那么它就可能对DHCP服务器发动ARP欺骗攻击。
- 假冒的DHCP服务器能够压制合法的服务器。这些假冒的服务器会模仿不同的以太地址，并向合法服务器发出请求。这样，合法的服务器会被这些查询请求淹没，全部可用的IP地址会被耗尽。

域名系统——DNS

域名系统（DNS）是一个分布式数据库，用来实现“域名→IP地址”或“IP地址→域名”的影射。



DNS的安全性

- DNS欺骗攻击： 就是攻击者假冒域名服务器的一种欺骗行为。DNS欺骗的基本原理：如果可以冒充域名服务器，然后把查询的IP地址设为攻击者的IP地址，这样的话，用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了。

- DNS缓存中毒攻击：攻击者给DNS服务器注入非法网络域名地址，如果服务器接受这个非法地址，以后响应的域名请求将会受黑客所控。当这些非法地址 进入服务器缓存，用户浏览器或邮件服务器就会自动跳转到DNS指定的地址。

- DNS重定向攻击：攻击者将DNS名称查询重定向到恶意DNS服务器上，域名解析就会被劫持，完全处在攻击者的控制之下。

对DNS的防护措施

- 强烈建议那些暴露的主机不要采用基于名称的认证。基于地址的认证虽然也很脆弱，但要优于前者。
- 攻击者可以从主机名中找出有用的信息，因此不要把秘密的信息放在主机名中。
- 抵御DNS攻击的有效方法是采用DNSsec新标准，但目前此协议还存在很多问题，从而延缓了DNSsec的推广。

第2章 低层协议的安全性

一 基本协议

二 网络地址和域名管理

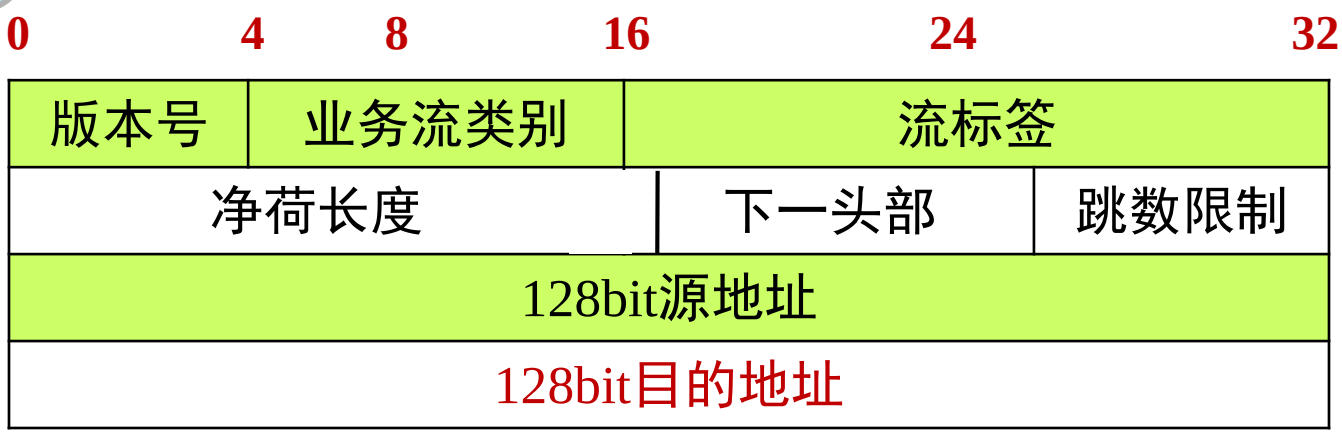
三 IPv6

四 网络地址转换

IPv6简介

IPv4头部介绍

IPv6头部介绍



过滤IPv6——IPv6协议的安全性

- IPv6与IPv4一样，它通过IPSec协议来保证IP层的安全，但是两者之间有差别：IPSec是IPv6的一个组成部分，而对IPv4来说是可选的。因此，本质上IPv6并不能比IPv4更安全。要保证IPv6网络的安全性，仍然需要传统的安全设备，如防火墙、IDS等。

- 目前，IPv6在全球还没有得到广泛应用，所以人们开发了许多协议，以实现从IPv4到IPv6的过渡。如果想让IPv6数据通过防火墙，防火墙就必须支持IPv6。若防火墙不支持IPv6，就要开通IPv6隧道，这些隧道终止于防火墙的外部。

过滤IPv6——开凿IPv6隧道的方法

6to4协议	采用41号端口。在BSD操作系统中都有6to4协议的代码。
6over4协议	与6to4协议类似，在IPv4数据包中封装了IPv6的数据流。
Teredo协议	该协议使用3544号UDP端口，并且允许隧道穿过NAT盒。
电路中继	在发送路由器上，中继代理将每个IPv6的TCP连接映射到IPv4的TCP连接上；在接收路由器上，中继代理会将IPv4的TCP连接映射到IPv6的TCP连接上。

目前，许多防火墙不能实现对IPv6的过滤。

第2章 低层协议的安全性

一 基本协议

二 网络地址和域名管理

三 IPv6

四 网络地址转换

网络地址转换协议-NAT

- NAT的主要作用是解决当前IPv4地址空间缺乏的问题。

- 从概念上讲，NAT非常简单：它们监听使用了所谓专用地址空间的内部接口，并对外出的数据包重写其源地址和端口号。外出数据包的源地址使用了ISP为外部接口分配的Internet静态IP地址。对于返回的数据包，它们执行相反的操作。

- NAT存在的价值在于IPv4的短缺。协议的复杂性使NAT变得很不可靠。在这种情况下，我们在网络中必须使用真正意义的防火墙，并希望IPv6的应用尽快得到普及。

NAT的安全性

- NAT盒可以将数据路由到特定的静态主机和端口，但并不能处理任意应用协议。商用的NAT产品确实能处理一些常用的高层协议，但是NAT盒并不支持一些不常见的应用程序或新的协议。

- 从安全的角度看，NAT最严重的问题是它不能与加密协调工作。第一，NAT不能对加密的数据流进行检查；第二，IPsec与NAT会产生冲突。原因是：IPsec要保护传输层协议头，而NAT盒却要重写的该协议头中的IP地址。

- 有人把NAT盒看作是某种形式的防火墙。在某种意义上，它是一种非常低级的防火墙。最多我们把它看成是某种形式的包过滤器，因为它缺少专业防火墙所具有的应用级过滤。

谢谢！