第3章 Internet协议的安全性

TCP/IP协议族在诞生之初，网络中的用户彼此之间被认为是互相信任的，不需要任何安全措施。现今，我们不再假设网络中的用户是互相信任的，不能认为网络是安全的。

3.1 Internet协议概述

Internet协议的主要协议及其层次关系如图3-1所示。

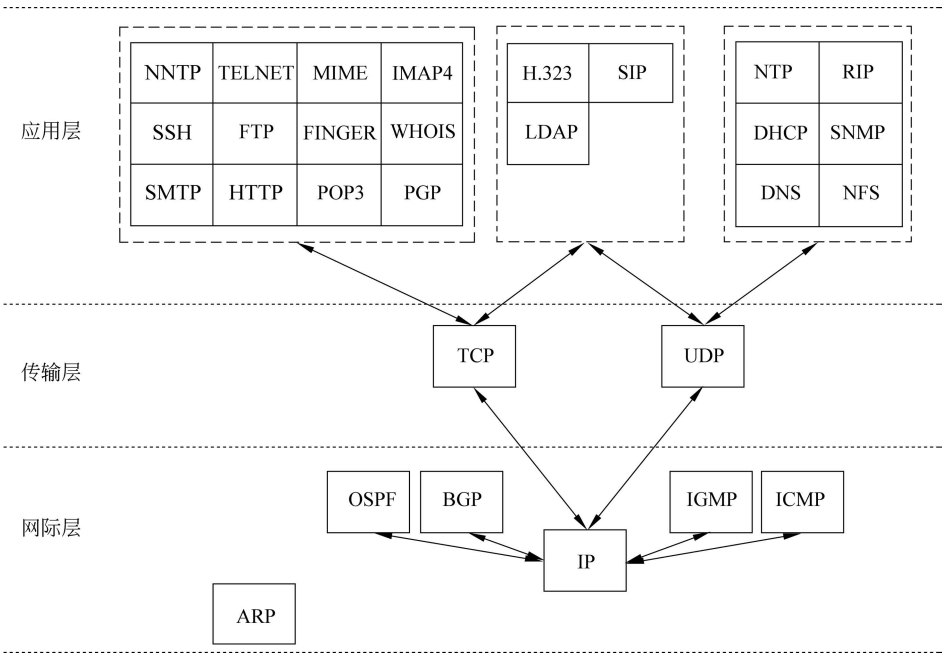

图3-1 Internet协议的主要协议及其层次关系

3.2 网际层协议

3.2.1 IP

1．概述

网际协议（Internet Protocol，IP）是TCP/IP协议族的核心，也是网际层中最重要的

协议。IP 数据包构成了 TCP/IP 协议族的基础。典型的 IP 数据包有几百字节，其中头部占 20～60 字节，其余为数据净荷部分。

IP 层接收由更低层（例如网络接口层）发来的数据包，对数据包进行处理后交付到更高层（TCP 或 UDP）；相反，IP 层也把从 TCP 或 UDP 发来的数据包传送到更低层。IP 采用尽最大努力交付的服务，是一种不可靠的无连接数据包协议。每个 IP 数据包独立路由，各个数据包可能沿不同路径由发送方传送到接收方，因此，IP 无法确认数据包是否丢失、失序或延迟到达。另外，虽然 IP 头部中存在校验位，但此校验位只用于检测 IP 数据包头部的正确性，并没有使用任何机制保证数据净荷传输的正确性，因此，无法确认 IP 数据包是否损坏。较高层的协议（如 TCP）负责处理这些问题，以便为应用程序提供一条可靠的网络通信链路。

2．IP 的安全问题及防护措施

IP 存在一系列典型的安全问题。

（1）IP 数据包在传递过程中易被攻击者监听、窃取。此种攻击是一种被动的攻击方式，攻击者并不改变 IP 数据包的内容，但可截取 IP 数据包，解析数据净荷，从而获得数据内容。这种类型的攻击很难被检测，因为攻击过程并不影响 IP 数据包的正确传递。针对这种攻击的方法是对 IP 数据包进行加密。

（2）由于 IP 层并没有采用任何机制保证数据净荷传输的正确性，攻击者可截取 IP 数据包，修改数据包中的内容后，将修改结果发送给接收方。抵抗这种攻击的方法是对 IP 数据包中的净荷部分进行完整性检测。接收方在收到 IP 数据包时，可先应用完整性检测机制检测数据包的完整性，从而保证收到的 IP 数据包在传输过程中未被恶意篡改。

（3）高层的 TCP 和 UDP 服务在接收 IP 数据包时，通常假设数据包中的源地址是有效的。事实上，IP 层不能保证 IP 数据包一定是从源地址发送的。任意一台主机都可以发送具有任意源地址的 IP 数据包。攻击者可伪装成另一台网络主机，发送含有伪造源地址的数据包以欺骗接收者。此种攻击称为 IP 欺骗攻击。针对此种攻击可以通过源地址鉴别机制加以防御。一般来说，认证需要采用高层协议中的安全机制来实现。

（4）IP 数据包在传递过程中，如果数据包太大，该数据包就会被分段。也就是说，大的 IP 数据包会被分成两个或多个小数据包，每个小数据包都有自己的头部，但其数据净荷仅是大数据包净荷的一部分。每个小数据包可以经由不同的路径到达目的地。在传输过程中，每个小数据包可能会被继续分段。当这些小数据包到达接收方时，它们会被重组到一起。按照协议规则，中间节点不能对小数据包进行拼装组合。一般来说，包过滤器完成 IP 数据包的分段和重组过程。然而，正是由于 IP 数据包在传输过程中要经历被分段和重组的过程，攻击者可在包过滤器中注入大量病态的小数据包，破坏包过滤器的正常工作。当重要的信息被分成两个 IP 数据包时，过滤器可能会错误地处理数据包，或者仅传输第 2 个 IP 数据包。更糟糕的是，当两个重叠的 IP 数据包含有不同的内容时，重组规则并不提示如何处理这两个 IP 数据包。许多防火墙能够重组分段的 IP 数据包，以检查其内容。

（5）使用特殊的目的地址发送 IP 数据包也会引入安全问题。如发送目的地址是直接

广播地址的 IP 数据包，发送这样的数据包是非常危险的，因为它们可以很容易地被用来攻击许多不同类型的主机。许多攻击者已将定向广播作为一种网络攻击手段。其实许多路由器具有阻止发送这类数据包的能力，因此，强烈建议网络管理员在配置路由器时，一定要启用路由器的这个功能。

3.2.2 ARP

1．概述

在通常情况下，当我们访问一台计算机时，一定可以知道它的逻辑地址，但不一定知道其物理地址。如果不知道物理地址，则不能把网络层的数据包封装成 MAC 帧，通信不能完成。ARP 正是为了解决这个问题而设置的。

在每台主机上都设置有一个所在网段上的各主机和路由器的 IP 地址到硬件地址的映射表，也称为 ARP 高速缓存。在数据发送方，当网络层的数据包要封装成 MAC 帧时，首先在高速缓存中查看有无该数据包头部的目的地址所对应的硬件地址，若有，则将该硬件地址写入 MAC 帧的目的地址中，完成数据包的封装。若无，ARP 则在本局域网上广播发出一个 ARP 请求分组。在 ARP 请求分组中，发送方的 IP 地址和发送方的硬件地址以及目标 IP 地址都应写入已知的数据，要寻找的目标硬件地址写入全 0。当该请求分组到达每台机器时，每台机器都要拿自己的 IP 地址和请求分组中的目标 IP 地址进行比较，如果不同则不做任何动作；若相同则发送一个 ARP 相应分组给请求方（这里不再使用广播，而是单播）。在相应分组中发送方已写明自己的硬件地址。当这一通信过程完成时，通信双方都要对自己的 ARP 高速缓存进行修改，添加上一条记录。

2．ARP 的安全问题及防护措施

通过上述 ARP 的工作原理可知，一名黑客只要能把他的主机成功插入某个网段，这台主机就能够接收到所在网段的 ARP 请求分组，从而获知该网段上主机 IP 和 MAC 地址的对应关系。从这里也可以看出，ARP 攻击仅仅在内网进行，它无法对外网（互联网、非本区域内的局域网）进行攻击。

ARP 欺骗攻击的原理如下：假设局域网中有一台主机 C，其 MAC 地址为 00-AA-00-F2-C8-04，感染了 ARP 木马。那么主机 C 将会向某主机 A 发送一个伪造的 ARP 响应，告知主机 A：主机 B 的 IP 地址 192.168.10.8 对应的 MAC 地址是 00-AA-00-F2-C8-04（其实是主机 C 的 MAC 地址），于是，主机 A 将这个对应关系写入自己的 ARP 缓存表中。以后当主机 A 向主机 B 发送数据时，都会将本应发往主机 B 的数据发送给攻击者（主机 C）。同样地，如果攻击者向主机 B 也发送一个伪造的 ARP 响应，告诉主机 B：主机 A 的 IP 地址 192.168.0.1 对应的 MAC 地址是 00-AA-00-F2-C8-04，主机 B 也会将数据发送给攻击者。至此攻击者就控制了主机 A 和主机 B 之间的流量，他可以选择被动地监测流量，获取密码和其他涉密信息，也可以伪造数据，改变主机 A 和主机 B 之间的通信内容。

为了解决 ARP 欺骗攻击问题，可以在网络中的交换机上配置 802.1x 协议。IEEE 802.1x 是基于端口的访问控制协议，它对连接到交换机的用户进行认证和授权。在交换机上配置 802.1x 协议后，攻击者在连接交换机时需要进行身份认证（结合 MAC、端口、

账户、VLAN 和密码等），只有通过认证后才能向网络发送数据。攻击者未通过认证就不能向网络发送伪造的 ARP 报文。

另外，建立静态 ARP 表也是一种有效地抵抗 ARP 攻击的方法，而且对系统影响不大，缺点是破坏了动态 ARP。

3.2.3　ICMP

1．概述

Internet 控制报文协议（Internet Control Message Protocol，ICMP）是一个重要的错误处理和信息处理协议，运行在网际层。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。ICMP 的主要功能之一是向 IP 节点发送一个简单消息，并将消息回显到发送主机。因而，它可以提供目的节点的可达性和到达目的节点所采用的传输路径等信息，在网络监控和故障诊断方面具有重要作用，是网络管理员常用的两个监控工具——Ping 和 Traceroute 的重要组成部分。

ICMP 提供了 IP 路由和交付问题的关键反馈信息，以及重要的 IP 诊断和控制能力，可用于网络的可达性分析、拥塞控制、路由优化和超时错误报告等方面。ICMP 最典型的用途是差错报告。例如，当某个网关发现传输错误时，该协议会立即向信源主机发送 ICMP 报文，报告出错信息，让信源主机采取相应处理措施。在运行 Telnet、FTP 或 HTTP 会话时，通常会遇到如“目的网络不可达”之类的错误报文，这些报文就是在 ICMP 中产生的。

IPv6 有新版本的 ICMP。ICMPv6 与 ICMPv4 的很多消息是相似的，如 Echo 请求与应答消息、路由请求和公告等，但 ICMPv6 也新增了一些消息，如路由器重编号等。

2．ICMP 的安全问题及防护措施

ICMP 能够提供有关网络配置和连接状态等信息，为网络监控和故障诊断提供了重要依据。然而，黑客也能够利用 ICMP 提供的这些信息，进行各种网络攻击和信息侦察。例如，一些黑客会滥用 ICMP 中断某些连接，网上流行的 nuke.c 黑客程序就采用了这类攻击方式。此外，ICMP 还存在一些典型的安全问题。

（1）ICMP 重定向攻击。ICMP 可以用来对主机之间的消息进行重定向，同样，黑客也能够用 ICMP 对消息进行重定向，进而使得目标机器遭受连接劫持和拒绝服务等攻击。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。然而，网络管理员有时可能会使用 ICMP 创建通往目的地的新路由。这种非常不谨慎的行为最终会导致非常严重的网络安全问题。

（2）ICMP 路由器发现攻击。在进行路由发现时，ICMP 并不对应答方进行认证，这使得它可能遭受严重的中间人攻击。例如，在正常的路由器响应 ICMP 询问之前，攻击者可能会假冒正常的路由器，使用伪造的响应信息应答 ICMP 询问。由于在路由发现的过程中，ICMP 并不对应答方进行认证，因此接收方将无法知道这个响应是伪造的。

（3）防火墙穿越攻击。通过防火墙穿越攻击技术（Firewalking），攻击者能够穿越某个防火墙的访问控制列表和规则集，进而确定该防火墙过滤的内容和具体的过滤方式。

尽管防火墙面临着启用 ICMP 所带来的风险，但在防火墙上封堵所有的 ICMP 消息并不妥当。这是因为主机常采用一种称为 Path MTU 的机制，来测试究竟多大的数据包可以不用分段发送，而这种测试需要依赖于地址不可达的 ICMP 数据包穿过防火墙。

3.2.4 IGMP

1．概述

IGMP（Internet Group Management Protocol）作为 Internet 组播管理协议，是 TCP/IP 协议族中的重要协议之一，所有 IP 组播系统（包括主机和路由器）都需要支持 IGMP。IGMP 运行于主机和组播路由器之间，用于在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。到目前为止，IGMP 共有三个版本，即 IGMP v1、v2 和 v3。

IGMP 实现的主要功能包括：主机通过 IGMP 通知路由器希望接收或离开某个特定组播组的信息；路由器通过 IGMP 周期性地查询局域网内的组播组成员是否处于活动状态，实现所连网段组成员关系的收集与维护。

2．IGMP 的安全问题及防护措施

IGMP 组播报文在 IP 数据包的基础上封装了组播地址等信息，鉴于组播报文基于 UDP 进行传输并缺少用户认证措施，网络中任何主机都可以向组播路由器发送 IGMP 包，请求加入或离开，导致非法用户很容易加入组播组，窃听组播数据或者发动其他针对计算机网络系统的攻击。目前，针对 IGMP 的攻击主要有以下几种：

（1）利用查询报文攻击。利用具有较低数值的 IP 地址路由器发送伪造的查询报文，由当前的查询方转变为响应查询请求，并且不再发出查询报文。攻击产生的效果包括：组播路由器对子网内各主机的加入请求不做任何响应，将屏蔽合法用户；组播路由器对子网内主机撤离报文不做响应，造成该子网内不存在组播用户，但是，组播数据又不断向该子网组播路由器发送请求报文，浪费有限的带宽和资源。

（2）利用离开报文进行 DoS 攻击。子网内非法用户通过截获某个合法用户信息来发送伪造的 IGMP 离开报文，组播路由器接收到报文后误认为该合法用户已经撤离该组播组，则不再向该用户发送询问请求，导致该合法用户不能再接收到组播数据包，造成拒绝服务攻击。

（3）利用报告报文攻击。非法用户伪装报告报文，或截获合法用户的报告报文向组播路由器发送伪造报文，使组播路由器误以为有新用户加入，于是将组播树扩展到非法用户所在的子网，此后非法用户就可以接收到来自组播路由的组播报文，并分析该报文以展开新的攻击。

IGMP 安全性的基本要求是只有注册的合法主机才能够向组播组发送数据和接收组播数据。但是，IP 组播很难保证这一点。首先，IP 组播使用 UDP，网络中任何主机都可以向某个组播地址发送 UDP 包；其次，Internet 缺少对于网络层的访问控制，组成员可以随时加入和退出组播组；最后，采用明文传输的 IGMP 组播报文很容易被窃听、冒充和篡改，使得组播安全性问题仍然是一个技术难点。

针对以上安全问题，一种有效的安全增强措施是利用 IGMP v3 的扩展性在组播报文中未使用的辅助字段部分增加认证信息，即在每个首次加入组播的报文中添加关联主机身份的认证信息，组播路由器接收到认证信息并通过公钥密码技术实现成员身份的认证，随后，在发送给组播成员的查询信息中添加成功/失败标识的认证信息。通过此认证机制来保证 IGMP 的安全运行。

3.2.5　OSPF 协议

1．概述

由于 Internet 规模宏大，所以常把它划分成许多较小的自治系统（Autonomous System，AS）。自治系统内部的路由协议称为内部网关协议，自治系统之间的协议称为外部网关协议。常见的内部网关协议有 RIP 和 OSPF 协议；外部网关协议有 BGP。OSPF 协议和 BGP 都位于网络层，但 RIP 位于应用层。OSPF 协议是分布式的链路状态路由协议。链路在这里代表该路由器和哪些路由器是相邻的，即通过一个网络是可以连通的。链路状态说明了该通路的连通状态以及距离、时延、带宽等参数。在该协议中，只有当链路状态发生变化时，路由器才用洪泛法向所有路由器发送路由信息。所发送的信息是与本路由器相邻的所有路由器的链路状态。为了保存这些链路状态信息，每个路由器都建立有一个链路状态数据库，因为路由器交换信息时使用的是洪泛法，所以每个路由器都存有全网的链路状态信息，也就是说每个路由器都知道整个网络的连通情况和拓扑结构。这样每个路由器都可以根据链路状态数据库的信息来构造自己的路由表。路由表内包含数据包去往目的地地址的下一跳路由信息。OSPF 协议是 TCP/IP 工作的基础。

2．OSPF 协议的安全问题及防护措施

OSPF 协议的数据包中包含了认证类型以及认证数据字段，如图 3-2 所示。其中主要有密码认证、空认证以及明文认证这 3 种认证模式。明文认证是将口令以明文的方式进行传输，只要可以访问到网络的人都可以获得这个口令，易遭受来自网络内部的攻击。密码认证则能够提供良好的安全性。为接入同一个网络或者是子网的路由器配置一个共享密钥，然后这些路由器所发送的每一个 OSPF 报文都会携带一个建立在这个共享密钥基础之上的消息认证码。当路由器接收到报文之后，根据路由器上的共享密钥以及接收到的报文通过 MD5Hash 函数生成一个消息认证码，并将生成的消息认证码与接收到的消息认证码进行对比，如果两者一致就接收，反之则丢弃。OSPF 协议规定了认证域，但其作用非常有限，主要原因如下：

（1）即使 OSPF 协议提供了较强的认证，但某些节点仍然使用简单的口令认证。那些能够欺骗路由协议的人也就有能力收集到本地以太网上传送的口令。

（2）在路由对话中，如果有一个合法的用户遭到破坏，那么它的消息就不再可信。

（3）在许多路由协议中，每台机器只与邻近的计算机对话，而这些邻近的计算机将会重复旧的会话内容。这样，欺骗就会得到传播扩散。路由信息确定了两条通道：一条是从主叫机器到目标主机，另一条是从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。如果两条通道不是逆通道的时候，则称为非对称路由。这种

情况在 Internet 上非常普遍。当网络有多个防火墙时，就会产生问题。从安全的角度看，返回通道通常更加重要。当目标主机遭到攻击的时候，反向流动的数据包是通过什么通道到达攻击主机的呢？如果敌人能够破坏路由机制，那么目标主机就会被欺骗，使其相信敌人的机器是一台真正可信赖的机器。如果这种情况发生，那么依赖于源地址验证的认证机制将会失败。

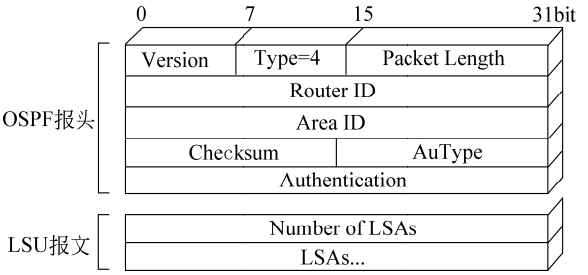

图 3-2　OSPF 协议的数据包结构

3.2.6　BGP

1．概述

BGP（Border Gateway Protocol）是边界网关协议，它将单一管理的网络转化为由多个自治系统分散互联的网络。BGP 通常工作于 ISP 内部或 ISP 之间，有时也工作于 Intranet 内部。BGP 使用 TCP 作为路由交换的底层传输协议，其以增量的更新实现路由信息交换。首个 BGP 版本在 RFC1105 中规定，目前实际运行版本为 BGP-4（RFC4271）。有关 BGP 的详细描述可参阅相关文献。

2．BGP 的安全问题及防护措施

BGP 最主要的安全问题在于：每个自治系统向外通告自己所拥有的 CIDR（Classless Inter-Domain Routing）地址块，并且协议无条件信任对等系统的路由通告，这就导致一个自治系统向外通告不属于自己的前缀时，也会被 BGP 用户认为合法，从而接受和传播。有研究人员将问题归结为 BGP 缺乏一个安全可信的路由认证机制，即 BGP 无法对所传播的路由信息的安全性进行验证。为了抵抗针对 BGP 的攻击，研究人员主要提出了两类方案：路由认证类方案和前缀劫持检测类方案。

路由认证类方案利用数字证书、签名和其他密码学技术保护路由信息的真实性和完整性。

（1）首先出现的是针对劫持 BGP TCP 会话的 MD5 BGP 认证技术。会话者通过验证 TCP 伪头部、头部、数据段和共享秘密的 MD5 杂凑值实现认证。这种方法比较成熟，也具有很高的效率，但是其安全性随着 MD5 算法的安全性减弱已经逐渐降低。

（2）S-BGP 方案利用 PKI 技术增强 BGP 的安全性。该方案在 BGP 会话者接收到的整个路径上提供数字签名链。这种方案受到 PKI 技术的制约，存在计算开销大等问题。同时，受制于各厂商和管理机构的标准难于统一，该方案难以推广与部署。

（3）为了解决 S-BGP 方案不易部署等缺陷，出现了许多基于 S-BGP 的改进方案。如

Cisco 公司的 soBGP 方案、IRV（Interdomain Routing Validation）方案以及 IETF 的 SIDR 工作组开发的 RPKI（Resource Public Key infrastructure）& BGPsec 方案。

前缀劫持检测类方案利用异常检测（Anomaly Detection）技术提取 BGP 运行中的异常信息，对前缀劫持行为进行检测，从而提高 BGP 的安全性。

（1）多源 AS（Multiple Origin AS，MOAS）检测技术通过获取网络中控制平面的信息，对比 MOAS 列表的一致性，区分有效的 MOAS 和攻击的 MOAS。PHAS（Prefix Hijack Alert System）检测技术通过审查 BGP 协议获得的路由数据，发现前缀劫持威胁，并向管理者通报路由异常。

（2）主动探测技术利用数据平面反馈的信息发现前缀劫持行为。根据观测点（Vantage Point）与被测自治系统位置的对应关系，可以分为由外及内探测和由内及外探测两类主动探测技术。

为了综合利用以上两类检测技术的优点，研究人员也提出了将主动探测技术和 MOAS 检测技术结合的前缀劫持混合检测技术。

3.3 传输层协议

本节将主要讨论传输层协议及其安全性分析。传输层的任务是在源主机和目的主机之间提供可靠的、性价比合理的数据传输功能，向下利用网络层提供给它的服务，向上为其用户（通常为应用层中的进程）提供高效、可靠和性价比合理的服务。传输层的存在使得传输服务有可能比网络服务更加可靠，丢失的分组和损坏的数据可以在传输层上检测出来，并进行纠正。Internet 传输层有两个主要协议，一个是面向连接的 TCP，另一个是无连接的 UDP。

3.3.1 TCP

1．概述

TCP 是一个面向连接的可靠传输协议，提供某些用户所期望的而 IP 又不能提供的功能。例如，IP 层的数据包非常容易丢失、被复制或以错误的次序传递，无法保证数据包一定被正确递交到目标端。而 TCP 会对数据包进行排序和校验，未按照顺序收到的数据包会被重排，而损坏的数据包也可以被重传。TCP 的原始正式定义在 RFC793 中，此外在 RFC1122 中详细阐述了一些错误的修补方案，在 RFC1323 中又进一步作了扩展。

2．TCP 的安全问题及防护措施

目前针对 TCP 的攻击主要可以划分为以下 3 类。

（1）第一类攻击是针对 TCP 连接建立阶段的三次握手过程。TCP 是一个面向连接的协议，即在数据传输之前要首先建立连接，然后传输数据，当数据传输完毕后释放所建立的连接。TCP 通过三次握手建立连接，这种方式大大增强了传输的可靠性，例如，防止已失效的连接请求报文段到达被请求方，产生错误造成资源的浪费。具体过程如图 3-3

所示。但与此同时，三次握手机制却给攻击者提供了可以利用的漏洞，这类攻击中最常见的就是 SYN FLOOD 攻击，攻击者不断向服务器的监听端口发送建立 TCP 连接的请求 SYN 数据包，但收到服务器的 SYN 数据包后却不回复 ACK 确认信息，每次操作都会使服务器端保留一个半开放的连接，当这些半开放连接填满服务器的连接队列时，服务器便不再接受后续的任何连接请求，这种攻击属于拒绝服务（Denial of Service，DoS）攻击。防御这类攻击的主要思路是在服务器前端部署相应的网络安全设备（如防火墙设备），过滤 SYN FLOOD 攻击数据包。

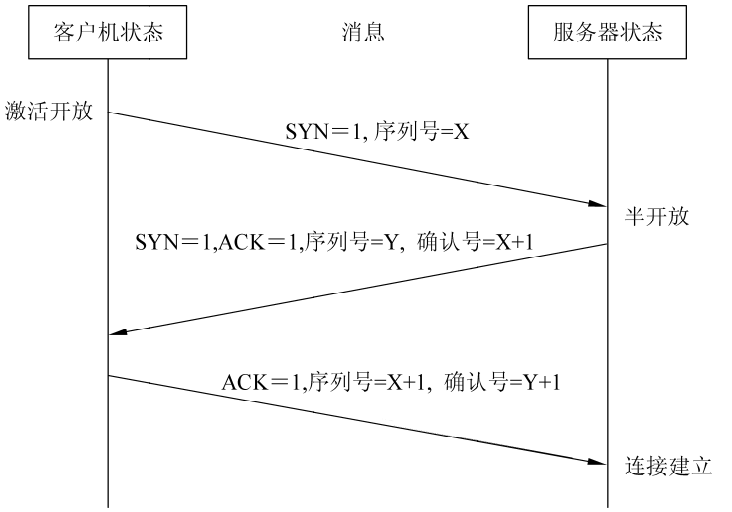

图 3-3　TCP 三次握手连接建立过程

（2）第二类攻击针对 TCP 不对数据包进行加密和认证的漏洞，进行 TCP 会话劫持攻击。TCP 有一个关键特征，即 TCP 连接上的每一字节都有它自己独有的 32 位序列号，数据包的次序就靠每个数据包中的序列号来维持。在数据传输过程中所发送的每一字节，包括 TCP 连接的打开和关闭请求，都会获得唯一的标号。TCP 确认数据包的真实性的主要根据就是判断序列号是否正确，但这种机制的安全性并不够，如果攻击者能够预测目标主机选择的起始序号，就可以欺骗该目标主机，使其相信自己正在与一台可信主机进行会话。攻击者还可以伪造发送序列号在有效接收窗口内的报文，也可以截获报文并篡改内容后再发送给接收方。防御此类攻击的思路是在 TCP 连接建立时采用一个随机数作为初始序列号，规避攻击者对序列号的猜测。

（3）第三类攻击是针对 TCP 的拥塞控制机制的特性，在 TCP 连接建立后的数据传输阶段进行攻击，降低网络的数据传输能力。拥塞控制是 TCP 的一项重要功能，所谓拥塞控制就是防止过多的数据注入网络，使网络中的链路和交换结点（路由器）的负荷不致过载而发生拥塞，TCP 的拥塞控制主要有以下 4 种方法：慢启动、拥塞避免、快重传和快恢复。发送端主机在确定发送报文段的速率时，既要考虑接收端的接收能力，又要考虑网络的传输能力。因此，每一个 TCP 连接都需要维护接收窗口和拥塞窗口两个状态变量，接收窗口是接收端主机根据其目前的接收缓存大小所许诺的最新窗口值；拥塞窗口的大小表示当前网络的传输能力，由发送端设置。发送窗口取这两者中的较小值。攻击

者会利用发送端计算拥塞窗口的漏洞，通过缩小拥塞窗口缩小发送窗口。拥塞窗口的计算采用了所谓的慢启动（slow start）算法，其具体特征就是拥塞窗口在传输正常时成指数增大，增大到一定阈值后按线性增长，一旦出现数据包传输超时，则拥塞窗口变为最小值，阈值变为原来的一半。有经验的攻击者可以利用这种特性，周期性地制造网络关键节点的拥塞，不断触发拥塞窗口的慢启动过程，最终达到降低正常数据传输能力的目的。因为此类攻击的具体手段比较灵活，防御此类攻击的难度较大，需要网络管理人员实时监测网络的异常流量，避免攻击者制造网络关键节点的拥塞。

3.3.2　UDP

1．概述

相较于 TCP 提供的丰富功能，UDP 只在 IP 的数据包服务之上增加了少量功能，即端口功能和差错检测功能。虽然 UDP 用户数据包只能提供不可靠的交付，但 UDP 在某些方面有其特殊的优点：第一，发送数据之前不需要建立连接，因此减少了开销和发送数据之前的时延；第二，不使用拥塞控制，也不保证可靠交付，因此，主机不需要维持多参数的、复杂的连接状态表；第三，UDP 用户数据包只有 8 字节的头部开销；第四，由于没有拥塞控制，网络出现的拥塞不会使源主机的发送速率降低。这对某些实时应用是很重要的。

表 3-1 列出了常用的几种使用 UDP 进行传输的应用层协议及相应端口号。

表 3-1　常用的几种使用 UDP 进行传输的应用层协议及相应端口号

序号	应用名称	应用层协议	端口号
1	域名系统	DNS	53
2	简单文件传输协议	TFTP	69
3	网络时间协议	NTP	123
4	动态主机配置协议	DHCP	67、68
5	简单网络管理协议	SNMP	161、162
6	网络文件系统	NFS	2049

2．UDP 的安全问题及防护措施

DoS 攻击是一种最常见的 UDP 攻击，而 UDPFlood 攻击又是 DoS 攻击中最普遍的流量型攻击。其攻击原理：攻击源发送大量的 UDP 小包到攻击目标，目标可以是服务器或者网络设备（前提是攻击目标已经开放 UDP 端口），使其忙于处理和回应 UDP 报文，系统资源使用率飙高，最后导致该设备不能提供正常服务或者直接死机，严重的会造成全网瘫痪。可以说 UDP 攻击是一种消耗攻击目标资源，同时也消耗自己资源的攻击方式，技术含量较低。

使用 UDP 进行传输的应用层协议之间差异极大，因此，防御不同情况下的 UDP 攻击需要采取不同的防护措施：①如果攻击包是大包，则根据攻击包大小设定包碎片重组大小，通常不小于 1500 字节，极端情况下可以考虑丢弃所有 UDP 碎片；②当攻击端口为业务端口，根据该业务 UDP 最大包长设置 UDP 最大包以过滤异常流量；③当攻击端

口为非业务端口，通常通过设置 UDP 连接规则，要求所有去往该端口的 UDP 包，必须首先与 TCP 端口建立 TCP 连接，不过这种方法需要借助专业安全设备。

3.4 应用层协议

3.4.1 RIP

1．概述

RIP（Routing Information Protocol）是一种动态内部路由/网关协议，适用于简单的 IP 网络。该协议虽然解决的是网络互联的路由问题，但它是应用层协议。RIP 最早在 RFC 1058 中提出，RIPv2（RFC1723）是它的改进方案。RIPv2 新增了变长子网掩码的功能，支持无类域间路由、组播、认证功能，同时对 RIP 路由器具有后向兼容性。

RIP 采用距离矢量算法与相邻的路由器交换路由信息，它以“跳数”（即 metric）来衡量到达目的地的距离。路由器到直连网络的 metric 标记为 0，每经过一个路由器到达下一网络时 metric 增加 1。为限制收敛时间，RIP 规定一条有效路由信息的 metric 不能超过 15，这就使得该协议不能应用于大型的网络。

RIP 的工作原理如下：①路由器最初启动时只包含了其直连网络的路由信息，随后定期（30s）和相邻路由器交换路由信息（就是路由器当前的路由表），路由信息以 RIP 报文传送。②路由器根据接收到的 RIP 报文来更新路由表，具体方法是添加或更新自己的路由表项。③如果接收到与已有表项的目的地址相同的路由信息，则分为三种情况对待：第一种情况，已有表项的来源端口与新表项的来源端口相同，那么根据最新的路由信息更新其路由表；第二种情况，已有表项与新表项来源于不同的端口，那么比较它们的 metric 值，将 metric 值较小的一个作为自己的路由表项；第三种情况，新旧表项的 metric 值相等，通常的处理方法是保留旧的表项。④若接收到的目的网络不在自己的路由表中，则把该项目加到路由表中，并将其 metric 值加 1。经过一系列路由更新，网络中的每个路由器都具有一张完整的路由表，这个过程称为收敛。RIP 使用 UDP 的 520 端口发送和接收 RIP 报文。路由器每隔 30s 向其邻居路由器发送本地路由表。如果经过 180s 都没有接收到更新报文，那么将其标记为不可达，即 metric 值标记为 16。如果在其后的 120s 仍然没有收到更新信息，就将该路由从路由表中删除。

2．RIP 的安全问题及防护措施

RIPv1 有其固有的不安全因素，因为它没有使用认证机制，并通过不可靠的 UDP 进行传输。RIPv2 的分组格式中包含了一个选项，可以设置 16 个字符的明文加密字符串或者对 MD5 杂凑值的签名。虽然 RIP 报文很容易伪造，但 RIPv2 对 MD5 杂凑值的签名与认证使得欺骗的操作难度大大提高。攻击者可以伪造 RIP 路由更新信息，并向相邻路由器发送，伪造内容为目的网络地址、子网掩码地址与下一条地址，经过若干轮的路由更新，网络通信将面临瘫痪的风险。此外，攻击者会利用一些网络嗅探工具（如 tcpdump 和 rprobe 等）获得远程网络的 RIP 路由表，通过欺骗工具（如 srip）伪造 RIPv1 或 RIPv2

报文，再利用重定向工具（如 fragroute）截取、修改和重写向外发送的报文，以控制网络中的报文信息。

针对 RIP 的不安全因素，中小型网络通常采取以下两种防范措施：

（1）将路由器的某些接口配置为被动接口，配置为被动接口后，该接口停止向它所在的网络广播路由更新报文，但是允许它接收来自其他路由器的更新报文。

（2）配置路由器的访问控制列表，只允许某些源 IP 地址的路由更新报文进入列表。

目前，大多数企业网络使用的是采用 MD5 安全机制的 RIPv2，或者是引进了安全认证机制的 OSPF 协议来提高安全性。

3.4.2　HTTP

1．概述

超文本传输协议（Hyper Text Transfer Protocol，HTTP）是一种承载于 TCP 之上的应用层协议，能够从服务器传输超文本到本地浏览器，是互联网上应用最广泛的一种网络协议。HTTP 协议是一个客户端和服务器端之间请求和应答的标准，其具体过程是：首先由客户端发起一个请求，建立到服务器指定端口（默认是 80 端口）的连接，HTTP 服务器接收请求后，会向客户端返回一个状态，包括协议版本号、成功或错误的代码和返回内容等信息，客户端收到信息后通过浏览器显示内容，最后断开连接。

2．HTTP 的安全问题及防护措施

由于 HTTP 设计之初未考虑安全方面，数据直接通过明文进行传输，不提供任何方式的数据加密，因此存在较大的安全缺陷。

（1）攻击者可以通过网络嗅探工具轻易获得明文的传输数据，从而分析出特定的敏感信息，如用户的登录口令、手机号码和信用卡号码等重要资料。

（2）HTTP 是一种无状态的连接，在传输客户端请求和服务器响应时，唯一的完整性检验就是包头包含了数据传输长度，而未对传输内容进行消息完整性检测，攻击者可以轻易篡改传输数据，发动中间人攻击，因此 HTTP 不适合传输重要信息。

针对 HTTP 的这些安全问题，超文本传输安全协议（Hyper Text Transfer Protocol Secure，HTTPS）在 HTTP 和 TCP 之间增加了安全层以增强安全性。安全层主要通过安全套接层（Secure Sockets Layer，SSL）及其替代协议传输层安全协议（Transport Layer Security，TLS）实现。与 HTTP 不同，SSL 协议通过 443 端口进行传输，主要包含记录协议（SSL Record Protocol）和握手协议（SSL Handshake Protocol），记录协议确定了对传输层数据进行封装，具体实施加密解密、计算和校验等安全操作。握手协议使用 X.509 认证，用于验证传送数据，协商加密算法，并利用非对称加密算法进行身份认证和生成会话密钥等操作，从而对通信双方交换的数据加密，保证客户端与服务器应用之间的通信不被攻击者窃听。

HTTPS 通过增加安全层，可实现双向身份认证、生成会话密钥、传输数据加密、数据完整性验证和防止数据包重放攻击等安全功能，主要改进在于使用非对称加密算法在不可信的互联网上安全传输了用来对称加密的会话密钥，从而建立了安全信道，因此很

多银行和邮箱等安全级别较高的服务都使用 HTTPS。但由于 HTTPS 会额外增加握手过程并对数据进行加密，因此会在一定程度上降低网页加载速度。

由于 SSL 使用了非对称加密算法传输会话密钥，在大多数情况下，HTTPS 本身不会直接遭遇威胁，针对 HTTPS 的攻击方式主要发生在 SSL 连接尚未建立时的中间人攻击，利用 SSLstrip 工具可攻击从非安全连接到安全连接的通信，即从 HTTP 到 HTTPS 的过程中发起中间人攻击，模拟客户端向服务器提供证书，再从安全网站收到流量提供给客户端，进而窃取敏感信息。

多数 SSL 加密的网站都使用名为 OpenSSL 的开源软件包，2014 年 4 月曾爆发著名的心脏滴血（Heartbleed）漏洞，影响了全球绝大多数使用 HTTPS 的安全网站，目前该漏洞已被修补。

3.4.3 Telnet 协议

1．概述

远程登录（Telnet）协议是 TCP/IP 协议族中的一员，是 Internet 远程登录服务的标准协议。Telnet 协议可以让用户使用的本地计算机成为远程主机系统的一个终端。用户可以在本地终端上使用 Telnet 协议远程访问服务器并输入命令，命令会在服务器上执行，并将执行结果返回给用户。Telnet 协议侧重于访问远程主机所拥有的信息资源，如果希望在本地计算机与远程主机间传递文件，那么相较而言 FTP 会更加快捷有效。Telnet 协议默认采用 TCP 23 号端口。

2．Telnet 协议的安全问题及防护措施

Telnet 协议现今并不多用，许多服务器都禁止了 Telnet 服务。因为在注重安全性的现代网络环境中，我们不再假设通信网络与通信各方是可信任的，大多数 Telnet 会话都来自不可信的终端，这些终端与服务器之间的网络也是不可信任的。而工作在上述环境下的 Telnet 协议是一种明文传输协议，它明文传输用户的通信内容，包括用户名和密码。因此 Telnet 协议缺乏对数据保密性与完整性的保护，具体存在以下两类主要安全问题：

（1）攻击者可以通过嗅探器（Sniffer）监听 Telnet 会话，并记录用户名和口令组合甚至所有会话内容。事实上，近年来在许多主要 ISP 的主机上都发现存在嗅探器。这些嗅探器捕获 Internet 业务流的成功率相当高，它们记录 Telnet，FTP 和 rlogin 会话的前 128 个字符，这足以记录目标主机的地址、登录用户名和口令。

（2）除了监听 Telnet 会话等被动的攻击方式，攻击者还可以采取主动的攻击方式，比如从通信线路着手劫持 Telnet 会话并在认证完成后篡改或插入一些命令，或者在会话结束后仍然保持已建立的连接。事实上，已经有黑客掌握了使用 TCP 劫持工具的方法，他们能够在某种条件下劫持 TCP 会话。对黑客而言，Telnet 和 rlogin 会话是极具吸引力的目标。在 Telnet 会话遇到上述的主动攻击时，即使用户没有采用传统的静态口令，而是采用一次性口令（One-Time Password，OTP）或称动态口令的机制（它采用密码学中的 HMAC 算法构造的动态口令，这部分内容将在第 10 章中详细讨论）认证登录，也只能避免泄露用户名与静态口令的组合，而不能避免会话被劫持。

对 Telnet 会话进行加密是解决上述安全问题的可行方案。但是，如果通信双方互不信任，单钥加密（在第 7 章中会详细介绍）则有害无益，因为通信一方必须将密钥提供给不可信的另一方，这样会泄露该密钥。目前存在多种 Telnet 的加密解决方案，比如 stel，SSLtelnet，stelnet 和 SSH。虽然已经出现了对 Telnet 加密的标准化版本，但是尚不清楚有多少用户使用它。而 SSH 已经成为远程登录事实上的标准协议。

3.4.4　SSH 协议

1．概述

安全壳（Secure Shell，SSH）协议是一种在不安全的网络上建立安全的远程登录或其他安全网络服务的协议，由 IETF 的网络工作小组（Network Working Group）所制定。SSH 是建立在应用层和传输层基础上的安全协议。SSH 设计的初衷是为了取代原 UNIX 系统上的 rcp、rlogin 和 rsh 等不安全的指令程序，现在被用来取代 Telnet 实现安全的远程登录，并可以为 POP、FTP 甚至 PPP 等网络应用程序提供一个安全的“隧道”。SSH 提供多种身份认证和数据加密机制，并采用“挑战/响应”机制替代传统的主机名和口令认证。SSH 对所有传输的数据使用 RSA 公钥加密算法进行处理，避免了如 Telnet 等传统的网络服务程序明文传输口令和数据带来的信息泄露隐患，同时能够有效防止“中间人攻击”（Man-in-the-middle Attack）、DNS 欺骗和 IP 欺骗。SSH 协议默认采用 TCP22 端口。

SSH 的通信流程主要分为 6 步：建立 TCP 连接、版本协商、算法协商、密钥建立和服务器认证、用户认证、通信会话。

2．SSH 协议的安全问题及防护措施

SSH 协议主要由 3 层协议组成：传输层协议、用户认证协议和连接协议，其中高层协议要运行在底层协议的基础上，因此远程登录过程的安全性是由 3 个安全协议共同保证的。SSH 协议虽然目前来讲较为可靠，专为远程登录会话和其他网络服务提供安全性的协议，但仍有一些安全性问题需要关注，并会面临多种网络攻击。

（1）服务器认证。SSH 协议主要面向互联网网络中主机之间的互访与信息交换，拥有一套以主机密钥为基础的完备的密钥机制。然而在某些安全性不高的网络环境中，没有可信的认证机构对服务器的真实性进行验证；同时为了客户端使用方便，SSH 协议提供了一个可选功能，即在客户机第一次连接到服务器时，可以不对服务器的主机密钥进行验证。这一功能会产生一些安全问题，虽然此时客户端与服务器之间的通信仍然是加密的，第三方不可能获得双方通信的内容，但攻击者可能假冒成真正的服务器，从而使得整个系统的安全都受到威胁。因此，在系统中，应尽量避免把该功能设为默认配置，即必须尽可能检验主机密钥，使用验证服务器正确性的方法，例如要求传送 SHA-1 哈希算法生成的主机公钥的 MAC 值等。

（2）协议版本协商。SSH 协议运行的第一步是进行服务器与客户端协议版本的协商。服务器会打开端口 22 与客户端建立 TCP 连接，之后发送的包含协议版本号的 TCP 报文至客户端，客户端接收报文并解析，之后返回服务器一个包含协议版本号的报文。如果双方的版本号不同，由服务器决定是否可以运行；如果可以，则双方都以较低的版本运

行。如果攻击者采用有安全漏洞的版本建立连接，协商的结果是采用有安全漏洞的 SSH 协议版本，则可能会采取进一步的攻击。所以在 SSH 协议软件的配置中需考虑版本问题，对于采用的软件版本有安全问题的通信方，可以采用中断 TCP 连接的办法。SSH 是 Client /Server 结构，并且有两个不兼容的版本，分别是 1.x 和 2.x，其中 1.x 存在许多安全问题，已很少使用。

（3）主机密钥文件安全。SSH 协议在工作时，服务器的主机密钥存储在一个 root 用户可读的主机密钥文件中，如果该文件被窃取或篡改，则会对协议的认证机制造成严重威胁。攻击者可以利用有效的主机密钥实施一系列攻击，如假冒攻击、重放攻击和中间人攻击等。因此，主机密钥文件必须用非常安全的机制进行管理。

OpenSSH 是 SSH 的替代软件，其源代码是开放的，而且是免费的，且同时支持 SSH 1.x 和 2.x，预计将来会有越来越多的人使用 OpenSSH。现在已经有各种基于 Windows 的 SSH 版本，这些版本的功能和价格各不相同。PuTTY 是一个不错的免费自由软件，该软件不需要安装就可以运行。

3.4.5 DNS 协议

1．概述

域名系统（Domain Name System，DNS）是一个分布式数据库系统，用以实现域名到 IP 地址或 IP 地址到域名的映射。在 Internet 上，域名与 IP 地址之间是一一对应的。域名虽然便于人们记忆，但计算机之间只能通过 IP 地址互相识别，它们之间的转换过程称为域名解析，域名解析需要由专门的域名解析服务器自动完成。域名解析服务器也称作 DNS 服务器，DNS 服务使用的是 53 号端口。

2．DNS 协议的安全问题及防护措施

从安全角度看，DNS 存在一定的问题。在正常工作模式下，备份服务器可使用“区转移”获得域名空间中所属信息的完整备份，黑客也常使用这种方式快速获得攻击目标列表。如果将前向命名和后向命名分离，则可能带来安全问题，黑客若能够掌控部分反向映射树，就能实施欺骗，也就是说，反向记录中可能含有可信赖的那台计算机的名称（伪造）。针对 DNS 的攻击还有破坏力更强的变种，攻击者在发起呼叫之前，会扰乱目标计算机中 DNS 响应的高速缓存，当目标计算机进行交叉检验时，验证结果似乎是成功的，但此时黑客却已经获得了访问权。另外，黑客采用呼叫响应的方法淹没目标的 DNS 服务器，使其陷入混乱，此类攻击案例十分常见，黑客只需用非常简单的程序就可以摧毁 DNS 的高速缓存。

虽然我们无法阻止黑客对 DNS 服务器的攻击，但是可以通过采取相应的措施加以控制，如可以限制授权的第二级服务器使用“区转移”功能。DNSSEC 是 DNS 的安全扩展（Domain Name System Security Extensions），由 IETF 提供的一系列 DNS 安全认证机制组成，它可以对 DNS 记录进行数字签名，是消除欺骗性 DNS 记录的最简便的方法。当某个区的所有者有不良动机时，DNSSEC 就会签署一个欺骗性的记录，进而可以有效防止此类欺骗。此外，对域的签名可以离线进行，从而降低了域签名私钥泄露的风险。虽然

DNSSEC 应对以上欺骗攻击很有效，但也有一些不足之处，所以迄今它还没有成为主流的 DNS 查询方式。

3.4.6　SMTP

1．概述

E-mail 是 Internet 上使用最广泛的服务之一。尽管网络上有多种邮件收发服务，但最常用的就是简单邮件传输协议（Simple Mail Transfer Protocol，SMTP）。SMTP 属于 TCP/IP 协议族，SMTP 服务使用的是 25 号端口。

传统 SMTP 使用简单的协议传输 7b ASCII 文本字符，SMTP 会话样本日志记录如图 3-4 所示，箭头表明数据的流向。它还有一种扩展形式，称为 ESMTP，允许扩展协商，包括 8b 的传输。这样，它就不仅能够传输二进制的数据，还可以传输非 ASCII 字符集。从图 3-4 中可以看出：远程站点 sales.mymegacorp.com 向本地主机 fg.net 发送了一封电子邮件。这是一个简单协议，其命令可以手动输入网络管理员和黑客都知道如何使用。

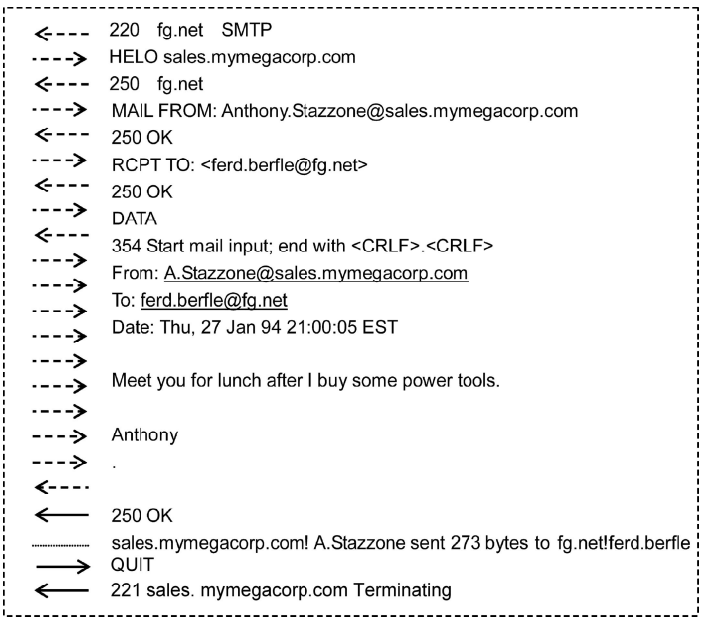

图 3-4　SMTP 会话样本日志记录

注意： 主叫方在 MAIL FROM 命令中指定了一个返回地址。在这种情况下，本地主机没有可靠的办法验证该返回地址的正确性，更无从知晓是谁用 SMTP 给你发送了邮件。如果需要更高的可信度或保密性，就必须使用更高级的安全机制。

一个组织机构至少需要一个邮件服务器。内部网络用户的邮件服务器通常设置在网关上。这样，内部管理员只须从网关上的邮件服务器收取其邮件。此网关能够保证发出的邮件头部符合标准。如果本地的邮件服务器出现故障，管理员可以方便、及时地排除故障。

通过邮件服务器，公司内部的每个人都可以有一个独立的邮箱。但是这些邮件账户

列表必须严加保护，以防被人窃取而成为黑客攻击的目标。

2．SMTP 的安全问题及防护措施

从安全角度看，基本的 SMTP 自身是完全无害的，但是它可能成为拒绝服务攻击的发源地。攻击者可以采用拒绝服务攻击阻止用户合法使用该邮件服务器。假设攻击者能控制 50 台计算机，每台计算机都向邮件服务器发送 1000 个 1MB 大小的邮件，恐怕邮件服务器将很难处理数量如此之多的邮件。

邮件的别名有时也会给黑客提供一些有用的信息。如以下命令：

```
VRFY <postmaster>

VRFY <root>
```

通常可以把邮件别名翻译成实际的登录名称。它可能提供一些关于谁是系统管理员、攻击成功后哪个账户最有价值等线索。这些信息是否敏感，完全取决于安全策略。

EXPN 子命令扩展了邮件列表的别名。这个命令存在很大的风险，可能破坏机密性。要避免这种风险，一种有用的做法是将暴露的邮件服务器主机的别名指向一台内部的计算机，这台计算机从外部不可达，从而消除这种扩展所带来的风险。

不管运行何种邮件服务程序，应该将其配置成仅接收内部网络中的邮件，或仅接收发给你的用户的邮件。所谓的“开放中继”（Open Relay）就是允许在任何人之间进行邮件传递，这是非常危险的。许多网站都拒绝接收那些来自已知“开放中继”的电子邮件。

SMTP 攻击者（spammer）寻找 SMTP 服务器是为了传递他们的 spam（垃圾邮件）。他们需要连接到高带宽的邮件服务器上，将简单的信息传递到不同的地址。SMTP 服务（尤其是 Sendmail）是入侵系统的最常用方法之一，因为它们必须完整地暴露于 Internet，且邮件的路由是复杂的（暴露+复杂=弱点）。

如果想支持移动用户，可以使用 SMTP 认证，且最好与加密 SMTP 会话结合使用。SMTP 认证的主要目的是要避免“开放中继”的存在。因为“开放中继”会吸引 spammer，并导致在网站上添加一条 reject all mail from this clowns 信息。这种 SMTP 的用法有时被称为“邮件托付”（Mail Submission），以区别于更通用的邮件传输。

3.4.7　MIME 协议

1．概述

多用途网际邮件扩充协议（Multipurpose Internet E-mail Extension，MIME）最早于 1992 年应用于电子邮件系统，后来也应用于浏览器。服务器通过说明发送的多媒体数据的 MIME 类型，通知浏览器该多媒体数据的类型，从而让浏览器知晓接收到的哪些信息是 MP3 文件，哪些是 Shockwave 文件等。

2．MIME 协议的安全问题及防护措施

当 MIME 应用于浏览器时，浏览器接收文件后，会进入插件系统进行查找，查出哪种插件可以识别并打开接收的文件。如果浏览器不确定调用哪种插件，它可能会通知用户缺少某插件，或者直接选择现有的某个插件尝试打开接收的文件。传输的信息中缺少

MIME 标识可能导致的情况很难估计，因为某些计算机系统可能不会出现故障，但某些计算机系统可能会因此崩溃。

当 MIME 应用于电子邮件系统时，即使不考虑邮件客户端软件的缺陷，自动运行 MIME 编码消息就潜藏着巨大的风险，因为这些消息中被编码的结构信息能够指示客户端软件要采取何种行动。

对于 MIME，还有一种分段攻击。有一种 MIME 类型允许将单个电子邮件消息分成几段。如果消息分段巧妙，就可以逃避基于网关的病毒检测。当然，如果邮件客户端软件不能重组这些分段的消息，这种攻击也是无效的，然而微软的 Outlook Express 确实可以重组这些分段的消息。应对分段攻击有两种方法，一是在网关上重组这些消息，二是拒绝那些分段发来的邮件。

MIME 存在的其他风险包括邮寄可执行程序和含有危险操作的 PostScript 文件。通过电子邮件发送可执行程序是传播蠕虫和病毒的主要根源。当然，攻击者也可能通过电子邮件发送一条含有伪造的“From:”命令行的 MIME 消息。许多流行的蠕虫和病毒就是采用这种方式传播的。

上述这些问题和其他一些安全问题在 MIME 技术文档中已有详细说明。但是，很多基于 Windows 系统的邮件服务器几乎都忽视了这些建议。

3.4.8　POP3

1．概述

邮局协议（Post Office Protocol，POP）是一个邮件接收协议，它的第 3 个版本称为 POP3。它规定了如何将个人计算机连接到遵循 POP3 的接收邮件服务器并下载电子邮件，是 Internet 电子邮件的第一个离线协议标准。其具体过程是：电子邮件发送到邮件服务器，客户机通过邮件客户端软件连接服务器，并下载所有未阅读的电子邮件，同时删除保存在邮件服务器上的邮件（目前很多 POP3 服务器在邮件被下载后，并不删除邮件）。当客户机长时间保持在线时，邮件客户端软件会每隔一定的时间就收取一次新邮件。POP3 服务允许用户设置本地浏览器的接收/发送邮件服务器名称，客户机采用 POP3 和 SMTP，用同一个或不同的邮件服务器来收发电子邮件。在 TCP/IP 中，POP3 服务采用的 TCP 端口号为 110。

2．POP3 的安全问题及防护措施

POP3 非常简单，邮件服务器通过 Perl 脚本程序可轻而易举地实现。正是因为简单，所以它也不安全。在使用 USER/PASS 组合的旧版本中，用户在访问邮箱时采用的口令是以明文传输的，攻击者很容易窃取到用户名和口令，从而获取用户邮箱中的所有邮件。最近开发的邮件客户端软件采用 APOP 命令接收邮件，可以安全地传输用户口令。APOP 基于口令认证中常用的“挑战/响应”机制，对用户名和口令进行加密。但 APOP 对邮件内容不作保护，即使得不到用户名和口令，攻击者也很容易窃取到以明文形式传输的邮件内容。以上两种协议均将口令以明文形式存储在服务器上，一旦服务器遭到攻击，则可能造成用户名和口令的泄露。此外，攻击者也可能对认证交换的口令发起字典攻击。

为保障邮件安全传输，可以利用 SSL/TLS 协议对传输的数据进行加密。目前，很多站点支持基于 SSL/TLS 的 POP3 服务，而有些客户端不支持这一服务。

如果邮件服务器运行的是 UNIX 操作系统，那么 POP3 服务器软件在认证结束前通常以 root 用户权限运行，用户必须在服务器上开设一个账号。其实这很不利：一方面它增加了邮件服务器的管理难度，另一方面意味着用户可以登录到邮件服务器上。这种设计思想非常危险，因为用户可能给服务器带来非常大的安全风险。尽管如此，仍然可以使用 POP3 服务器收发邮件，但要保证 POP3 服务器仅对其用户数据库和电子邮件进行维护。

3.4.9 IMAP4

1．概述

Internet 消息访问协议（Internet Message Access Protocol，IMAP）是由美国斯坦福大学的 Mark Crispin 教授研发的一种邮件接收协议。它的主要作用是邮件客户端（如 MS Outlook Express）可以通过这种协议从邮件服务器上接收邮件的信息并下载邮件。正如 POP3 是 POP 的第 3 个版本一样，IMAP4 是 IMAP 的第 4 个版本，它提供了同 POP3 一样方便的邮件下载服务，而且在对邮箱的访问控制功能上比 POP3 更加强大。IMAP4 运行在 TCP/IP 之上，使用的端口号是 143。

IMAP4 同样提供了方便的邮件下载服务，让用户能进行离线阅读，但 IMAP4 还有其他一些功能。首先，IMAP4 提供的摘要浏览功能可让用户在阅读完所有邮件的到达时间、主题、发件人、大小等信息后才做出是否下载的决定；其次，用户还可以享受选择性下载附件服务。例如一封邮件里含有 5 个附件，用户可以选择下载其中的两个附件；最后，在支持离线阅读的同时，IMAP4 既允许用户把邮件存储在服务器上，也允许用户把邮箱作为信息存储工具。

IMAP4 适用于 C/S 构架中，IMAP4 是对提供邮件访问服务且使用广泛的 POP3 的另一种选择，基本上两者都是规定个人计算机如何连接到互联网上的邮件服务器进行收发邮件。IMAP4 支持对服务器上的邮件进行扩展性操作，IMAP4 也支持 ASCII 码明文传输密码。

与 POP3 不同的是，IMAP4 支持以离线和在线两种模式传输数据：①离线方式指客户端程序会不间断地连接服务器下载未阅读过的邮件到本地磁盘，当客户端需要接收或者发送邮件时才会与服务器建立连接，这就是离线访问模式。POP3 典型地以离线方式工作。②在线模式中，一直都是由客户端程序来操作服务器上的邮件，不需要像离线模式那样把邮件下载到本地才能阅读（即使用户把邮件下载到本地，服务器上也会保存一份副本，而不会像 POP 那样把邮件删除）。用户可以通过客户端程序或者 Web 在线浏览邮件。一些 POP3 服务器也提供了在线功能，但是，它们没有达到 IMAP4 的浏览功能的级别。

IMAP4 是分布式存储邮件方式，以后再连接时，本地磁盘上的邮件状态和服务器上的邮件状态，可能与现在不一样。此时，IMAP4 的分布式存储机制解决了这个问题。IMAP4 邮件的客户端软件能够记录用户在本地的操作，当连上网络后会把这些操作传送给服务器。当用户离线的时候服务器端发生的事件，服务器也会告诉客户端软件，比如有新邮

件到达等，以保持服务器和客户端的同步。

IMAP4 处理线程都处于 4 种处理状态的其中一种。大部分的 IMAP4 命令都只会在某种处理状态下才有效。如果 IMAP4 客户端软件企图在不恰当的状态下发送命令，则服务器将返回协议错误的失败信息，如 BAD 或 NO 等。

总的来说，IMAP4 同时兼顾 POP3 和 WebMail 的优点，是一种较好的通信协议。目前，支持 IMAP4 的免费邮件系统并不多，较常见的有 777 免费电子邮箱（http://mail.777.net.cn）等。

IMAP4 使用户可以对服务器上的邮箱进行远程访问。它可以使客户机和服务器的状态同步，并支持多重文件夹。如同 POP3 一样，邮件仍然通过 SMTP 发送。

典型的 UNIX IMAP4 服务器提供了与 POP3 服务器相同的访问方式，同时还增加了许多功能。虽然 POP3 服务器已能满足用户的需求，但是 IMAP4 服务器的应用也很有潜力。

2．IMAP4 的安全问题及防护措施

IMAP4 能够支持一些认证方法，并且有些方法非常安全。前面提到的“挑战/响应”机制很有用，但是它并没有达到人们预期的安全性。在“挑战/响应”机制中使用了一个共享的秘密，这个秘密信息必须存储在服务器上。如果将该秘密与域字符串进行杂凑运算，这对消除口令的等值性可能会更有利。

对于 IMAP4 来说，最大的代价是协议的复杂度太高，它当然也需要一个更复杂的服务器。如果该服务器能够采用小而简单的认证模块恰当地实现，认证的安全性将会得到保障。但是，这需要对服务器的设计进行验证。

3.4.10　PGP

1．概述

PGP（Pretty Good Privacy）协议是常用的安全电子邮件标准之一。1991 年，Phil Zimmermann 提出 PGP，可用于文本、E-mail、文件或整个磁盘分区的签署或加密，也可用于提高 E-mail 通信的安全性。PGP 安全体制包括 5 种服务：认证、保密、压缩、电子邮件兼容性和分段，详细描述见表 3-2。

表 3-2　PGP 服务概述

功　能	使 用 算 法	描　述
数字签名	DSS/SHA 或 RSA/SHA	消息的 Hash 码利用 SHA-1 产生，将此消息摘要和消息一起用发送方的私钥按 DSS 或 RSA 加密
消息加密	CAST 或 IDEA，或使用 3DES 或 RSA	将消息用发送方生成的一次性会话密钥按 CAST-128 或 IDEA 或 3DES 加密。用接收方公钥按 Diffie-Hellman 或 RSA 算法加密会话密钥，并与消息一起加密
压缩	ZIP	消息在传送或存储时可用 ZIP 压缩
电子邮件兼容性	基数 64 转换	为了对电子邮件应用提供透明性，一个加密消息可以用基数 64 转换为 ASCII 串
分段	—	为了符合最大消息尺寸限制，PGP 执行分段和重新组装