TCP/IP 协议栈安全

TCP/IP协议工作原理 P11

纵向横向传递 P11-19

局域网中的client远程访问Server时，在数据传递处理的每一步，都有可能产生安全问题：DNS劫持，ARP污染，嗅探监听，地址伪造、路由劫持，TCP连接劫持、DoS攻击。

链路层安全 P19

链路层功能 P20

功能主要有：将数据组合成帧；控制帧在物理信道上的传输，包括处理传输差错，调节发送速率；提供数据链路通路的建立、维持和释放的管理。

ARP欺骗与污染 P21~29

ARP欺骗（ARP spoofing），又称ARP污染（ARP poisoning），是针对以太网地址解析协议（ARP）的一种攻击技术；可让攻击者成为中间人（Man-in-the-Middle, MITM），获取局域网上的数据包，甚至可篡改数据包，同时迫使受害主机无法正常接收报文。

安全问题：在ARP回复时，主机A并不会验证ARP回复包的真实性。由此引出一个局域网攻击方式

ARP欺骗：恶意主机C，企图冒充B，欺骗A

网络监听与嗅探 P30

网络嗅探（Sniffers）是一种网络流量数据分析的手段，常见于网络安全攻防技术使用，也有用于业务分析领域。嗅探所使用的工具称为“嗅探工具”，也称为“数据包分析器”，还有别称为“嗅探器”、“抓包工具”等。常见的开源嗅探工具包括TCPDUMP，WIRESHARK等。

网络嗅探具有**两面性**：

- 网络管理员使用嗅探器，通过捕获分析网络流量，进行高效的网络管理
- 恶意攻击者使用嗅探器，攫取网络中的大量敏感信息，进行网络攻击

恶意的网络嗅探，取决于攻击者的位置和攻击能力：

- 共享网络传输链路场景下，攻击者的恶意嗅探监听
- 攻击者控守了网络设备，对流经的流量进行拦截嗅探

防御方法：

洋葱路由：洋葱路由网络的主要目的是保护用户的隐私和匿名性，使得在网络上进行监听和嗅探变得更加困难。通过在多个洋葱路由器之间进行多重加密的数据转发，洋葱路由网络可以有效地防止攻击者通过监听和嗅探获取用户的信息和通信内容。即使攻击者能够捕获到数据包，由于数据的多重加密，攻击者难以解密数据内容或者追踪数据包的发送者和接收者。

网络层安全 P35

网络层功能：分组与分组交换，路由，网络互联，网络连接复用，差错检测与恢复，服务选择，网络管理，分片与重组

源地址假冒攻击 P38

互联网在设计之初，对分组的源IP地址并不进行合法性验证，因此恶意的攻击者很容易篡改或伪造分组的源IP地址。网络层的源IP地址假冒攻击（IP spoofing），是最常见的一种针对IP协议的攻击。通常，IP spoofing也是进行复杂网络攻击，如会话劫持，DNS污染、TCP劫持等攻击，的能力基础和先决条件。攻击者在发送数据包时伪造源IP地址，从而隐藏其真实身份或者导致网络流量被错误地发送到其他目标。随着真实地址、真实身份等技术标准的出现，这一问题得到了缓解，但要彻底解决这一攻击威胁，仍需持续的技术推动和投入。

IP 分片攻击 P46

当互联网上的两台远程主机进行数据传输时，如果传输路径上的各跳间，存在不同的链路**最大传输单元**（Maximum Transmission Unit, **MTU**），那么可能会发生IP分组分片（IP fragmentation），以满足链路MTU的要求。

P46 ~ 48 分片攻击原理

IP分组的这种先分片、再重组的机制，为攻击者暴露出了IP层的一个攻击面。分组的碎片化发生在**源主机或中间路由器**上，而重组往往都在目的接收端发生。根据不同的攻击效果，IP分片攻击可以分为3种：

1. 拒绝服务攻击 P49~51：攻击者发送大量的IP分片，使得目标主机在重组分片时耗尽资源，从而导致拒绝服务
2. 污染攻击 P52~61：一种更高级的攻击方式，原始报文被分片、传输过程中，攻击者伪造一些分片，注入到正常分片流中，篡改原始报文内容
3. 安全策略逃逸 P62~64：通常网络防火墙会对IP分片进行重组，然后审查其中的恶意载荷。但防火墙和接收端主机往往存在重组策略不一致现象，即当分片出现重叠时，二者可能会采用不同的覆盖策略。因此，攻击者可以通过设置合理的分片偏移，逃逸防火墙的审查，但形成对接收端的破坏。

为了避免IP分片，一些相关技术标准也陆续被提出。例如，路径MTU发现（Path MTU Discovery，PMTUD）机制，该机制用于确定两台IP主机间的路径MTU。TCP协议有MSS选项，可以通过调整MSS、适合路径MTU，从而避免分片。

针对 UDP 的 IP 分片 P72

UDP是面向事务的，与IP层是松耦合的，UDP报文的大小直接由应用给定，因此UDP不能依据路径MTU大小、对传输层报文进行适应性调整，即针对UDP报文的IP分片很难避免。新的RFC标准提出，应用层和UDP协议合作、发现路径MTU，从而避免IP分片，但这些新标准和机制的实际部署，仍需很长时间。

安全防御一：IPSec协议 P80

IPSec (Internet Protocol Security，RFC4301)，即Internet协议安全性，是一种开放标准的框架结构，通过对IP协议的分组进行加密和认证，来保护基于IP协议的网络传输。在 IPv4 中， IPSec 的使用是一个可选项，在 IPv6 （RFC 6434 ）中，初始设为必选项，未来随着 IPv6 的进一步流行，IPSec 可以得到更为广泛的使用。

IPSec协议工作在TCP/IP协议的第三层，使其在单独使用时适于保护基于IP协议的所有上层协议。

认证机制 AH P76

提供数据源认证、数据完整性校验和防报文重放功能，它能保护通信免受篡改，但不能防止窃听，适合用于传输非机密数据。AH 的工作原理是在每一个数据包上添加一个身份验证报文头，此报文头插在标准IP包头后面，对数据提供完整性保护。可选择的认证算法有MD5（Message Digest）、SHA-1（Secure Hash Algorithm）等。

加密机制 ESP P77

提供加密、数据源认证、数据完整性校验和防报文重放功能。ESP的工作原理是在每一个数据包的标准IP包头后面添加一个ESP报文头，并在数据包后面追加一个ESP尾。与AH协议不同的是，ESP将需要保护的用户数据进行加密后再封装到IP包中，以保证数据的机密性。常见的加密算法有DES、3DES、AES等。同时，作为可选项，用户可以选择MD5、SHA-1算法保证报文的完整性和真实性。

在实际进行IP通信时，可以根据实际安全需求同时使用这两种协议或选择使用其中的一种。同时使用AH和ESP时，设备支持的AH和ESP联合使用的方式为：先对报文进行ESP封装，再对报文进行AH封装。封装之后的报文从内到外依次是原始IP报文、ESP头、AH头和外部IP头 。

IPSec 的两种工作模式 P79~80

- 传输模式：只是传输层数据被用来计算AH或ESP头，AH或ESP头以及ESP加密的用户数据被放置在原IP包头后面。主要用于主机和主机之间，端到端通信的数据保护。封装方式：不改变原有的IP包头，在原数据包头后面插入IPSec包头，只封装数据部分。
- 隧道模式：用户的整个IP数据包被用来计算AH或ESP头，AH或ESP头以及ESP加密的用户数据被封装在一个新的IP数据包中。主要用于私网与私网之间，通过公网进行通信，建立安全VPN通道。封装方式：增加新的IP（外网IP）头，其后是IPSec包头，之后再将原来的整个数据包封装。

网络入侵检测系统 IDS P81

入侵检测系统（Intrusion Detection System, IDS）是一种网络安全设备或应用软件，可以监控网络数据传输（NIDS），或者主机系统行为（HIDS），检查是否有可疑活动或者违反预定义的安全策略。从主要技术途径上区分，主要分为两类：

基于特征匹配的 IDS P83

基于专家知识或经验，预定义攻击行为特征或规则，然后对网络流量或主机行为进行匹配，如果匹配成功，则判定为攻击事件。优点：误报率低，检测速度快。缺点：无法识别未知攻击，存在漏报。

基于异常检测的 IDS P94

首先通过学习建模的方法，构建网络或主机的正常行为基线。然后结合当前网络或主机态势进行判断，如果网络或主机的行为偏离该基线，则判断发生了入侵或攻击，进行告警。优点：可以识别未知攻击。缺点：存在误报，检测速度慢。

路由协议安全 P86

路由（routing）是通过互联的网络，把信息从源地址传输到目的地址的活动。路由发生在TCP/IP协议的第三层即网络层。路由引导分组转送，经过一些中间的节点后，到它们最后的目的地。Internet被划分为多个**自治系统**（AS），每个自治系统可以制定自己的路由策略。自治系统内部的路由器通过**域内路由协议**彼此交换路由信息；自治系统边界路由器通过**域间路由协议**交换路由信息。

域间路由安全 P88

AS （恶意攻击者）宣告一个其实际上并不控制的IP地址前缀，进行虚假路由宣告。如果虚假路由宣告未被有效过滤，就有可能发生路由劫持攻击。

BGP 劫持成功，恶意攻击者的宣告必须满足以下条件：宣告比以前其他 AS 更具体的 IP 地址范围；提供一条通往目标IP 地址块的较短路径。需要注意的是，要发生 BGP 劫持，通常需要 AS 的运营商权限。目前，针对BGP协议暴露出的安全问题，已有相关的安全标准被提出，但这些标准技术的实际部署，还需要很长一段时间。

域内路由安全 P92

OSPF协议是目前使用最广泛的域内路由协议，因此针对域内路由的威胁攻击，也主要是针对OSPF协议展开。

OSPF攻击基本原理：攻击者通常假装成合法的域内路由器，伪造多个OSPF协议的LSA报文广播出去，迷惑其他路由器路由表的计算。

- P93：Fight-back安全机制：现有关于OSPF协议的威胁破坏，其核心就是如何在伪造LSA的时候，避免触发源合法路由器的fight-back机制。
- P94~96：PPeriodic injection 攻击
- P97~98：Disguised LSA 攻击

目前，随着OSPF协议的不断改进，之前的安全漏洞大多已被修补，其安全性也已大为改善。

传输层安全 P100

传输层主要负责提供不同主机应用程序进程之间的端到端的服务。传输层的基本功能如下：分割与重组数据，按端口号寻址，连接管理，差错控制和流量控制、纠错的功能。

拒绝服务攻击 P101

指任何对服务的干涉，使得其可用性降低或者失去可用性。例如一个计算机系统崩溃，或其带宽耗尽，或其硬盘被填满，导致其不能提供正常的服务，就构成拒绝服务。

最常见的DoS攻击有**计算机网络带宽攻击**和**连通性攻击**：带宽攻击指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽；连通性攻击指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽。

SYN Flooding P103~105

针对TCP协议主要的DoS攻击方式之一，通过发送大量伪造的TCP连接请求，使被攻击方资源耗尽，CPU满负荷或内存不足，一般发生在TCP协议中的三次握手（Three-way Handshake）阶段。

TCP 劫持攻击 P106

相比较针对TCP的DoS攻击，针对TCP的劫持攻击是一种更高级、更隐蔽、危害也更大的攻击方式。TCP劫持攻击是指，一个TCP连接外的的非法攻击者（即Client和Server之外的一个Attacker），将自己伪造的TCP报文，注入到TCP连接双方的合法数据流中，进而对连接进行攻击破坏。

包括：1. 伪造控制报文、如RST报文等，恶意阻断该连接；2. 伪造数据报文，污染数据流。

TCP 劫持原理 P107~114

1. 三种攻击攻击模式 P109~110
2. 基于challenge ACK侧信道漏洞的TCP连接劫持 P111~112
3. 基于IPID侧信道漏洞的TCP连接劫持 P113

TLS协议 P115~119

传输层安全性协议（Transport Layer Security, TLS）及其前身安全套接层协议（Secure Sockets Layer, SSL）是一种广泛采用的安全性协议，旨在促进 Internet 上通信的隐私和数据安全性。

TLS 应用 P120

TLS 协议通常在TCP等传输层协议之上运行，提供以下三个安全功能：

加密：阻止第三方对传输数据的窃听

身份验证：确保交换信息的各方是他们声称的身份

完整性：验证数据是否伪造而来或未遭篡改过

广泛应用：TLS是目前采用最广泛的一种安全性协议，应用于多个网络场景，如：对Web 应用程序和服务器之间的通信进行加密保护，还可用于电子邮件、消息传递和 IP 语音（VoIP）加密等。

网络安全共性分析 P122

通过梳理分析上述针对网络协议栈的攻击，可以发现这些攻击基本都具备2个共性特征：1. 攻击者可以进行身份欺骗，伪装成网络通信的一端；2. 攻击者可以进行推理猜测，成功构造出可被通信对端接受的数据报文。

两个共性特征映射到实际的网络系统中，本质上是利用了当前协议栈中的两个基础安全缺陷：

1. P124：一是网络地址缺乏足够的真实性验证，可以被恶意伪造；
2. P125：二是网络系统在实现和部署过程中，随机化程度不高，致使网络的状态信息可被恶意攻击者预测推理。

协议栈安全的基本防御原理 P126

1. **基于真实源地址的网络安全防御**：网络地址验证，约束主机只能使用预分配给自己的IP地址发送数据，进行网络通信
2. **增强协议栈随机化属性**：另一方面也可以通过增强网络协议栈的随机化属性，提升攻击者猜测、推理出目标网络状态信息的难度。代表性的包括**移动目标防御**（Moving Target Defense，MTD），**拟态防御**等。