

internet协议的安全性

◆ 为什么叫“第三层”隧道协议？

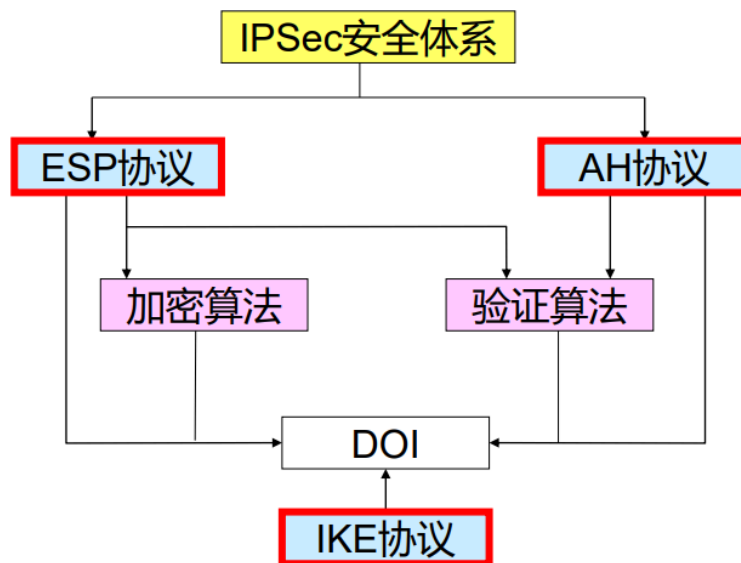
因为它封装的是 IP 数据包（即网络层数据），然后再通过另一个 IP 网络进行传输。相比之下：

- 第二层隧道协议（L2TP、PPPoE）封装的是 以太网帧。
- 第三层隧道协议（GRE、IPsec、VXLAN、MPLS）封装的是 IP 数据包。

IPSec

是一种端到端的确保ip层通信安全的机制。ipsec不是一个单独的协议，而是一组协议，ipsec协议的定义文件包括了12个RFC文件和几十个internet草案，已经成为工业标准的网络安全协议。ipsec在ipv6中是必须支持的，在ipv4中是可选的

IPSec体系结构图



- AH协议（Authentication Header 验证头）：可以进行数据源身份验证、保障数据的完整性以及防止相同数据包在因特网重放
- ESP协议（封装安全载荷）：具有所有AH功能，还可以利用加密技术保障数据机密性

虽然二者都可以提供身份认证，但是有两点区别

- ESP要求使用高强度的加密算法，会受到许多限制
- 多数情况下使用AH的认证服务已经能满足需求，相对来说ESP开销大

有两套不同的安全协议意味着可以对ipsec网络进行更细粒度的控制，选择方案灵活性更大

- AH和ESP可以单独使用也可以组合使用，可以在两台主机，两台安全网关，或者主机和安全网关之间使用

IKE (Internet key exchange)

- IKE 负责密钥管理，定义了通信实体间进行身份认证，协商加密算法以及生成共享的会话密钥的方法
- IKE把密钥协商结果保留在安全联盟中SA，供AH和ESP以后通信时使用

DOI (解释域)

- 解释域定义IKE所没有定义的协商的内容
- DOI为使用IKE进行协商SA的协议统一分配标识符。共享一个 DOI的协议从一个共同的命名空间中选择安全协议和变换、共享密码以及交换协议的标识符等

IPSec功能

- **作为一个隧道协议实现了VPN通信。**第三层隧道协议，可以在ip层上创建一个安全的隧道，使两个异地的私有网络连接起来。
- **保证数据可靠来源。**
 - ipsec通信前，双方要先用IKE认证对方并协商密钥，只有IKE协议协商成功后才能通信
 - 由于第三方不肯知道验证和加密的算法，以及相关密钥，所有保证了安全性
- **保证数据完整性。**ipsec通过验证算法，保证数据的任何数据篡改和丢失都可以检测
- **机密性。**加密算法

6.3.2 IPSec的工作原理



AH

- 只涉及认证，不涉及加密
- RFC 2402 把AH服务定义如下。**非连接的数据完整性校验。数据源点认证。**

AH (Authentication Header, 验证头部协议) : RFC2402

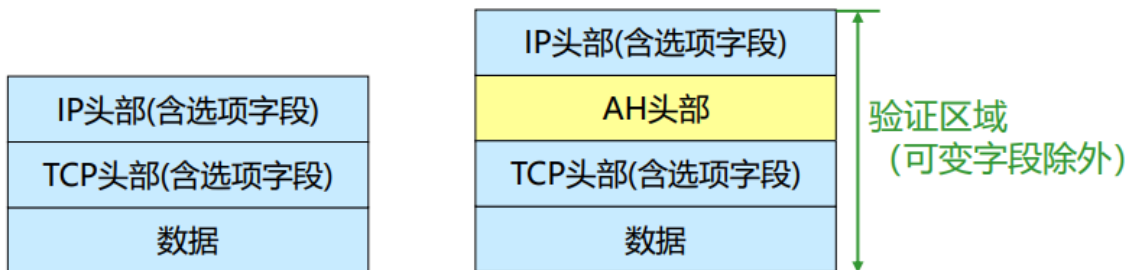
- AH对IP层的数据使用**验证算法MAC**，从而对完整性进行保护。
- MAC (Message Authentication Codes, 报文验证码)，即报文摘要，是从HASH算法演变而来，又称为HMAC，如HMAC-MD5、HMAC-SHA1、HMAC-RIPEMD-160。
- 通过HMAC可以检测出对IP包的头部和载荷的修改，从而保护IP包的内容完整性和来源可靠性。
- 不同IPSec系统可用的HMAC算法可能不同，但**HMAC-MD5和HMAC-SHA1是必须实现的**。

AH协议和TCP、UDP协议一样，是被IP协议封装的协议之一，可以由IP协议头部中的协议字段判断，AH的协议号是51。



AH传输模式下

- AH插入IP头部之后，传输层协议 (UDP, TCP) 或其他ipsec协议之前



图a 应用AH之前

图b 应用AH之后

AH隧道模式下

- AH插入原始IP头部之前，然后在AH之前再增加一个新的IP头部

AH与NAT冲突


- 被AH验证的是整个IP包（除了可变字段），包括IP头部。因此IP地址修改会被检测出来
- AH不能穿越NAT

数据完整性检查


- **在发送方。**整个ip包和验证密钥被作为输入，经过HMAC算法计算后得到的结果被填充到AH头部的“验证数据”字段
- **在接收方。**整个IP包和验证算法所用的密钥也被作为输入，经过HMAC算法计算的结果和AH头部的“验证数据”进行对比

IPv4头部中的不定字段和固定字段

版 本	首部长度	服 务 类 型	总 长 度	
标 识			标志	片 偏 移
生 存 时 间		协 议	首 部 检 验 和	
源 地 址				
目 的 地 址				
选 项 字 段				

不定字段（在通信过程中可能被合法修改）：

- 在计算HMAC时先临时用0填充；
- 另外，AH头部的验证数据字段在计算之前也要用0填充，计算之后再填充验证结果。

应被AH保护的内容（在通信过程应该不被修改）：

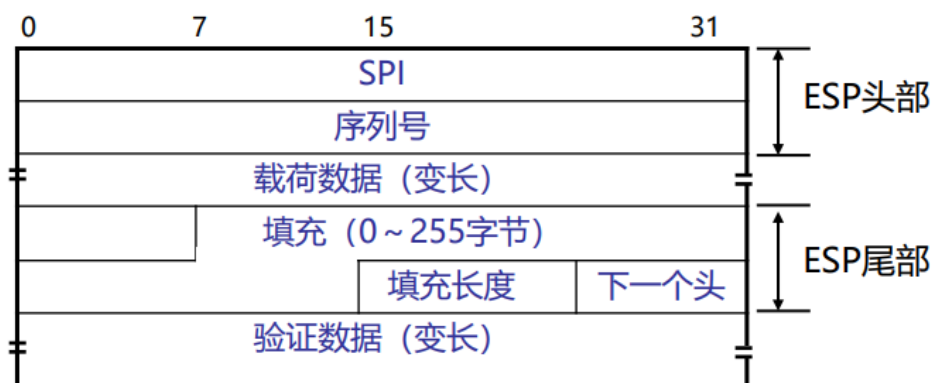
- 固定字段；
- AH头中除“验证数据”以外的其他字段；
- 数据：指经过AH处理之后，在AH头部后面的数据。传输方式下，指TCP、UDP或ICMP等传输层数据；隧道模式下，指被封装的原IP包。

ESP

2 ESP (Encapsulating Security Payload)

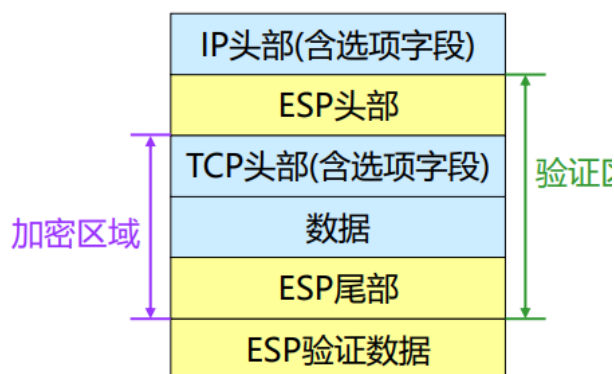
- ESP协议主要用于对IP数据包进行加密，此外也对认证提供某种程度的支持。
- ESP协议也有两种工作模式：**传输模式**和**隧道模式**。
 - ① 与AH相比，ESP验证的数据范围要小一些。ESP协议规定了所有IPSec系统必须实现的验证算法：**HMAC-MD5、HMAC-SHA1、NULL**。
 - ② ESP的加密采用的是**对称密钥加密算法**。不同的IPSec实现，其加密算法也有所不同。为了保证互操作性，ESP协议规定了所有IPSec系统都必须实现的加密算法：**DES-CBC、NULL**。
 - ③ 但ESP协议规定加密和认证不能同时为NULL。即**加密和认证必须至少选其一**。

ESP协议和TCP、UDP协议一样，是被IP协议封装的协议之一，可以由IP协议头部中的协议字段判断，ESP的协议号是50。



ESP运行模式(1) - 传输模式

- 保护的是IP包的载荷；
- ESP插入到IP头部（包括IP选项字段）之后，任何被IP协议所封装的协议（如传输层协议TCP、UDP、ICMP，或者IPSec协议）之前。



图b 应用ESP之后

☁️ ESP加密不包括SPI、序号字段和验证数据；

☁️ ESP的验证不包括IP头部：

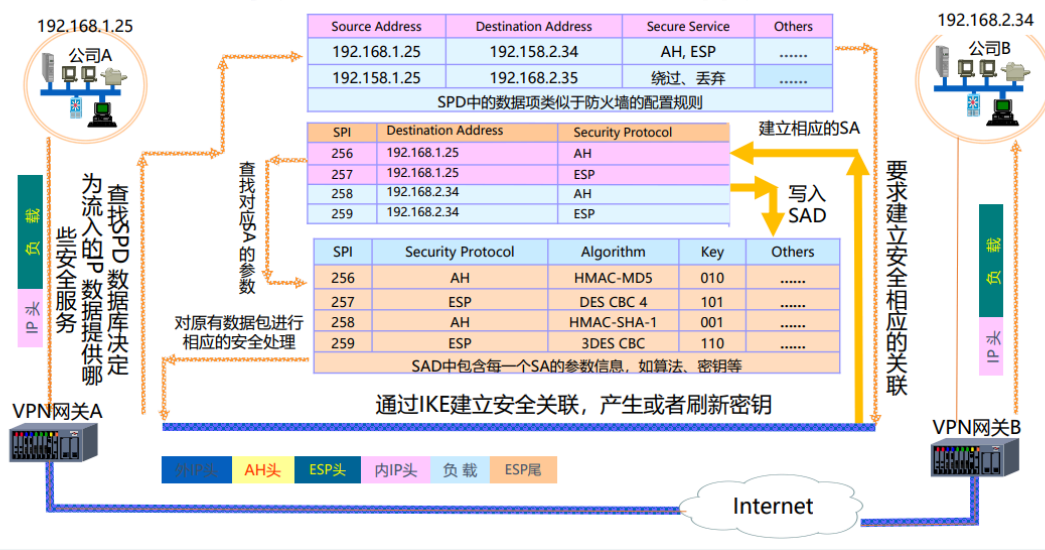
- 优点：不存在与NAT冲突的问题；
- 缺点：除了ESP头部之外，任何IP头部字段都可以修改，只要保证其校验和计算正确，接收端就不能检测出这种修改。所以，**ESP传输模式的验证服务要比AH传输模式弱一些**。如果需要更强的验证服务并且通信双方都是公有IP地址，应该采用AH来验证，或者将AH认证与ESP验证同时使用。

☁️ **ESP隧道模式的验证和加密能够提供比ESP传输模式更加强大的安全功能**，因为隧道模式下对整个原始IP包进行验证和加密，可以提供数据流加密服务；而ESP在传输模式下不能提供流加密服务，因为源、目的IP地址不被加密。

☁️ 不过，隧道模式将占用更多的带宽，因为增加了一个 额外的IP头部。

☁️ 尽管ESP隧道模式的验证功能不像AH传输模式或隧道模式那么强大，但ESP隧道模式提供的安全功能已经足够了。

一个完整的IPSecVPN工作原理



IKE没加上去.....

IP

IP协议中的安全问题

IP地址欺骗

IP协议对IP地址的真实性没有进行验证，地址有可能被假冒

- 源IP地址欺骗：攻击者拦截正常用户，然后冒充正常用户
- 目的IP地址欺骗:dns欺骗

防范：

- 抛弃基于地址的信任策略，采用更高层认证
- 进行包过滤，配置路由器使其能拒绝网络外部与本网内具有相同IP地址的连接请求

ip定向广播攻击

ip地址还包括有广播地址，可以向某个网络的广播地址发送报文，该网络中所有主机都能收到，这个广播应该慎用。

- 攻击者采用定向广播攻击主机，主机对广播包响应，消耗主机资源和网络带宽

防范

- 在路由器上关闭定向广播转发选项

ip数据监听

ip协议未提供加密机制

防范

- 采用加密措施

数据篡改

ip协议只有对首部的校验，攻击者完全可以修改数据包内容

防范

- 对ip数据报净荷部分实行完整性检测机制，IPSEC

ip分片重组攻击

在 IP 协议（IPv4）中，数据包的最大传输单元（MTU）受限于链路的物理特性（如以太网的 MTU 为 1500 字节）。当 IP 数据包大于 MTU 时，必须拆分为多个片段，然后在接收端进行重组。

- **小片段攻击。**攻击者故意把恶意代码拆成多个极小的 IP 片段，使得入侵检测系统（IDS）无法一次性检测出完整的攻击指令，导致绕过安全检查。
- **分片重叠攻击。**攻击者故意发送偏移量重叠的 IP 分片，后续分片可能覆盖前面分片的部分数据，导致数据篡改或绕过防火墙检测。
- **teardrop撕裂攻击。**发送两个 IP 分片，它们的 偏移量 设计成不连续但有重叠，导致目标系统在重组时计算错误，引发 缓冲区溢出

防范

过滤畸形分片

防火墙或 IDS 规则

丢弃 偏移量重叠 的 IP 分片。

拦截过小的 IP 片段（如小于 100 字节）。

限制总分片数，避免资源消耗攻击。

统一重组策略

使用“后到优先”策略（尽量不要使用“先到优先”）。

只允许连续的偏移量，防止 Teardrop 攻击。

MTU 配置优化

设置 Path MTU Discovery（PMTUD），减少网络中的分片需求。

深度包检测（DPI）

部分 NGFW（下一代防火墙）具备 DPI（Deep Packet Inspection），可在数据重组前检测恶意负载。

重放攻击

定义

重放攻击是指攻击者截获并记录合法用户与系统之间的通信数据，然后在之后的某个时间点重新发送这些数据，以欺骗系统，从而达到非法获取信息或执行操作的目的。

原理

在正常的网络通信中，客户端和服务端之间会交换一系列的消息，这些消息可能包含身份验证信息、交易指令等。攻击者通过网络嗅探等手段，截获这些消息，并不对其进行修改，而是在合适的时机重新发送给目标系统。由于目标系统通常只验证消息的合法性，而不检查消息是否是重复发送的，因此可能会将重放的消息当作正常消息进行处理。

常见场景

- **身份验证过程**：在用户登录系统时，会向服务器发送包含用户名和密码等身份验证信息的数据包。攻击者截获该数据包后，在用户登出系统后重新发送该数据包，若系统没有有效的防重放机制，可能会误以为是合法用户再次登录，从而允许攻击者登录系统。
- **金融交易**：在银行转账等金融交易场景中，客户端会向服务器发送包含转账金额、收款账户等信息的交易指令。攻击者截获该指令后，重放该指令，可能导致同一笔资金被多次转出。

危害

- **数据泄露**：攻击者通过重放身份验证消息，可能会非法登录系统，从而获取系统中的敏感数据，如用户个人信息、商业机密等。
- **资金损失**：在金融交易场景中，重放攻击可能导致资金被多次转移，给用户或企业带来经济损失。
- **系统被非法控制**：攻击者重放包含系统操作指令的消息，可能会对系统进行非法操作，如修改系统配置、删除重要数据等，影响系统的正常运行。

防范措施

- **时间戳机制**：在消息中加入时间戳信息，服务器在接收到消息后，检查时间戳是否在合理的范围内。如果时间戳与当前时间相差过大，则认为该消息是重放的，拒绝处理。例如，服务器规定只接受时间戳与当前时间相差不超过 5 分钟的消息。

ARP

ARP缓存中毒（ARP欺骗，ARP重定向）

使用伪造ARP消息欺骗受害者接受无效的IP-MAC映射，并把映射存储在其缓存中

- 第一种就是伪造ARP的请求报文。攻击者构造一个ARP请求包，来发送给主机。这个ARP请求报文中的源IP地址、源MAC地址都可能伪造，目的主机收到以后，就会更新ARP表；
- 第二种方式，可以使用ARP的响应报文，因为ARP协议允许没有请求报文的情况下，直接发送响应报文。它的格式跟请求报文基本上差不多，其中的源IP、源MAC，都可以伪造。
- 另外，还可以使用免费ARP报文，免费ARP也是一种响应报文，只不过源IP和目的IP都是发布免费ARP主机的地址，MAC地址为广播地址。

免费ARP一般是当主机需要上其他主机的ARP缓存进行更新的时候使用。

防范

- 在关键系统之间设置静态的ARP项，比如防火墙和边界路由上（不太灵活）
- 在交换机上配置802.1x协议，攻击者连接交换机时，需要验证身份

ICMP

icmp没有验证机制，攻击者可以伪造报文，形成拒绝服务，重定向等攻击

- 针对带宽的ICMP DoS，伪造受害主机的源地址，向网络的广播地址发送大量ping包，目标系统很快会被大量的echo reply信息淹没
- 针对连接的ICMP DoS，通过发送一个伪造的ICMP Destination Unreachable 来中止合法的连接
- ICMP重定向。利用ICMP路由重定向报文来改变主机的路由表。自己伪装成路由器，向目标机器发送重定向信息，使目标机器的数据报文发送到攻击机，实现监听、会话劫持、拒绝服务攻击

防范

仅支持必要的ICMP类型通信

- 支持ICMP——允许向外发送icmp响应请求，并允许向内发送响应答复信息
- 支持路径MTU——允许向内发送需要分片但DF置位的ICMP消息
- 阻止其他的类型的ICMP

基于 ICMP 的网络攻击及防范措施

ICMP（Internet Control Message Protocol，互联网控制报文协议）用于在 IP 网络中传递控制消息和错误信息。然而，攻击者也常利用 ICMP 的特性实施网络攻击。以下是几种常见的基于 ICMP 的攻击方式及其防范措施：

1. Ping of Death 攻击

原理：

- 在 IPv4 中，IP 数据包的最大长度理论上为 65,535 字节（包含首部）。攻击者构造超长的 ICMP 数据包，或发送多个分片后在目标系统重组时超出长度限制，导致缓冲区溢出，使系统崩溃、死机或重启。

防范措施：

- 及时更新操作系统和网络设备补丁，修复缓冲区溢出漏洞。
- 在防火墙或入侵检测系统（IDS）中设置规则，过滤掉长度异常的 ICMP 数据包。

2. ICMP 洪水攻击 (ICMP Flood)

原理：

- 攻击者向目标主机发送大量 ICMP Echo Request (Ping) 请求，使其系统资源（CPU、内存、带宽）被耗尽，导致拒绝服务（DoS）。若攻击流量来自多个不同的源地址，则成为 DDoS（分布式拒绝服务）攻击。

防范措施：

- 在防火墙上限制 ICMP 流量速率。
- 采用流量清洗服务识别并过滤异常的 ICMP 流量。
- 部署入侵防御系统（IPS）实时监测和阻断攻击。

3. Smurf 攻击

原理：

- 攻击者向某网络的广播地址发送大量伪造源地址为目标主机的 ICMP Echo Request 数据包。网络中的所有主机都会向目标主机回复 ICMP Echo Reply，导致目标主机因流量激增而崩溃。

防范措施：

- 在路由器上禁止向广播地址转发 ICMP 数据包。
 - 在防火墙中阻止来自广播地址的 ICMP 流量。
 - 通过子网划分减少广播域的影响。
-

4. ICMP 重定向攻击

原理：

- ICMP 重定向消息用于通知主机更改路由。攻击者伪造 ICMP 重定向消息，欺骗目标主机将流量引导至恶意设备，实现中间人攻击（MITM），从而窃取或篡改通信数据。

防范措施：

- 在网络设备上严格控制 ICMP 重定向消息，仅接受来自可信源的重定向信息。
 - 使用 SSL/TLS 等加密技术保护数据传输，防止信息泄露。
-

5. ICMP 信息泄露攻击

原理：

- 攻击者通过发送 ICMP 请求，并分析返回的 ICMP 错误消息（如“目标不可达”“超时”等），推测目标网络的拓扑结构、主机状态、防火墙策略等信息，为后续攻击提供情报。

防范措施：

- 通过防火墙和路由器限制 ICMP 错误消息的返回范围。
 - 对网络设备进行合理的安全配置，避免泄露敏感信息。
-

总结

ICMP 作为网络控制协议，在正常通信中发挥着重要作用，但其易被滥用，成为多种网络攻击的载体。为了防范 ICMP 攻击，应合理配置防火墙、路由器和入侵检测系统，限制 ICMP 流量，减少潜在攻击面，同时及时更新系统补丁，增强网络安全防护能力。

运输层

TCP

服务多路复用，多路分解

可靠传输：校验和，确认重传，超时机制，字节编号

面向连接：建立连接——数据传输——释放连接

流量控制：接受窗口

拥塞控制：拥塞窗口，慢启动，拥塞避免

第一类攻击

- SYN泛洪。针对三次握手过程中，的攻击

第二类攻击

针对TCP协议不对数据包加密和认证的漏洞

- TCP序列号攻击
- TCP会话劫持
- 数据嗅探

第三类攻击

针对拥塞控制机制的特性

- 拒绝服务攻击

SYN Flood

利用TCP连接的半开放状态

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，无法完成三次握手过程，占用资源（也是一种拒绝服务攻击）

检测技术

- 半开连接数检测。从平衡变成突然增多说明被攻击了
- 新建连接速率检测。在服务器记录每秒新连接的数量，设定警报阈值

防御

缩短SYN timeout时间

设置SYN cookie：给每一个请求连接的IP地址分配一个cookie，如果短时间内连续受到某个IP的重复SYN文，认定是受到了攻击，以后从这个IP地址来的包会被丢弃

设置SYN可疑队列：

使用网关：

1.SYN 网关： 防火墙收到客户端的SYN包时，直接转发给服务器：防火墙收到服务器的SYN/ACK包后，一方面将SYN/ACK包转发给客户端，另一方面以客户端的名义给服务器回送一个ACK包。完成TCP的三次握手，让服务器端由半连接状态进入连接状态。

2.SYN中继：SYN中继防火墙在收到客户端的SYN包后，并不向服务器转发而是记录该状态信息后主动给客户端回送SYN/ACK包，如果收到客户端的ACK包。表明是正常访问，由防火墙向服务器发送SYN包并完成三次握手。

2.被动式SYN网关：被动式SYN网关：设置防火墙的SYN请求超时参数，让它远小于服务器的超时期限。防火墙负责转发客户端发往服务器的SYN包，服务器发往客户端的SYN/ACK包、以及客户端发往服务器的ACK包。这样，如果客户端在防火墙计时器到期时还没发送ACK包，防火墙则往服务器发送RST包，以使服务器从队列中删去该半连接。

序号攻击

TCP序列号产生方式（ISN：初始序列号）

- 总是使用相同的ISN
- 每次建立TCP连接的ISN增量总是使用同样的递增值
- 伪随机，每过一段时间ISN加上一个小小的固定的数
- 随即增量，每次建立连接时候的ISN的增量随机生成
- 真随机，完全借助于随机数生成函数，在32位的ISN空间选择下一次连接ISN

TCP会话劫持

- 监听数据包
- 确认动态会话
- 猜测序列号
- 使客户主机下线
- 接管会话

防范

针对TCP序列号猜测和会话劫持这类攻击如何进行防范呢？序列号攻击冒充了其它合法用户，因此防范的一个措施就是不要把网络安全信任关系建立在IP基础上或者MAC基础上；

TCP会话劫持是建立在嗅探的基础上，因此其防范的关键措施是防止ARP欺骗，可以通过设置静态的ARP，上层采用安全加密协议等措施。

- 不把网络安全信任关系建立在IP基础上或MAC基础上
- 设置静态的MAC——>IP对应关系表，不要让主机刷新设定好的转换表
- 停止使用ARP，把需要的ARP作为永久条目保存
- 上层采用安全加密协议

为防止 TCP 序号攻击，现代操作系统和协议栈通常采用以下安全机制：

1. **随机化 TCP 初始序列号 (ISN)**：避免攻击者预测 TCP 序列号。
2. **加密与身份验证**：
 - 使用 **IPSec**、**TLS** 保护 TCP 连接，防止攻击者篡改数据。
 - BGP 等协议可使用 **TCP MD5** 或 **TCP-AO (Authentication Option)** 确保数据完整性。
3. **启用 TCP 严格验证**：
 - 采用 **SYN cookies** 防止 SYN 泛洪攻击。
 - 服务器可使用 **ACK 认证**，确保返回的 TCP 数据包匹配正确的序列号。

为什么“防止 ARP 欺骗”是关键防御手段？

既然 TCP 会话劫持依赖于攻击者监听网络流量，而 ARP 欺骗是最常见的流量嗅探手段，那么防止 ARP 欺骗就可以有效阻止攻击者获取 TCP 序列号，从而防止 TCP 会话劫持。

2. TCP 签名 (MD5 / TCP-AO) 是如何防止劫持的？

(1) TCP MD5 签名 (RFC 2385)

工作原理：

- 在 TCP 头部附加一个 **MD5 哈希签名**，该签名由 **发送方和接收方共享的密钥** 计算得到：


$$\text{TCP Signature} = MD5(\text{TCP Header} + \text{TCP Payload} + \text{Shared Secret})$$

- 接收方收到 TCP 包后，也会使用相同的密钥计算签名，并与报文中的签名进行对比，只有匹配的才会被接受。

如何防止劫持？

- 攻击者即使能伪造 TCP 报文，但**没有密钥**，就无法计算出正确的 MD5 签名，因此服务器会拒绝伪造的 TCP 报文。
- 即使攻击者窃听了 TCP 报文，他也无法直接修改报文内容，否则签名会不匹配。

缺陷：

- **密钥管理困难**：所有 TCP 连接的通信双方都必须共享相同的密钥，但密钥无法自动更新，容易被暴力破解。
- **MD5 不够安全**：MD5 可能受到彩虹表攻击， 不符合现代安全需求。

3. TCP 签名 vs TCP 会话劫持

方式	防止 TCP 伪造	防止 TCP 序列号预测	防止中间人攻击 (MITM)
普通 TCP	✗ 无认证，容易被伪造	✗ 序列号可以预测	✗ 易受 MITM 影响
TCP MD5	✓ 需密钥匹配，防伪造	✓ 随机序列号+MD5 验证	✗ 无加密，仍可能被窃听
TCP-AO	✓ 更强认证	✓ 更强防护	✗ 无加密，仍需 TLS 等配合
TLS (SSL/TLS)	✓ 公钥认证防伪造	✓ TLS 内部处理	✓ 数据加密防 MITM

Land Attack (Land 攻击)

原理：攻击者伪造 TCP 包的源 IP 和目标 IP 相同，使服务器向自己发送数据，从而导致系统死锁或资源耗尽。

影响：服务器 CPU 过载，可能导致崩溃。

防御手段：
在防火墙或 IDS 规则中屏蔽相同源/目标 IP 的 TCP 报文。

TCP 由于其 **连接管理、窗口控制、序列号机制**，成为攻击者的目标，常见的攻击方式包括：

攻击类型	影响	主要防御措施
SYN Flood	服务器连接耗尽	SYN Cookies、限流
RST 注入	连接被强制关闭	TCP MD5、随机序列号
会话劫持	连接被劫持	TLS、TCP-AO
窗口操控	传输受干扰	限制窗口调整
分片攻击	资源耗尽、缓冲区溢出	禁止异常分片
ACK Flood	CPU 过载	限制 ACK 速率
Slowloris	连接耗尽	设置超时、检测慢连接
伪造 TCP 包	误操作、MITM	TCP MD5 / TLS
Land Attack	服务器死锁	防火墙规则限制

UDP

没有纠错和重传机制，检测丢包，复制或重新排序的机制。误码检测也是可选项

- UDP Flood，UDP用于大量的数据传输时，**协议自身缺少流量控制特征，能阻塞主机或路由器，造成丢包**

防护

- 依靠上层的认证措施，数据加密，完整性验证
- IDS，防火墙过滤

UDP反射放大攻击

UDP反射放大攻击的原理基于UDP协议的无连接特性和某些开放服务（如NTP、DNS、Memcached等）的响应机制，很多协议在响应包处理时，要远大于请求包，一个字节的请求十个字的响应，十个字节的请求一百个字的响应

攻击方式	放大倍数	目标端口
DNS 放大	28 - 54 倍	53
NTP 放大	20 - 200 倍	123
SSDP 放大	30 - 100 倍	1900
Memcached 放大	10000 倍以上	11211

- 防火墙启用一些DDOS防护服务
- 限制或阻止来自非信任源的UDP流量，特别要关注那些已知易受UDP反射放大攻击影响的端口，如NTP的123端口、DNS的53端口等。
-

应用层

常见应用及协议

- 动态主机配置协议——DHCP
- 域名与用户查询——DNS、Whois、FINGER
- 电子邮件系统——SMTP、POP3、IMAP4、MIME、PGP
- 文件传输与文件共享——FTP、TFTP
- 远程登录——TELNET、SSH
- Web服务——HTTP
- 网络管理——SNMP
- 多媒体——H.323、SIP
- 其它网络应用——NNTP、LDAP、NTP、NFS

DHCP(动态主机配置协议)

DHCP是局域网协议：不能发动远程攻击

但是DHCP没有认证机制，可以使用欺骗攻击

- 冒充服务器，假装服务器应答:中间人攻击
- 冒充客户端，模仿不同的mac地址，发出请求，耗尽服务器地址池IP，DoS攻击

DHCP 协议的安全性

- DHCP只能在本地网络上使用，不能发动远程攻击
- 没有认证，会遭受欺骗攻击，中间人攻击，和DoS攻击

防范

- 针对假冒服务器和中间人攻击：交换机只接收信任端口的报文；交换机采用802.1x认证
- 针对DoS攻击，可以扫描局域网内所有mac并记录，检查报文中客户端MAC地址，跟记录的MAC进行对比

DNS(域名系统)

是一个分布式数据库系统，实现 域名——IP映射

DNS最大的缺陷是，解析的请求者无法验证他所受到的应答信息真实性

- DNS欺骗攻击。伪造来自本地DNS服务器的响应包
- DNS缓存中毒。伪造外部DNS服务器的响应，毒化本地DNS服务器缓存
- DNS重定向。把DNS查询重定向到恶意DNS服务器

防范

- 不要采用基于名称的认证。基于地址的认证虽然也很脆弱，但是要优于前者
- 不要把秘密信息放在主机名中 ???
- 采用DNSSec新标准（有效，但是没有全面推广）

DNSsec (DNS安全扩展)

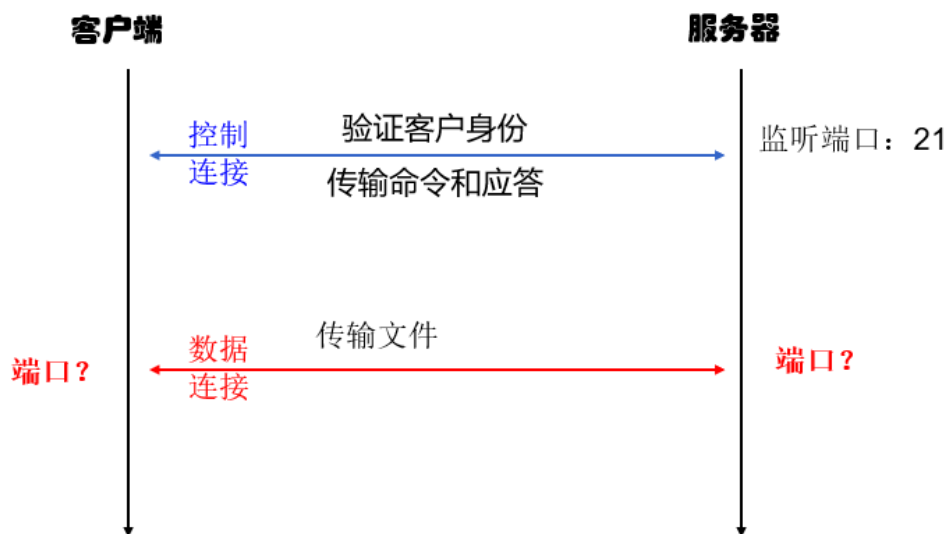
提供了一种来源鉴定和数据完整性的扩展，但不保障可用性，加密性，和证实域名不存在

- 从根区域到最终域名的查找过程中的每一步部署该技术，每个级别都进行签名，且拥有其自己的签名生成密钥

FTP

FTP协议

FTP工作过程



主动模式PORT

- (数据连接) FTP客户机用PORT命令把新端口发给服务器。服务器从20端口向客户端的新端口发起数据连接

被动模式PASV

- FTP客户端向服务器发送PASV命令，服务器回应新端口号发给客户端，客户端新临时端口向服务端的新端口发起数据连接

安全性问题

- 明文传输。登录用户名，密码，传输内容容易被窃听
- 地址端口信息在应用层PORT (PASV) 命令中出现。
- 两种方向的数据连接。可能需要开放从外到内的数据访问，造成安全隐患
- PORT命令中指定了服务器连接的地址和端口，容易造成FTP反弹攻击，将数据发给第三方
- FTP用户权限限制若是不合理，会导致非授权访问
- 匿名FTP问题。ü全球可读写目录常用来存储和发布盗版软件或其它违法的软件或数据
- **FTP反弹攻击**。如果攻击者修改PORT 后面的地址和端口为第三方的地址和端口，那么服务器端就会用20号端口连接第三方的这个地址和端口，将数据发给第三方。

安全改进

- 使用SFTP（SSH文件传输协议）代替。进行加密；采用SSH（22端口），避免了开放大量数据连接端口
- 禁用PORT方式。可以解决两种方向数据连接的风险
- 防止反弹攻击。针对FTP反弹攻击，服务器端口可以增加检查，PORT命令的IP地址只能为客户端的地址，且端口号大于1024（防止系统端口被攻击）
- 用户权限问题。最小权限，不用root
- 匿名用户。可以只允许读，或者取消匿名用户

Telnet(远程登录协议)

是一种因特网远程终端访问标准。仅提供基于字符应用的访问

提供对各种终端设置的规定，如自然模式，字符回显等

telnet后台通过调用login程序进行口令认证和引发会话

多数Telnet客户端程序都支持以任意端口访问基于文本的TCP服务的能力

安全问题

- 传输明文，可能泄露信息
- 没有强认证过程，攻击者可能对每个账号进行口令猜测，或者通过嗅探器嗅探口令
- 基于TCP，容易遭受会话劫持攻击

SSH(安全Shell)

- 安全登录和远程命令执行，默认22端口。是为了取代rlogin,rsh设计的
- 支持身份认证和数据加密
- 对数据进行压缩处理，加快传输速度
- 可以为FTP，POP等服务提供一个安全的隧道
- 从客户端来看，SSH提供两种级别的安全验证：
 - （基于口令的安全验证）：所有传输的数据都会被加密，但是不能保证服务器的真实性
 - （基于公私钥的安全验证）：登录过程会稍慢
- OpenSSH 。SSH的替代，免费开源，提供了服务端后台程序和客户端工具

SSH的安全问题及防护措施

1 第一类问题： 服务器认证	2 第二类问题： 协议版本协商	3 第三类问题： 主机密钥文件安全
● 问题描述： SSH协议在不安全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；SSH协议提供了可选功能使得客户机第一次连接到服务器时可以对服务器主机密钥验证。	● 问题描述： SSH协议运行第一步是进行服务器与客户端协议版本的协商。如果攻击者采用有安全漏洞的版本建立连接，则可能采取进一步攻击。	● 问题描述： SSH协议服务器的主机密钥存储在一个主机密钥文件中，若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，进一步实施假冒、重放和中间人攻击等。
● 防护措施： 必须检验主机密钥来验证服务器的正确性。	● 防护措施： 对采用有安全问题软件的通信方，服务器可以中断TCP连接。	● 防护措施： 增强安全机制进行主机密钥文件的管理。

电子邮件系统

发送邮件：简单邮件传输协议SMTP

收取邮件：

邮局协议POP3

因特网邮件访问协议IMAP

安全问题

- 全部信息明文传输
- 采用固定端口25进行邮件发送
- 对邮件源没有任何验证
- 攻击者只要对TCP25端口的数据流进行监听，就能分辨出SMTP命令及其参数内容

邮件炸弹

- 任何一个人都可以没有任何限制地向因特网中的任意一个电子邮箱发送邮件
- 攻击者可以向某个邮件服务器的某个电子邮箱发送大量邮件
 - 用户邮箱挤爆，无法正常接受
 - 邮件炸弹所携带的大量无用信息占用网络带宽

垃圾邮件产生的原因

- SMTP没有严格的源验证
- 邮件中继/开放转发（OpenRelay）

可以通过邮件头的原始信息查看其中继路径

- SMTP最常用的实现方案是Sendmail。Sendmail有一个致命的缺陷：常以root用户权限工作。违背“最小信任”原则。SMTP后台程序不必以root权限运行

防范措施

- SMTP没有对源认证的问题
- 使用SMTPS (SMTP over SSL) ,加密
- 关闭开放中继
- 一些命令导致的安全问题，少用那些命令

反垃圾邮件技术

- 过滤技术，地址列表技术
- 行为模式识别。采用概率统计模型，对时间，品读，发送Ip，协议声明特征，发送指纹等。不需要过滤邮件内容，提高速度
- 电子邮件认证技术，针对伪造地址或伪造回复地址的有效阻断技术

POP3

把服务器上的邮件存储到本地主机，同时删除保存在邮件服务器上的邮件

- 协议简单，明文传输
- user命令：口令明文传输
- POP3服务器常常以root权限运行，存在风险

针对明文传输，可以采用POP3S (POP over SSL)

IMAP4

h是邮件获取协议，类似POP3

- 提供邮件下载服务，支持离线阅读
- 支持在线离线传输数据，服务端采用分布式存储邮件方式
- 支持用户对服务器的远程加密访问

电子邮件安全协议和标准

- 1 PGP (Pretty Good Privacy) : 实现邮件的加密、鉴别、签名、压缩等, 采用以**个人为中心的信任模型**。
- 2 PEM(Privacy Enhanced Mail)保密增强邮件PEM美国RSA实验室开发, 在电子邮件标准格式上增加了加密、鉴别和密钥管理的功能, 采用基于层次的严格认证。
- 3 S/MIME(the Secure Multipurpose Internet Mail Extensions, 安全多用途因特网邮件扩展)协议, 从PEM和MIME发展而来, 采用**基于CA的认证**, 被认为是商业环境下**首选**的安全电子邮件协议。

IMAP4的安全性问题

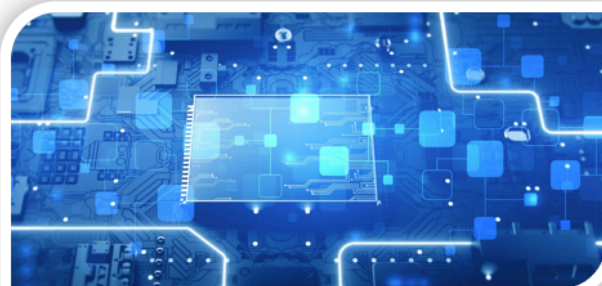
网络层协议的安全性分析

- IP: IP欺骗、源路由、IP碎片、定向广播、监听
- ARP: ARP欺骗、ARP重定向
- ICMP: ICMP flood、ICMP重定向
- 路由协议:OSPF、BGP、RIP的安全性

IMAP4的安全性问题

运输层协议的安全性分析

- TCP: syn flood、序列号猜测
- UDP: UDP flood、UDP欺骗



网络扫描/网络监听

扫描对象的信息状态有哪些

- 目标网络哪些主机是活动的
- 主机的操作系统类型
- 开放了哪些端口，提供哪些服务
- 运行的应用程序版本号
- 使用什么报文过滤器/防火墙
- ...

扫描策略

- 隐蔽扫描：对非连续端口进行扫描，并且源地址不一致，时间间隔长没有规律。又叫乱序扫描，慢速扫描
- 主动扫描：对连续的端口扫描，源地址一直，时间间隔短

常用工具

- Nmap
- X-Scan
- nessus

主机扫描

确定在目标网络中的主机是否可达

传统技术

- ICMP Echo (ping) 扫描
- ping sweep扫描
- 广播ICMP扫描
- 非ECHO的ICMP扫描

ICMP Echo (ping) 扫描

向目标主机发送ICMP ECHO REquest (type8) 数据包，等待回复的reply包 (type0)

如果能收到回复，说明可达。

- 系统自带，简单
- 很容易被防火墙限制

ping sweep扫描

使用ICMP ECHO轮询多个主机

- 对于中小型网络尚可接受，大型网络速度比较慢
- 工具 fping


```
[root@localhost src]# ./fping -g 192.168.1.250 192.168.1.254
192.168.1.251 is alive
192.168.1.252 is alive
192.168.1.253 is alive
ICMP Host Unreachable from 192.168.10.145 for ICMP Echo sent to 192.168.1.250
ICMP Host Unreachable from 192.168.10.145 for ICMP Echo sent to 192.168.1.250
ICMP Host Unreachable from 192.168.10.145 for ICMP Echo sent to 192.168.1.250
ICMP Host Unreachable from 192.168.10.145 for ICMP Echo sent to 192.168.1.250
```

广播ICMP扫描

通过向广播地址发送ICMP ECHO报文来发现目标网络中活动的主机

- 只适用于目标网络中的Unix主机
- ping -b

```
root@localhost:~# ping -b 192.168.255.255
WARNING: pinging broadcast address
PING 192.168.255.255 (192.168.255.255) 56(84) bytes of data.
64 bytes from 192.168.88.147: icmp_seq=1 ttl=64 time=0.464 ms
64 bytes from 192.168.1.252: icmp_seq=1 ttl=64 time=0.693 ms (DUP!)
64 bytes from 192.168.50.1: icmp_seq=1 ttl=64 time=0.708 ms (DUP!)
64 bytes from 192.168.1.252: icmp_seq=1 ttl=64 time=888 ms (DUP!)
64 bytes from 192.168.1.252: icmp_seq=1 ttl=64 time=889 ms (DUP!)
64 bytes from 192.168.88.147: icmp_seq=1 ttl=64 time=889 ms (DUP!)
64 bytes from 192.168.88.147: icmp_seq=1 ttl=64 time=890 ms (DUP!)
64 bytes from 192.168.88.147: icmp_seq=1 ttl=64 time=890 ms (DUP!)
```

非ECHO的ICMP扫描

- TimeStamp Request (Type 13) & Reply (Type 14) ✓ 请求系统返回当前时间，目的是查看系统所在的时区
- Address Mask Request (Type 17) & Reply (Type 18) ✓ 地址掩码请求分组，即能请求返回某个设备的子网掩码
- hping3

主机扫描对策

- 使用可以检测并记录ICMP扫描的工具
- 在防火墙中设置ICMP过滤规则
- 使用IDS

端口扫描

目的是确定目标主机哪些TCP，UDP端口可访问

类型：开放扫描，半开放扫描，隐蔽扫描

工具：nmap, netcat

2.1 TCP端口扫描原理

动作	响应
一个SYN ACK或FIN报文到达一个关闭的端口	返回一个RST报文
一个SYN ACK或FIN报文到达一个开放的端口	报文被丢弃
一个包含ACK的报文到达一个开放端口	报文被丢弃，同时返回一个RST报文
一个不包含SYN位的报文到达一个开放端口	报文被丢弃
一个SYN报文到达一个开放端口	正常三次握手，回答一个SYN ACK报文

TCP Connect扫描——开放扫描

原理

- 调用socket函数connect()连接目标
- 成功则端口开放，失败说明端口关闭

优点

- 稳定可靠
- 不需要特殊的权限

缺点

- 不隐蔽，目标产生很多记录
- 容易被防火墙发现并屏蔽

TCP STN扫描——半开扫描

原理

- 向目标主机端口发SYN包，如果返回RST包，端口关闭，如果返回SYN|ACK包，端口打开
- SYN扫描，连接未完全建立，成为半连接扫描

优点

- 隐蔽性比全连接好

缺点

- 构造SYN包需要超级用户权限系统调用

TCP FIN扫描——隐蔽扫描

实现原理

- 向目标主机发送FIN包
- 如果返回RST包，端口关闭；没有任何返回，端口可能打开

优点

- 不包含TCP三次握手的任何部分，隐蔽性强

- FIN能够通过只监测SYN包的包过滤器

缺点

- 构造FIN包，需要超级用户权限调用
- 适用于多数UNIX，不支持win95/NT（端口是否打开都会返回RST）

UDP端口扫描

原理

- 向目标主机发送UDP数据包
- 如果返回ICMP端口不可达，端口关闭；否则端口打开

优点

- 简单

缺点

- 可靠性不高。是开放？还是丢失？
- 扫描速度慢，ICMP错误报文的生成速度是有限制的