# 网络安全大纲

实验部分：

lab2：ARP缓存中毒。

lab3：SYN洪泛（SYN cookie）、TCP RST攻击、TCP会话劫持（通过向该会话中注入恶意内容来劫持两个受害者之间的现有TCP连接,eg使用会话劫持创建反向shell)

lab4：DNS缓存中毒（攻击DNS服务器）、DNS重定向。

lab5：有无状态防火墙比较优缺点。

# 零.网络体系结构

## 网络层次结构

早期计算机只进行简单的文件传输和远程访问，因此不进行数据中继。计算机间采用数据中继的第一个应用是电子邮件。

制定标准旨在让网络上不同种类设备实现通信。

下一层为上一层提供服务，由某一层提供的服务称为服务访问点SAP，指定了N如何与N-1进行通信。

同层之间的通信依靠协议(一种规则)，通过下层提供的服务与同层进行通信。功能由同层间实体提供。

协议数据单元PDU是上层数据与协议或控制信息的组合。

层提供的基本功能(协议提供的基本功能)

**分段与重组**：分段时要将重组的指令放在头部，指明数据包数目以及数据相对位置等。

**封装**：将控制信息添加到数据包的头部，通常包含地址、检错码、协议控制信息等。

**连接控制**：面向连接：传输实体间要先建立逻辑连接(根据数据包头部进行确定)，三个阶段：请求/连接阶段、数据传输阶段、终止阶段。无连接：不需要事先协调，数据包之间独立，传递是无序的。

**顺序递交（有序交付）**：数据传输是无连接协议传递的，要向头部添加控制信息对数据包编号，使得接收方按序重组。

**流控制**：确保传输层不会导致接收层溢出，在大多数面向连接的协议中采用。

**差错控制**：恢复丢失或损坏的协议数据单元，三种机制：积极确认、超时重传、错误检测。

**复用**：上行多路复用：多个上层数据包共享同一下层连接。下行多路复用：一个上层连接多个下层（不常见）要在头部包含地址指出上一层识别号（寻址来实现）。

## ISO/OSI七层模型

并非所有设备都需要每一层的支撑。

**物理层**

实现系统间比特流的透明传输，点对点或多点。要为数据链路层提供识别端点的方法。

全双工与半双工、可串行或并行、按数据链路层的传输顺序传输bit。

**数据链路层**

屏蔽上层不受传输介质的影响，为上层提供无错误的可靠传输。

帧即网络层的数据单元与数据链路层协议信息集合，提供识别帧开始和结束的方法。

**网络层**

将传输层提交的所有数据传输到网络中的任何地方（透明传输），ip协议。

处理数据包的路由，可以是路由器的最高层。

**传输层**

两个会话实体间的透明传输，不关心下层拓扑结构。

可能提供额外服务，流量控制、差错控制。

**会话层**

并不关心网络，协调表示层之间的会话，把表示层的数据传给传输层。

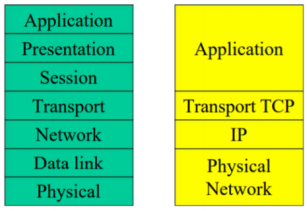
**表示层**

把数据转换成对等层可以翻译的普通格式。

**应用层**

提供一般服务和特定服务：telnet、web等，为应用程序访问OSI堆栈提供方式。

用户针对上三层，操作系统针对下四层。




分层模型如今不能满足一些服务需求，有些服务需要访问每一层，从而引入了不分层体系结构：但这也带来了安全隐患。

# 一.网络协议

**开放协议**：结果多轮讨论其健壮性更好缺陷小。大多数协议是为了实现特定功能而不考虑安全需求，开放使得更容易发现安全缺陷。

**专利协议**：多家提供商要合作显得不切实际，因为很难发现缺陷容易被攻击者利用。

**协议规范**：英文描述（可能导致解释不同）、实施过程中存在缺陷。

**协议规定**：提供的服务（本层SAP），请求的服务（下一SAP）、提供的功能、协议格式报文格式（数据包格式，头部含义）、数据包时序。

协议填写RFC（请求评议申请表）以得到广泛使用。

基带是用于网络通信的软件，接收无线电信号、解码消息、发送响应或更新状态

**寻址**

首先把信息送到发送人的互联网服务提供商ISP，再路由。

以tcp/ip分层

**物理网络层**：地址用于识别物理网络中的设备，硬件地址允许网络接口过滤目标不是本计算机的流量减少处理要求。（可能有另外一个地址决定哪个网络层协议处理数据包）

**网络层**：需要一个地址唯一识别大网络（互联网）中的计算机（全局识别设备），还有一个地址识别所使用的传输层协议。

**传输层（TCP）：**使用端口号识别运行的程序。

**应用层**：应用程序用户地址识别应用程序中的项。

地址静态分配：系统配置或内置，动态分配：协议层提出请求、地址服务器分配。

硬件地址由供应商分配给网络适配器，将硬件地址视为过滤器，可以被更改（危险）。

ip地址：由ip地址授权机构分配保证全局唯一，DHCP动态分配或静态分配，也可以被修改。

端口号的分配更缺少控制，有熟知的端口号，或基于配置，或基于用户输入。

主机名（域名），政治或商业驱动，注册官方机构分配，由DNS与ip对应。

**头部**

头部由两部分组成：固定的数据包类型:容易解析，功能有限。

可选类型（freedom type）：更难解析，容易扩展。

固定部分包含地址（协议层地址和载荷类型）、控制数据、头部数据。

可选部分包含扩充的固定数据、可选控制数据、可选的载荷控制数据。

无限制头部：常出现在应用层，数据流为bit串而非数据包，分析比较复杂、但并非完全无限制。

# 二.网络

**互联网：**

互联网：通过网络协议将不同设备互连在一起的设备集合。

部分互联设备运行应用程序，与用户通过接口交互；部分用于设备与网络的连接。

一个ISP由一组互连设备组成，可以理解为互联网是由互连的ISP组成。

**寻址：**

基本过程：

**基本过程**

从用户和应用角度看：用户给应用提供目标计算机地址、目标应用地址、目标用户。

应用提供上面三个+源应用、源用户（便于数据发回）。

应用和用户要向TCP层提供目标端口号、目标ip地址、用户数据，TCP层再提供源端口号、将上述及tcp控制信息一并作为载荷发给IP层，IP层提供传输协议类型、源ip地址、目标硬件地址（下一个路由器），物理层再最后追加其源mac地址。

路由器收到不关心传输层和应用层，物理网络层先检查网络层协议类型，若是ip数据包就剥去头部传给网络层，由其检查源和目标ip地址决定下一跳，添加新的源和目标MAC地址。

互联网上4个标识（源目的ip，源目的应用端口号）组成全球唯一识别标志，唯一的识别每个方向上数据包。

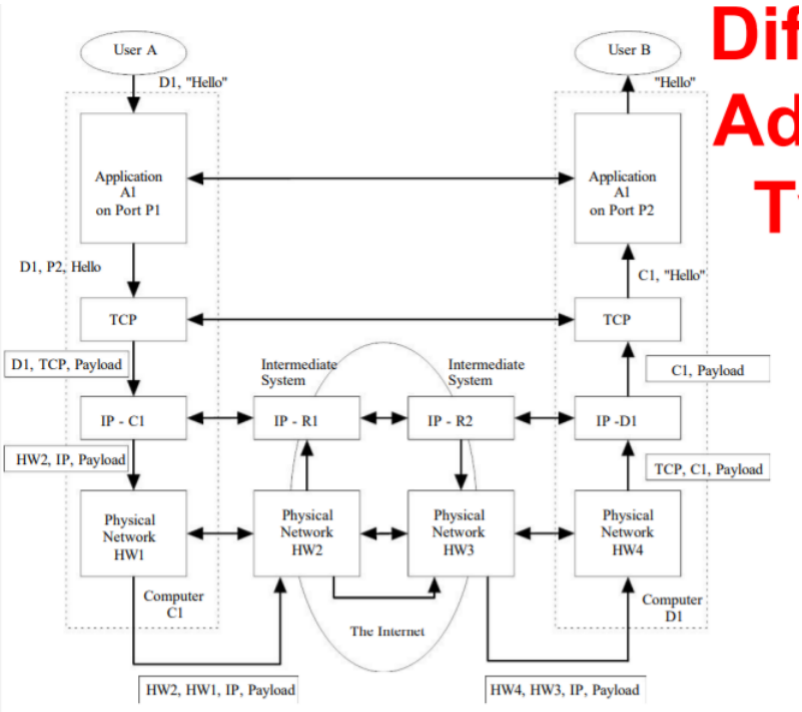



表 3.1　互联网地址

| 地　址 | | 用　户 | 应　用 | TCP | IP | 网络 |
|---|---|---|---|---|---|---|
| 用户或文件 | SRC | X | X | | | |
| | DST | X | | | | |
| 计算机地址 | SRC | | | | X | |
| | DST | X | | | | |
| 应用 ID(端口)号 | SRC | | | X | | |
| | DST | X | X | | | |
| 传输协议 | | | | | X | |
| IP 地址 | SRC | | | | X | |
| | DST | X | X | | | |
| 网络层协议 ID | | | | | X | |
| 硬件地址 | SRC | | | | | X |
| | DST | | | | X | |

用户和应用向TCP层提供：目的端口、目的IP、用户数据；

TCP提供：源端口号；

IP层提供：传输协议类型、源IP地址、目标硬件地址（下一跳路由器）；

物理层：追加源硬件地址。

路由器不关心传输层和应用层，物理网络层先检查网络层协议类型，若是IP数据包就剥去头部传给网络层，由其检查源和目标IP地址决定下一跳，添加新的源和目标MAC地址。

互联网上**4个标识**可唯一识别每个方向上数据包。

**地址欺骗**

域名服务：分布式服务器集合，域名到IP转换。

网络掩码：指定IP地址哪一部分表示网络。

针对上述过程，欺骗就是改变地址的能力，思考谁能看（嗅探）到流量。

地址欺骗即数据包源地址改变成不属于发送数据包的设备的值（虚假的源地址）。

ip地址由网络和主机组成。

连接服务器和应用时主要使用主机全名（主机名+域名）vulcan.dougj.net中vulcan为主机名，dougj.net为域名，主机在域内是唯一的。

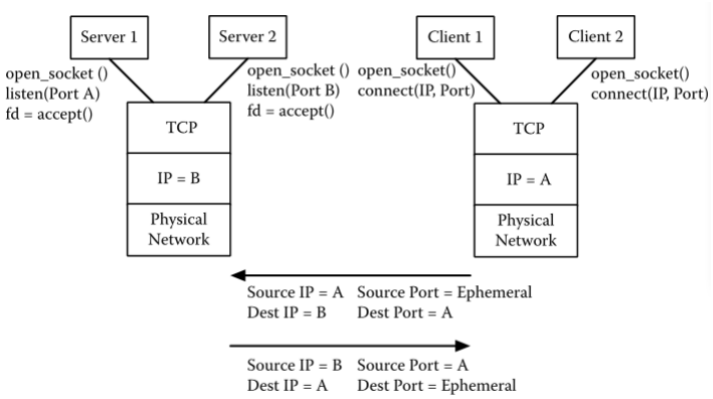
域名到ip的转换使用DNS分布式应用实现，先问本地DNS服务器，没有再问根域名服务器-顶级域名服务器-。

**CS模式**

等待另一个应用请求连接的应用程序为服务器（通常在熟知端口号上等待客户端连接）。

服务器应用程序要求操作系统打开一个到tcp层的套接字（ip+端口号，用于应用程序与os连接），再侦听发送到侦听端口号上的连接请求（80是侦听端口号）。

客户端也要向OS申请一个套接字，端口号可以让os选择（临时端口号）。




每个服务器各打开一个套接字并监听端口，客户端连接服务器时调用accept函数返回新套接字描述符<连接标识符>（即相当于客户端的套接字，当然也继承了服务端的套接字，两者组成四元组代表唯一的连接）此时创建一个新进程与该客户端连接，原进程继续监听等待新连接。

服务端的一个套接字是可以建立多个连接的，只有四元组才是全网唯一的。

默认端口号与监听端口号相同，但其是服务器应用程序的默认端口号，与服务器交互的所有客户机应用程序都知道该端口号。例如，端口80是web的默认端口。(。。。)

**路由**

早期网路在源和目的之间先建立路由，属于面向连接的，数据按序到达。因特网是无连接的，数据包分别处理。

静态路由（系统配置时构建，适于小型网络和仅一个出口的网络）和动态路由（会根据网络参数调整），对于只有一条路径，不会从动态路由中获益。

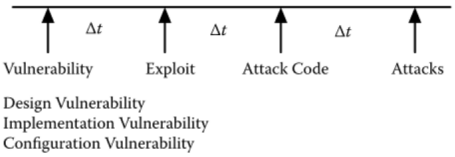
对于路由表，查看数据包的可能目的地，其有网络地址表示，该地址由ip和子网掩码组成。

默认路由：目的地址与路由表中任何一个目的地址都不匹配时采用的路由。

# 三.网络漏洞分类

**威胁模型**

每层的载荷都不是由该层分析处理，而是直接传给下一层。




漏洞可以出现在设计（往往不容易在协议本身得到缓解，可能只是设计忽略了安全性）、实现（代码错误，规范解释错误等，难发现但易修复）、配置（用户本身不正确的配置，如使用默认设置）过程中。

漏洞存在到发现的时间可能很长，漏洞挖掘到攻击代码的时间为0。

零日攻击：漏洞发掘和攻击代码已经在使用后，才被广泛认识到。风险评估：决定某件事有多重要以及将如何努力保护它的过程。其理念是：不是每个设备都需要在相同的级别上得到保护。

威胁：设备或应用程序受到攻击的可能性的度量。难度量，取决于考虑的攻击类型。

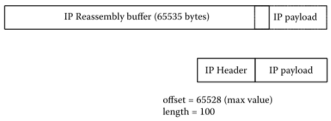
影响：安全漏洞对组织的总体影响。

**分类**

**基于头部的漏洞与攻击**（被发现易于处理，但难于如何发现）：

漏洞：头部违反标准（如无效值导致无效头部）攻击的后果通常取决于实现。协议的不同实现将以不同的方式处理这些头违规。

攻击：例如死亡之ping




重组缓冲区最大65535字节，发送相对值为65528（最大值）的包且长度大于7的数据包，其被放到重组缓冲区，从而溢出缓冲区尾部。

**基于协议的漏洞和攻击**

数据包都是有效的，但与协议执行过程冲突。

攻击：不按序发送数据包（最好丢弃）、发送报文过快或过慢（很难进行）、未发送数据包（相当于丢失了数据包很难处理，因为不知道要等待多长时间）

常见针对tcp开放连接协议的攻击——SYN泛洪攻击

在三次握手中客户端发送数据包请求连接，服务器会响应数据包以表示接收连接，此时会为其分配内存以维持连接。

attacker发送大量的SYN包到不确认，直至服务器缓冲区被完全分配。

**基于验证的漏洞和攻击**

欺骗其实就是对认证的的攻击。

用户到用户的认证：依赖于密钥、证书等，用户可能还需要向应用、主机、协议层认证：用户名和密码。上述两种在传输过程中也有风险。

层与层之间的认证：两个程序、两个主机、两个网络层之间实际是主机到主机的验证，依赖ip地址、mac地址。

**基于流量的漏洞和攻击**

流量过多或attacker能截取流量获得信息。

大量数据被送到某层导致无法及时处理，就丢弃或不处理。例如向远程网络发送广播包，一个包就能得到整个网络的n个回应，造成瘫痪。

数据包嗅探，捕获网络上的流量，漏洞取决于协议。

上述四种有重合，如果破坏身份验证的目标是使用其他三种方法中的一种来实现的，那么它就不被归类为基于身份验证的攻击。

# 四.物理层

物理网络层在最底层，用于到网络的连接，核心是一个网络访问控制器（硬件如网卡）。

该层分硬件部分和软件部分，硬件部分负责将转换字节数据到比特位到物理介质上的信号，软件部分为上一层提供服务、维护缓冲区等待发送和接收的数据包。

**常见攻击**

**硬件地址欺骗**

目标知道发送者的什么，发送者知道目标的什么：只能确定最后发送数据包的设备在同一网络上在大多数局域网中，网络上的所有设备都可以接收到发送到其他设备的报文，这些设备使用目的地址过滤掉不需要的报文。（交换机不行）。

可以伪造源mac地址绕过检查，但真假同时存在可能导致网络故障。

伪造目的mac地址，若是别的网络的则是无效的。

**网络嗅探**

网络访问控制器忽略目标地址并读取它收到的每一个包。

流量进入ISP不需要担心嗅探问题，包嗅探最常见的是无线网。

**物理攻击**

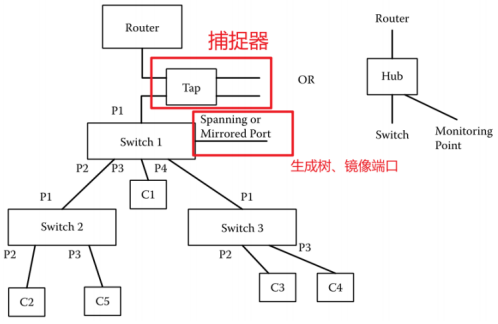
。。。

**有线网络协议**

**以太网协议**作为局域网的主导协议，设计很简单，主要为了提供对共享介质的访问，并使连接到同一共享媒介的所有设备具有同等的访问权限。

有线使用CSMA/CD，先听后说，冲突只发生在共享介质中，不会通过路由器等网络设备传播（冲突域）。问题：连接的设备增加，碰撞的可能性就会增加。

总线、集线器都一个意思，易受到嗅探攻击。交换机按端口转发，提高了以太网网络的性能，因为碰撞(当两个或多个设备试图同时通话时)减少了，并且流量只发送到需要它的设备。以太网交换机还允许同时传输和接收数据，这被称为**全双工**。




针对交换机情况下管理员要监控流量的方法：①生成树/镜像端口，存在速度问题②带交换机的集线器，但集线器是半双工低速率的③网络捕捉器，看不到整个流量。

以太网帧中mac地址（6字节）：单播地址、多播地址（仅在目的地址）、广播地址（FF:FF:FF:FF:FF:FF）。

mac地址前三字节分配给硬件提供商，后三字节由提供商分配。硬件地址存于网卡的只读存储器中在系统启动时由软件复制到控制器，因此可以通过软件修改。

**基于头部攻击**：。。。没啥

**基于协议攻击**：。。。没啥

**基于验证攻击**：重点放在源和目的mac地址。攻击者使设备相信目的mac地址就是攻击者的mac地址，例如伪装成路由器。

ARP中毒（arp地址解析协议）：attacker骗D1自己是R2，再骗R2自己是D1，从而让流量先流经自己。

NAC网络访问控制，使用源mac地址验证发送方。也用于认证与ISP相连的设备，防止有未向ISP付费的设备，但大多数路由器可以改变源地址。

attacker发送带不同源地址的数据包，欺骗交换机是其它设备的数据包，从而改变交换机的地址转换表。交换机要么两个相同mac地址都发，要么发给mac最后出现的端口。

attacker将自己的mac设置为其它设备的mac，这不算一个有效的攻击但可以是另一设备无法工作。

**只有attacker能访问网络上的某设备时才有效，不然难以实现！**

**基于流量攻击**：

主要是流量嗅探（将硬件控制器设置为混杂模式），但是用交换机可以是影响降低（针对攻击方法见上），或者用vlan虚拟局域网、或者用加密来减少影响（有线以太网层不常见，主要是上层和无线）。

再者是用大量流量使网络崩溃，使网络发送的真实流量减少。例如发送大量广播包，所有设备都会收到并不得不处理它们。不好缓解，只要能访问某一设备就可以攻击。

**无线网络协议**

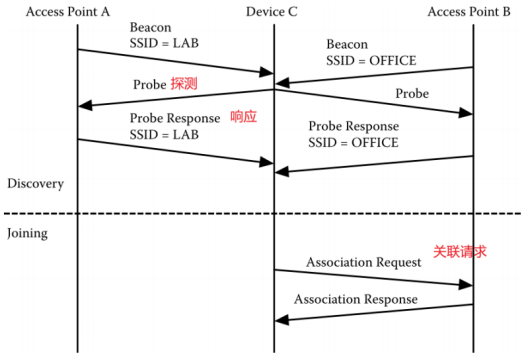
最常见的无线协议是以太网协议，常用的2.4 GHz的协议也是移动电话的常用协议，所以会产生冲突。

信号强度上的变化也会引起安全问题，网络嗅探是无线网络中最大的安全漏洞。

与有线以太网不同，有线以太网中每个设备都实现相同的协议，没有设备是特殊的。无线以太网需要有一个负责网络的设备。这个设备被称为**访问接入点(AP)**，它有两个主要功能。第一个是创建无线网络并帮助管理对网络的访问。第二是提供对有线网络的访问。

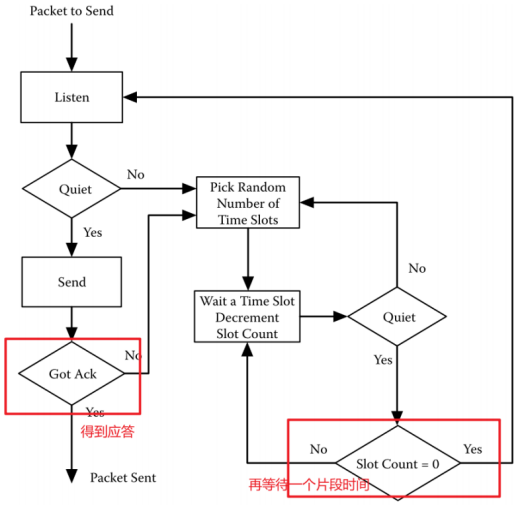
**发现**：访问点广播其SSID（信号指示），设备监听服务集标识SSID或已知的SSID，向其发送探测包，访问点响应探测包。通过上述过程建立了可用接入点列表。

**接入**：选择一个接入点，发送加入网络的请求（关联请求包），接入点恢复关联请求响应包。



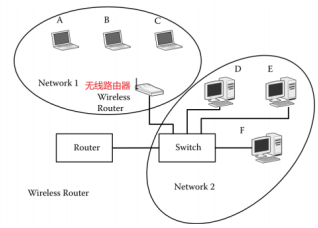

最后用以太网协议在两者之间发送流量，使用CSMA/CA（除了没有碰撞检测与CSMA/CD差不多）

但在无线环境下，它将等待一个确认数据包。如果收到确认报文，表示设备已经成功发送了确认报文。




当媒体空闲时，设备将等待额外的时间。这就避免了一旦设备空闲，所有设备都请求传输。

常见的是无线路由器作为访问接入点，从而成为一个独立的网络，起到了很好的隔离。




无线以太网帧格式

**基于头部攻击**：在帧中设置值欺骗无线设备，是设备失去与接入点关联，无法访问网络。

**基于协议攻击**：利用计算机和软件探测广播SSID的接入点，并绘制出它们的位置。没有什么必要防护，但可以用加密或NAC，使得attacker要想使用接入点需要加密机制或身份验证，转化为了基于验证的攻击。

对CSMA/CA攻击，例如发送大量信号使得无法接收应答信号，设备无法对网络连续访问。

**基于验证攻击**：

设备验证：无限设备验证访问接入点是否有效，接入点对设备身份验证（有可能对设备的用户）。

访问接入点配置验证：获得访问接入点配置菜单的权限（禁用或修改安全属性）。

恶意访问接入点：有效用户将接入点连接到组织内部网络，可能会使attacker能够访问内部网络，也可能使用户绕过一些内部安全方法如NAC，削弱整体安全。不太好防护，可以阻止未经授权用户访问有线网络，或寻找SSID广播，嗅探无限流量等。

非法访问接入点：attacker安装假接入点，伪装成组织中的有效接入点，用户接入假的接入点，流量被捕获（第一需要attacker已经能够安全访问网络，第二未采用无线加密）。

接入点配置验证：对接入点控制软件的访问权（修改默认密码）。

**基于流量攻击**：

无线以太网的网络控制器可以配置成混杂模式，捕获到所有流量——**加密机制**

WEP有线等效保密协议：无线设备先发送用共享密钥加密的消息来证明自己，再发送关联请求。（通常同一点的设备共用一个密钥）流量用共享密钥加密。

WPA（Wi-Fi访问保护协议）共享一个密码只用于身份认证。无线设备和接入点先建立关联，再发送共享密码的hash以通过验证，之后协商一个会话密钥用于通信。

以上是针对家庭的WPA，针对企业，接入点起初不提供对公司网络的访问，如果无线设备用户被授权使用网络，那么无线设备和接入点协商一个会话加密密钥。

**对策**

更多的是上层协议的措施，在此只讨论减少嗅探和身份认证攻击的对策

**虚拟局域网VLAN**：在物理网络中创建逻辑网络。D2和D1通信必须经过路由器。

静态VLAN基于交换机端口分配（防止了ARP中毒，交换机端口映射表被攻击，但只是分成了小份的网络，每个网络还是存在安全问题），动态VLAN基于设备硬件地址分配（隔离了位置的设备，但地址可修改）。

把接入点放置在一个或多个vlan中，就可以强迫无线流量通过它自己的路由器和任何其他安全设备。

**网络访问控制NAC**：NAC根据用户和设备的认证结果，决定设备的接入权限。NAC环境通常使用动态vlan来强制执行策略，根据策略对设备进行隔离。

# 五.网络层

## 基于头部攻击：

其他字段无效会使数据包被拒绝，主要是长度、标志和偏移字段。

ip头部的字段可分为：

**端点字段**（源端和目的端使用的字段，在传递过程中不进行检测，包括长度、id、标志、偏移量、协议和源IP地址），死亡之ping等。

**传递字段**（路由器检查并可能修改的字段，针对该字段的攻击通常会被路由器丢弃）。

## 基于协议攻击：

针对ip和icmp协议的攻击主要瞄向数据包路由traceroute可被认为是一种基于协议的攻击，跟踪路由。

icmp协议：攻击者若能嗅探到路径上的流量，则能根据ip包创建icmp错误信息从而导致拒绝服务或重定向等。

arp协议：attacker要在真正的arp响应前做出响应（有些主机探测到冲突并标记警告），要么无效的硬件地址被放到缓存中使得无法 联系，要么错误的地址导致发给错误的主机（arp投毒，最好归为认证的攻击）。

## 基于认证攻击：

**ip地址欺骗：**

例如发送icmp回应请求数据包，A会给B响应，attacker可以发送大量的包。或发送一个广播包，则所有计算机都会向B发送响应。（可以让路由器不允许内部广播或不允许一些icmp包进入）。

ip地址欺骗不能盗取另一个设备的身份。

**ip会话欺骗：**需要attacker和受害者在同一网络，通常使用arp欺骗路由器。

路由器被配置检查与它直连的网络发往外部的包源ip与对应网络不匹配的情况，但无法阻止同一网络内冒用ip的情况。

### 基于流量的攻击：

骨干网络是受到物理保护的，因此嗅探骨干网非常困难。

从嗅探的角度加密可以放置其他人看到数据，但加密也是对流量的监控变得不可能（如果数据含有不应该流出的机密资料）。

大量的流量会导致服务器或主机崩溃，有些设备会根据流量特征减少进入的流量（大多工作在传输层）。

使用ip广播地址的雪崩攻击。

远程的arp广播雪崩：向目标网络的每个地址发送数据包，路由器发送大量arp请求（大多没有响应），并且每个请求会尝试4次。则每次远程扫描会产生大量广播包，若多台设备同时扫描。

**对策**：路由器或其他网络设备可以限制进入网络的数据包数量，但合法的流量会受到影响。

## 引导协议BOOTP

一种老的动态ip地址分配协议，用UDP，目的ip和目的mac都是广播，响应数据包依据请求数据包的mac地址发送，目的ip为广播。

基于请求ip地址设备的硬件地址，每次都将同一ip分配给同一设备，可以使用BOOTP中继克服同一网络的局限。

因为是广播包，attacker也可以做出响应，但必须在同一网络。

## DHCP

BOOTP协议需要配置并知道所有设备的硬件地址。该协议不适用于移动设备或不断添加和删除设备的网络。

静态池：同BOOTP依据mac分配。

动态池：分配给未知设备，有租期需要续约。

客户端广播DHCP查找数据包，发送6个都没响应就放弃。响应中包含IP和租期。客户端收到响应发送请求报文，服务器发送ACK用了一半时发送请求租期更新。

**基于头部攻击**：无

**基于协议攻击**：

用大量虚假的mac地址发送查找数据包消耗掉动态池中的ip（服务器每收到一个都会保留一个ip），attacker也可以回答并接受ip（Dos）。

向服务器发送释放数据包，导致相同的ip地址被分给多台计算机，如果不能嗅探之前的发现和响应数据包，就每个ip都释放一次。

**基于验证攻击**：

如果担心将地址分配给未授权的客户，那么典型的解决方案是使用网络访问控制伪装成服务器发送虚假消息，可能分配一个无效的地址使其无法通信（非法DHCP服务器）。

**基于流量攻击**：可以发送大量请求，不是重点。

# 对策

# IP过滤

通常路由器完成，过滤条件为ip地址、端口号、协议类型。

设置黑名单：例如可以阻止传入的icmp请求响应，这无疑增加了每个包的处理时间，就算只允许一个端口号因为端口号由发送方设置，故阻塞并不完美。

基于IP地址的过滤由于攻击者一直在转移，黑名单永远是过时的。

IP过滤做第一道防线，但不能取代防火墙等。

# NAT

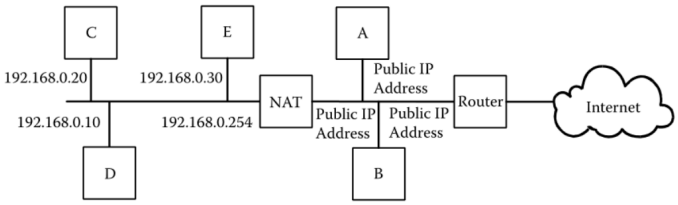
**静态**：外部地址和内部地址一对一映射。

**动态**：内部设备多于公共IP地址。

对于私有设备NAT相当于路由器，对于互联网NAT相当于最终的目的地址。

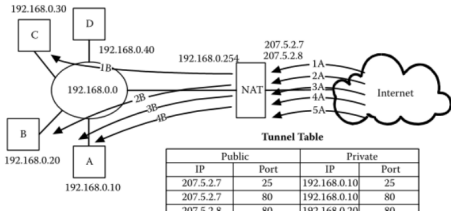
NAT并非出于安全目的，但其提供了安全性。它会阻塞所有不在映射表中的入站数据包，攻击者无法向私网发送数据包。

而对于私网中存在服务器需要访问的情况：一种是把服务器放到公网上（非军事区）。




如果想访问私有主机就建立隧道，一个公共IP地址和端口号映射到一个私有IP地址和端口号。当报文从一个已隧道化的端口到达NAT时，NAT将接收到的报文，改写IP地址和端口号，并根据隧道表中的值将报文发送给私网中的计算机。

**隧道局限**：若公共IP地址和端口连接到多个私有计算机，每个公共IP地址和端口号只能与1个私有设备组合。

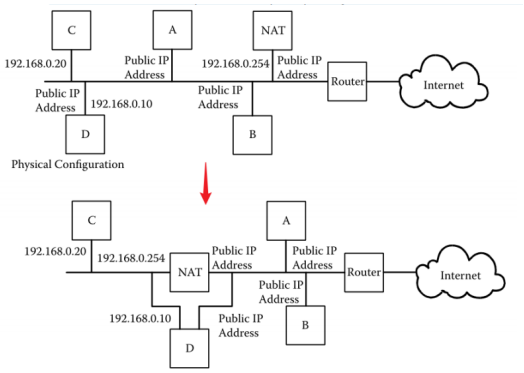



**Tunnel Table**

| Public | | Private | |
|---|---|---|---|
| IP | Port | IP | Port |
| 207.5.2.7 | 25 | 192.168.0.10 | 25 |
| 207.5.2.7 | 80 | 192.168.0.10 | 80 |
| 207.5.2.8 | 80 | 192.168.0.20 | 80 |
| 207.5.2.8 | 100 | 192.168.0.30 | 80 |

| Packet | IP | | Ports | |
|---|---|---|---|---|
| | SRC | DST | SRC | DST |
| 1A | Internet | 207.5.2.8 | 8357 | 100 |
| 1B | Internet | 192.168.0.30 | 8357 | 80 |
| 2A | Internet | 207.5.2.8 | 7384 | 80 |
| 2B | Internet | 192.168.0.20 | 7384 | 80 |
| 3A | Internet | 207.5.2.7 | 2345 | 80 |
| 3B | Internet | 192.168.0.10 | 2345 | 80 |
| 4A | Internet | 207.5.2.7 | 2554 | 25 |
| 4B | Internet | 192.168.0.10 | 2554 | 25 |
| 5A | Internet | 207.5.2.7 | 6623 | 22 |

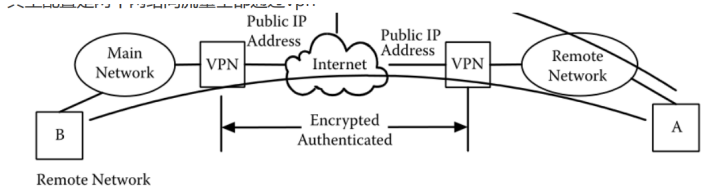
**特殊配置:**既可以有私有IP也可有公网IP（pass-by，不是很安全，降低了安全性）。

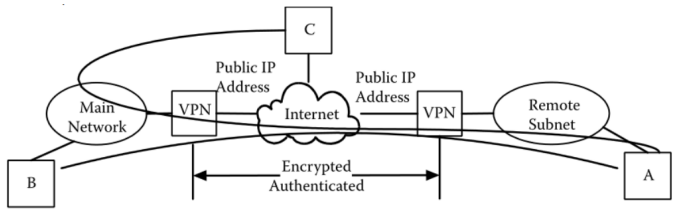



# 虚拟专用网VPN

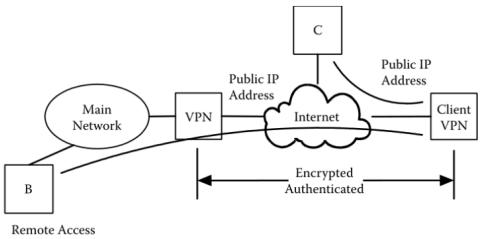
**IP层VPN可分为三类:**网络到网络、客户端到客户端和客户端到网络。

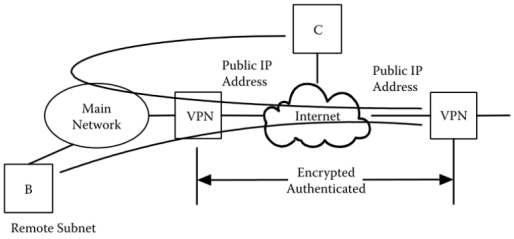
**网络到网络VPN：**典型配置是两个网络间流量全部通过vpn，或者通过vpn成为主网络的一部分。




**客户端到网络的vpn：**所有到主网络的通过vpn，其他的通过互联网，也可以全部流量通过互联网。

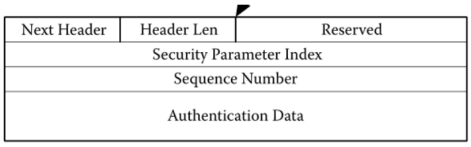



vpn可以避免嗅探和验证，可以只允许vpn流量通过从而只让通过验证的设备访问网络。

# IPSEC

网际协议，完全为ipv6开发的协议，可用作vpn。




第一部分作为一个扩展头部，**验证**数据未被改动（将数据包哈希，再用密钥加密）。

第二种扩展头部支持载荷**加密和身份验证**：esp头部+载荷+esp尾部+验证数据，载荷和esp尾部通过密钥加密，验证数据为前三者的hash。

加密协议为ESP（**封装安全载荷**）。

IPSEC可以缓解嗅探和认证攻击，但是**分发密钥**是一个问题。

# 六.传输层

## TCP

用端口号来区分数据包，实现多路复用。有些过滤器只允许固定端口的流量进入，但前提是只有对应的应用使用端口。

面向连接的，分连接建立（三次握手）、连接维护、连接终止（通过数据包交换来友好终止FIN，会等待数据全部传输完毕。也可以发送一个数据包来强行终止RST，可能数据会丢失）。

提供可靠的数据传输，有流量控制。

### 基于头部攻击

攻击者发送无效头部扰乱tcp运行，最常见的是攻击标志字段，创建标准中未指定的标志组合（过去os会因此断开连接，现在不会了），也有在已建立的连接中发送无效序列号，会中断单个连接。

**探测攻击：**利用特征列表（如某无效标志组合对某些操作系统响应是唯一的，也可以利用初始序列号、开始窗口的大小）。因为标准没有规定头部值所有的组合。

### 基于协议攻击

**端点协议攻击：**

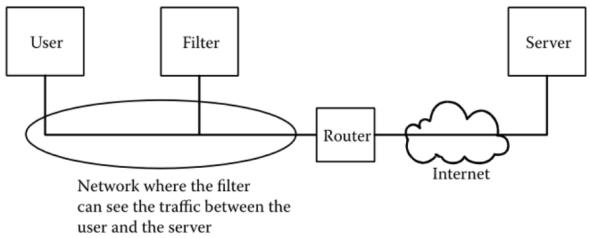
发送超出序列的数据包（只会终断当前连接，也可以用来确定os类型例如向等待连接的端口发送RST）或不完成握手（SYN洪泛攻击，可在网络入口处安装相应的过滤器，但分布式的就不好解决）。

嗅探流量，将数据包插入tcp流中，例如插入RST来关闭连接。直到最近TCP实现才检查RST报文中的序列号和确认号，需要嗅探流量。

如果攻击者同时将源硬件地址设置为受害者或路由器，那么就不可能确定是哪个设备在实施攻击。（加密可以）

**会话劫持：**

从两方中的一方窃取连接伪装成一方设备。攻击者将源IP地址设置为服务器的IP地址，将目的IP地址设置为攻击者的IP地址，伪装服务器向攻击者发送复位报文。攻击者使用在嗅探的序列号向服务器发送数据，服务器用自己的数据响应。攻击者需要继续嗅探流量，以获得发送给受害者的数据。受害者仍然接收流量但由于连接已经关闭它没有响应。 **（对策：TCP加密技术）**




**被动网络过滤器：**用于阻止不希望的连接，监视（流量不会通过，从而不影响网络瓶颈）网络流量，当发现应该被阻止的连接时，使用会话劫持或RST数据包来终止连接。

**流量整形器：**旨在减少低优先级应用程序之间的通信量，置于流量经过处，调整窗口大小。

### 基于验证攻击

基于网络的安全设备不能依赖端口号来验证应用程序流量。

### 基于流量攻击

泛洪的攻击，如前面的SYN泛洪攻击，可以使用流量整形器等QOS（服务质量）设备。

## UDP

无连接的传输层，端口号实现多路复用。tcp基于数据流、udp基于数据包。

没有针对头部的攻击，没有协议故无针对协议的攻击。

**基于验证攻击：**同tcp，通常会过滤除53（DNS）端口的所有udp流量。

**基于流量攻击：**嗅探（加密可以解决，应用完成）。

## 域名服务DNS

域名转ip地址，DNS处理两种域名：

**FQDN全限定域名：**完整的主机名+域名。

**PQDN部分限定域名：**FQDN的一部分，通常引用同一域中的设备顶级域名com、cn等。

DNS使用UDP53端口号。

**两种DNS工作模式：**递归和迭代。

**递归优点：**每个服务器都可以缓存回复，缺点：所以请求都经过根服务器。

**迭代：**数据包总数相同，每个服务器只收发一个包。

**基于头部攻击**：头部值不正确会被丢弃，很少能攻击。用DNS包不被防火墙检测从而泄露数据缓慢不是很有效。

**基于协议攻击**：使用DNS端口号与防火墙外的另一个非法应用程序通信。

**基于验证攻击**：只对服务器ip地址进行认证，attacker可以替换DNS服务器中的条目（入侵该服务器，或当其向另一服务器查询时发送伪造的响应，使错误条目存入缓存中），或伪造响应数据包（类似于DNS缓存中毒攻击）。

**基于流量攻击**：UDP接收缓冲区填满将只是丢弃数据包。不会造成太大的损害，因为一定时间内没有得到响应DNS客户端将重试几次。对DNS进行冗余设置。

**对策**

传输层安全性由较低层或应用程序提供。

传输层安全(transport layer security, TLS)或安全套接字层(Secure Sockets layer, SSL)

**TLS**：是应用程序和tcp间的一个单独层，旨在减轻嗅探和基于主机的身份验证攻击。

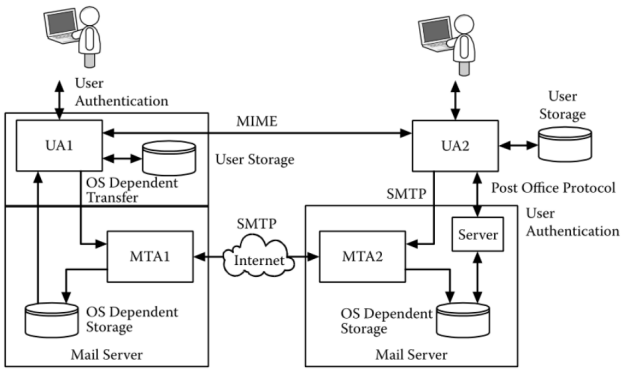
对服务器和客户端进行身份验证，通过后客户端和服务器创建一个加密密钥对通信进行加密。

**四个阶段：**①客户机和服务器同意使用加密和身份验证方法。②服务器提供其证书，并选择性地向客户端请求证书。③客户端提交其证书的阶段。④客户机和服务器交换会话加密密钥加密之间的所有数据。

**唯一有效攻击：**中间人攻击，只能在客户端不知道服务器的情况下伪装成有效服务器。减少验证和嗅探。

# 七.电子邮件

电子邮件服务器用于将发送的电子邮件发送到下一个服务器，并接收和存储发送给用户的入站电子邮件。



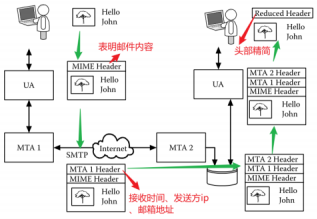

MAT消息传输代理用于存储转发电子邮件的服务器，通过简单邮件传输协议SMTP进行通信（tcp），MTA不相互认证。

UA用户代理，与用户交互的应用程序。UA可以是本地的（上左图，UA和MAT在一台计算机上，交互依赖OS）或远程的（上右图，用SMTP发送发送出站电子邮件信息，使用POP或IMAP等协议从服务器获取电子邮件）。

本地UA由本地计算机对用户做身份认证，远程UA在用户检索邮件前进行认证。出站的email都不进行认证。

MIME多用途互联网邮件扩展协议：MTA不关心邮件内容，MIME负责告诉UA如何编码数据以及电子邮件消息中数据的类型（attacker可以用MIME将病毒、蠕虫等直接发给用户）。

电子邮件消息由消息头和消息体组成。




**SMTP**

邮件服务器监听25端口号，tcp流，电子邮件信息为7位ASCII格式。

SMTP是命令-回应协议，一方发命令，另一方做出响应。

**基于头部攻击**：早期的SMTP存在缓冲区溢出，命令和响应只有固定的缓冲区大小。现在基本已被修补

**基于协议攻击**：消息的时间和顺序是受控的，任何违反都被忽略。

**基于验证攻击**：SMTP缺乏认证——电子邮件欺骗

因为没有过程验证发送者，唯一操作是通过DNS验证域是否有效，例如john.iseage.org则MTA会验证iseage.org的有效性但不会验证john是否在域中。

电子邮件地址欺骗：发垃圾邮件和恶意电子邮件。例如设置返回地址，当接收者地址无效时会见邮件返回发送者（受害者），发大量填满其存储空间。

电子邮件中继？？？

用户名探测，RCPT TO不存在会返回错误，易实施但少安全隐患。

**基于流量攻击**：大量消息消耗磁盘空间，但随着磁盘空间增加。。

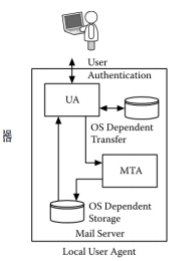
嗅探：SMTP协议不进行加密，attacker可以读取电子邮件消息

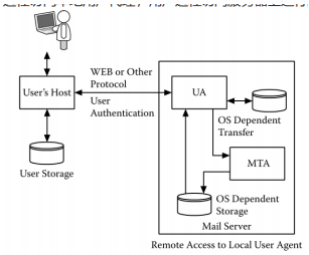
**对策**

基于身份验证的对策以提高安全性，STARTTLS命令（协商TLS参数，向MTA发送经验证和加密的邮件）和AUTH命令（对连接到MTA的用户进行身份验证）。

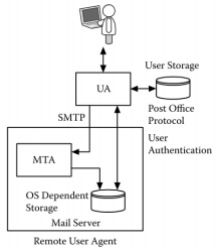
安全应由UA来处理，SMTP保留不验证

**POP和IMAP**

本地用户代理，用户通过账户登录服务器。 




远程访问本地用户代理，用户远程访问服务器上运行的用户代理（web电子邮件）。



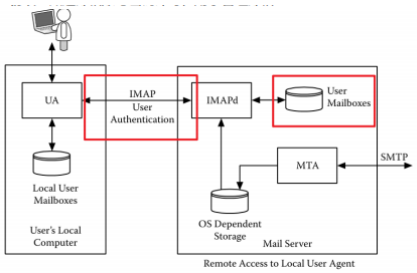

远程用户代理，用户代理远离邮件服务器，**两种协议**用于支持远程用户代理访问电子邮件。

**POP(3)协议**：用户通过服务器进行身份验证，提供了预览电子邮件和有限管理远程电子邮件的能力。使用TCP将UA与MTA连接。

也是命令-响应协议。

用户名和密码发送到服务器时没有进行加密。如果用户名不正确，大多数POP3服务器仍然会提示输入密码，从而不让攻击者知道他或她是否猜到了有效的用户名。

POP3协议的设计是为了方便从服务器向客户端传输电子邮件消息,不是为了将电子邮件保存在服务器上而设计的，针对多设备同不问题。**IMAP协议**：知道邮箱账号密码即可，用于管理邮箱。




没有基于头部和协议的攻击

**基于验证攻击**：对账号密码进行爆破攻击因为对尝试次数无限制（要修改默认密码，限制用户登录的ip范围是不实际的）。

通过VPN软件，限制POP和IMAP协议只在组织的网络内运行。

只允许用web客户端访问。

**基于流量攻击**：

POP和IMAP最大的问题是用户名和密码以明文传输，攻击者可能会捕获用户名和密码（加密PKI没有被广泛使用，最新的使用TLS）。

**MIME**

对电子邮件消息进行格式化。随着发展需要设计一种协议让用户代理可以用来交换非ascii数据。

接收UA将使用MIME报头来解释消息的每个部分。

三个规定头部（MIME版本、内容类型、内容传输编码类型）+三个可选头部（内容id、内容描述、内容配置）

**基于头部攻击**：

无效的头部会被UA处理。

利用头部隐藏消息的实际内容，attacker生成一个电子邮件宣称有图片附件实际是可执行代码。

邮件信息可以包含到网页的超链接。用户为了访问超链接而单击的文本可以表达任何内容。

**基于协议攻击**：

使用MIME协议来附加恶意文件。用户可以通过查看电子邮件或打开附件来激活恶意代码。有的病毒利用一些用户代理直接查看附加数据类型的能力。

对策：禁止直接查看附加数据的能力/使用基于主机的扫描器和防火墙防止未经授权的程序访问网络来限制恶意代码的传播。

**基于验证攻击**：

跟踪电子邮件在何时何地被打开：在电子邮件中插入图片作为HTML文档的一部分。图片实际存储在一个远程网络服务器上。当用户读取电子邮件消息时，图片从远程web服务器下载。

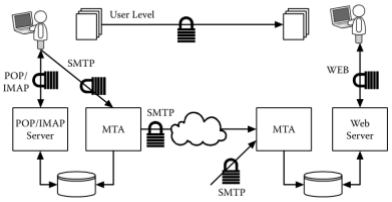
**基于流量攻击**：

创建更大的电子邮件消息，并且带有附件。对策是对MTA可以接收的电子邮件消息的大小设置一个限制。

**电子邮件一般对策**

验证最终用户，并确保电子邮件消息以未更改、未读取和已验证的方式发送。

**加密与认证**：防止数据被查看，嗅探流量，也可验证双方。

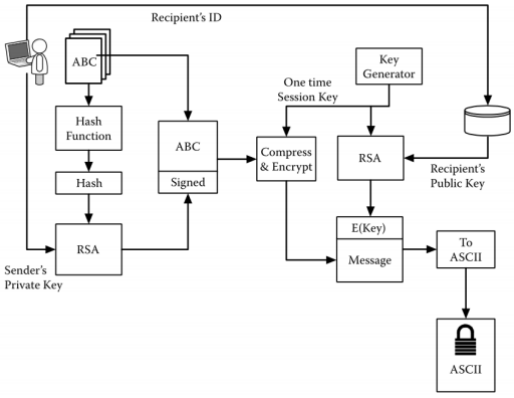



MTA之间的流量加密，可以减少垃圾邮件。但密钥的保护以及分发是一个问题，同时匿名邮件的处理？MTA的保护？

用户和MTA之间的流量加密：对用户身份验证，密钥的分发问题。

MTA与接收方之间：安全版本的POP和IMAP。

提供端到端安全性和身份验证的唯一逻辑方法是依赖用户代理：PGP协议。




发送方生成签名（消息哈希用自己的私钥加密），与消息一起用生成的密钥加密，密钥通过接收方公钥加密传输。接收方逆过来。强度取决于对私钥的保护。

**电子邮件过滤**

位于接收方电子邮件服务器之前，最先收到email的MTA。

出站和入站的邮件都要经过扫描和处理。

可以检测垃圾邮件和钓鱼攻击，方法：

一种是训练分类能力、用户也可设置，存在误报所以一般不会删除。针对性的攻击方法是添加不会检测的图片内容。

一种是使用过滤列表：使用ip过滤或者使用发件人地址信息（更好）。

黑名单需要不断维护因为垃圾邮件信息在改变，白名单限制较多对于私人内部使用，对公共不适用。灰名单：利用SMTP特性阻止智能垃圾邮件发送，针对第一次发送的新发送者先以451失败做相应，正常MTP会再次尝试从而允许通过，智能垃圾邮件则只尝试一次。

**内容过滤处理**

查找可能导致安全问题的特定内容。

电子邮件病毒扫描程序，它扫描所有电子邮件中的病毒。如果发现病毒，内容过滤器将删除违规邮件。

理解MIME协议，以便解码消息并扫描它们。针对出站和入站的邮件。

另一种内容过滤器的目标是不应该离开网络的出站内容。

缺点：无法扫描过滤被加密的邮件

**电子邮件取证**

通常不可能跟踪电子邮件追溯到实际的人，但可以跟踪电子邮件追溯到发送MTA。

从顶部或底部分析邮件标题。每个接触电子邮件的设备都会添加一个标题。

# BGP

- BGP session runs over TCP
  - TCP connection between neighboring routers
  - BGP messages sent over TCP connection
  - Makes BGP vulnerable to attacks on TCP
- Main kinds of attacks
  - Against confidentiality: eavesdropping
  - Against integrity: tampering
  - Against performance: denial-of-service
- Main defenses
  - Message authentication or encryption
  - Limiting access to physical path between routers
  - Defensive filtering to block unexpected packets

攻击：

**C：窃听：**监视BGP会话上的消息，通过点击邻居之间的链接。**揭示敏感信息：**推断业务关系，分析网络稳定性。

**困难：**加密（IPSec），难以连接（eBGP会话遍历一个链接）。

**I：篡改：**中间人，信息插入、删除、修改或重播信息。**导致不正确的BGP行为：**删除：邻居不学习新的路线；插入/修改：邻居学习虚假的路线。

**困难：**进入两个路由器之间是很难的；使用身份验证（签名）或加密；欺骗TCP包正确的方式是困难的。

**Dos：**超载路由器之间的链路导致数据包丢失和延迟...中断BGP会话的性能相对容易做到，可以在终端主机之间发送流量，只要数据包穿过链路（你可以从跟踪器中找到）；对策：给予BGP分组更高的优先级，例如，通过将分组放在单独的队列中。

前缀劫持：

拥有eBGP会话路由，已配置为可生成该前缀。获得路由访问：网络运营商犯了配置错误，不满的运营商发起攻击，局外人闯入路由器并重新配置。使其它ASes相信虚假路由（没过滤）。

**IP TTL：**

BGP speaker常间隔一跳，以阻止攻击者，可以检查携带BGP消息的数据包是否没有移动太远

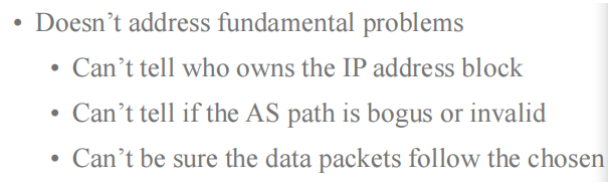
IP实时时间（TTL）字段减少每跳一次避免数据包永远停留在网络中。

通用TTL安全机制（RFC 3682）发送BGP数据包的初始TTL为255接收BGP扬声器检查TTL是254。

第三方远程注入数据包很难。

Applying best common practices (BCPs)

- Securing the session (authentication, encryption)
- Filtering routes by prefix and AS path
- Packet filters to block unexpected control traffic




**安全BGP：**

**PKI：**证书的双重层次结构将前缀所有权绑定到AS，将路由器绑定到AS。分布和验证的证书层次结构。路由器只接受有效证书覆盖的更新。

**使用"onion"签名进行路线认证：**每个BGP更新都由播音员签名——这些签名随着更新的传播而累积——任何接收到公告的AS都可以验证每个AS添加回源的签名。

# 防火墙

计算机系统或网络的一部分，设计用于阻止未经授权的流量从一个网络流到另一个网络。分离网络的受信任和不可信任组件。主要功能是过滤数据、重定向流量和防止网络攻击。

**入口过滤：**检查传入的流量，以保护内部网络，防止来自外部的攻击。**出口过滤：**检查传出的网络流量，防止内部网络中的用户接触到外部网络。比如在学校里屏蔽社交网站。

**数据包过滤防火墙：**对每个传入/传出的IP包应用一组规则，然后转发（允许）或拒绝（拒绝）包（在两个方向上）。包过滤器通常设置为基于匹配IP或TCP头上下文中字段的规则列表。优点：简单，高速，对用户更透明。缺点：没有应用层的灵活性，IP地址欺骗。

代理（应用层）：作为应用程序级流量代理的中继，从用户获取应用程序特定的信息并中继到服务器；可选地对用户进行身份验证，只有允许的应用程序可以通过；基于特性的处理可能在每个连接上产生额外的处理开销。

堡垒主机：一个被防火墙管理员确定为网络安全的关键强项的系统——用于各种防火墙配置。（程序级网关）

屏蔽子网防火墙：在防火墙之间创建一个隔离的子网。

# IDS

匿名检测 滥用检测

入侵:系统的授权用户，即试图获得他们未被授权的额外特权的授权;滥用给予他们的特权。

入侵检测:监视和收集发生在计算机系统或网络中的事件;分析它们是否有入侵的迹象，定义为试图破坏机密性、完整性、可用性，或绕过计算机或网络的安全机制。

**HIDS（基于主机）：**从单个计算机系统中收集到的信息进行操作。通常使用两种类型的信息源，即操作系统审计跟踪和系统日志。

**优点：**

可以检测到基于网络的IDS无法看到的攻击。

基于主机的信息源是在数据加密之前和/或在目标主机上解密数据之后生成的。

基于主机的IDS不受交换网络的影响。

当基于主机的IDS操作操作系统审计跟踪时，它们可以帮助检测特洛伊木马或其他涉及软件完整性破坏的攻击。

**缺点：**

必须为被监控的每个主机配置和管理信息。

IDS可能会作为攻击的一部分而被攻击和禁用。

基于主机的IDS正在对被监控的系统造成性能成本。

**NIDS：**通常由一组放置在网络的不同点上的单用途传感器或主机组成。监视网络流量，进行本地分析，并报告攻击。由于传感器仅限于运行IDS，它们可以更容易地抵御攻击。许多这些传感器被设计成在"隐形"模式下运行，以便使攻击者更难确定它们的存在和位置。

优点:

NIDS使用一个被动接口来捕获网络数据包以进行分析。

放置在全球各地的NIDS传感器可以配置为向中心站点报告，使一个由安全专家组成的小团队能够支持大型企业。

NIDS系统可以很好地扩展到网络保护中，因为网络上实际的工作站、服务器或用户系统的数量并不重要——流量是重要的。

大多数基于网络的IDS都是独立于操作系统的，提供更好的抵御DOS攻击的安全性。

缺点：

不能扫描协议或内容如果网络流量加密。

入侵检测变得更加困难在现代交换网络。

当前网络监控方法不能有效地处理高速网络。

大多数基于网络的系统是基于预定义的攻击签名，签名将总是比利用晚一步。

AIDS：基于应用程序的IDS所使用的最常见的信息源是应用程序的事务日志文件。在分析引擎中包含重要领域或应用程序特定知识的。检测由于授权用户超出其授权而导致的可疑行为。

优点：

基于应用程序的IDS可以向个人用户跟踪未经授权的活动。

基于应用程序的IDS通常可以在加密的环境中工作。

缺点：

应用程序日志没有像用于基于主机的IDS的操作系统审计跟踪那样得到很好的保护。

基于应用程序的IDS通常在用户抽象级别上监控事件，它们通常无法检测到特洛伊木马或其他此类软件篡改攻击。

---复习没时间部分参考了前人---