北京郵電大學

计算机网络

第九章 网络安全

网络空间安全学院

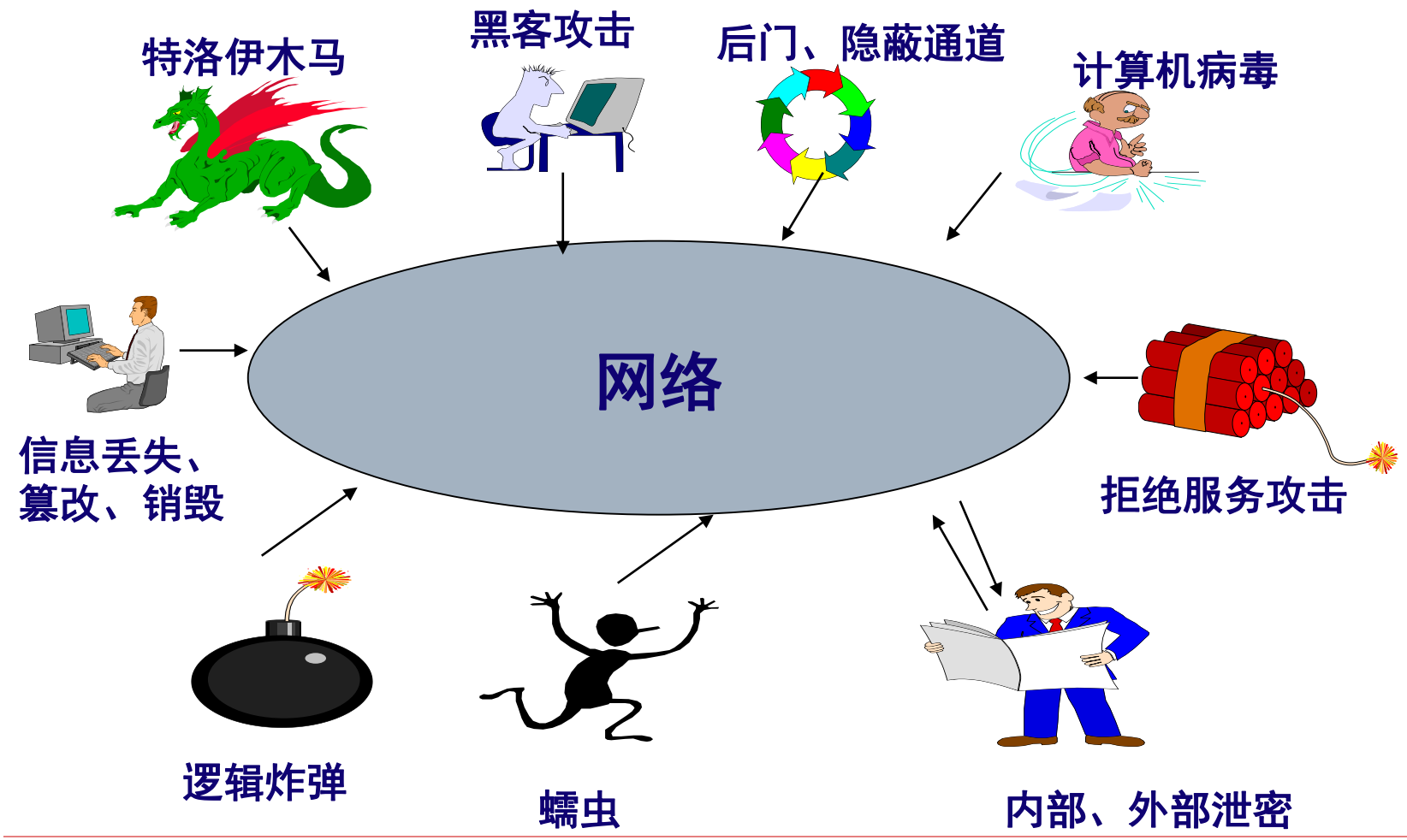
主要内容

- 9.1 网络安全问题概述
- 9.2 网络安全体系
- 9.3 因特网使用的安全协议

主要内容

- 9.1 网络安全问题概述
- 9.2 网络安全体系
- 9.3 因特网使用的安全协议

网络安全问题概述



网络安全问题概述

- 计算机网络上的通信面临以下的四种威胁：

  (1) 截获——从网络上窃听他人的通信内容。

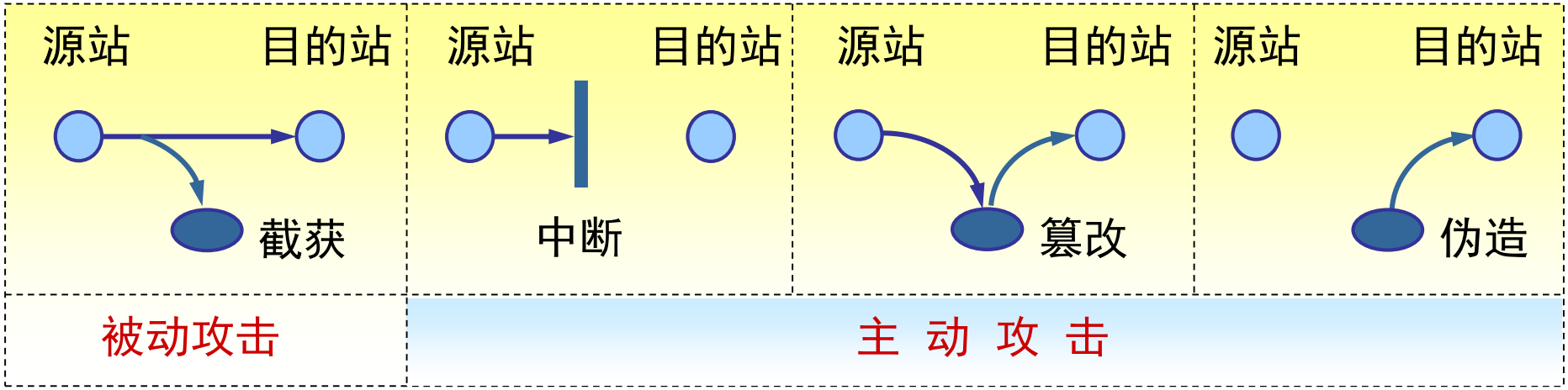
  (2) 中断——有意中断他人在网络上的通信。

  (3) 篡改——故意篡改网络上传送的报文。

  (4) 伪造——伪造信息在网络上传送。

网络安全问题概述

- 截获信息的攻击称为被动攻击
- 更改信息和拒绝用户使用资源的攻击称为主动攻击。



网络安全问题概述

- 在被动攻击中，攻击者只是观察和分析某一个协议数据单元 PDU 而不干扰信息流。重点是防范而不是检测
- 主动攻击是指攻击者对某个连接中通过的PDU 进行各种处理。重点是检测而不是防范
  - 更改报文流 ，对PDU的真实性、完整性和有序性进行攻击
  - 拒绝报文服务，使服务器无法提供正常服务
  - 伪造连接初始化 ，重放以前的合法连接，或伪造身份而企图建立连接

网络安全问题概述

- 计算机网络通信安全的目标

  (1) 防止析出报文内容；

  (2) 防止通信量分析；

  (3) 检测更改报文流；

  (4) 检测拒绝报文服务；

  (5) 检测伪造初始化连接。

网络安全问题产生的根源

- **Internet** 的迅速普及
  - 多数的新用户缺乏网络和信息安全方面的经验
  - 系统和网络配置的复杂性导致的安全性问题
  - 系统自身的设计缺陷
  - 外来入侵者的攻击
  - ……
- 归根结底，威胁网络和信息安全的主要因素可分为两大类，即：
  - 系统自身的安全性问题：自身缺陷
  - 来自外部的安全性威胁：
    - 网络的开放性
    - 外来攻击：病毒、木马、黑客、…

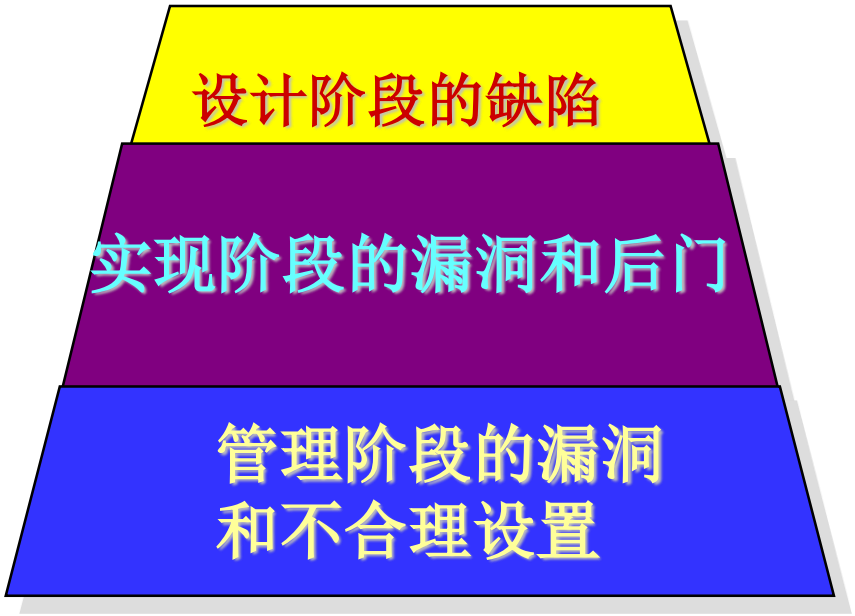
威胁网络安全的主要因素（1）

- 网络和系统自身的安全性漏洞
  - 技术上的因素
    - 系统和协议的开放性
    - 系统自身的漏洞弱点（**vulnerability**）
    - 配置的失误
    - 网络通信协议的漏洞
    - …
  - 非技术因素
    - 人员
    - 系统安全管理制度上的问题
    - 维护、使用人员的安全意识薄弱
    - …

威胁网络安全的主要因素（2）

- 来自外部的安全性威胁
  - 系统物理上的安全性
  - 病毒、蠕虫及其他破坏性程序
    - 特洛伊木马
    - 程序后门
    - ……
  - 黑客的攻击
    - 利用系统、网络、服务、通信协议等的安全性漏洞对目标系统进行的攻击
    - 破坏系统
    - 窃取信息

系统的安全性缺陷和漏洞



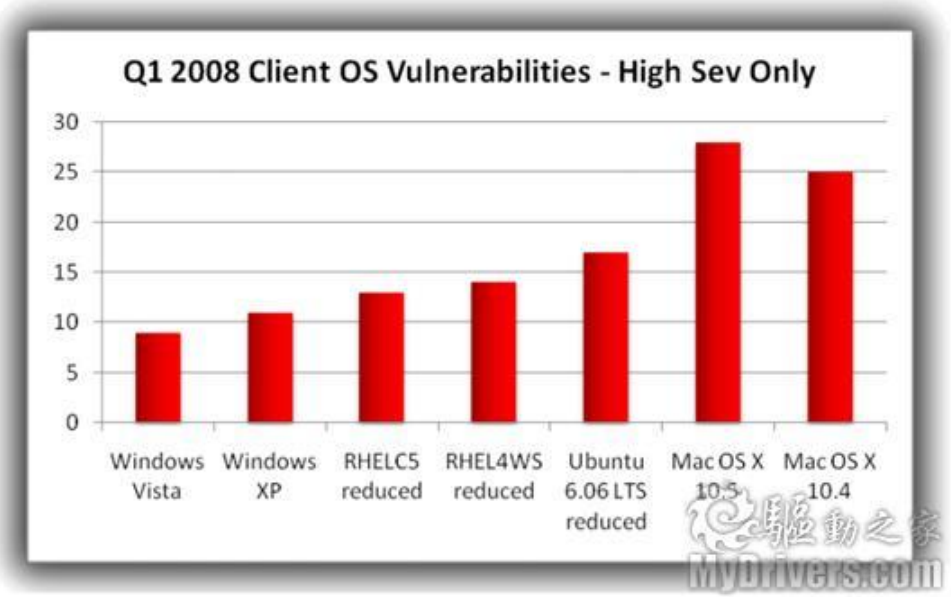
系统内部自身的缺陷（1）

- 计算机软件系统缺陷（BUG）是广泛存在的
  - 原因：程序员的认知能力和实践能力的局限性
  - 一般认为，程序每千行中有**1** 个以上的**BUG (IBM,1999)**
  - 软件系统的**BUG** 在客观上导致了整个系统安全上的脆弱性，最有可能被攻击者利用
- 众多的软硬件都被证明存在大量安全隐患
  - 操作系统：**MS Windows**、**UNIX**、**Netware**、**……**

操作系统	WIN3.1	WIN95	WIN NT	WIN98	WIN2K
代码量（万行）	300	500	1650	1800	3500+

操作系统漏洞统计

Client OS	Vulnerabilities fixed	Security Advisories	Patch Events
Windows Vista	9	6	2
Windows XP	12	8	2
Red Hat RHELD 5 (reduced)	60	19	12
Red Hat RHEL WS 4 (reduced)	75	18	14
Ubuntu 6.06 LTS (reduced)	54	15	13
Mac OS X 10.5 Leopard	83	6	5
Mac OS X 10.4 Tiger	81	5	5

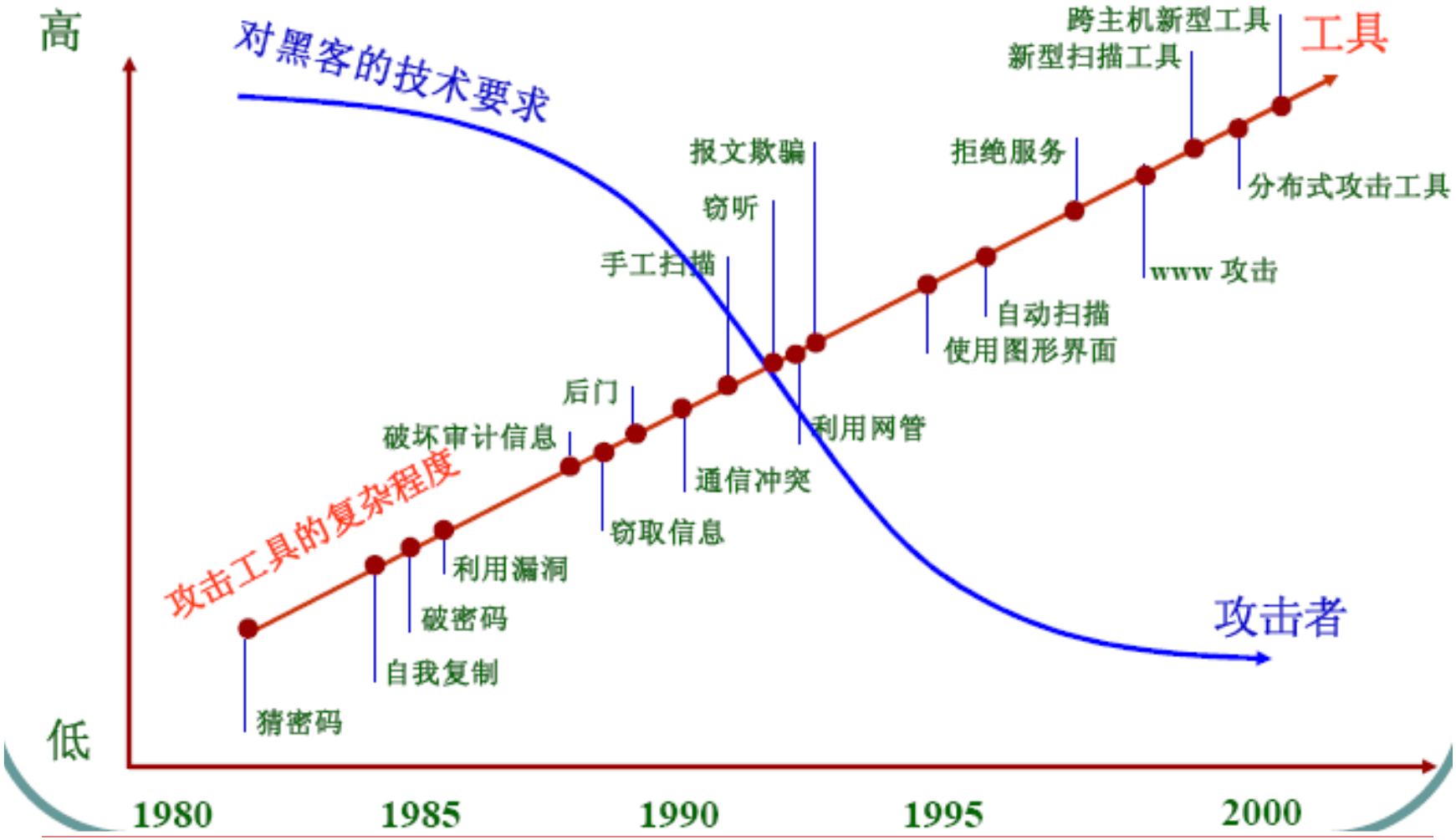


系统内部自身的缺陷（2）

- 常见的系统安全漏洞
  - **UNIX** 远程登录和远程命令（**r-commands**）
    - **rlogin、rsh、rcp、……**
  - 信息收集（**Finger**）
  - 后门（**Backdoor**）
  - 远程过程调用（**RPC**）
  - 网络文件系统（**NFS**）
  - 防火墙/入侵检测系统（**Firewall & IDS**）自身的漏洞
    - **IP Spoofing、Source Porting、Source Routing、……**
  - 网络服务（**Internet Service**）
    - **Web（NCSA、MS IIS、Apache、CGI、…）、FTP、Mail（SMTP）…**
  - 通信协议实现
    - **TCP/IP、DNS、SNMP、Port Scanning ……**
  - 拒绝服务（**DoS - Deny of Service**）缺陷
  - **……**

网络的开放性

- 最初，使用TCP/IP 实现连接的基本前提是：连接在网络上的计算机来自彼此信任团体
  - 因此， 使用公开的**TCP/IP** 的协议体系是可能的
  - 协议的公开性大大普及了**Internet** 的应用
- 但是在现在的Internet 上，这种情况发生了改变
  - 连接在一起的用户是相互不可信任的
  - **Internet** 服务基于公开的协议，使得不可信的攻击者能够通过远程访问，无需到现场就能获得成功
  - 目标可远程访问，行为可远程获知
- 开放性（包括各种资源的公开的共享），使得各种攻击工具很容易获得和使用


高
低
对黑客的技术要求
攻击工具的复杂程度
工具
攻击者
跨主机新型工具
新型扫描工具
分布式攻击工具
拒绝服务
www 攻击
自动扫描
使用图形界面
报文欺骗
窃听
手工扫描
后门
破坏审计信息
利用网管
通信冲突
窃取信息
利用漏洞
破密码
自我复制
猜密码
1980
1985
1990
1995
2000

通信协议的缺陷（1）

- TCP/IP 协议体系自身缺乏完整的安全策略
  - **Internet** 起源于研究项目，安全不是主要的考虑
  - 开放性：协议的体系和实现都是公开的，设计和实现中的缺陷也是公开的，可能被攻击者所利用。
  - 信息的传输是未加密传输的，容易被窃听、伪造和欺骗。
  - **TCP/IP** 所提供的网络服务安全性也较差，容易被利用。
  - 配置的复杂性和专业性，配置上的缺陷也给了企图入侵系统的人以可乘之机
  - 协议的实现存在安全漏洞。协议的具体实现中可能存在大量的**BUG**。

通信协议的缺陷（2）

- TCP/IP 协议体系的安全缺陷
  - 网络层（**IP**）
    - 缺乏安全认证和保密机制，易出现**IP** 地址欺骗等问题
  - 传输层（**TCP/UDP**）
    - **TCP**连接建立时的“三次握手”
    - **TCP**连接能被欺骗、截取、操纵
    - **UDP**易受**IP** 源路由和拒绝服务的攻击
  - 应用层
    - 没有定义认证、访问控制、完整性、保密性等各种安全机制
    - 提供的网络服务也没有定义安全性机制，如**Web**、**Finger**、**FTP**、**Telnet**、**E-mail**、**DNS**、**SNMP**、…

对通信协议的安全威胁

从协议层次看，常见主要威胁手段：

- 物理层：
  - 信息窃取、插入、删除等，但需要一定的设备
- 数据链路层
  - 很容易实现数据监听
- 网络层
  - IP 地址欺骗、针对网络层协议的漏洞的攻击、…
- 传输层：
  - 对TCP 等连接欺骗等针对传输层协议的漏洞的攻击
- 应用层：
  - 存在着几乎所有类型的安全性问题：认证、访问控制、完整性、保密性等所有安全问题

外来的安全威胁

- 计算机病毒
  - 是一种有害程序
  - 特征：能够利用系统进行自我复制和传播
    - 传统病毒：引导型、文件型、宏病毒
    - 网络、邮件病毒
  - 通过特定事件触发
    - 触发条件：时间、日期、用户的特定操作等
    - 危害：破坏计算机系统、窃取用户信息、阻塞网络服务
  - 发展趋势：利用网络、邮件来传播，并结合多种黑客攻击手段，破坏性更强
  - 利用系统漏洞进行攻击和破坏

外来威胁——各种攻击者Hacker

- 对网络和计算机系统的各种攻击者（attackers）
  - **Amateurs**
  - **Insiders**
  - **Kids**
  - **hackers**
  - **Criminals**
  - **Spies**
  - **Sociopath（terrorist ...）**
- Hackers
  - 早期的**hacker** 是一些独立思考、奉公受法的计算机迷，他们享受智力上的乐趣（褒义）
  - 当今的**hacker** 是破坏者，专门闯入电脑系统、网络、电话系统和其他的通信系统

Hacker

- Hacker
  - 具有不同的目的
  - 政治的、经济的、商业的、个人的、为了显示其能力、或者仅仅是恶作剧
  - 他们在不懈努力，试图攻破各种系统的安全方案
  - 从网络内部或外部进行非法的入侵，攻击系统，达到破坏系统或窃取信息的目的
  - 具有丰富的资源
  - 在Internet 上大量公开的攻击手段和攻击程序
- 黑客攻击的主要目标
  - 政府和国家要害部门计算机系统
  - 商业网站
  - 公共信息服务站点

Hacker的入侵

- Hacker 攻击的一般过程：三个阶段
  - 信息搜集
    - 获得目标系统的信息：OS 版本、服务、端口.....
    - 利用的协议：ICMP、SNMP、Whois、Finger
    - 利用的工具：Traceroute、Ping、Telnet、FTP、PortScan
  - 扫描漏洞
    - 使用通用工具（如SATAN 等）
    - 使用自制工具
  - 攻击
    - 在目标主机上建立账户
    - 安装远程监控程序
    - 获取特权
    - 获取信息、篡改信息
    - 删除证据退出

Hacker的入侵手段（1）

- 常见的系统入侵手段
  - 口令攻击
  - 网络窃听和信息截取、分组欺骗（地址欺骗及DNS 欺骗）
  - 扫描和利用系统及配置上的安全弱点、程序后门
  - 禁止安全审计
  - 散布病毒或有害程序，破坏系统、窃取用户信息
  - 拒绝服务攻击/ 分布式的攻击
  - ……
- 入侵方法的分类
  - 信息收集型攻击和欺骗型攻击
  - 口令攻击
  - 拒绝服务攻击
  - 利用型攻击

Hacker的入侵手段（2）

- 利用型攻击
  - 试图直接对主机进行控制：
    - 口令猜测
    - 特洛伊木马
    - 缓冲区溢出
    - ……
  - 利用已知系统弱点和安全缺陷
    - 操作系统的安全性缺陷和安全性极差的局域网服务：X-Window 终端服务、RPC、NFS、r-Commands、……
    - Web 服务的安全缺陷：WWW、CGI、SSI、Java 小程序……
    - 其它网络服务：Mail、Finger、FTP、……

Hacker的入侵手段（3）

- 信息收集型攻击
  - 被动性的攻击方式
  - 网络窃听和信息截取
  - 在广播网络中必然存在窃听和信息截取的问题，很多应用中密码都是明文传送的
- 欺骗型攻击
  - 发送欺骗性的假冒消息，导致目标系统不正确的动作和配置
  - 原因：Internet 体系中没有认证机制
  - 包括：
    - DNS 欺骗
    - IP 地址欺骗
    - 伪造电子邮件
    - ……

Hacker的入侵手段（4）

- 拒绝服务（DoS - Deny of Service）攻击
  - 通过各种手段，将资源（CPU、内存、网络带宽等等）耗尽，使系统不能再提供服务。
  - 包括：
    - 电子邮件炸弹
    - 崎型消息攻击
    - Land 攻击
    - Smurf 攻击
    - Syn Flooding
    - ……
  - 分布式拒绝服务攻击（DDoS）
  - 目前没有特别有效的办法来防止

垃圾邮件

- 垃圾邮件
  - UCE: Unsolicited Commercial Email
  - UBE: Unsolicited Bulk Email
  - Spam
- 危害
  - 网络资源的浪费
    - 欧洲委员会公布的一份报告，垃圾邮件消耗的网络费用每年高达100亿美元
  - 资源盗用
    - 利用他人的服务器进行垃圾邮件转发
  - 威胁网络安全
    - DOS攻击

垃圾邮件特点

- 内容：
  - 商业广告
  - 宗教或个别团体的宣传资料
  - 发财之道,连锁信等
- 接收者
  - 无因接受
  - 被迫接受
- 发送手段
  - 信头或其它表明身份的信息进行了伪装或篡改
  - 通常使用第三方邮件转发来发送

物理层攻击

- 电磁泄漏：
  - 指电子设备的杂散（寄生）电磁能量通过导线或空间向外扩散。任何处于工作状态的电磁信息设备，如：计算机、路由器、交换机、电话机等，都存在不同程度的电磁泄漏，这是无法摆脱的电磁学现象。如果这些泄漏“夹带”着设备所处理的信息，就构成了所谓的电磁信息泄漏。

数据链路层攻击

- 数据窃听：
  - 以太网中，信道是共享的，任何主机发送的每一个以太网帧都会到达别的与该主机处于同一网段的所有主机的以太网接口，一般地，CSMA/CD协议使以太网接口在检测到数据帧不属于自己时，就把它忽略，不会把它发送到上层协议（如ARP、RARP层或IP层）。如果我们对其稍做设置或修改，就可以使一个以太网接口接收不属于它的数据帧。例如大多数以太网卡的实现包括一种称为混杂模式的工作方式，一旦设定该种方式，数据链路层即能接收所有经过该节点的数据帧。

IP攻击

- IP欺骗：
  - 由于IP协议不对数据包中的IP地址进行认证，所以攻击者假冒他人IP地址发送数据包，或直接将自身IP修改成他人IP地址。前者可能造成网络通信异常、流量迅速增大；后者可以骗取基于IP的信任。
  - IP欺骗的局限性：远程主机只向伪造的IP地址发送应答信号，攻击者不可能收到远程主机发出的信息，即用C主机假冒B主机IP，连接远程主机A，A主机只向B主机发送应答信号，C主机无法收到。

IP攻击

- ICMP/PING 攻击原理

  早期的路由器对包的最大尺寸都有限制，比如许多操作系统对TCP/IP栈的实现在ICMP包上都是规定64KB，并且在对包的标题头进行读取之后，要根据该标题头里包含的信息来为有效载荷生成缓冲区。当产生畸形的，声称自己的尺寸超过ICMP上限的包也就是加载的尺寸超过64K上限时，就会出现内存分配错误，导致TCP/IP堆栈崩溃，致使接受方死机。如在Linux下输入Ping -t 66510 IP（未打补丁的Win95/98的机器），机器就会瘫痪。

IP攻击

- ping flooding:

典型的拒绝服务攻击，在某一时刻多台主机对目标主机使用Ping程序，就有可能耗尽目标主机的网络带宽和处理能力。如果一个网站一秒钟收到数万个ICMP回应请求报文就可能使它过度繁忙而无法提供正常的服务。当然可以编制程序以最快的速度向目标主机发送ICMP回应请求报文，并且使用伪造的IP地址。99年有“爱国主义黑客”发动全国网民在某一时刻开始ping某美国站点，试图ping死远程服务器就是一次典型的ping flooding 攻击。

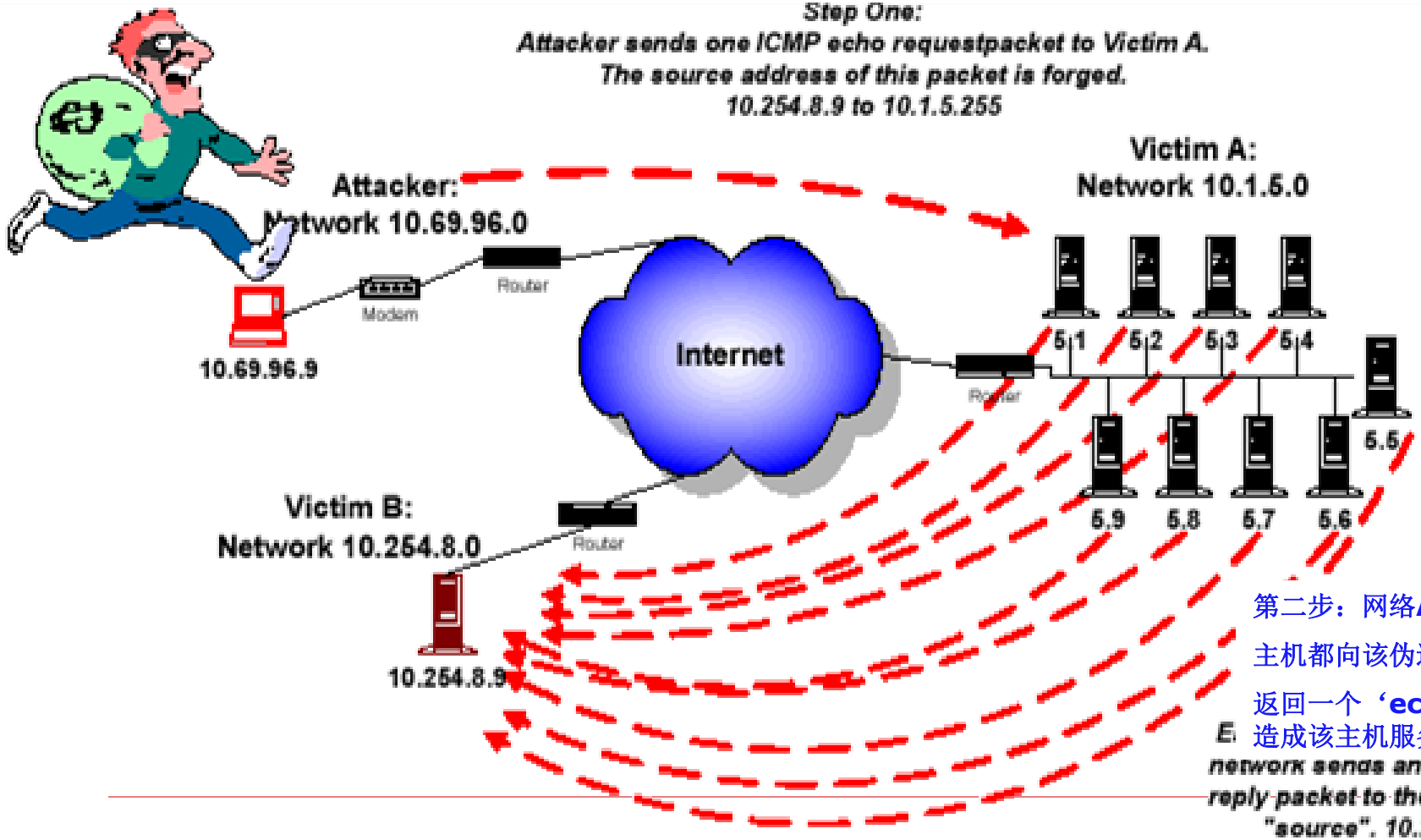
IP攻击

ICMP/SMURF 攻击原理

ICMP/SMURF攻击利用IP欺骗和ICMP回复方法使大量网络传输充斥目标系统，引起目标系统拒绝为正常系统进行服务。首先向一个具有大量主机和因特网连接的网络的广播地址发送一个欺骗性Ping分组（echo 请求），而欺骗性Ping分组的源地址就是被攻击的机器本身的地址。因而所有接收到此包的主机都将给发包的地址发送一个ICMP回复包。Smurf的原理和ping flooding类似，只不过利用了反弹网络发送ICMP回应应答数据包来耗尽目标主机资源，若反弹网络规模较大，此攻击威力巨大。

Smuff攻击示意图

第一步：攻击者向被利用网络**A**的广播地址发送一个**ICMP** 协议的’**echo’**请求数据报，该数据报源地址被伪造成**10.254.8.9**



第二步：网络**A**上的所有主机都向该伪造的源地址返回一个‘**echo’**响应，造成该主机服务中断。

TCP攻击

TCP/SYN 攻击原理

当一台黑客机器A要与另外一台ISP的主机B建立连接时，它的通信方式是先发一个SYN包告诉对方主机B说“我要和你通信了”，当B收到时，就回复一个ACK/SYN确认请求包给A主机。如果A是合法地址，就会再回复一个ACK包给B主机，然后两台主机就可以建立一个通信渠道了。

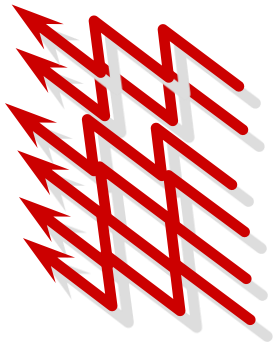
可是黑客机器A发出的包的源地址是一个虚假的IP地址，或者可以说是实际上不存在的一个地址，ISP主机B发出的那个ACK/SYN包当然就找不到目标地址了。如果这个ACK/SYN包一直没有找到目标地址，那么也就是目标主机无法获得对方回复的ACK包。而在缺省超时的时间范围以内，主机的一部分资源要花在等待这个ACK包的响应上，假如短时间内主机A接到大量来自虚假IP地址的SYN包，它就要占用大量的资源来处理这些错误的等待，最后的结果就是系统资源耗尽以至瘫痪。

TCP 同步 泛滥


攻击者
172.18.1.1
Code
Internet
目标
192.0.2.1
欺骗性的 IP 包
源地址不存在
目标地址是 192.0.2.1
TCP Open

TCP SYN 泛滥

攻击者
172.18.1.1



目标
192.0.2.1

同步应答响应
源地址 192.0.2.1
目标地址不存在
TCP ACK

应用层攻击

- Finger服务攻击
  - 很多装有UNIX系统的服务器经常开放Finger服务（端口79），远程客户端可以通过finger服务查询到站点上的在线用户清单及其他一些有用的信息。由于finger服务一般都是提供在线用户的用户名，因此攻击者通过finger服务可以轻松地取得有效用户名列表（如果耐心地多试几次,基本上可以得到大部分的用户名），然后使用暴力密码破解器。由于一些用户的安全意识薄弱，经常使用简单的口令，攻击者往往能在较短的时间里得到一个有用的"身份"（如ftp权限或telnet权限，要是运气好，没准能得到一个有写权限的账号），以此作为进一步行动的跳板。利用Finger服务，攻击者还可以取得用户的登陆时间，查看邮件时间等有用的信息,这个也是入侵者需要的重要信息（可以了解用户的登录时间和习惯，有利于隐藏行踪）。

其他攻击

- UDP攻击
- DNS欺骗
- Web欺骗攻击
- Email攻击
- .....

主要内容

- 9.1 网络安全问题概述
- 9.2 网络安全体系
- 9.3 因特网使用的安全协议

网络安全体系

- 网络安全是一个涉及范围较广的研究领域，研究人员一般只是在该领域的一个小范围内从事研究工作，开发出某些能够解决特定网络安全问题的方案。需要从整体上研究计算机网络安全问题的解决方案。
- 1982年ISO开始OSI安全体系结构的研究，发布了ISO 7498-2标准，作为OSI参考模型的新补充。1990年，ITU决定采用ISO 7498-2作为它的X.800推荐标准。
- ISO 7498-2标准现在已成为网络安全专业人员的重要参考，它为网络安全共同体提供一组公共的概念和术语，用来描述和讨论安全问题和解决方案。因此，OSI安全体系结构只是安全服务与相关安全机制的一般性描述，说明了安全服务怎样映射到网络的层次结构中，并简单讨论了它们在OSI参考模型中的合适位置。
- OSI安全体系结构包括：安全服务、安全机制和安全管理。

安全服务（1）

- 安全服务的概念
  - 为加强网络信息系统安全性及对抗安全攻击而采取的一系列措施
- 主要内容：
  - 安全机制、安全连接、安全协议、安全策略
- ISO 7498-2《信息处理系统开放系统互连基本参考模型第2部分—— 安全体系结构》中定义了五大类可选的安全服务
  - 鉴别（Authentication）： 对等实体鉴别与数据源鉴别
  - 访问控制（Access Control）
  - 数据保密性（Data Confidentiality）
  - 数据完整性（Data Integrity）
  - 不可否认（Non-Repudiation）

安全服务（2）

- 鉴别（认证）：确保通信的真实性
  - 数据源鉴别：能向接收方保证该消息确实来自它所宣称的源
  - 对等实体鉴别：在连接发起时，确保这两个实体是可信的；确保该连接不被干扰，第三方不能假冒
- 访问控制：
  - 限制和控制实体对资源访问的能力（以鉴别为基础）
- 不可否认：防止实体抵赖其行为
  - 发送方不能抵赖发送；接收方不能抵赖接收
- 数据保密性：
  - 保护被传输的数据免受被动攻击；保护通信量免受分析，包括通信双方的位置、通信的次数及消息的长度等信息
- 数据完整性：
  - 确保收到的消息真实性如同发送的消息一样，免受篡改和伪造

安全服务（3）实施位置

安全服务		OSI层次						
		1	2	3	4	5	6	7
鉴别服务	同等实体鉴别	N	N	Y	Y	N	N	Y
	数据源鉴别	N	N	Y	Y	N	N	Y
访问控制	访问控制服务	N	N	Y	Y	N	N	Y
数据完整性	带恢复功能的连接完整性	Y	N	N	Y	N	N	Y
	不带恢复功能的连接完整性	N	N	Y	Y	N	N	Y
	选择字段连接完整性	N	N	N	N	N	N	Y
	选择字段无连接完整性	N	N	Y	Y	N	N	Y
	无连接完整性	N	N	N	N	N	N	Y
数据保密性	连接保密性	Y	Y	Y	Y	N	Y	Y
	无连接保密性	N	Y	Y	Y	N	Y	Y
	信息流保密性	Y	N	Y	N	N	N	Y
非否认服务	发送非否认	N	N	N	N	N	N	Y
	接受非否认	N	N	N	N	N	N	Y
注：“Y”表示提供安全服务，“N”表示不提供安全服务								

安全服务（4）安全机制

- 安全机制是实现安全服务的技术手段
  - 实施位置可以为操作系统、软硬件功能部件、管理程序以及它们的任意组合
- ISO 7498-2中的八类安全机制
  - 加密机制（Encryption ）
  - 数字签名机制（Digital Signature Mechanisms）
  - 访问控制机制（Access Control Mechanisms）
  - 数据完整性机制（Data Integrity Mechanisms）
  - 鉴别交换机制（Authentication Mechanisms ）
  - 通信业务填充机制（Traffic Padding Mechanisms）
  - 路由控制机制（Routing Control Mechanisms）
  - 公证机制（Notarization Mechanisms）

安全服务（4）与安全机制的关系

	机密性	完整性	鉴别	访问控制	不可否认
加密	Y	Y	Y	-	-
数字签名	-	Y	Y	-	Y
访问控制	-	-	-	Y	-
数据完整性	-	Y	-	-	Y
鉴别	-	-	Y	-	-
业务填充	Y	-	-	-	-
路由控制	Y	-	-	-	-
公证	-	-	-	-	Y

系统安全结构的层次及主要技术

应用层提供安全服务的特点

- 只能在通信两端的主机系统上实施
- 优点：
  - 安全策略和措施通常是基于用户制定的
  - 对用户想要保护的数据具有完整的访问权，因而能很方便地提供针对用户的服务
  - 不必依赖操作系统来提供这些服务
  - 对数据的实际含义有着充分的理解
- 缺点：
  - 效率太低
  - 对现有系统的兼容性太差
  - 改动的程序太多，出现错误的概率大增，为系统带来更多的安全漏洞

传输层提供安全服务的特点

- 只能在通信两端的主机系统上实施
- 优点：
  - 与应用层安全相比，在传输层提供安全服务的好处是能为其上的各种应用提供安全服务，提供了更加细化的基于进程对进程的安全服务，这样现有的和未来的应用可以很方便地得到安全服务，而且在传输层的安全服务内容有变化时，只要接口不变，应用程序就不必改动。
- 缺点：
  - 由于传输层很难获取关于每个用户的背景数据，实施时通常假定只有一个用户使用系统，所以很难满足针对每个用户的安全需求。

网络层提供安全服务的特点

- 在端系统和路由器上都可以实现
- 优点：
  - 主要优点是透明性，能提供主机对主机的安全服务，不要求传输层和应用层做改动，也不必为每个应用设计自己的安全机制
  - 其次是网络层支持以子网为基础的安全，子网可采用物理分段或逻辑分段，因而可很容易实现VPN和内联网，防止对网络资源的非法访问
  - 第三个方面是由于多种传送协议和应用程序可共享由网络层提供的密钥管理架构，密钥协商的开销大大降低
- 缺点：
  - 无法实现针对用户和用户数据语义上的安全控制

数据链路层提供安全服务的特点

- 在链路的两端实现
- 优点：
  - 整个分组（包括分组头信息）都被加密，保密性强
- 缺点：
  - 使用范围有限。只有在专用链路上才能很好地工作，中间不能有转接点

主要内容

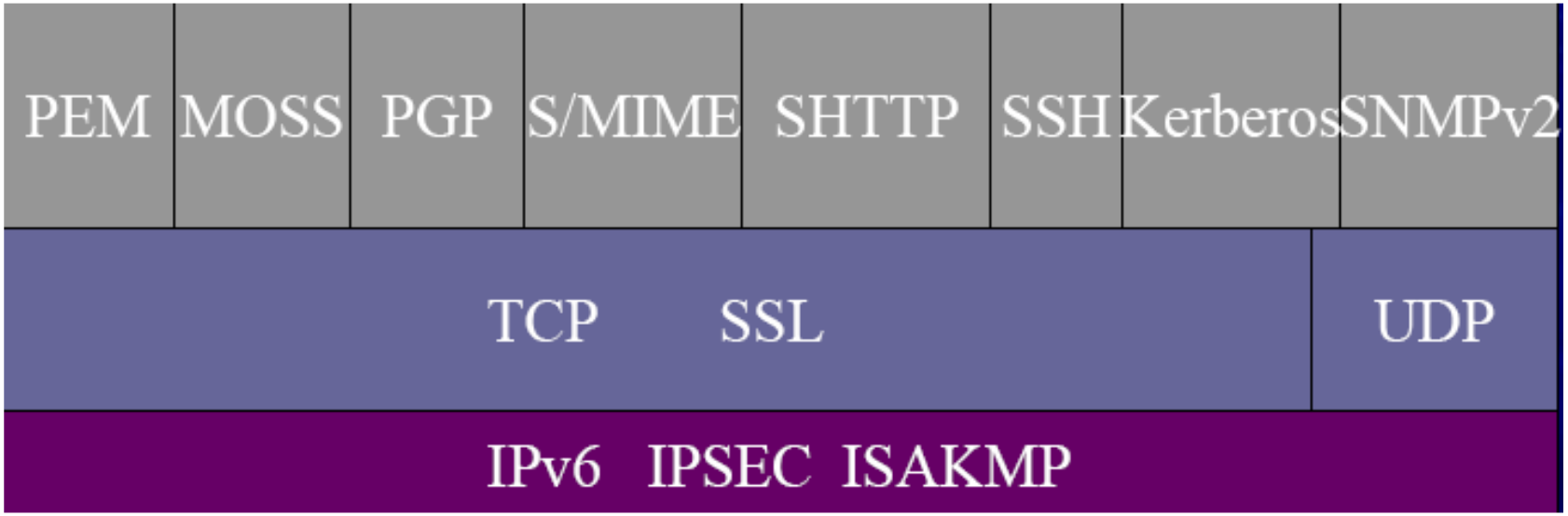
- 9.1 网络安全问题概述
- 9.2 网络安全体系
- 9.3 因特网使用的安全协议

9.3 因特网使用的安全协议

- 安全协议是建立在密码体制基础上的一种高互通协议，它运行在计算机通信网或分布式系统中，为安全需求的各方提供一系列步骤，借助于密码算法来达到密钥分配、身份认证、信息保密以及安全地完成电子交易等目的。
  - 密钥交换协议
  - 认证协议
  - 认证和密钥交换协议
  - 电子商务协议

安全协议（1）

- 基于TCP/IP协议的网络安全体系结构基础框架



安全协议（2）

- ISO7498-2映射而得的TCP/IP各层安全服务与安全协议的对应关系

层	安全协议	鉴别	访问控制	保密性	完整性	抗否认
IP层	IPSEC	Y		Y	Y	
TCP层	SSL	Y		Y	Y	
应用层	PEM	Y		Y	Y	Y
	MOSS	Y		Y	Y	Y
	S/MIME	Y		Y	Y	Y
	PGP	Y		Y	Y	Y
	SHTTP	Y		Y	Y	Y
	SNMP	Y		Y	Y	
	SSH	Y		Y	Y	
	Kerberos	Y	Y	Y	Y	Y

9.3.1 网络层安全协议

- Everything over IP(TCP/IP, VOIP…)。
  - 但是IP不能提供安全性，IP数据报可以被伪造、篡改和窥视。
- 在IP层采取安全机制，能够加强网络基础设施的安全性，不仅可以为已经具有安全机制的应用提供安全服务，也可以为那些没有考虑安全性的应用提供安全服务
- IP层上的安全应该并且能够包含3个方面的安全服务：鉴别、保密性和密钥管理。

9.3.1 网络层安全协议

- IETF中的IP Security Protocol Working Group工作组负责标准化，目标：
  - 该体制不仅适用于IP目前的版本（IPv4）,也能在IP的新版本（IPng或IPv6）下工作；
  - 可为运行于IP顶部的任何一种协议提供保护；
  - 与加密算法无关，即使加密算法改变了或增加新的算法，也不对其他部分的实现产生影响；
  - 必须能实现多种安全策略，但要避免给不使用该体制的人造成不利影响。
- IPSec工作组制定了目前的IP层的安全协议IPSec，可以“无缝”地为IP引入安全特性，为数据源提供身份验证、数据完整性和保密性机制。

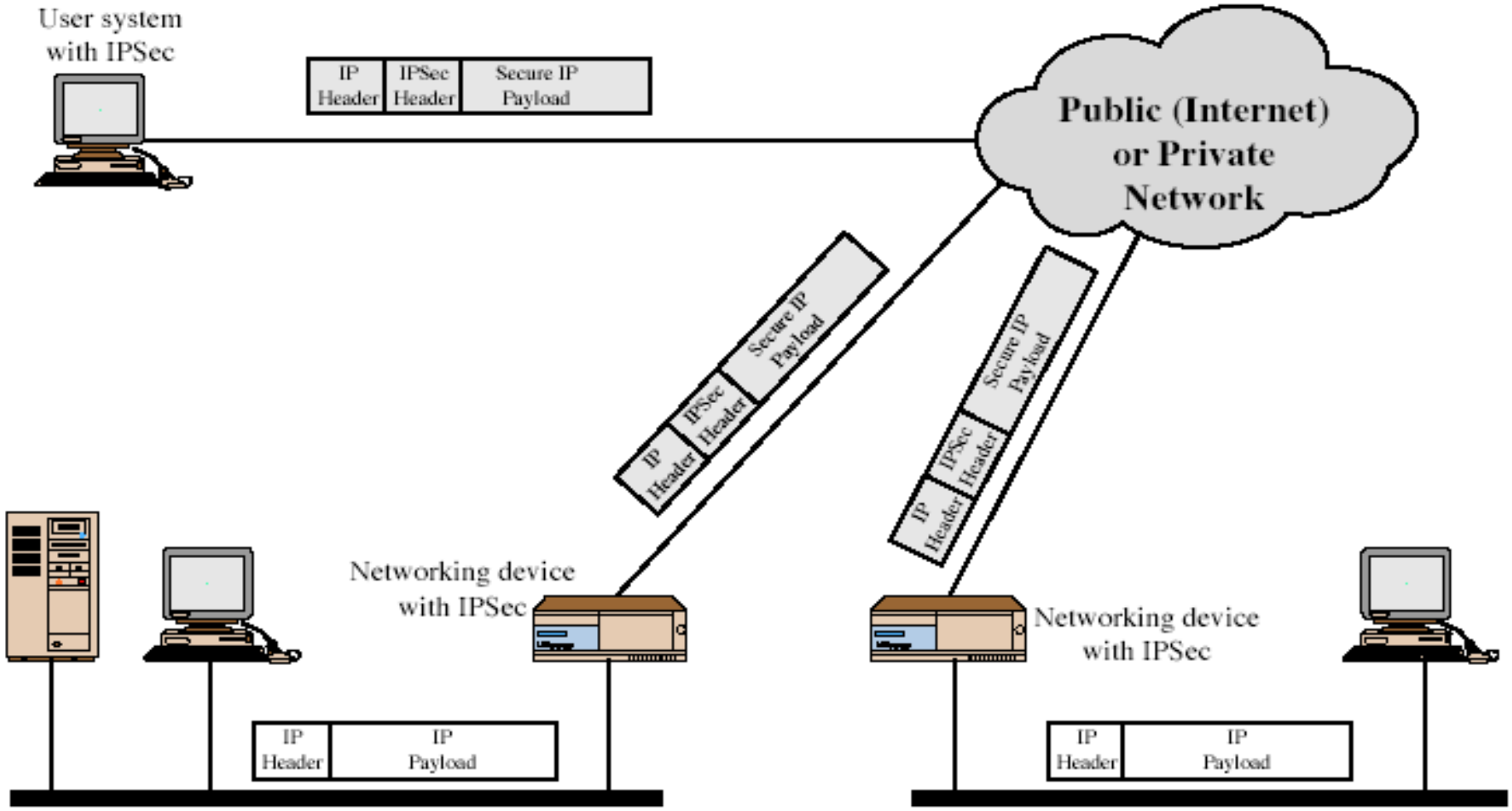
IPSec提供的安全机制

- 鉴别
  - 保证收到的数据包的确是由数据包头所标识的数据源发来的，且数据包在传输过程中未被篡改。
- 保密性
  - 保证数据在传输期间不被未授权的第三方窥视。
- 密钥管理
  - 解决密钥的安全交换。

IPSec的典型用途

- 保证因特网上各分支办公点的安全连接。
- 保证因特网上远程访问的安全。
- 通过外部网或内部网建立与合作伙伴的联系。

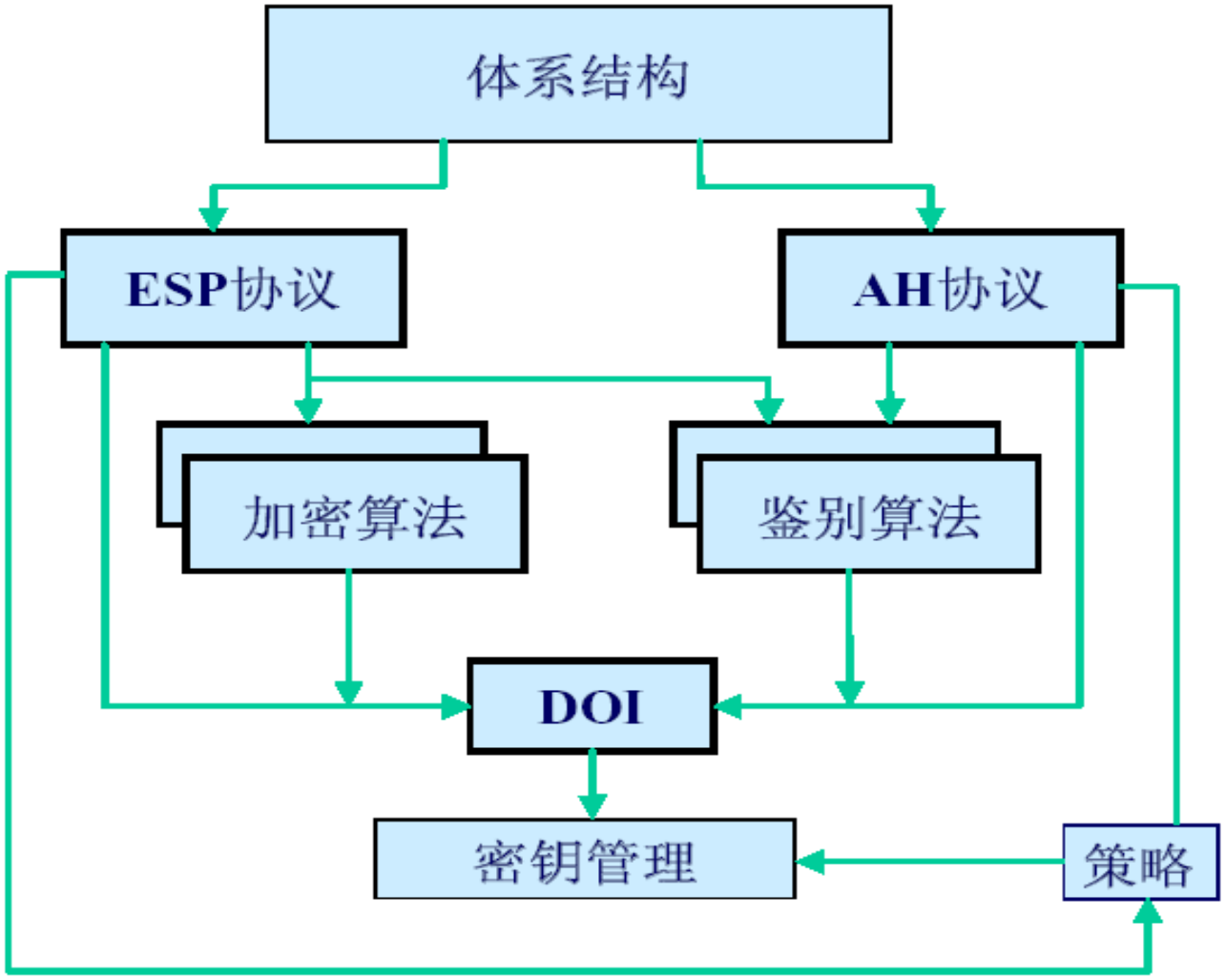
IPSec的典型用途


User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
IP Header
IPSec Header
Secure IP Payload
IP Header
IPSec Header
Secure IP Payload
Networking device with IPSec
Networking device with IPSec
IP Header
IP Payload
IP Header
IP Payload

IPSec的优点

- 如果在路由器或防火墙上执行了IPSec，它就会为周边的通信提供强有力的安全保障。一个公司或工作组内部的通信将不涉及与安全相关的费用。
- IPSec在传输层之下，对于应用程序来说是透明的。当在路由器或防火墙上实现IPSec时，无需更改用户或服务器系统中的软件设置。即使在终端系统中执行IPSec，应用程序一类的上层软件也不会被影响。
- IPSec对终端用户来说是透明的，因此不必对用户进行安全机制的培训。
- 如果需要的话，IPSec可以为个体用户提供安全保障，这样做就可以保护企业内部的敏感信息。

IPSec的安全体系结构



IPSec的安全体系结构

- 体系结构：包括IPSec的一般概念、安全需求、定义和机制
- 载荷安全性封装（ESP）：包括包格式和使用ESP加密/认证包的规定
- 认证头（AH）：包括包格式和使用AH认证包的规定
- 加密算法：一系列描述各种ESP中使用的加密算法
- 认证算法：一系列描述各种AH和可选ESP中使用的加密算法
- 密钥管理：描述密钥管理模式的文档
- 解释域：包括与其它文档相关的一些参数，如被认可的加密、认证算法和密钥生存周期的参数

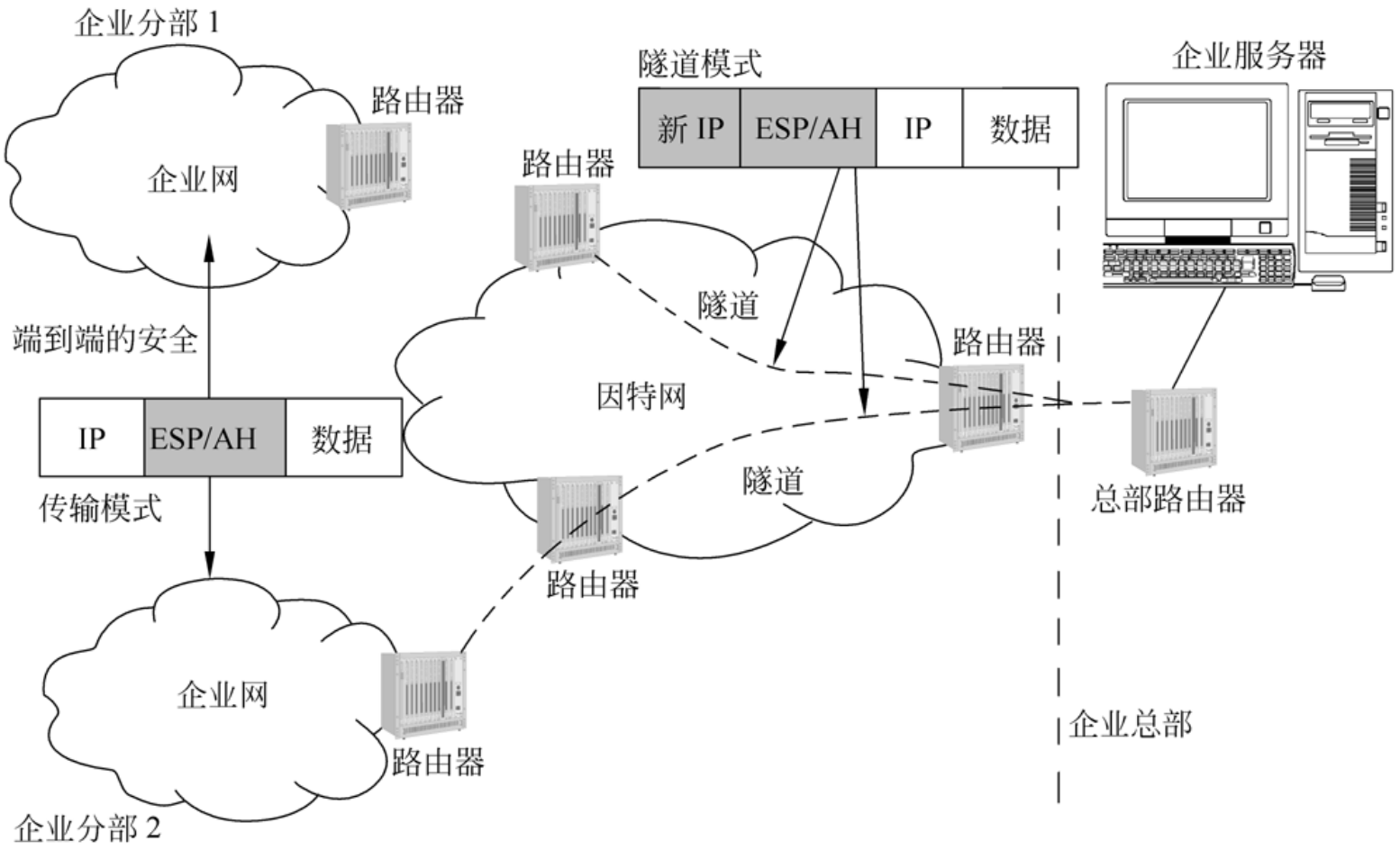
IPSec

Services	AH	ESP (encryption only)	ESP (encryption and authentication)
访问控制	✓	✓	✓
无连接完整性	✓		✓
数据源认证	✓		✓
拒绝重放	✓	✓	✓
保密性		✓	✓
受限制的流量保密性		✓	✓

IPSec的工作模式

- 传输模式
  - 传输模式保护的是IP载荷，如TCP段、UDP段、ICMP包等。
  - 只有在要求两个主机的端到端的安全保障时，才使用传输模式
- 隧道模式
  - 隧道模式保护的是整个IP包。
  - 将一个数据包用一个新的数据包封装
  - 通常在数据包的始发点或目的地不是安全终点的情况下，需要使用隧道模式
  - 一般在防火墙或路由器提供IPSec
- 传输模式对于保护两个支持IPSec的主机间的连接是很合适的，开销小；隧道模式对于那些包含了安全网关的配置是很有用的。

传输模式和隧道模式的比较



IPSec的实施位置—源端主机

- 优点：
  - 可以保障端到端的安全性；
  - 能够实现所有的IPSec安全模式；
  - 能够针对单个数据流提供安全保障；
  - 在建立IPSec的过程中，能够记录用户身份验证的相关数据和情况。
- 实施方案可分为两类：
  - 与主机中的操作系统集成；
  - 作为一个单独的部分在协议堆栈的网络层和数据链路层之间实施。

IPSec的实施位置—路由器

- 优点：
  - 能对两个子网（私有网络）间通过公共网络（如Internet）传输的数据提供安全保护；
  - 能通过身份验证控制授权用户从外部进入私有网络，而将非授权用户挡在私有网络的外面。
- 实施方案也可分为两类：
  - IPSec功能集成在路由器软件中；
  - IPSec功能在直接物理接入路由器的设备中实现，该设备一般不运行任何路由算法，只用来提供安全功能。

IPsec

- **IPsec 中最主要的两个部分**
  - 鉴别首部 **AH (Authentication Header)： AH 鉴别源点和检查数据完整性，但不能保密。**
  - 封装安全有效载荷 **ESP (Encapsulation Security Payload)：ESP 比 AH 复杂得多，它鉴别源点、检查数据完整性和提供保密。**

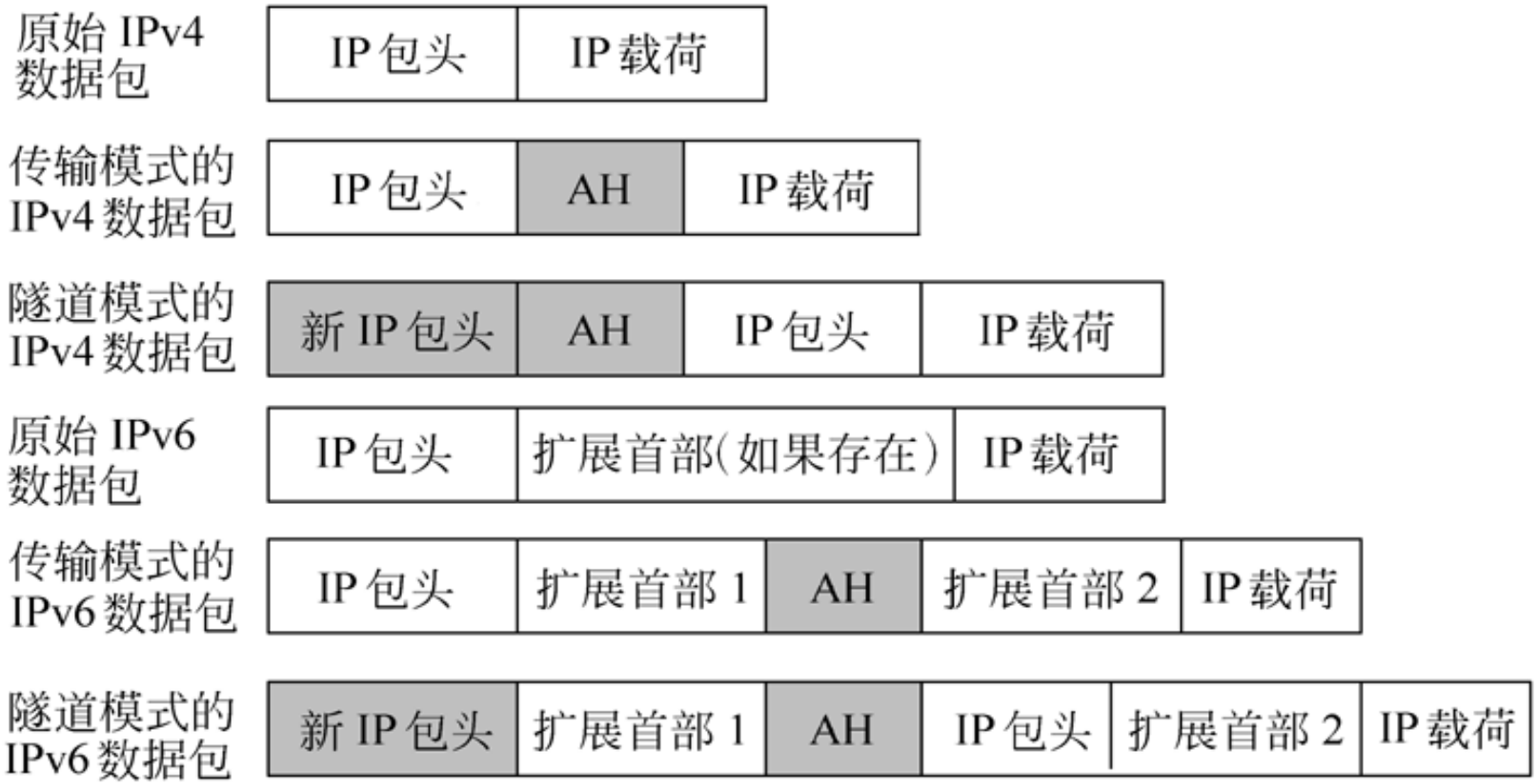
IPsec

- **鉴别首部协议 AH**
- 为IP包提供数据完整性和鉴别功能
- 利用MAC码实现鉴别，双方必须共享一个密钥
- 鉴别算法由SA指定
  - **鉴别的范围：整个包**
- 两种鉴别模式：
  - **传输模式：不改变IP地址，插入一个AH**
  - **隧道模式：生成一个新的IP头，把AH和原来的整个IP包放到新IP包的载荷数据中**

IPsec

- 鉴别首部协议 **AH**
  - 在使用鉴别首部协议 **AH** 时，把 **AH** 首部插在原数据报数据部分的前面，同时把 **IP** 首部中的协议字段置为 **51**。
  - 在传输过程中，中间的路由器都不查看 **AH** 首部。当数据报到达终点时，目的主机才处理 **AH** 字段，以鉴别源点和检查数据报的完整性。

传输模式和隧道模式的AH数据包格式

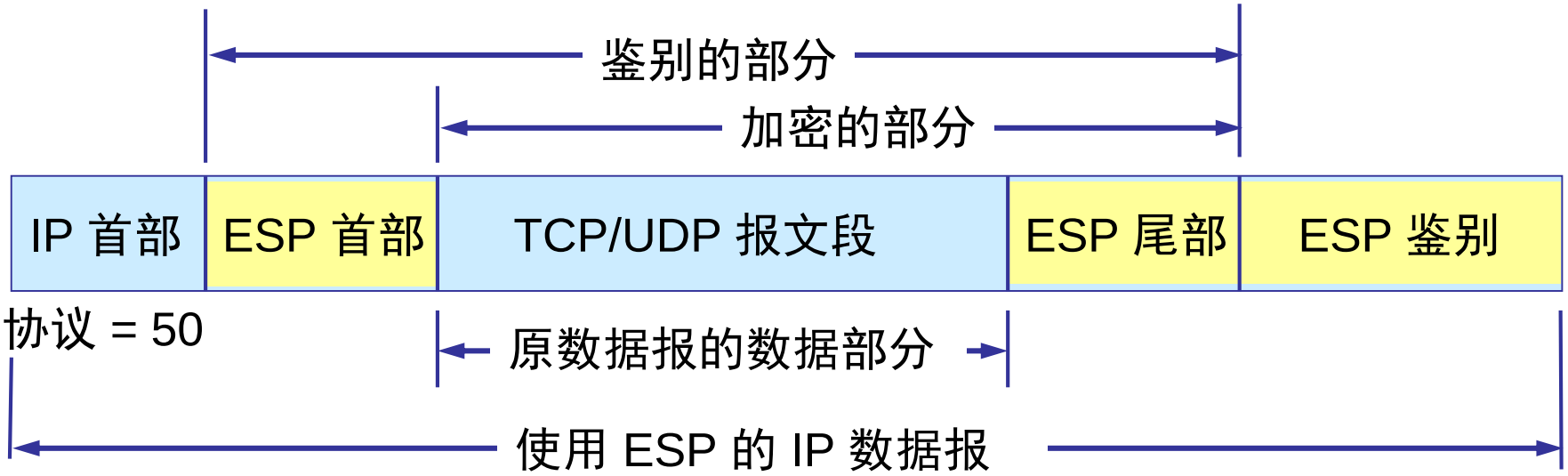


ESP

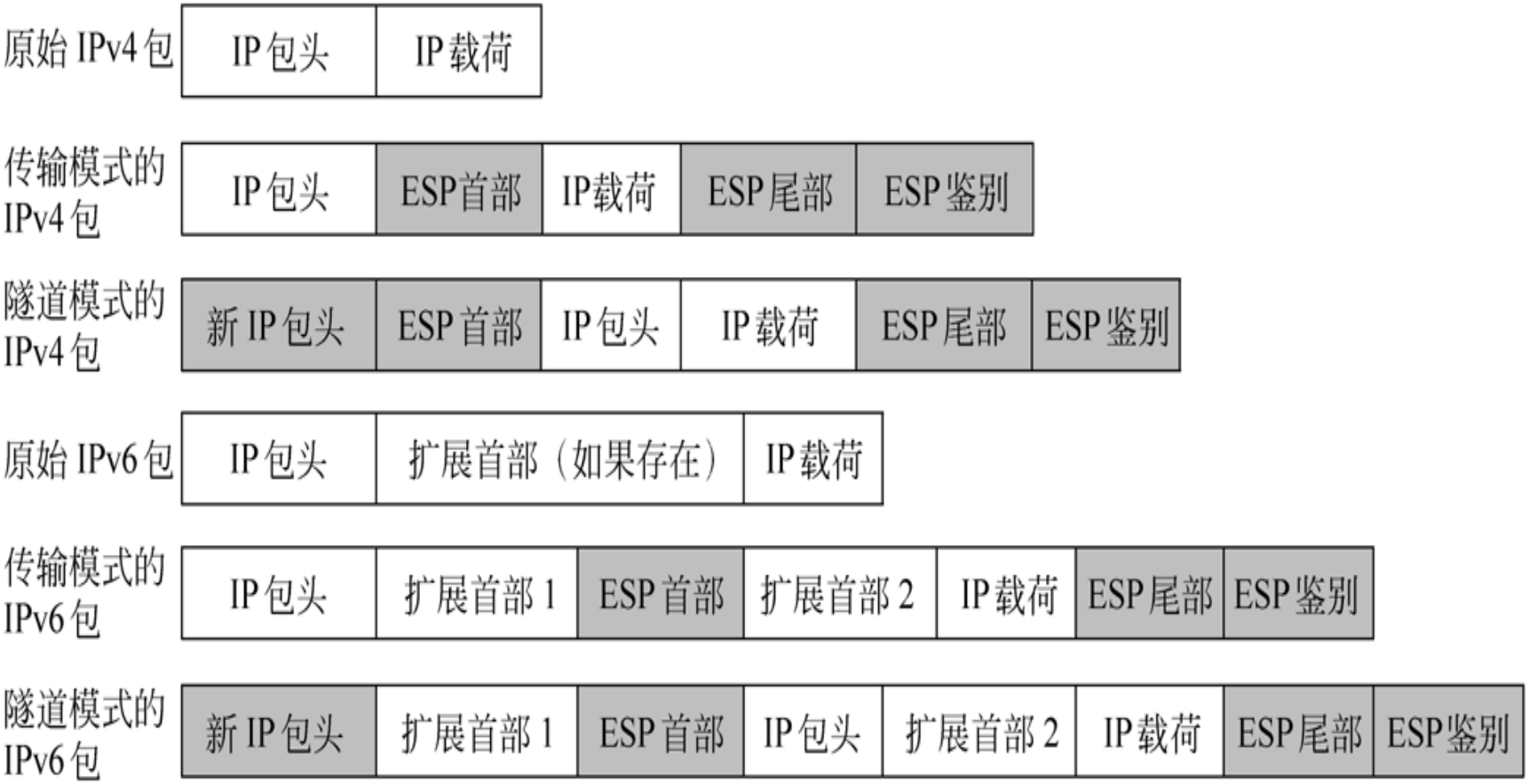
- 提供保密功能，包括报文内容的机密性和有限的通信量的机密性，也可以提供鉴别服务（可选）
- 将需要保密的用户数据进行加密后再封装到一个新的IP包中，ESP只鉴别ESP头之后的信息
- 加密算法和鉴别算法由SA指定
- 两种模式：传输模式和隧道模式

IPsec

- 在 IP 数据报中的ESP 的各字段



传输模式和隧道模式的ESP数据包格式



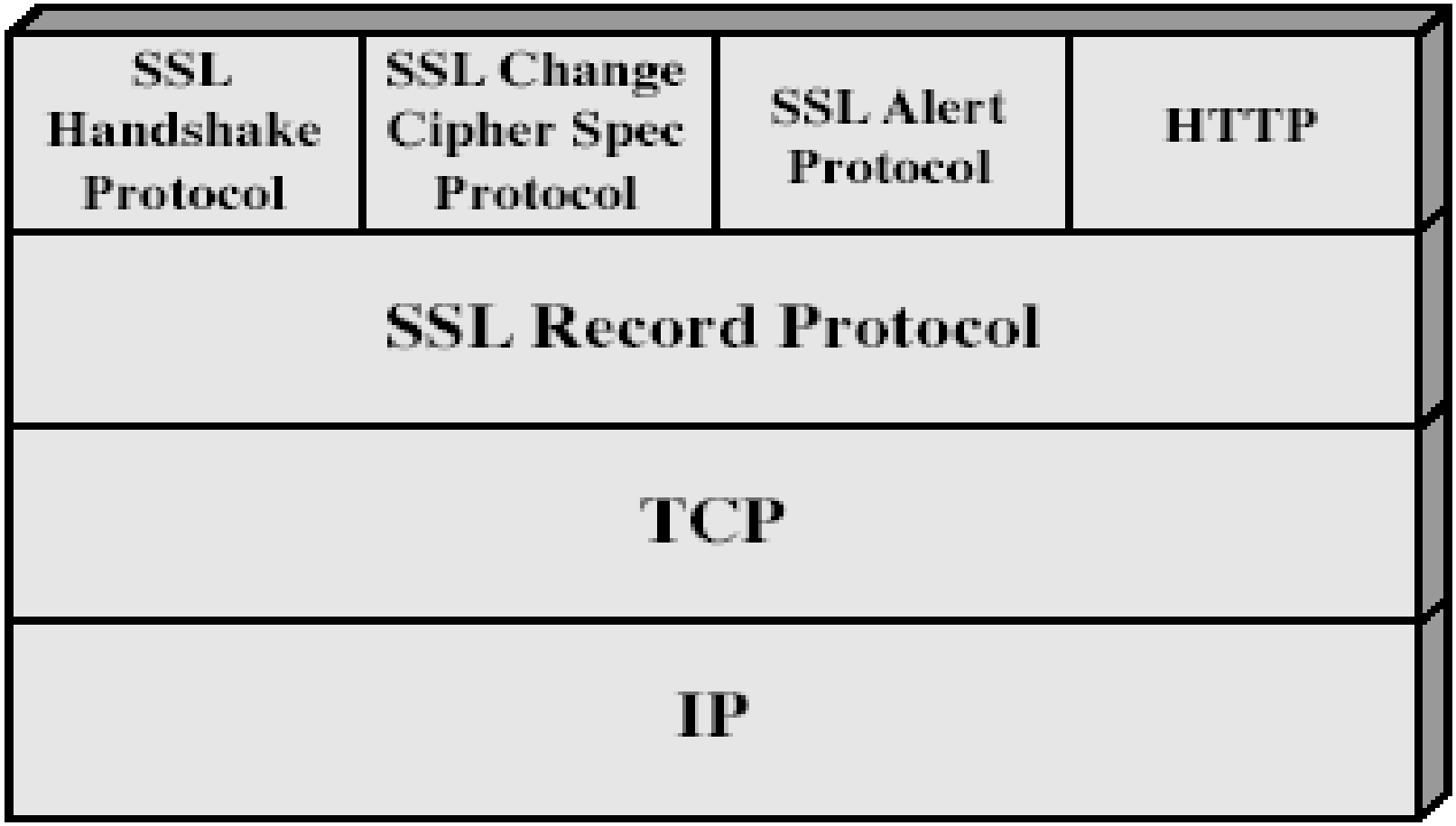
9.3.2 运输层安全协议

- 1. 安全套接层 SSL
  - SSL 是安全套接层 (Secure Socket Layer)，被设计用来使用TCP提供一个可靠的端到端安全服务，为两个通讯个体之间提供保密性和完整性(身份鉴别)
  - SSL 不仅被所有常用的浏览器和万维网服务器所支持，而且也是运输层安全协议 TLS (Transport Layer Security)的基础。

SSL 功能

- **SSL 提供四个基本功能**
  - ✓ **Authentication**
  - ✓ **Encryption**
  - ✓ **Integrity**
  - ✓ **Key Exchange**
- 采用两种加密技术
  - ✓非对称加密：认证、交换密钥
  - ✓对称加密：加密传输数据

SSL的体系结构


SSL Handshake Protocol
SSL Change Cipher Spec Protocol
SSL Alert Protocol
HTTP
SSL Record Protocol
TCP
IP

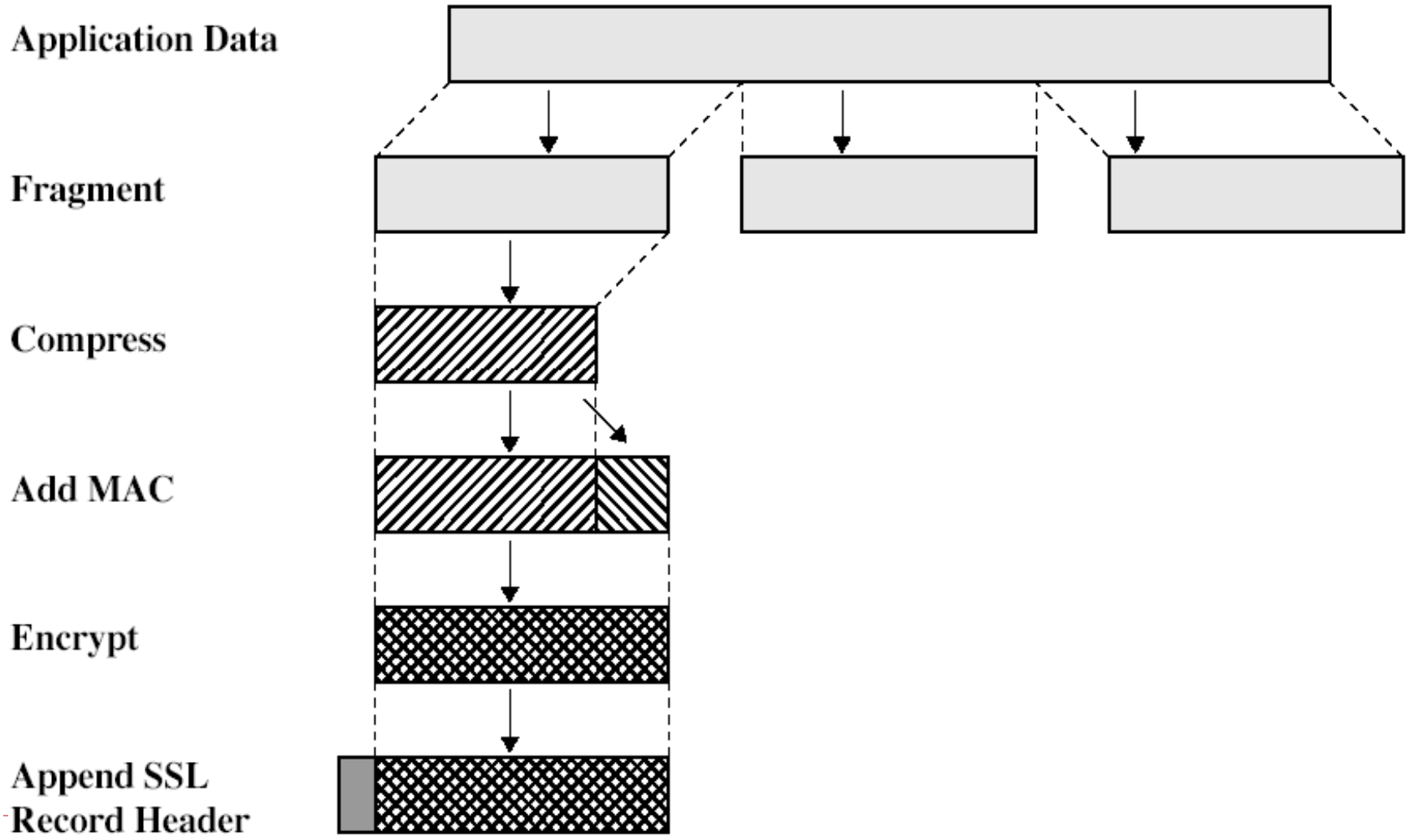
SSL记录协议层

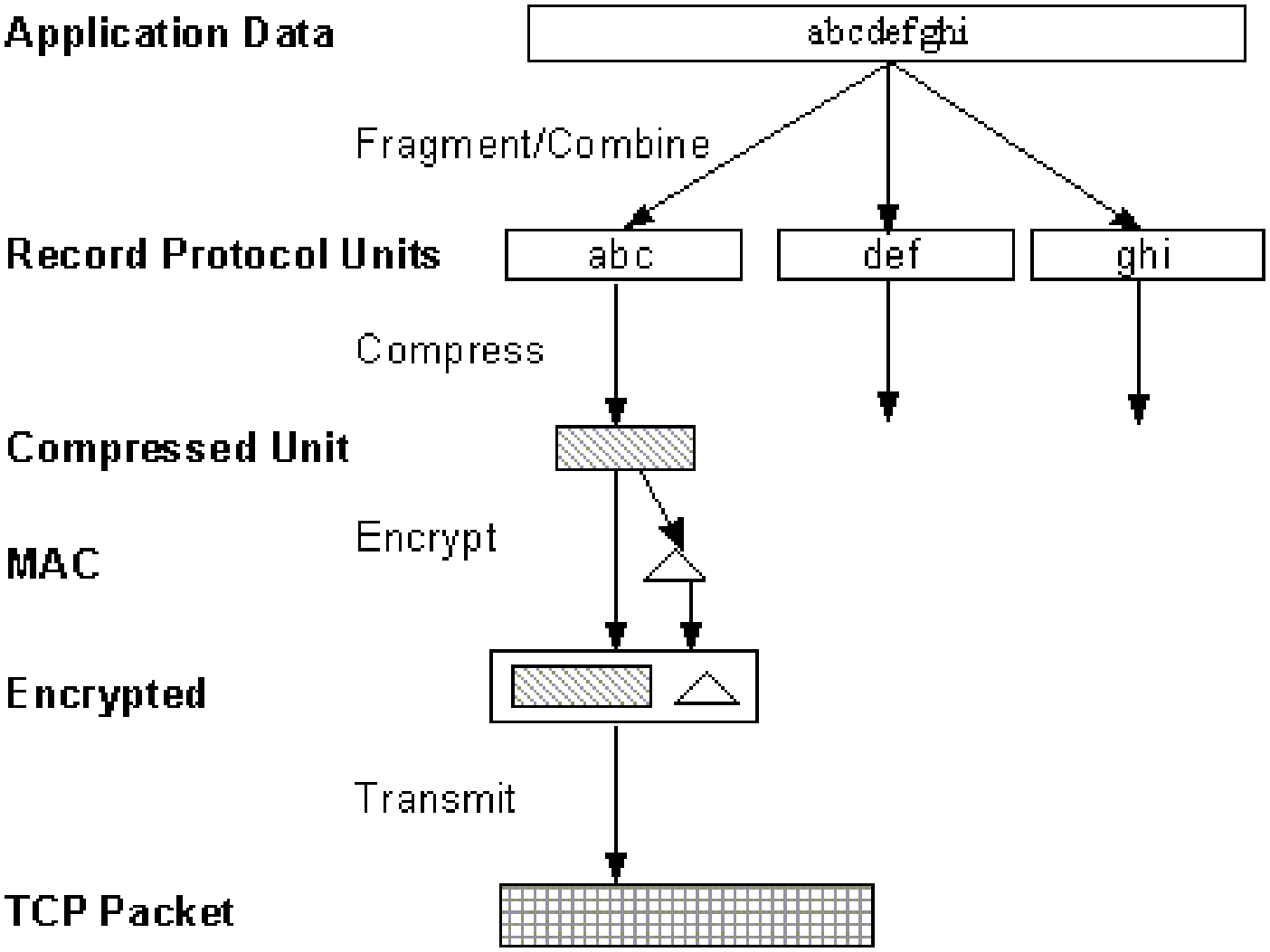
- SSL Record Protocol layer。
- 为高层协议提供基本的安全服务。
- 记录层封装各种高层协议。
- 具体实施压缩解压缩、加密解密、计算和校验MAC等与安全有关的操作。

SSL 记录协议

- SSL 记录协议为SSL连接提供两种服务
  - 保密性。利用握手协议所定义的共享密钥对SSL净荷（payload）加密 。
  - 完整性。利用握手协议所定义的共享的MAC密值来生成报文的鉴别码（MAC）。

SSL工作过程和SSL记录格式




Application Data
abcdefghi
Fragment/Combine
Record Protocol Units
abc
def
ghi
Compress
Compressed Unit
Encrypt
MAC
Encrypted
Transmit
TCP Packet

SSL记录协议操作

SSL工作过程

- 发送方的工作过程
  - 从上层接收要发送的数据（包括各种消息和数据）；
  - 对信息进行分段，成若干记录；
  - 使用指定的压缩算法进行数据压缩数据（可选）；
  - 使用指定的MAC算法生成MAC；
  - 使用指定的加密算法进行数据加密；
  - 发送数据。

- **接收方的工作过程**
  - ✓ 接收数据；
  - ✓ 使用指定的解密算法解密数据；
  - ✓ 使用指定的MAC算法校验MAC；
  - ✓ 使用压缩算法对数据解压缩（在需要时进行）；
  - ✓ 将记录进行数据重组；
  - ✓ 将数据发送给高层。

SSL握手协议层

- SSL HandShake Protocol layer。
- 用于SSL管理信息的交换，允许应用协议传送数据之前相互验证，协商加密算法和生成密钥等。
- 包括：
  - SSL握手协议（SSL HandShake Protocol）；
  - SSL密码参数修改协议（SSL Change Cipher Spec Protocol）；
  - 应用数据协议（Application Data Protocol）；
  - SSL告警协议（SSL Alert Protocol）。

9.3.3 应用层的安全协议

- **PGP (Pretty Good Privacy)**
  - **PGP** 是一个完整的电子邮件安全软件包，包括加密、鉴别、电子签名和压缩等技术。
  - **PGP** 并没有使用什么新的概念，它只是将现有的一些算法如 **MD5**，**RSA**，以及 **IDEA** 等综合在一起而已。
  - 虽然 **PGP** 已被广泛使用，但 **PGP** 并不是因特网的正式标准。