第九讲　网络安全协议与应用

§9.1 电子邮件安全

§9.2 Web安全

§9.3 电子商务安全

§9.4 IP安全

§9.1 电子邮件安全

- E-mail 是Internet上最大的应用，也是唯一的广泛跨平台、跨体系结构的分布式应用。
- E-mail系统组成：

（1）邮件分发代理：将邮件数据库中的邮件分发到用户的邮箱，并承担邮件自动过滤、自动回复和自动触发等任务。

（2）邮件传输代理：负责邮件的接收和发送，通常采用SMTP协议传输邮件。

（3）邮件用户代理：将邮箱中的邮件显示给用户，常用协议有POP3和IMAP

（4）邮件工作站：邮件用户直接操作的计算机，负责显示、撰写邮件等。

§9.1 电子邮件安全

- E-mail 的安全目标：

（1）邮件分发安全：阻止垃圾邮件和开放转发，查杀病毒。

（2）邮件传输安全：保障邮件传输的机密性和完整性。

（3）邮件用户安全：确认用户身份，并在工作站端支持病毒查杀功能。

- E-mail 的安全措施：

（1）身份认证：包括邮件转发认证，邮件收发认证等。

（2）加密、签名：保障重要邮件的机密性和完整性。

（3）协议过滤：防止邮件账号的远程查询。

（4）设立防火墙，安装邮件病毒过滤系统。

§9.1 电子邮件安全

- 安全的电子邮件主要是解决身份鉴别和保密性的安全问题。
- 邮件安全协议：
  - PGP— Pretty Good Privacy
  - PEM—Privacy Enhanced Mail
  - S/MIME—Secure/Multipurpose Internet Mail Extension

§9.1 电子邮件安全

- 实例分析：PGP
  - 作者：美国软件工程师Philip Zimmerman
  - 提供可用于电子邮件和文件存储应用的保密与鉴别服务。
- PGP发展特点
  - 选择最可用的加密算法作为系统的构造模块
  - 将这些算法集成到一个通用的应用程序中，该程序独立于操作系统和处理器，并且基于一个使用方便的小命令集
  - 程序、文档在Internet上公开
  - 一个商业公司提供全兼容、低成本的商业版本

§9.1 电子邮件安全

- PGP广泛应用的原因
  - 免费、可用于多平台
  - 选用算法的生命力和安全性公众认可
  - 具有广泛的可用性
  - 不由政府或标准化组织控制

§9.1 电子邮件安全

- PGP运行描述
  - 数字签名：DSS/SHA或RSA/SHA
  - 消息加密：CAST-128或IDEA或3DES + Diffie-Hellman或RSA
  - 数据压缩：ZIP
  - 邮件兼容：Radix 64
  - 数据分段

§9.1 电子邮件安全

- PGP功能：

一、身份认证功能的实现

- 发送者产生消息M
- 用SHA-1对M生成一个160位的散列码H
- H用发送者的私钥加密，并与M连接
- 接收者用发送者的公钥解密并恢复散列码H
- 对消息M生成一个新的散列码，与H比较。如果一致，则消息M被认证。

§9.1 电子邮件安全

二、加密功能的实现

采用CAST-128(或IDEA或3DES)、6464位CFB方式。

一次性密钥，单向分发，公钥算法保护。

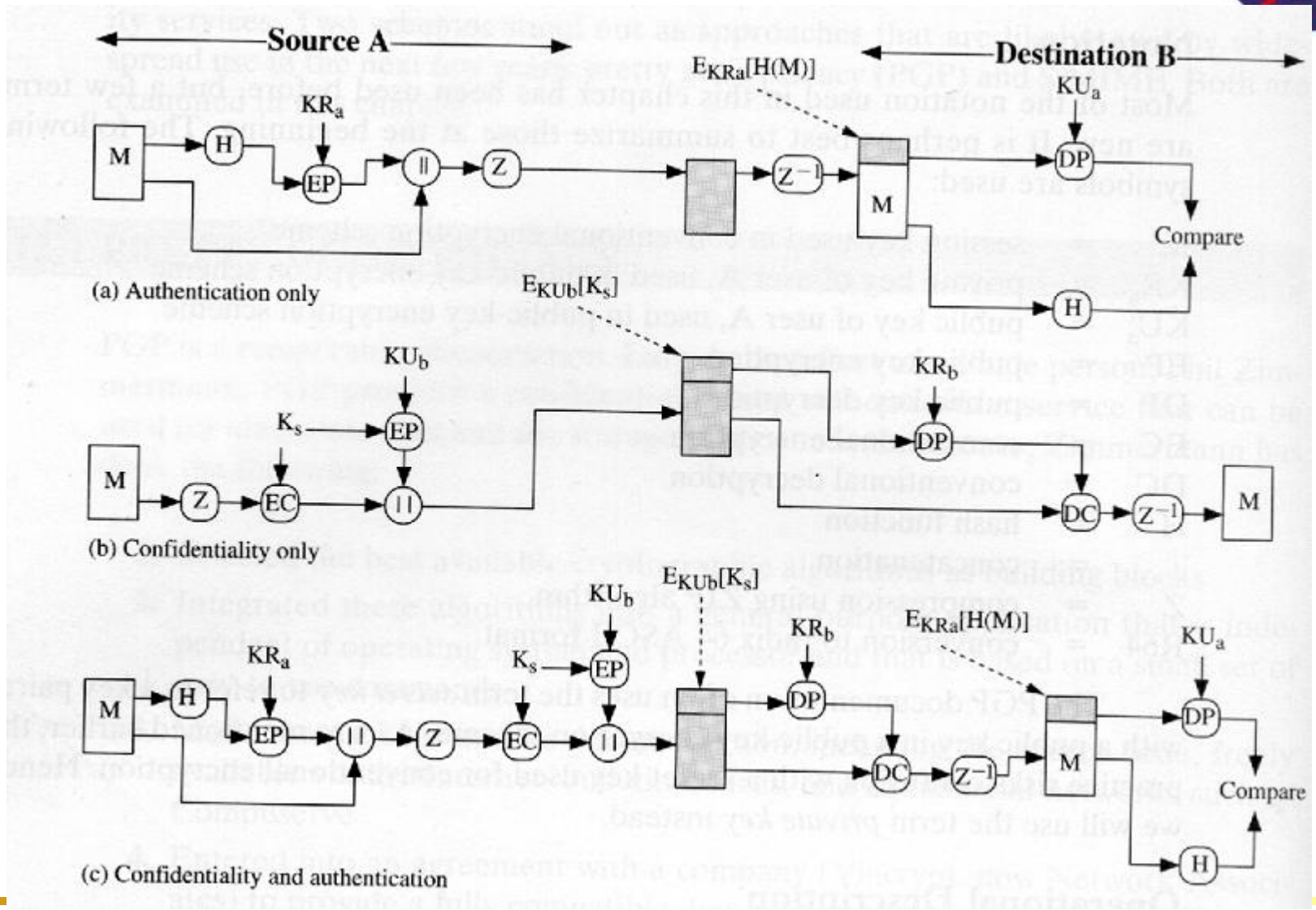
- 发送者生成消息M并为该消息生成一个128位的随机数作为会话密钥。
- M被加密，使用会话密钥、CAST-128算法（或 IDEA或3DES）
- 会话密钥用RSA及接收者的公钥加密并与消息M结合。
  （也可用Diffie-Hellman算法）
- 接收者用自己的私钥解密恢复会话密钥
- 用会话密钥解密恢复消息M。

§9.1 电子邮件安全

三、保密与认证同时运用

两种服务都需要时，发送者先用自己的私钥签名，然后用会话密钥加密，再用接收者的公钥加密会话密钥。

§9.1 电子邮件安全

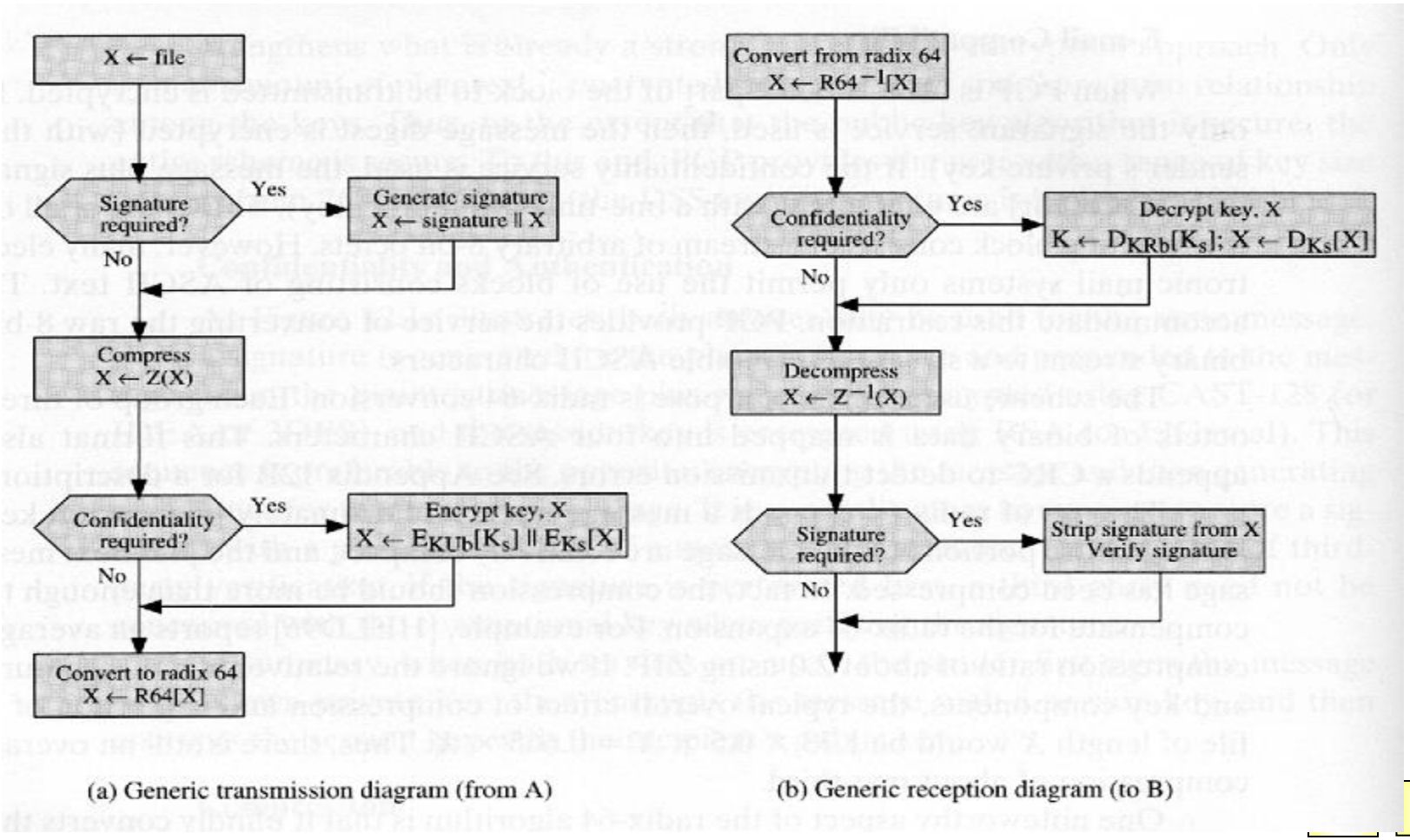

Source A
Destination B
$E_{KRa}[H(M)]$
KR_a
KU_a
M
H
EP
||
Z
Z^{-1}
DP
Compare
(a) Authentication only
$E_{KUb}[K_s]$
KU_b
K_s
KR_b
EC
DC
(b) Confidentiality only
(c) Confidentiality and authentication

§9.1 电子邮件安全

- 数据压缩
  - 发生在签名后、加密前。
  - 对邮件传输或存储都有节省空间的好处。
- E-mail兼容性
  - 加密后是任意的8位字节，需要转换到ASCII格式。
  - Base64将3字节输入转换到4个ASCII字符并带CRC校验。
- 分段与重组
  - Email常常受限制于最大消息长度
  - 更长的消息要进行分段，每一段分别邮寄
  - PGP自动分段并在接收时自动恢复
  - 签名只需一次，在第一段中

§9.1 电子邮件安全

- PGP消息的发送和接收



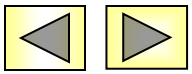
§9.1 电子邮件安全

- PGP密钥管理

（1）PGP密钥需求

使用四种类型的密钥：一次性会话密钥，公钥，私钥，基于通行短语的密钥。

- 需要一种生成不可预知的会话密钥的手段
- 需要某种手段来标识具体的密钥。
  - 一个用户拥有多个公钥/私钥对。（更换，分组）
- 每个PGP实体需要维护一个文件保存其公钥私钥对和一个文件保存通信对方的公钥。



§9.1 电子邮件安全

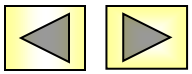
1、会话密钥的生成

- 输入包括一个128位的密钥和两个64位的数据块作为加密的输入。使用CFB方式，CAST-128产生两个64位的加密数据块，这两个数据块的结合构成128位的会话密钥。
- 作为明文输入的两个64位数据块，是从一个128位的随机数流中导出的。这些数是基于用户的键盘输入的。键盘输入时间和内容用来产生随机流。因此，如果用户以他通常的步调敲击任意键，将会产生合理的随机性。

§9.1 电子邮件安全

2、密钥标识符

- 一个用户有多个公钥/私钥对时，接收者如何知道发送者是用了哪个公钥来加密会话密钥？
  - 将公钥与消息一起传送
  - 将一个标识符与一个公钥关联。对一个用户来说做到一一对应
- 定义KeyID 包括64个有效位：(KUa mod 264)
- KeyID需要发送方进行数字签名



§9.1 电子邮件安全

（2）密钥环

PGP在每一个节点上提供一对数据结构

- 存储该节点拥有的公钥/私钥对---私钥环
- 存储本节点知道的其他用户的公钥---公钥环

§9.1 电子邮件安全

（3）PGP公钥管理问题

- 由于PGP重在广泛地在正式或非正式环境下应用，没有建立严格的公钥管理模式。
- 如果A的公钥环上有一个从BBS上获得B发布的公钥，但已暴露给C了，这样就存在两条通道。C可以向A发信并冒充B的签名，A以为是来自B；A与B的任何加密消息C都可以读取。
- 为了防止A的公钥环上包含错误的公钥，有若干种方法可用于降低这种风险。

§9.1 电子邮件安全

1、物理上得到B的公钥。

2、通过电话验证公钥。B将其公钥email给A，A可以用PGP对该公钥生成一个160位的SHA-1摘要，并以16进制显示。这一特点称作密钥的“指纹”。然后A打电话给B，让B在电话中对证“指纹”。如果双方一致，则该公钥被认可。

3、从双方都信任的个体D处获得B的公钥。D是介绍人，生成一个签名的证书。其中包含B的公钥，密钥生成时间。D对该证书生成一个SHA-1摘要，用其私钥加密这个摘要，并将其附加在证书后。因为只有D能够产生这个签名，没有人可以生成一个错误的公钥并假装是D签名的。这个签名的证书可以由B或D直接发给A，也可以贴到公告牌上。

4、从一个信任的CA中心得到B的公钥。

§9.1 电子邮件安全

➢ 信任关系的应用

尽管PGP没有包含任何建立认证权威机构或建立信任体系的规格说明，但它提供了一个利用信任关系的手段，将信任与公钥关联，利用信任信息：

- 密钥合法性字段：表明PGP将信任这是一个对该用户是合法的公钥；信任级别越高，这个userID对这个密钥的绑定越强。这个字段是由PGP计算的。
- 签字可信赖字段：每一个签名与一个签字可信赖字段关联，表明这个PGP用户对签名人对公钥签名的信任程度。密钥合法性字段是由多个签字可信赖字段导出的。
- 拥有人可信赖性字段：表明该公钥被信任用于签名其它公钥证书的信任程度。这一级别的信任是由用户给出的。

§9.1 电子邮件安全

- 信任关系的处理过程

1、当A向公钥环中插入一个新公钥时，PGP必须向trust flag 赋值，该标志与该公钥的主人相关。如果其主人是A，则该值为最高信任(ultimate trust)。否则，PGP询问用户，让用户给出信任级别。用户可选：该公钥的主人是不认识(unknown)、不信任(untrusted)、接近信任 (marginally trusted)或完全信任(complete trusted)

§9.1 电子邮件安全

- 信任关系的处理过程

2、当新公钥进入时，可能有一个或多个签名跟随其后。许多签名可以以后再加入。当一个签名插入到一个条目中时，PGP查找该公钥环中是否已有公钥的主人中包含该公钥的作者。如果包含，则这个主人的OWNER TRUST值被赋予该签名的SIGTRUST字段。否则，赋予unknown user值。

3、密钥合法性字段的值基于该条目中签名可信赖字段来计算。如果至少一个签名有一个签名信任值为ultimate，则密钥合法性字段的值设为complete。否则，PGP计算一个信任值的权重和。

§9.1 电子邮件安全

- 公钥的作废
  - 密钥暴露或定时更新导致需要公钥报废功能
  - 通常的报废方法是由主人签发一个密钥报废证书。这个证书具有与通常签名证书相同的形式，但包含一个指示符表明这个证书是要作废该公钥的使用。注意到所对应的私钥必须用来签名一个密钥报废证书，其主人应尽可能越广越快散布这个证书，以使得潜在的有关人员更新他们的公钥环。
  - 注意：对手也可以发出这个证书，然而，这将导致他自己也被否决。因此，这样比起恶意使用偷来的私钥来看似乎会减少漏洞。

§9.2 Web安全

- Web是一个运行于internet和TCP/IP intranet 之上的基本的client/server应用。
- Web安全性涉及前面讨论的所有网络信息的安全性内容，同时还具有新的挑战。
  - Web具有双向性，Web server易遭受Internet的攻击。
  - 实现Web浏览、配置管理、内容发布等功能的软件异常复杂。其中隐藏许多潜在的安全隐患。
  - Web通常是一个公司或机构的发布板，常和其它计算机联系在一起。一旦Web server被攻破，可能殃及其它。
  - 用户往往是偶然的和未经训练的，对安全风险没有意识，更没有足够的防范工具和知识。

§9.2 Web安全

➢ Web安全性威胁与对策

	威胁	后果	对策
完整性	修改用户的数据 特洛伊木马浏览器 修改内存 修改传输的数据流	信息丢失 机器暴露 其它所有威胁的弱点	加密校验和
保密性	网上偷听 从服务器处偷信息 从客户端处偷信息 关于网络配置的信息 关于客户连接的信息	丢失信息 丢失隐私	加密、Web 代理
业务否决	-中断用户连接 -用伪造的威胁淹没服务器 塞满硬盘或内存 攻击 DNS 隔离服务器	中断 骚扰 阻止用户完成正常工作	难以防范
认证鉴别	冒充合法用户 数据伪造	以假乱真 误信错误信息	加密技术

§9.2 Web安全

- Web安全防护技术
  - 基于主机的入侵检测
  - 文件I/O监测
  - 上载请求的合法性验证
  - 信息流的认证和加密
- 基于Web信息流的安全方法
  - 网络层——IP 安全性(IPSec)
  - 传输层—— SSL / TLS
  - 应用层——S/MIME，PGP，SET，Kerberos

§9.2 Web安全

- SSL -Secure Socket Layer
  - 安全套接层是一种用于网站安全连接的协议或技术
  - 所谓的安全连接有两个作用：
    - 首先是SSL可以提供信息交互双方认证对方的身份标识。显而易见地，这对当你开始与对方交换机密信息前确切了解对方身份是非常重要的。SSL通过数字证书的技术实现使得这一需求得以满足。
    - 另一个是它能够使数据以不可读的格式传输，以利于在不可信网络（例如互联网）上的安全传输需要。这种不可读格式通常由加密技术实现。

§9.2 Web安全

SSL体系结构

- SSL设计用来使用TCP提供一个可靠的端到端安全服务

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

- SSL记录协议为更高层提供基本安全服务。 特别是HTTP，它提供了Web的client/server交互的传输服务，可以构造在SSL之上
- SSL握手协议，SSL修改密文协议，SSL告警协议是SSL的高层协议，用于管理SSL交换

§9.2 Web安全

- SSL的两个重要概念
  - SSL连接（connection）
    - 一个连接是一个提供一种合适类型服务的传输。
    - SSL的连接是点对点的关系。
    - 连接是暂时的，每一个连接和一个会话关联。
  - SSL会话（session）
    - 一个SSL会话是在客户与服务器之间的一个关联。会话　由Handshake Protocol创建。会话定义了一组可供多个连接共享的加密安全参数。
    - 会话用以避免为每一个连接提供新的安全参数所需高昂的谈判代价。

§9.2 Web安全

- SSL 应用中的安全问题
  - Client系统、Server系统、Keys和Applications都要安全
  - 短的公开密钥、加密密钥以及匿名服务器需谨慎使用
  - 对证书、CA要谨慎选择
  - SSL的实现不出安全错误。在实现上最可能失败之处是sanity check和密钥管理

§9.3 电子商务安全

- 电子商务安全任务
  - 身份认证：持卡者、商家银行
  - 有效性
  - 机密性
  - 完整性
  - 抗抵赖

§9.3 电子商务安全

- 安全协议SET协议

  (Secure Electronic Transaction 安全电子交易协议)

  - 是由世界上两大信用卡商Visa和Master Card于1997年5月联合制定的实现网上信用卡交易的模型和规范。
  - SET规范，是一种为基于信用卡而进行的电子交易提供安全措施的规则；是一种能广泛应用于Internet上的安全电子付款协议。
  - SET中的核心技术主要有公开密匙加密、电子数字签名、电子信封、电子安全证书等

§9.3 电子商务安全

- SET协议的作用和地位
  - SET规范，为在Internet上进行安全的电子商务提供了一个开放的标准。SET综合使用私用密钥加密和公用密钥加密的电子认证技术，其认证过程使用RSA和DES算法。因此，可以为电子商务提供很强的安全保护。
  - SET主要是为了解决用户、商家和银行之间通过信用卡支付的交易而设计的，以保证支付信息的机密、支付过程的完整、商户及持卡人的合法身份，以及可操作性。
  - SET规范是目前电子商务中最重要的协议。SET得到了美国IT企业的支持，如GTE、IBM、Microsoft、Netscape、RSA、SAIC、Terisa 和VeriSign

§9.3 电子商务安全

- SET协议的参与实体
  - SET协议执行步骤与常规的信用卡交易过程基本相同，只是它是通过因特网来实现的。
  - 在SET协议系统中，参与交易的主要有四种：实体持卡人，电子商家，收单银行，发卡银行。持卡人主要指持有信用卡的消费者；电子商家主要职能支持网络购物的电子商店等提供电子交易服务的企业组织；收单银行主要使用支付系统的专用网关提供各商家的因特网在线借款服务；发卡银行负责处理信用卡的发放账目管理付款清算等。
  - 此外，在协议系统中还有认证中心（CA） 它是一些发卡机构共同委派的公证代理组织，其主要功能是产生、分配和管理发卡人、商家和参与电子交易等。

§9.3 电子商务安全

- SET协议的加密流程
  - 在一个典型的SET协议传输过程中，存在许多商家与客户之间、客户与银行之间的交互隐私信息，SET将两种隐私都包含在一个经过数字签名的交易过程中
  - 银行需要的信息用银行的公钥加密，商家的信息用商家的公钥加密。这意味着商家就无权访问信用卡信息，从而欺诈行为就基本上避免了
  - 除了加密数据，两套信息也需要数字签名，最后两个签名将被合并来产生整个交易过程中需要的签名

§9.3 电子商务安全

- SET协议规定的工作流程
  - 用户向商家发送购货单和一份经过签名、加密的信托书。书中的信用卡号是经过加密的，商家无从得知
  - 商家把信托书传送到收单银行，收单银行可以解密信用卡号，并通过认证验证签名
  - 收单银行向发卡银行查问，确认用户信用卡是否属实
  - 发卡银行认可，并签证该笔交易
  - 收单银行认可商家，并签证此交易
  - 商家向用户传送货物和收据
  - 交易成功，商家向收单银行索款
  - 收单银行按合同将货款划给商家
  - 发卡银行向用户定期寄去信用卡消费账单

§9.4 IP安全

- IP安全是整个TCP/IP安全的基础与核心。它可对上层的各种应用服务提供透明的安全保护。
- IP级安全问题涉及三个功能领域：认证、保密和密钥管理。
- IPSec是指IETF以RFC形式公布的一组安全IP协议集，属IP级安全保护协议标准。
- IPSec的主要特征是可以支持IP级所有流量的加密和/或认证。因此可以增强所有分布式应用的安全性。

§9.4 IP安全

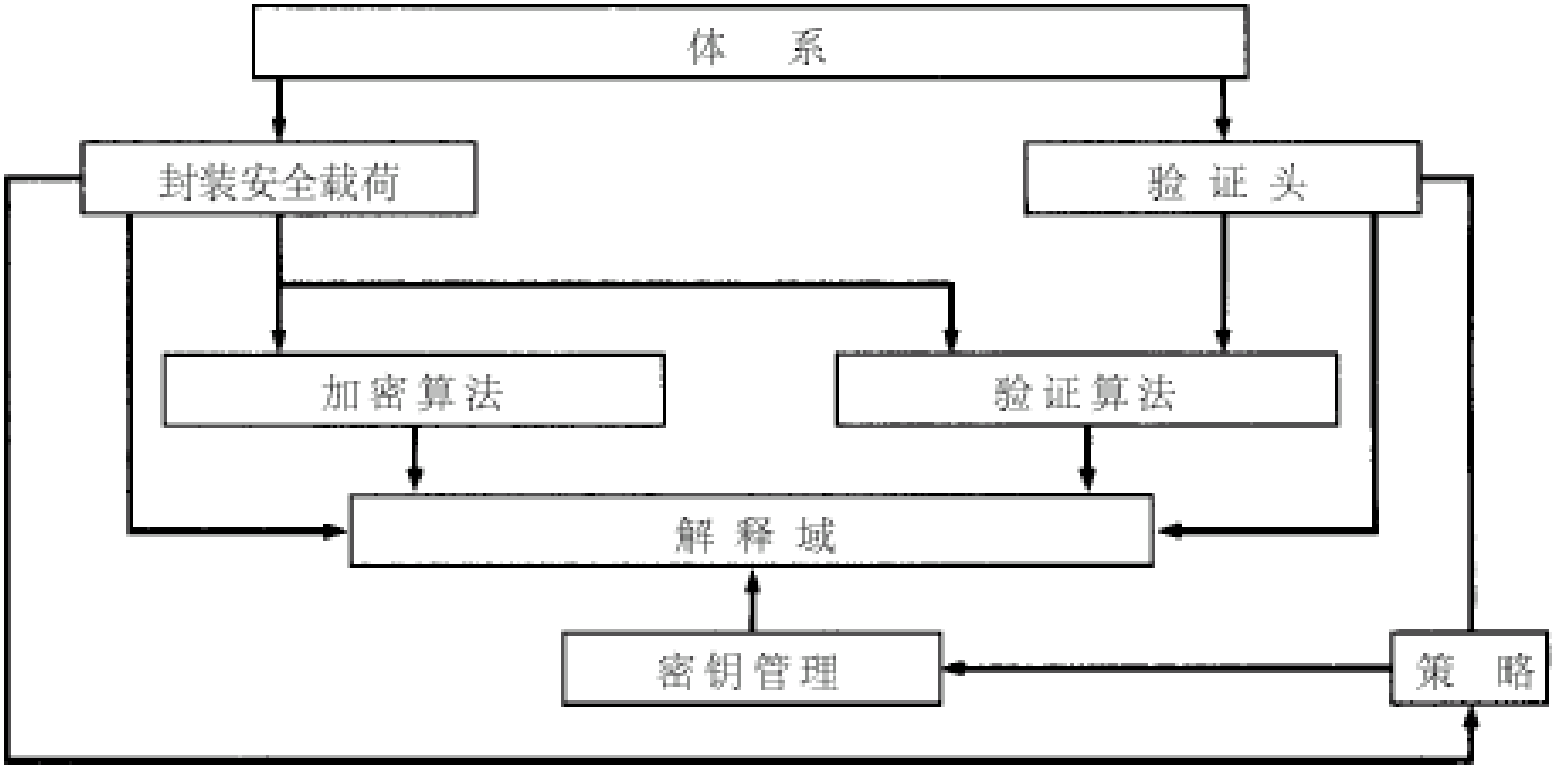
IPSec安全体系结构

包括总体概念，安全需求，定义以及定义IPSec技术的机制；

- ESP：使用ESP进行包加密的报文包格式和一般性问题，以及可选的认证；
- AH：适用于AH协议提供分组鉴别相关的分组格式和一般性问题；
- 加密算法：描述将各种不同加密算法用于ESP的文档；
- 认证算法：描述将各种不同认证算法用于AH以及ESP认证选项的文档；
- 密钥管理：描述密钥管理模式；
- DOI：其它相关文档，批准的加密和认证算法标识，以及运行参数等；

§9.4 IP安全

- IPSec安全体系结构图



§9.4 IP安全

- IPSec协议组成
  - 安全关联SA （Security Association）
  - 安全策略数据库SPD (Security Policy Database)
  - 认证头AH （Authentication Head ）
  - 封装安全载荷ESP(Encapsulation Security Payload)
  - IKE（Internet密钥交换）
  - ISAKMP/Oakley（密钥管理协议）

    ISAKMP：Internet Security Association and Key Management Protocol

    Oakley：是D-H密钥交换协议的改进

§9.4 IP安全

IPSec提供的服务

IPSec在IP层提供安全服务，使得系统可以选择所需要的安全协议，确定该服务所用的算法，并提供安全服务所需任何加密密钥。

- 访问控制
- 连接完整性
- 数据源认证
- 拒绝重放数据包
- 保密性（加密）
- 有限信息流保密性

§9.4 IP安全

- IPSec提供的服务

	AH	ESP（加密）	ESP（加密并认证）
访问控制	√	√	√
无连接完整性	√		√
数据来源认证	√		√
对重放数据的拒绝	√	√	√
保密性		√	√
受限业务流的保密性		√	√

§9.4 IP安全

- IPSec 两种不同的使用模式
  - 传送模式：保护上层协议；用于两主机之间；
  - 隧道模式：保护整个IP数据报；当一方为网关时采用

原始IP包： IP头 + TCP头 + 数据

传送模式： IP头 + IPSec头 + TCP头 + 数据

隧道模式：新 IP头 + IPSec头 + IP头 + TCP头 + 数据

§9.4 IP安全

安全关联

- 为正确封装及提取IPSec数据包，要将安全服务、密钥与要保护的通信数据联系到一起；同时要将远程通信实体与要交换密钥的IPSec数据传输联系起来。这样的方案称为安全关联（Security Association，SA）。
- SA是构成IPSec的基础。它由两个通信实体协商建立。它们决定了用来保护数据包安全的IPSec协议、密钥以及密钥的有效存在时间等。任何IPSec实施方案都会构建一个SA数据库（SAD），由它来维护保障数据包安全的SA记录。

§9.4 IP安全

安全关联

- SA是单向进行的，它仅朝一个方向定义安全服务，要么对通信实体收到的包进行“进入”保护，要么对实体外发的包进行“外出”保护。
- SA由一个三元组唯一标识：
  - 安全参数索引（SPI）：存在于IPSec协议头内
  - 安全协议（AH、ESP）标识符
  - 目标IP地址：它同时决定了关联方向
- 通常SA是以成对的形式存在的，每个朝一个方向。既可人工创建它，亦可采用动态创建方式。SA驻留在“安全关联数据库（SAD）”内。

§9.4 IP安全

认证头

- AH（Authentication Header）
- AH是一种IPSec协议，用于为IP提供数据完整性、数据原始身份认证和一些可选的、有限的抗重播服务。
- AH定义在RFC2402中。除了机密性之外，AH提供ESP能够提供的一切东西。不需要加密算法（加密器），而需要一个认证器（身份认证器）。
- AH定义保护方法、头的位置、身份认证的覆盖范围以及输出和输入处理规则，但没有对所用的身份认证算法进行定义。

§9.4 IP安全

封装安全载荷

- ESP（Encapsulating Security Payload）
- ESP属于IPSec的一种协议，可用于确保IP数据包的机密性、数据的完整性以及对数据源的身份认证。此外，它也要负责对重播攻击的抵抗。
- 具体做法是在IP头之后、需要保护的数据之前，插入一个新头——ESP头。受保护的数据可以是一个上层协议，或者是整个IP数据报。最后，还要在最后追加一个ESP尾。ESP是一种新的IP协议，对ESP数据包的标识是通过IP头的协议字段来进行的。

§9.4 IP安全

Internet密钥交换

- IKE的用途是在IPSec通信双方之间，建立起共享安全参数及认证过的密钥（即建立“安全关联”）。
- IKE协议是Oakley和SKEME协议的混合，并在由ISAKMP规定的一个框架内运作。ISAKMP是“Internet安全关联和密钥管理协议”的简称，即Internet Security Association and Key Management Protocol。ISAKMP定义了包格式、重发计数器以及消息构建要求。它定义了整套加密通信语言。

§9.4 IP安全

IPSec的应用

- IPSec是IPv6必须支持的功能，它与防火墙、安全网关结合可形成各种安全解决方案；与其他协议相结合将使安全性更高；能使企业将其Extranet扩展到贸易伙伴进行电子商务，而不用担心安全协议的兼容性。
- IPSec的典型应用是构建虚拟专用网VPN

  VPN通过保密隧道在非信任公共网络上产生安全私有连接。它能把远程用户、分支机构和商业伙伴连接组成一个自治网络，达到与专用网同样的安全、可靠、可扩充、可管理、服务质量。IPSec为VPN的互操作性、管理、通信提供了有力手段。

