(2020春季　课程编号：011184)

信息安全导论

第10章 Internet安全

中国科学技术大学 曾凡平

billzeng@ustc.edu.cn

第9章 安全审计与责任认定技术

第10章 Internet安全

10.1 OSI安全体系结构

- 安全攻击，安全服务，安全机制

10.2 IPSec协议

- IPSec体系结构，IPSec工作模式，AH协议

10.3 SSL/TLS协议

- SSL体系结构，SSL记录协议，SSL修改密码规范协议，
- SSL报警协议，SSL握手协议，TLS协议

10.4 安全电子交易

- SET的需求，SET系统构成，双向签名，支付处理

10.1 OSI安全体系结构

- 为了有效评估一个机构的安全需求，以及对各个安全产品和策略进行评价和选择，负责安全的管理员需要以某种系统的方法来定义对安全的要求并刻画满足这些要求的措施。
- 国际标准化组织ISO于1989年正式公布了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”，定义了开放系统通信的环境中与安全性有关的通用体系结构元素。
- 作为OSI基本参考模型的补充，**其核心内容是保证异构计算机之间远距离交换信息的安全。**

安全攻击、安全机制和安全服务

- **(1)安全攻击**：任何危及企业信息系统安全的活动。
- **(2)安全机制**：用来检测、阻止攻击或者从攻击状态恢复到正常状态的过程，或实现该过程的设备。
- **(3)安全服务**：加强数据处理系统和信息传输的安全性的一种处理过程或通信服务。其目的在于利用一种或多种安全机制进行反攻击。

10.1.1 安全攻击

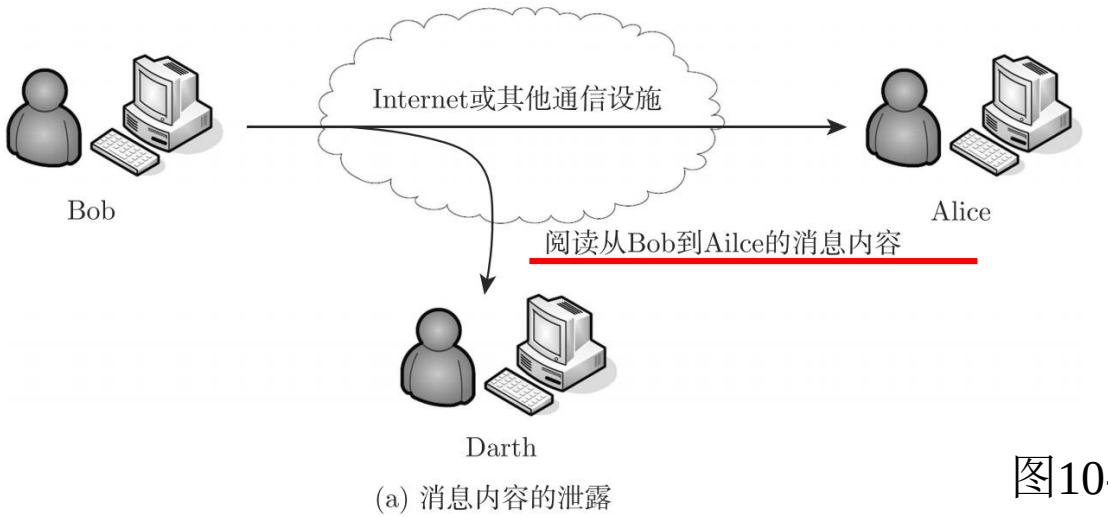
- 网络攻击是指降级、瓦解、拒绝、摧毁计算机或计算机网络中的信息资源，或者降级、瓦解、拒绝、摧毁计算机或计算机网络本身的行为。
- 在最高层次上，ISO 7498-2将安全攻击分成两类，即被动攻击和主动攻击。

① **被动攻击**试图收集、利用系统的信息，但不影响系统的正常访问，数据的合法用户对这种活动一般不会觉察到。

② **主动攻击**则是攻击者访问他所需信息的故意行为，一般会改变系统资源或影响系统运作。

1.被动攻击

- 被动攻击采取的方法是对传输中的信息进行窃听和监测，主要目标是获得传输的信息。有两种主要的被动攻击方式：**信息收集和流量分析**。
- (1)信息收集造成传输信息的**内容泄露**，如图10-1(a)所示。电话、电子邮件和传输的文件都可能因含有敏感或秘密的信息而被攻击者所窃取。



(a) 消息内容的泄露

图10-1 被动攻击

被动攻击

- (2)采用流量分析的方法可以**判断通信的性质**(图10-1(b))。为了防范信息的泄露，消息在发送之前一般要进行加密，使得攻击者即使捕获了消息也不能从消息里获得有用的信息。但是，即使用户进行了加密保护，攻击者仍可能获得这些消息模式。攻击者可以确定通信主机的身份和位置，可以观察传输的消息的频率和长度。这些信息可以用于判断通信的性质。

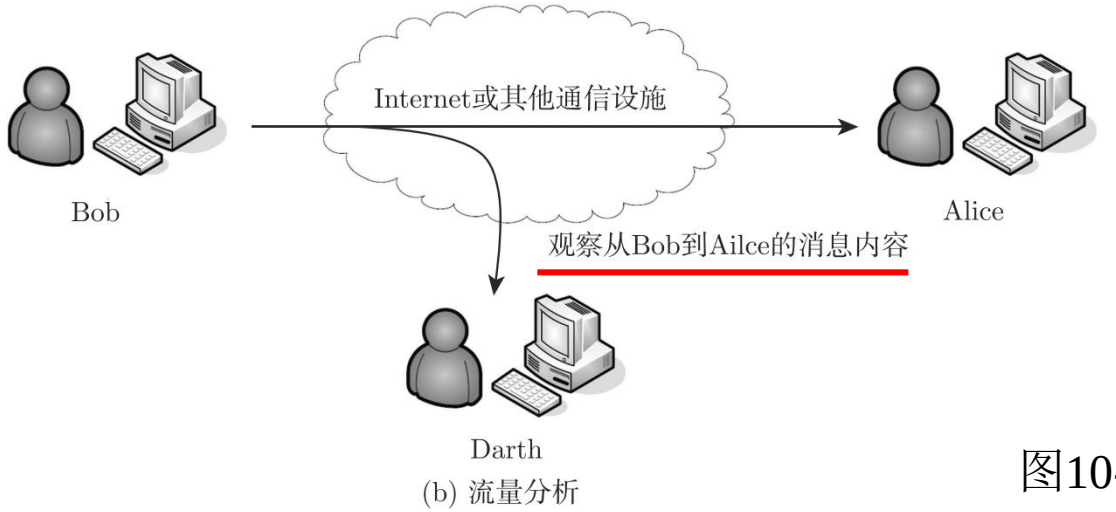


图10-1 被动攻击

2.主动攻击

- 主动攻击包括对数据流进行篡改或伪造数据流，可分为四类：伪装、重放、消息修改和拒绝服务。其实现原理如图10-2所示。
- (1)伪装：**某实体假装成别的实体**。典型的有，攻击者捕获认证信息，并在其后利用认证信息进行重放，这样它就可能获得其他实体所拥有的权限。

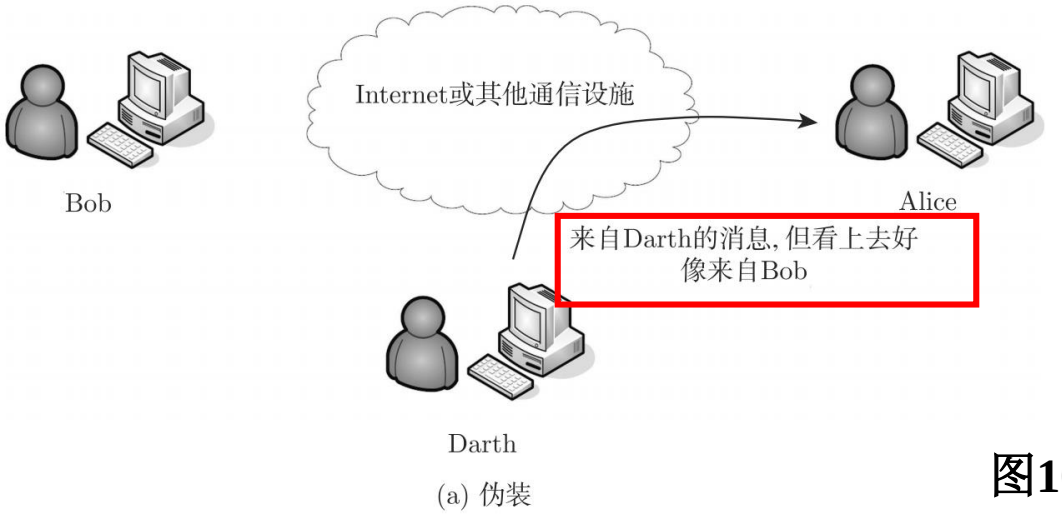


图10-2 主动攻击

2.主动攻击

- (2)重放：将攻击者获得的信息再次发送，从而导致非授权效应。

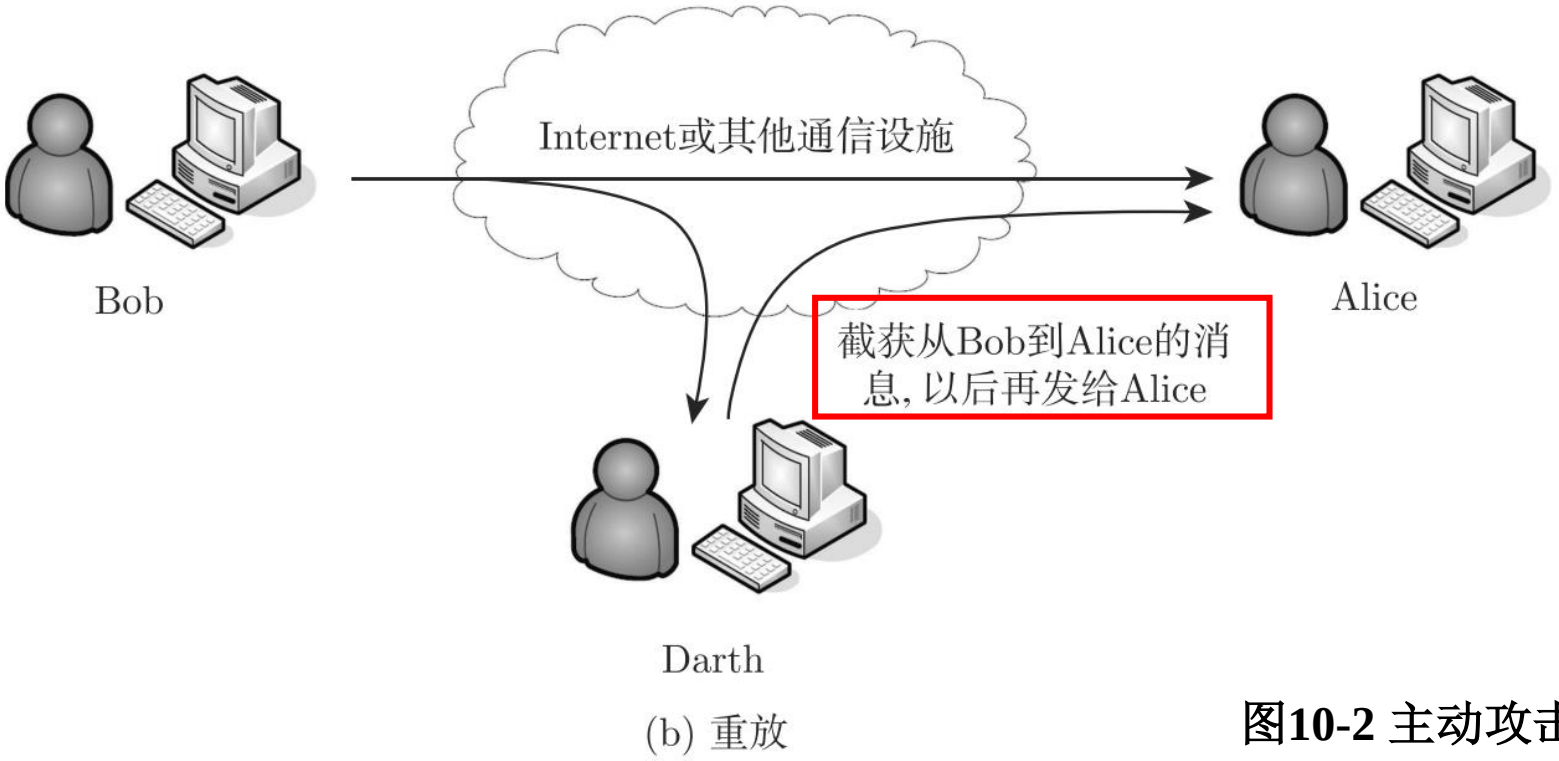


图10-2 主动攻击

2.主动攻击

- (3)消息修改：攻击者修改合法消息的部分或全部，或者延迟消息的传输以获得非授权作用。

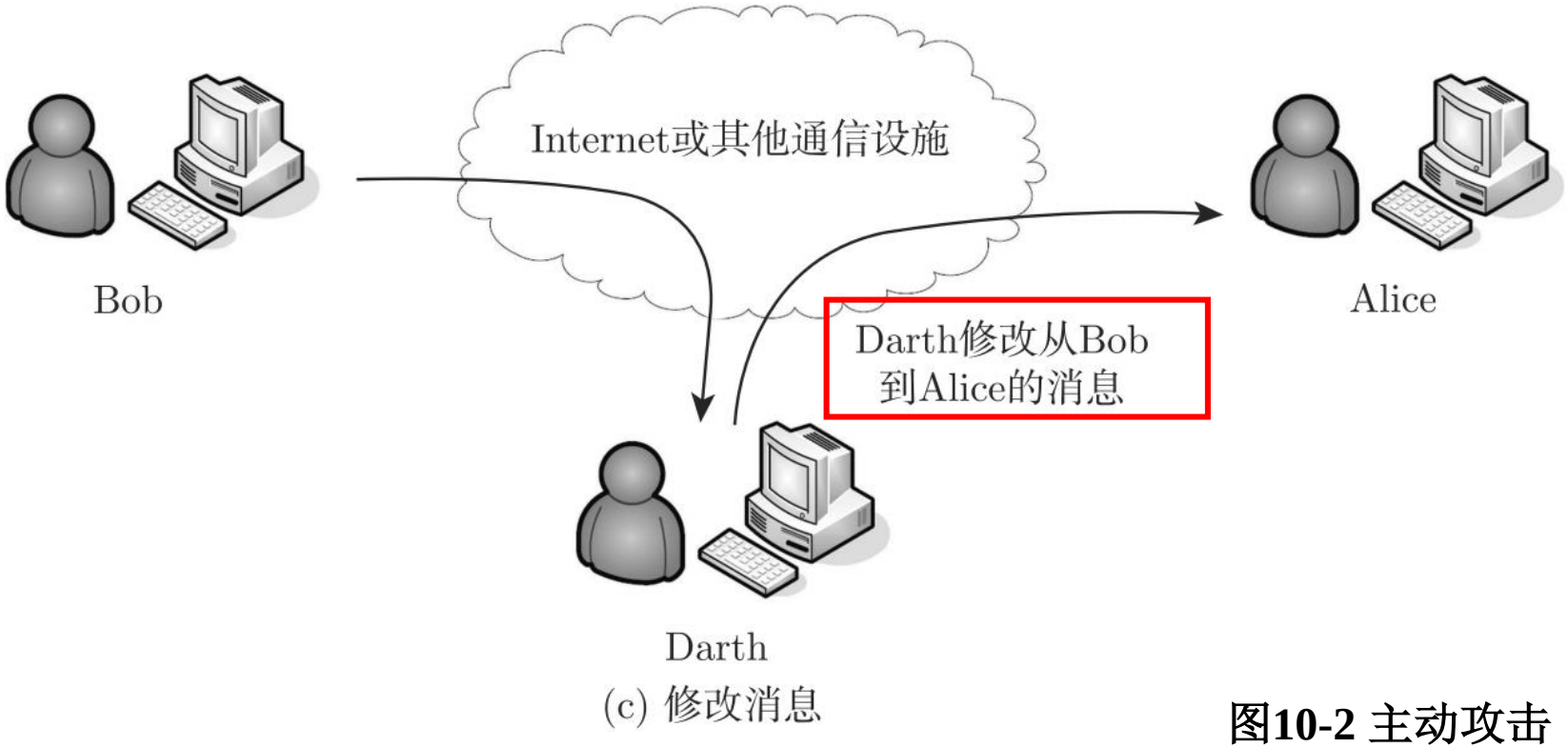


图10-2 主动攻击

2.主动攻击

- (4)拒绝服务：攻击者设法让目标系统停止提供服务或资源访问，从而阻止授权实体对系统的正常使用或管理。典型的形式有，查禁所有发向某目的地的消息，以及破坏整个网络，即或者使网络失效，或者是使其过载以降低其性能。

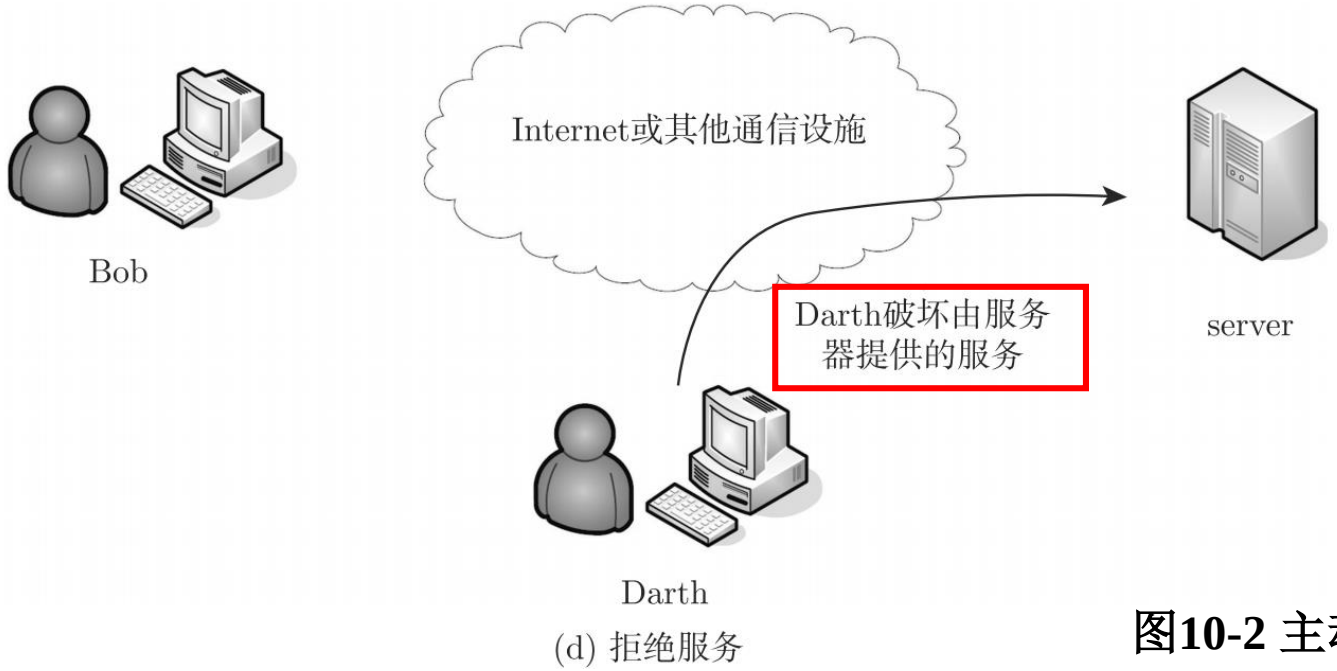


图10-2 主动攻击

10.1.2 安全服务

- OSI 安全体系结构将安全服务定义为通信开放系统协议层提供的服务，从而保证系统或数据传输有足够的安全性。
- RFC 2828将安全服务定义为，**一种由系统提供的对系统资源进行特殊保护的处理或通信服务。安全服务通过安全机制来实现安全策略。**OSI安全体系结构定义了5大类，共14个安全服务。

1.鉴别服务

- 鉴别服务与保证通信的**真实性**有关，提供对通信中对等实体和数据来源的鉴别。

1.鉴别服务

- 在单条消息的情况下，鉴别服务的功能是向接收方保证消息来自所声称的发送方，而不是假冒的非法用户。
- 对于正在进行的交互，鉴别服务则涉及两个方面。首先，在连接的初始化阶段，鉴别服务**保证两个实体是可信的**，即每个实体都是他们所声称的实体，而不是假冒的;其次，鉴别服务必须**保证该连接不受第三方的干扰**，即第三方不能够伪装成两个合法实体中的一个进行非授权传输或接收。
- **(1)对等实体鉴别：**该服务在数据交换连接建立时提供，识别一个或多个连接实体的身份，证实参与数据交换的对等实体确实是所需的实体，防止假冒。
- **(2)数据源鉴别：**该服务对数据单元的来源提供确认，向接收方保证所接收到的数据单元来自所要求的源点。它不能防止重播或修改数据单元。

2.访问控制服务

- 访问控制服务包括身份认证和权限验证，用于防止未授权用户非法使用或越权使用系统资源。

- 该服务可应用于对资源的各种访问类型（如通信资源的使用，信息资源的读、写和删除，进程资源的执行）或对资源的所有访问。

3.数据保密性服务

- 数据保密性服务为防止网络各系统之间交换的数据被截获或被非法存取而泄露，提供机密保护。同时，对有可能通过观察信息流就能推导出信息的情况进行防范。保密性是为防止传输的数据遭到被动攻击：
- (1)**连接保密性：**对一个连接中所有用户数据提供机密性保护。
- (2)**无连接保密性：**为单个无连接的N-SDU(N层服务数据单元)中所有用户数据提供机密性保护。
- (3)**选择字段保密性：**为一个连接上的用户数据或单个无连接的N-SDU内被选择的字段提供机密性保护。
- (4)**信息流保密性：**提供对可根据观察信息流而分析出的有关信息的保护，从而防止通过观察通信业务流而推断出消息的源和宿、频率、长度或通信设施上的其他流量特征等信息。

4.数据完整性服务

- (1)**带恢复的连接完整性：**为连接上的所有用户数据保证其完整性。检测在整个SDU序列中，任何数据的修改、插入、删除和重播，并予以恢复。
- (2)**不带恢复的连接完整性：**与带恢复连接完整性的差别仅在于不提供恢复。
- (3)**选择字段的连接完整性：**保证一个连接上传输的用户数据内选择字段的完整性，并以某种形式确定该选择字段是否已被修改、插入、删除或重播。
- (4)**无连接完整性：**提供单个无连接的SDU的完整性，并以某种形式确定接收到的SDU是否已被修改。一定程度上，还可以提供对连接重放的检测。
- (5)**选择字段无连接完整性：**提供在单个无连接SDU内选择字段的完整性，并以某种形式确定选择字段是否已被修改。

5.不可否认服务

- 不可否认服务用于防止发送方在发送数据后否认发送，以及接收方在收到数据后否认收到或伪造数据的行为。

- **(1)具有源点证明的不可否认：**为数据接收者提供数据源证明，防止发送者以后任何企图否认发送数据或它的内容的行为。

- **(2)具有交付证明的不可否认：**为数据发送者提供数据交付证明，防止接收者以后任何企图否认接收数据或它的内容的行为。

10.1.3 安全机制

- 为了实现上述安全服务，OSI安全体系结构还定义了安全机制。安全机制：用来检测、阻止攻击或者从攻击状态恢复到正常状态的过程，或实现该过程的设备。
- 这些安全机制可分成两类：一类在特定的协议层实现，另一类不属于任何的协议层或安全服务。在特定的协议层设置的一些安全机制主要为以下几种。

1.加密机制

- 这种机制提供对数据或信息流的保密，并可作为其他安全机制的补充。加密算法分为两种类型：一是对称密钥密码体制，加密和解密使用相同的秘密密钥；二是非对称密钥密码体制，加密使用公开密钥，解密使用私人密钥。网络条件下的数据加密必然使用密钥管理机制。

2.数字签名机制

- 数字签名是附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收方确认数据单元来源和数据单元的完整性，并保护数据，防止被人伪造。数字签名机制确定两个过程，对数据单元签名和验证签过名的数据单元。
- 签名过程使用签名者专用的保密信息作为私用密钥，加密一个数据单元并产生数据单元的一个密码校验值。验证过程则使用公开的方法和信息来确定签名是否是使用签名者的专用信息产生的。但由验证过程不能推导出签名者的专用保密信息。数字签名的基本特点是，签名只能使用签名者的专用信息产生。

3.访问控制机制

- 当实体试图使用非授权资源或以不正确方式使用授权资源时，访问控制功能将拒绝这种企图，产生事件报警并记录下来作为安全审计跟踪的一部分。访问控制机制可用以下一种或多种信息类型为基础。
- (1)**访问控制信息库**。该库存有对等实体的访问权限，这种信息可由授权中心或正被访问的实体保存。
- (2)**鉴别信息**。如通行字等。
- (3)用于证明访问实体或资源的权限的**能力和属性**。
- (4)按照安全策略，许可或拒绝访问的**安全标号**。
- (5)试图访问的**时间**。
- (6)试图访问的**路径**。
- (7)访问的**持续时间**。

4.数据完整性机制

- 数据完整性包括两个方面：一是单个数据单元或字段的完整性；二是数据单元或字段序列的完整性。
- 确定单个数据单元完整性包括两个过程：一是发送实体将数据本身的某个函数量（称为校验码字段）附加在该数据单元上；二是接收实体产生一个对应的字段，与所接收到的字段进行比较以确定在传输过程中数据是否被修改。但是，仅使用这种机制不能防止单个数据单元的重播。
- 对连接型数据传输中数据单元序列完整性的保护，要求附加明显的次序关系。例如，顺序编号、时间戳或密码链。对于无连接型数据传输，使用时间戳可提供一种防止个别数据单元重播的限定形式。

5.鉴别交换机制

- 鉴别交换机制是通过**互换信息**的方式来确认实体身份的机制。
- 这种机制可使用如下技术：发送方实体提供鉴别信息（如通行字），由接受方实体验证；加密技术；利用实体的特征或属性等。鉴别交换机制可与相应层次相结合以提供同等实体鉴别。
- 当采用密码技术时，鉴别交换机制可以和“握手”协议相结合以抵抗重放攻击。

- 鉴别交换机制的选择取决于不同的应用场合。

鉴别交换机制的选择

- (1)当对等实体和通信方式两者都可信时，一个对等实体的验证可由通行字实现。通行字可以防错，但不能防止蓄意破坏（如消息重放等）。每一方使用各自不同的通行字可以实现交互鉴别。
- (2)当每一实体信得过各自的对等实体，而通信方式不可信时，对积极攻击的防护由通行字和加密相结合实现。防止重放攻击的单向鉴别需两次“握手”，而具有重放防护的相互鉴别可由三次“握手”实现。
- (3)当一实体不能（或感觉到将来不能）相信对等实体或通信方式时，应使用数字签名或公证机制以实现不可否认服务。

6.通信业务填充机制

- 通信业务填充机制能用来提供各种不同级别的保护，对抗通信业务分析。这种机制产生伪造的信息流并填充协议数据单元以达到固定长度，有限地防止流量分析。只有当信息流受加密保护，本机制才有效。

7.路由选择机制

- 路由能动态地或预定地选取。在检测到持续的操作攻击时，端系统可以指示网络服务的提供者经不同的路由建立连接，带有某些安全标记的数据可能被安全策略禁止通过某些子网络、中继站或链路。
- 这种机制提供动态路由选择或预置路由选择。连接的起始端（或无连接数据单元的发送方）可提出路由申请，请求特定子网络、链路或中继站。端系统根据检测持续攻击网络通信的情况，动态地选择不同的路由，指示网络服务的提供者建立连接。根据安全策略，禁止带有安全标号的数据通过一般的（不安全的）子网络、链路或中继站。

8.公证机制

- 这种机制**确证两个或多个实体之间数据通信的特征：数据的完整性、源点、终点及收发时间。**这种保证由通信实体信赖的第三方——公证员提供。在可检测方式下，公证员掌握用以确证的必要信息。公证机制提供服务还使用到数字签名、加密和完整性服务。
- 除了以上8种基本的安全机制外，还有一些**辅助的安全机制**。它们不明确对应于任何特定的层次和服务，但其重要性直接和系统要求的安全等级有关。
- **(1)可信功能：**系统的软硬件应是可信的。获得可信的方法包括形式证明、检验和确认、对攻击的检测和记录，以及在安全环境中由可信成员构造实体。

- **(2)安全标签：**给资源（包括数据项）附上安全标签，表示其安全敏感程度。安全标签可以是与数据传输有关的附加数据，也可以是隐含的，如特定的密钥。
- **(3)事件检测：**包括检测与安全有关的事件（如违反安全的事件、特定的选择事件、事件计数溢出等），以及检测“正常”事件（如一次成功的访问）。
- **(4)安全审计跟踪：**独立地回顾和检查系统有关的记录和活动，以测试系统控制的充分性。它提供安全性违反的检测与调查，保证已建立的安全策略和操作过程的一致性。帮助评估损害，并推荐有关改进系统控制、安全策略和操作过程的指示。
- **(5)安全恢复：**受理事件检测处理和管理职能机制的请求，并应用一组规则来采取恢复行动。恢复行动有三种：一是立即行动。立即中止操作，如切断连接；二是暂时行动。使实体暂时失效；三是长期行动。使实体进入“空白表”或改变密钥。

10.2 IPSec协议

- 在TCP/IP协议分层模型中，IP层是可能实现端到端安全通信的最底层。通过在IP层上实现安全性，不仅可以保护各种带安全机制的应用程序，而且可以保护许多无安全机制的应用。
- 典型地，IP协议实现在操作系统中。因此，在IP层实现安全功能，可以不必修改应用程序。

- **IPSec将密码技术应用在网络层，提供端对端通信数据的私有性、完整性、真实性和防重放攻击等安全服务**。
- IPSec对于IPv4是可选的，对于IPv6是强制性的。

IPSec

- IPSec通过多种手段提供IP层安全服务：允许用户选择所需安全协议、允许用户选择加密和认证算法、允许用户选择所需的密码算法的密钥。
- IPSec可以安装在路由器或主机上，若IPSec装在路由器上，则可在不安全的Internet上提供一个安全的通道；若是装在主机上，则能提供主机端对端的安全性。

- 第一版IPsec协议在RFC2401—2409中定义。第二版IPsec协议的标准文档在2005年发布，新的文档定义在RFC 4301—RFC 4309中。

1. IPSec体系结构

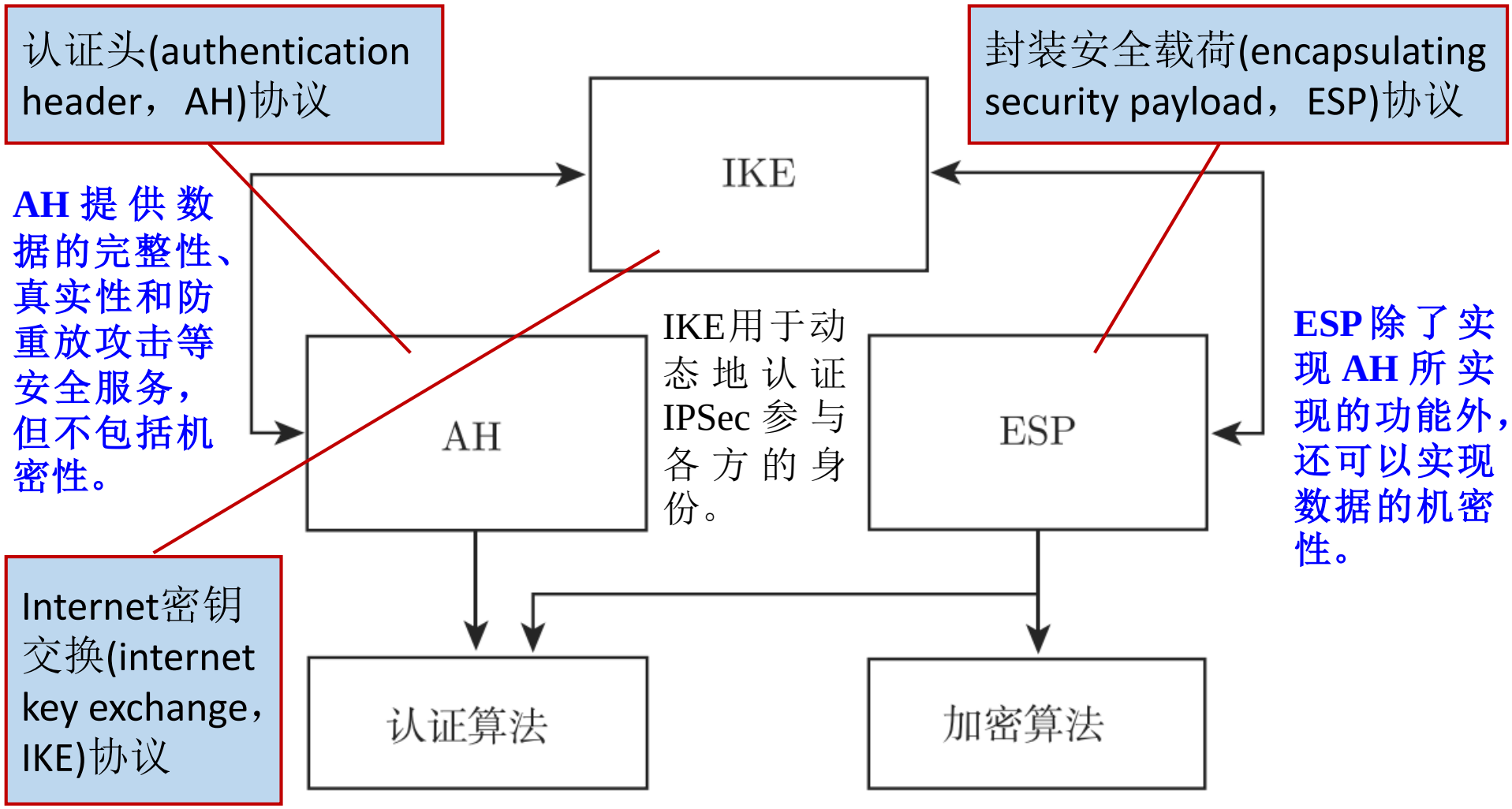


图10-3 IPSec组件

安全关联(SA)

- **一个安全关联是发送方和接收方之间的受到密码技术保护的单向关系**，该关联对所携带的通信流量提供安全服务：要么对通信实体收到的IP数据包进行“进入”保护，要么对实体外发的数据包进行“流出”保护。如果需要双向安全交换，则需要建立两个安全关联，一个用于发送数据，一个用于接收数据。安全服务可以由AH或ESP提供，但不能两者都提供。
- 一个安全关联由三个参数唯一确定。
- **(1)安全参数索引(SPI)：**一个与SA相关的位串，仅在本地有意义。这个参数被分配给每一个SA，并且每一个SA都通过SPI进行标识。发送方把这个参数放置在每一个流出数据包的SPI域中，SPI由AH和ESP携带，使得接收系统能选择合适的SA处理接收包。SPI并非全局指定，因此，SPI要与目标IP地址、安全协议标识一起来唯一标识一个SA。

安全关联的参数

- **(2)目标IP地址：**目前，IPSec SA管理机制中仅仅允许单播地址。所以，这个地址表示SA的目的端点地址可以是用户终端系统、防火墙或路由器。它决定了关联方向。
- **(3)安全协议标识：**标识该关联是一个AH安全关联或ESP安全关联。
- 处理与SA有关的流量时有两个数据库，即安全关联数据库(security association database，SAD)和安全策略数据库(security policy database，SPD)。SAD包含了与每一个安全关联相联系的参数，SPD则指定了主机或网关的所有IP流量的流入和流出分配策略。

2.IPSec的2种工作模式

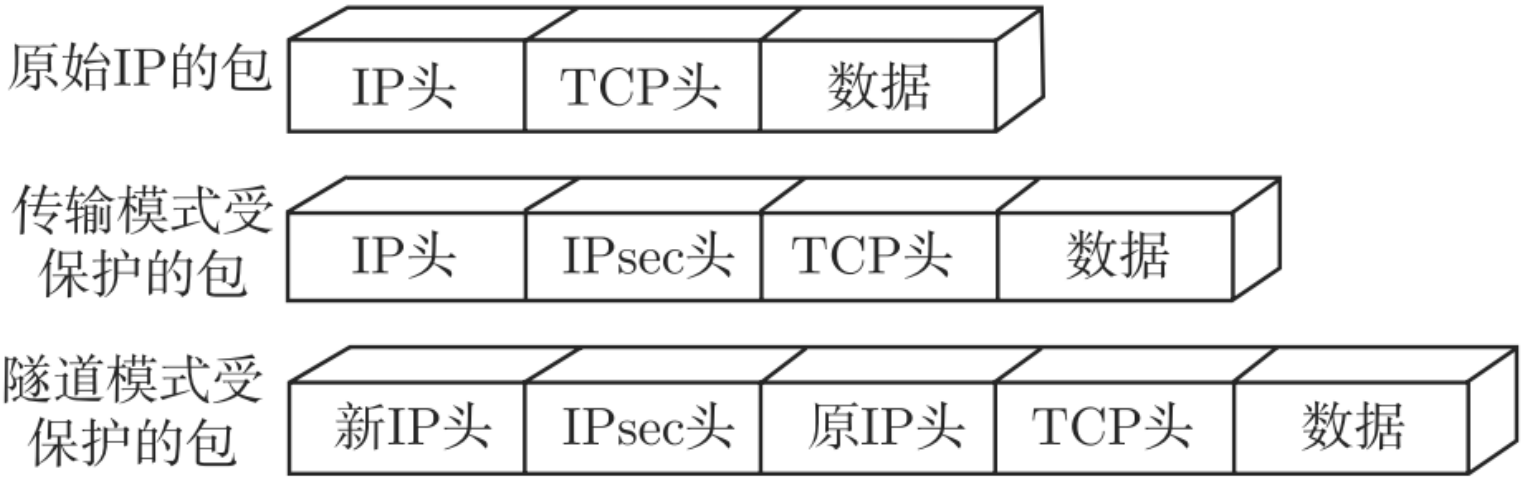


图10-4 IPSec工作模式

1)传输模式

- 传输模式主要为直接运行在IP层之上的协议，如TCP、UDP和ICMP，提供安全保护，一般用于在两台主机之间的端到端通信。

2)隧道模式

- 隧道模式对整个IP包提供保护。为了达到这个目的，当IP数据包附加了AH或ESP域之后，整个数据包加安全域被当做一个新IP包的载荷，并拥有一个新的外部IP头。一般用于两个网络之间的通信。

3.AH协议

- IP认证头(AH)协议为IP数据包提供数据完整性校验和身份认证，还有可选择的抗重放攻击保护，但不提供数据加密服务。
- 数据完整性确保在包的传输过程中内容不可更改，认证确保终端系统或网络设备能对用户或应用程序进行认证，并相应地提供流量过滤功能，同时还能防止地址欺诈攻击和重放攻击。
- 认证基于**消息鉴别码(MAC)**，双方必须共享同一个密钥。

认证头(AH)的结构

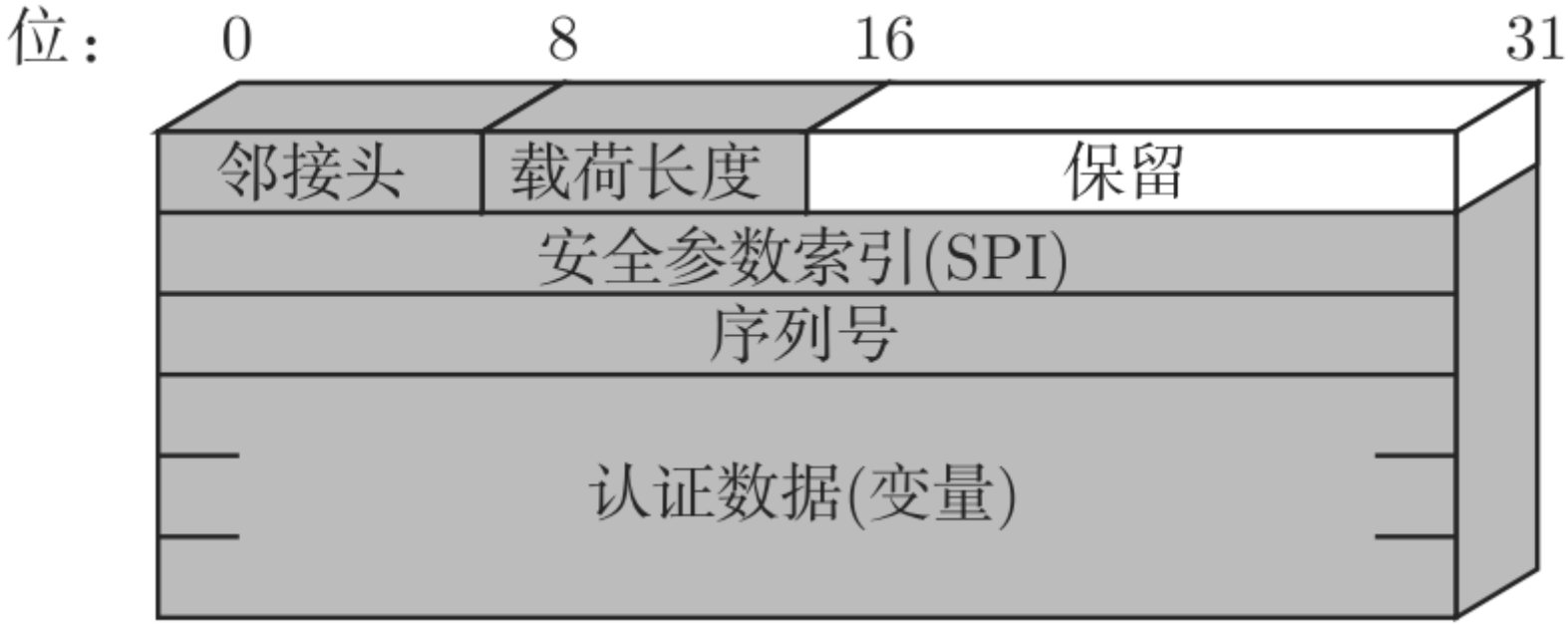


图10-5 IPSec认证头

① 邻接头(Next Header)：8-bits，标识AH头后的载荷（协议）类型。在传输模式下可为6(TCP)或17 (UDP);在隧道模式下将是4(IPv4)或41 (IPv6)。

② 载荷长度(Payload Length)：8-bits，表示AH头本身的长度，以32-bits为单位。

③ 保留(Reserved)：16-bits，保留字段，未使用时必须设为0。

④ 安全参数索引SPI (Security Parameters Index)：32-bits，接收方用于标识对应的安全关联(SA)。

⑤ 序列号(Sequence Number)：32-bits，是一个单向递增的计数器，提供抗重播功能（anti-replay）。

⑥ 认证数据ICV（Integrity Check Value）：这是一个可变长度（必须是32比特的整数倍）的域，长度由具体的验证算法决定。完整性验证数据ICV验证IP数据包的完整性，因此ICV的计算包含了整个IP数据包。

AH的传输模式

图10-6 AH传输模式

AH的传输模式只保护IP数据包的不变部分，它保护的是端到端的通信，通信的终点必须是IPSec终点，如图10-6所示。

在IPv4的AH传输模式中，AH插入到原始IP头之后、IP载荷（如TCP分段）之前，认证包括了除IPv4报头中可变的、被MAC计算置为“0”的域以外的整个包。

在IPv6中，AH被作为端到端载荷，即不被中间路由器检查或处理。因此，AH出现在 IPv6原IP头、跳、路由和分段扩展头之后。目的地址作为可选报头，在AH前面或后面，由特定语义决定。同样，认证包括了除IPv4报头中可变的、被MAC计算置为“0”的域以外的整个包。

AH的隧道模式

AH用于隧道模式时，整个原始IP包被认证，AH被插入到原始IP头和新外部IP头之间。原IP头中包含了通信的原始地址，而新IP头则包含了IPSec端点的地址，如图10-7所示。

使用隧道模式，整个内部IP包，包括整个内部IP头均被AH保护。外部IP头(IPv6中的外部IP扩展头)除了可变且不可预测的域之外均被保护。隧道模式可用来替换端到端安全服务的传输模式。但由于这一协议中没有提供机密性，因此，相当于就没有隧道封装这一保护措施，所以它没有什么用处。

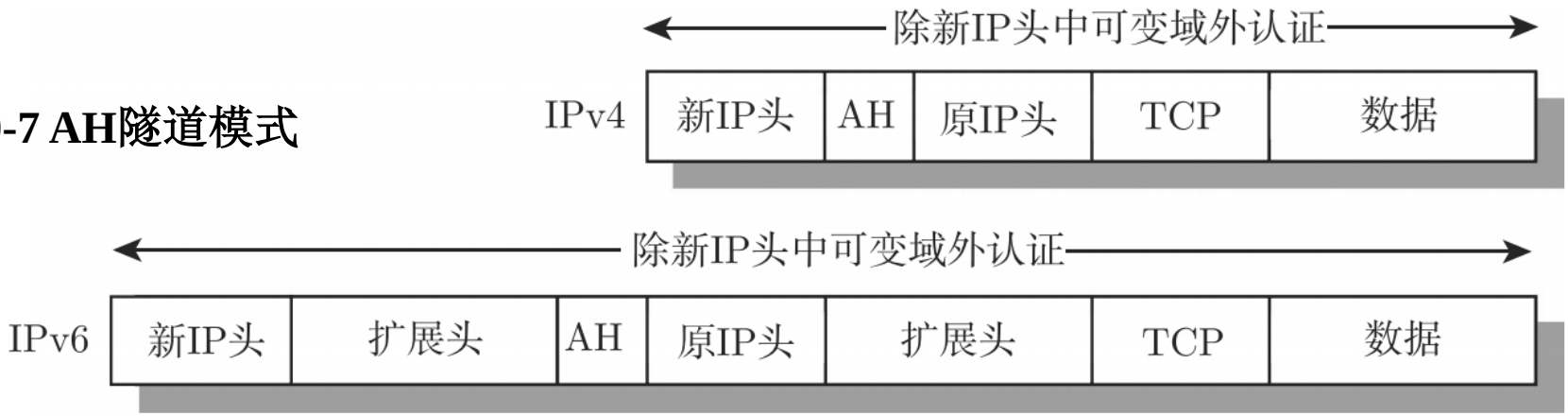


图10-7 AH隧道模式

4.ESP协议

- 封装安全载荷(ESP)协议为IP数据包提供数据完整性校验、身份认证和数据加密，还有可选择的抗重放攻击保护。ESP用一个密码算法提供机密性，数据完整性则由身份验证算法提供。通过插入一个唯一的、单向递增的序列号提供抗重放服务。保密服务可以独立于其他服务而单独选择，数据完整性校验和身份认证用作保密服务的联合服务。只有选择了身份认证时，才可以选择抗重放服务。

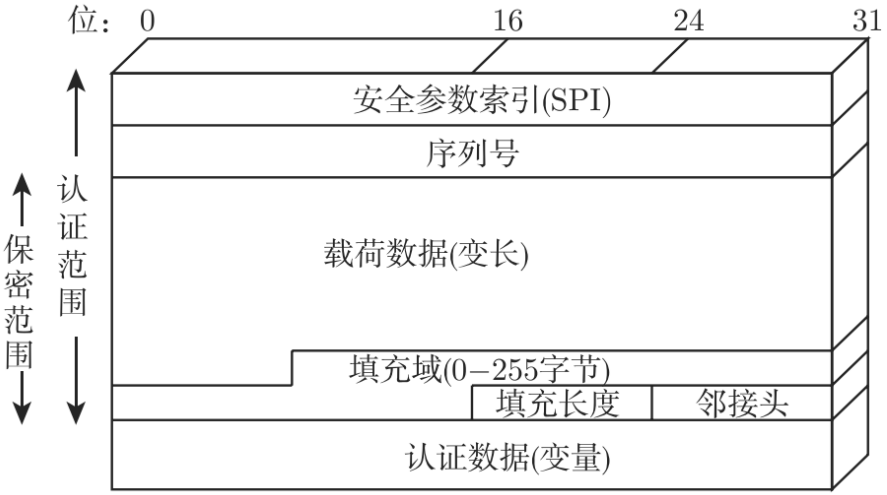
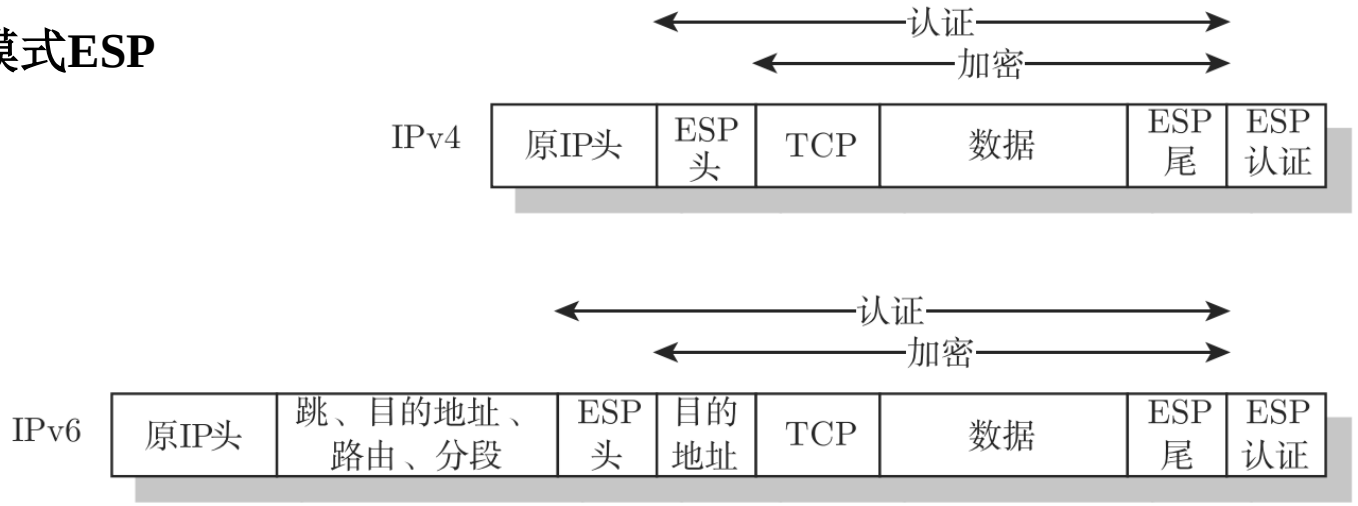


图10-8 ESP格式

- 安全参数索引SPI(32位)：标识安全关联。ESP中的SPI是强制字段，总要提供。
- 序列号(32位)：单调递增计数值，提供反重放功能。这是个强制字段，并且总要提供，即使接收方没有选择对特定SA的反重放服务。如果开放了反重放服务，则计数值不允许折返。
- 载荷数据（变量）：变长的字段，包括被加密保护的传输层分段（传输模式）或IP包（隧道模式）。该字段的长度是字节的整数倍。
- 填充域(0～255字节)：可选字段，但所有实现都必须支持生成和消费填充值。该字段满足加密算法的需要（如果加密算法要求明文是字节的整数倍），还可以提供通信流量的保密性。发送方可以填充0~ 255字节的填充值。
- 填充长度(8位）：紧跟填充域，指示填充数据的长度，有效值范围是0～255。
- 邻接头（8位）：标识载荷中第一个报头的数据类型（如IPv6中的扩展头或上层协议 TCP等）。
- 认证数据（变长）：一个变长域（必须为32位字长的整数倍）包含根据除认证数据域外的ESP包计算的完整性校验值。该字段长度由所选择的认证算法决定。

传输模式的ESP

图10-9传输模式ESP



传输模式ESP用于加密和认证(可选)IP携带的数据（如TCP分段），如图10-9所示。

在此模式下使用IPv4，ESP头位于传输头(TCP，UDP，ICMP)之前，ESP尾（填充数据、填充长度和邻接头域）放入IP包尾部。如果选择了认证，则将ESP的认证数据域置于ESP尾之后，整个传输层分段和ESP尾一起加密。认证覆盖ESP头和所有密文。

在IPv6中，ESP被视为端到端载荷，即不被中间路由器校验和处理。因此，ESP头出现在IPv6基本头、跳、路由和分段扩展头之后，目的可选扩展头可根据不同情况出现在ESP头之前或之后。如果可选扩展头在ESP头之后，则加密包括整个传输段、ESP尾和目的可选扩展头。认证覆盖了ESP头和所有密文。

隧道模式的ESP

隧道模式ESP用于加密整个IP包，如图10-10所示。在此模式中，将ESP头作为包的前缀，并在包后附加ESP尾，然后对其进行加密。该模式用于对流量计数分析。

由于IP头中包含目的地址和可能的路由以及跳信息，不可能简单地传输带有ESP头的、被加密的IP包，因为这样中间路由器就不能处理该数据包。因此，必须用新的IP头封装整个数据块(ESP头、密文和可能的认证数据)，其中拥有足够的路由信息，却没有为流量分析提供信息。

然而，传输模式适合于保护支持ESP特性的主机之间的连接，而隧道模式则适用于防火墙或其他安全网关，保护内部网络，隔离外部网络。后者加密仅发生在外部网络和安全网关之间或两个安全网关之间，从而内部网络的主机不负责加密工作，通过减少所需密钥数目简化密钥分配任务。另外，它阻碍了基于最终目的地址的流量分析。

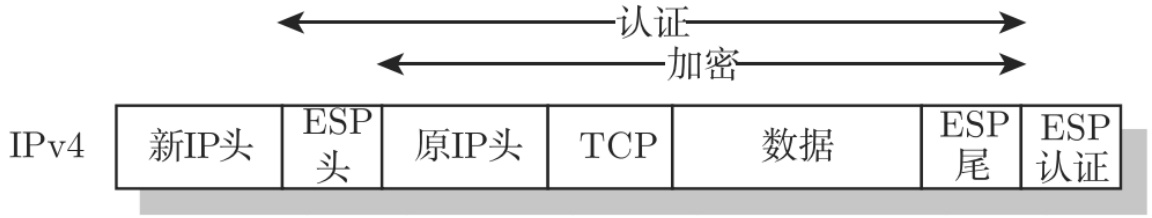
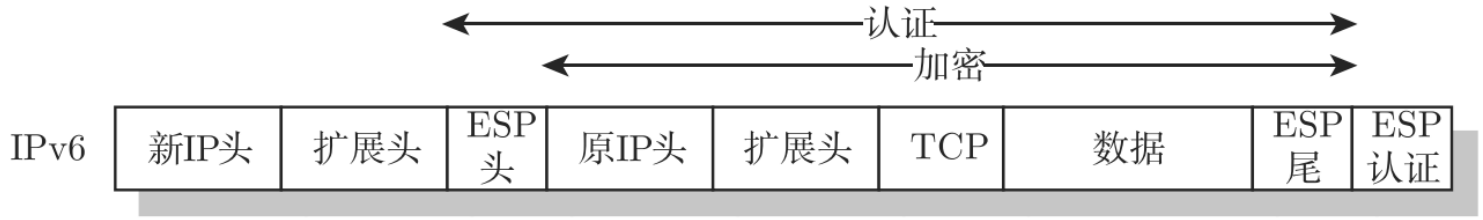


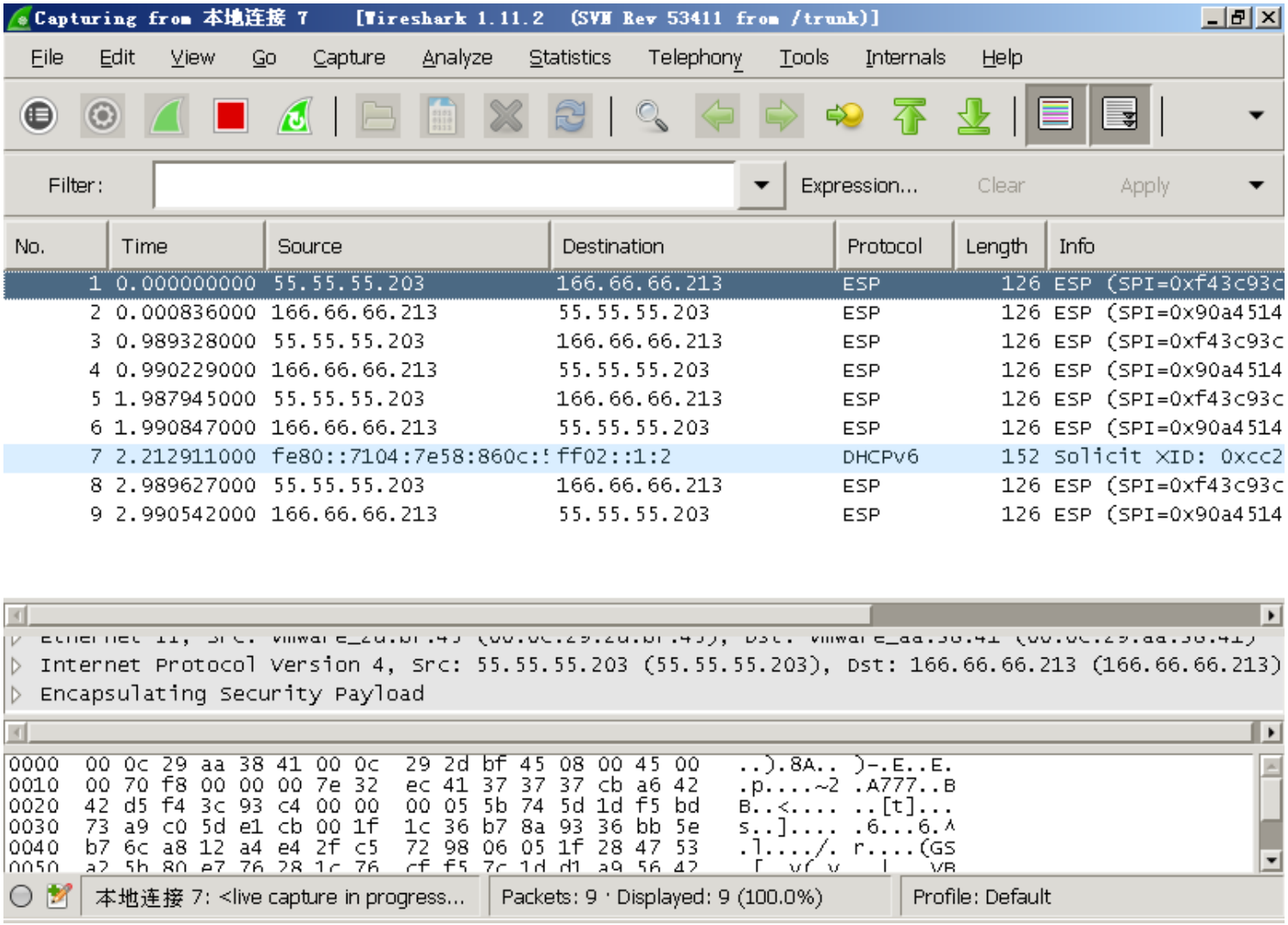
图10-10隧道模式ESP



5.IKE协议

- IPSec的密钥管理包括密钥的建立和分发。IPSec体系结构文档要求支持两种密钥管理类型。
  - **手动**：系统管理员手动地为每个系统配置自己的密钥和其他通信系统密钥。这种方式适用于小规模、相对静止的环境。
  - **自动**：在大型分布系统中使用可变配置为SA动态按需创建密钥。
- Internet密钥交换(internet key exchange，IKE)用于动态建立SA和会话密钥。在建立安全会话之前，通信双方需要一种协议，用于自动地、以受保护的方式进行双向认证、建立共享的会话密钥和生成IPSec的SA。IKE的目的是使用某种长期密钥进行双向认证并建立会话密钥，以保护后续通信。IKE代表IPSec对SA进行协商，并对安全关联数据库(SAD)进行填充。IETF设计了IKE的整个规范，主要由三个文档定义：RFC2407、RFC2408和RFC2409。

IPSec的典型应用：IPSec 网关——网关VPN



10.3 SSL/TLS协议

- **安全套接层(secure socket layer，SSL)协议**最初是由Netscape公司于1994年设计的，主要目标是为Web通信协议—HTTP协议提供保密和可靠通信。1996年，Netscape公司发布了SSL3.0，该版本发明了一种全新的规格描述语言，以及一种全新的记录类型和数据编码，还弥补了加密算法套件反转攻击这个安全漏洞。SSL3.0与SSL2.0是向后兼容的，SSL3.0相比SSL2.0更加成熟和稳定，因此很快成为事实上的工作标准。
- 1997年，IETF基于SSL协议发布了传输层安全(transport layer security，TLS)协议的Internet Draft。1999年，IETF正式发布了关于TLS的RFC2246。
- SSL/TLS被设计为运行在TCP协议栈的传输层之上，使得该协议可以被部署在**用户级进程**中，而不需要对操作系统进行修改。

SSL/TLS协议提供的服务具有以下三个特性

- 一端写入的数据完全是另一端读取的内容，这种透明性使得几乎所有基于TCP的协议稍加改动就可以在SSL上运行。

SSL/TLS协议提供的服务具有以下三个特性。

- (1)**保密性**：在初始化连接后，数据以双方商定的密钥和加密算法进行加密，以保证其机密性，防止非法用户破译。
- (2)**认证性**：协议采用非对称密码体制对端实体进行鉴别，使得客户端和服务器端确信数据将被发送到正确的客户机和服务器上。
- (3)**完整性**：协议通过采用散列函数来处理消息，提供数据完整性服务。

1.SSL体系结构

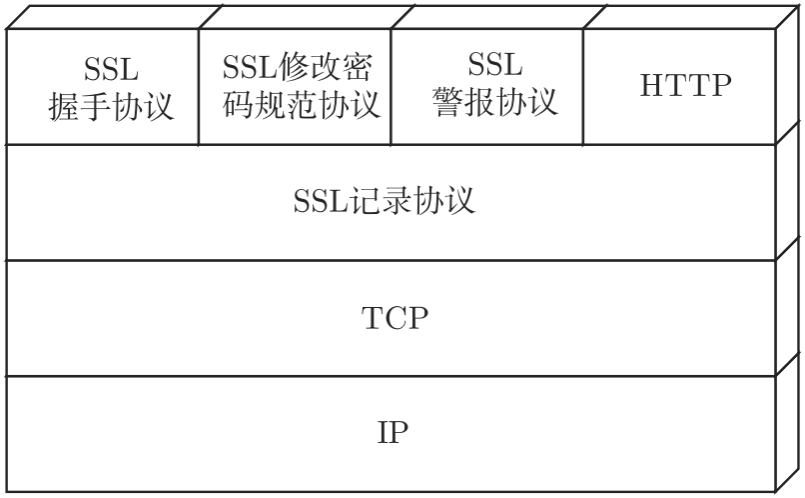


图10-13 SSL协议的分层模型

1) SSL协议分层模型

- 发送时，SSL记录协议接收上层应用消息、将数据分段为可管理的块、可选择地压缩数据、应用MAC、加密、添加一个头部，并将结果传送给TCP。接收到的数据则被解密、验证、解压缩、重组后交付给高层。
- 握手协议允许客户端和服务器彼此认证对方，并且在应用协议发出或收到第一个数据之前协商加密算法和加密密钥。

1.SSL体系结构—2) SSL会话

- SSL会话是一个**客户端和服务器间的关联**，会话是通过握手协议创建的，定义了一组密码安全参数，这些密码安全参数可以由多个连接共享。会话可用于减少为每次连接建立安全参数的昂贵协商费用。
- SSL会话协调服务器和客户端的状态。每个会话具有多种状态。一旦会话建立，则进入针对读和写（即接收和发送）的当前操作状态。
- 在握手协议中，创建了读挂起状态和写挂起状态；在握手协议成功完成后，挂起状态成为当前状态。

一个会话状态由以下参数定义（参见SSL规范）。

- **会话标识符**：一个由服务器生成的数值，用于标识活动的或恢复的会话状态。
- **对等实体证书**：对等实体的一个X509.v3证书，此状态元素可以为空(Null)。
- **压缩方法**：在加密前使用的压缩数据的算法。
- **密码规范**：描述了大量数据的加密算法（如Null、AES等）和用于计算MAC的散列算法(如MD5或SHA-1)，同时也定义了密码学属性（如散列值大小等）。
- **主密码**：一个由客户端和服务器共享的48字节的秘密数值，提供用于生成加密密钥、MAC秘密和初始化向量IV的秘密数据。
- **可恢复性标志**：一个标志，表明会话能否用于初始化一个新的连接。

1.SSL体系结构— 3) SSL连接

- 连接是提供合适服务类型的一种传输(OSI层次模型定义)。
- 对SSL来说，连接表示的是对等网络关系，且连接是短暂的；而会话具有较长的生命周期，**在一个会话中可以建立多个连接**，每个连接与一个会话相关。这是因为，SSL/TLS被设计为与HTTP1.0协同工作，而HTTP1.0协议具有可在客户端和Web服务器之间打开大量TCP连接的特点。

连接状态可用以下参数定义。

- 服务器和客户端随机数
- 服务器写MAC密码
- 客户端写MAC密码
- 服务器写密钥：一个服务器加密和客户端解密数据时，使用的常规的密钥。
- 客户端写密钥：一个客户端加密和服务器解密数据时，使用的常规的密钥。
- 初始化向量IV
- 序列号：会话的各方为每个连接传送和接收消息维护一个单独的序列号。当接收或发送一个修改密码规范协议报文时，消息序列号被设为0。序列号不能超过2^{64} -1。

1.SSL体系结构— 4) SSL基本流程

- 简化的SSL协议如图10-14所示。在基本流程中，客户端A发起与服务器B的连接，然后B把自己的证书发送给A。A验证B的证书，从中提取B的公钥，然后选择一个用来计算会话密钥的随机数，将其用B的公钥加密发送给B。基于这个随机数，双方计算出会话密钥(主密钥)。然后通信双方使用会话密钥对会话数据进行加密和完整性保护。

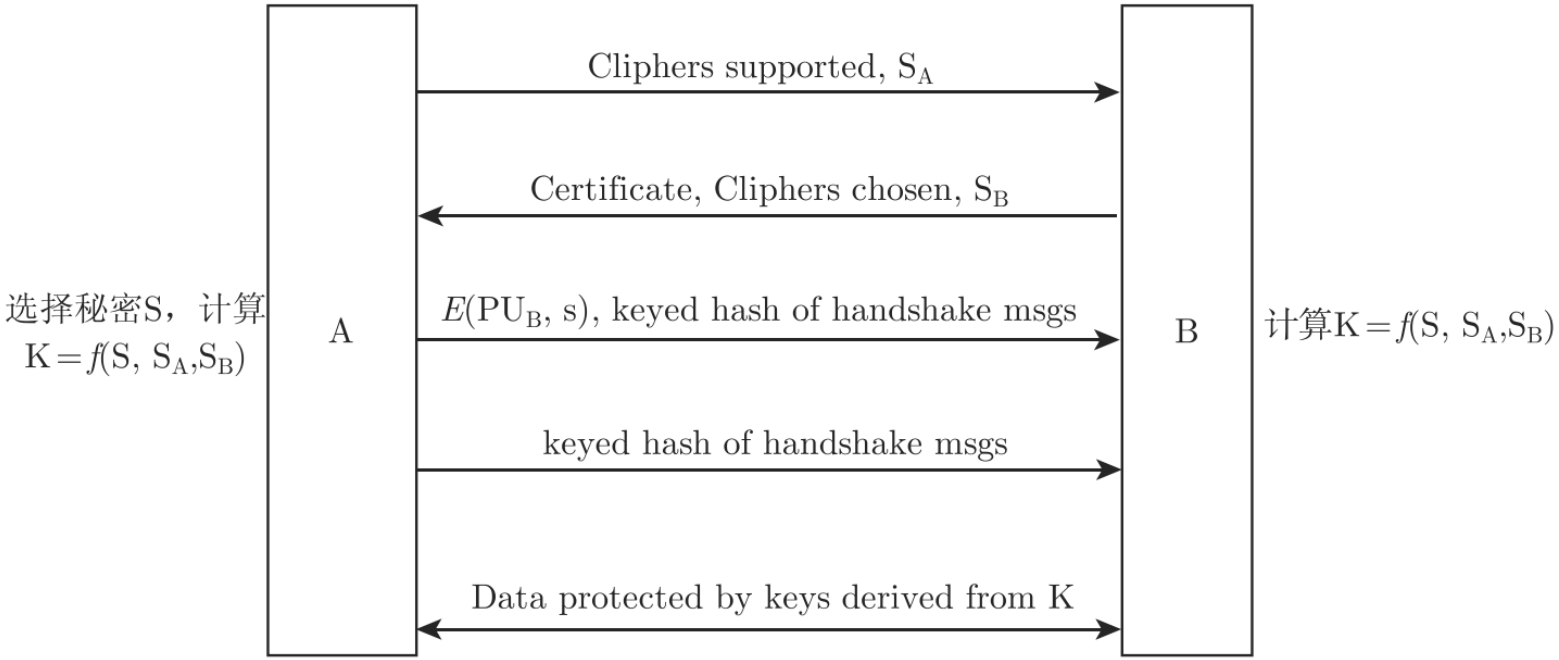


图10-14 简化的SSL协议

2.SSL记录协议

- 在SSL协议中，所有的传输数据都被封装在记录中。
- 记录是由记录头和长度不为0的记录数据组成的。**所有的SSL通信**，包括握手消息、安全空白记录和应用数据，**都使用SSL记录层**。
- SSL记录协议包括了记录头和记录数据格式的规定，为SSL连接提供两种服务。
- SSL记录的格式如图10-15所示。

- 保密性：握手协议定义了加密SSL载荷的加密密钥。
- 消息完整性：握手协议也定义了生成消息认证代码(MAC)的共享密钥。

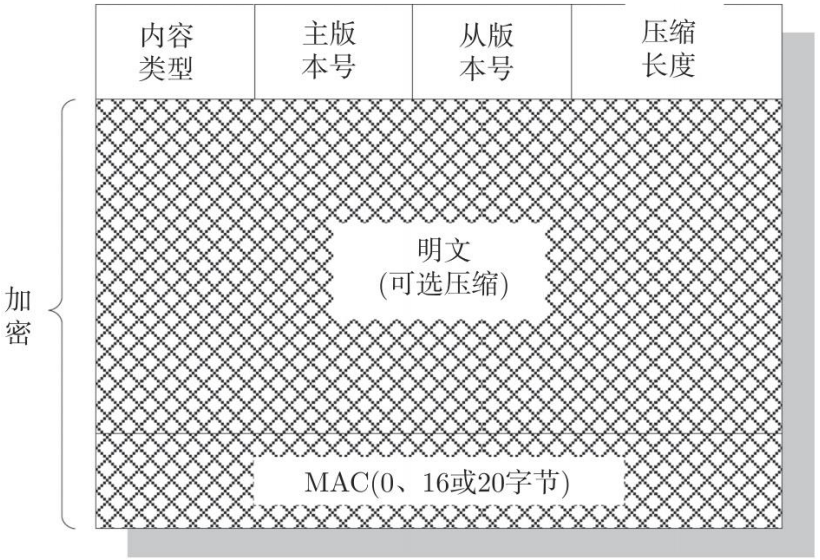


图10-15 SSL记录格式

SSL记录可能的有效载荷

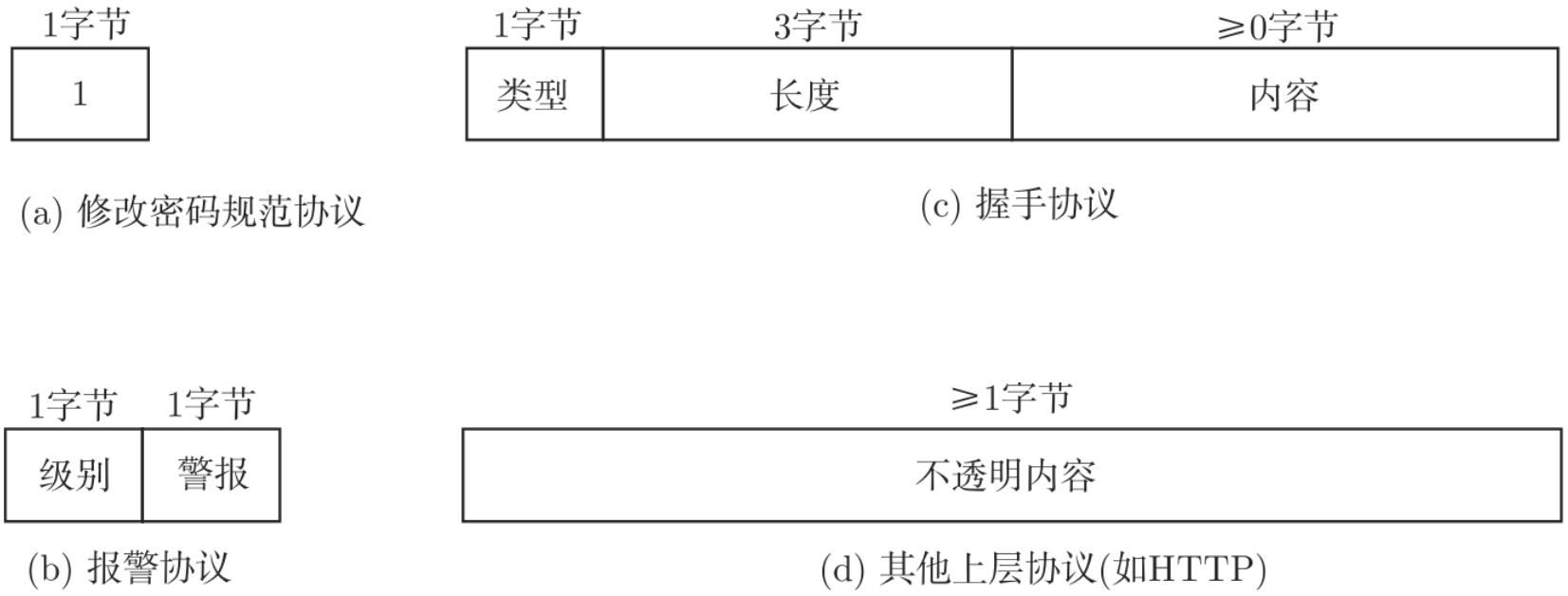


图10-16 SSL记录协议有效载荷

SSL记录协议的整个操作过程

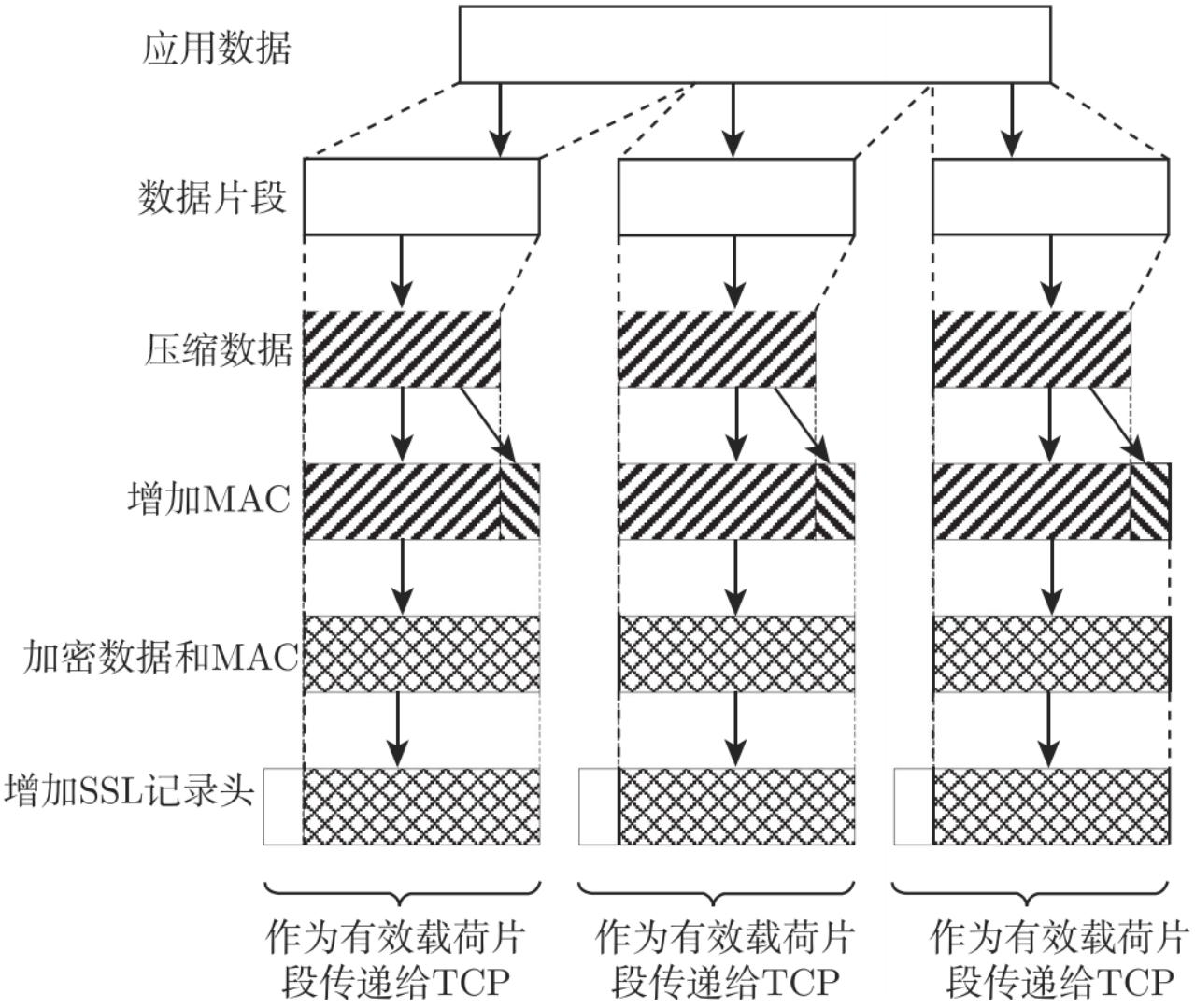


图10-17 SSL记录协议的操作

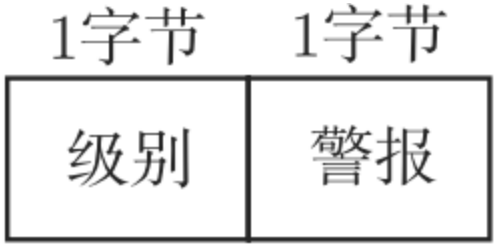
3.SSL修改密码规范协议

- 修改密码规范协议是SSL三个特定协议之一，也是最简单的一个。
- 该协议由一条消息组成，该消息只包含一个值为1的单个字节，如图10-16(a)所示。客户端和服务器端都能发送改变密码说明消息，通知接收方后续记录将使用刚刚协商的密码算法和密钥来加密后续的记录。这条消息的接收引起未决状态被复制到当前状态，更新本连接中使用的密码组件、加密算法、散列算法以及密钥等。
- 客户端在握手密钥交换和验证服务器端证书后发送修改密码规范消息，服务器则在成功处理从客户端接收的密钥交换消息后发送该消息。
- 为了保障SSL传输过程的安全性，双方应该每隔一段时间改变加密规范。

(a) 修改密码规范协议

4.SSL报警协议

- 报警协议用于向对等实体传递SSL相关的报警。如果在通信过程中某一方发现任何异常，就需要给对方发送一条警示消息通告。报警消息传达此消息的严重程度的编码和对此报警的描述。最严重一级的报警消息将立即终止连接，在这种情况下，本次对话的其他连接还可以继续进行，但对话标识符必须设置为无效，以防止此失败的对话重新建立新的连接。像其他的消息一样，报警消息是利用由当前连接状态所指出的算法加密和压缩的。



(b) 报警协议

- 此协议的每个消息由两个字节组成，如图10-16 (b)所示。第一个字节表示消息出错的严重程度，值“1”表示警告，值“2”表示致命错误。如果级别为致命，则SSL将立即终止连接，而会话中的其他连接将继续进行，但不会在此会话中建立新连接。第二个字节包含描述特定报警信息的代码。

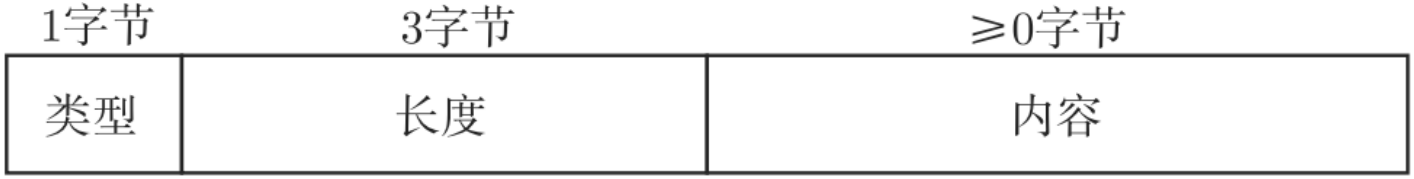
5.SSL握手协议

- 握手是指客户端与服务器端之间建立安全连接的过程。在客户端和服务器的一次会话中，SSL握手协议对它们所使用的SSL/TLS协议版本达成一致，并允许客户端和服务器端通过数字证书实现相互认证，协商加密和MAC算法，利用公钥技术来产生共享的私密信息等。握手协议在传递应用数据之前使用。
- 握手协议由客户端和服务器间交换的一系列消息组成，这些消息的格式如图10-16 (c)所示。每个消息由三个域组成。

① 类型(1字节）：表明10种消息中的一种

② 长度（3字节）：消息的字节长度。

③ 内容（≥0个字节）：与消息相关的参数。



(c) 握手协议

图10-18 握手协议处理过程：阶段1和2

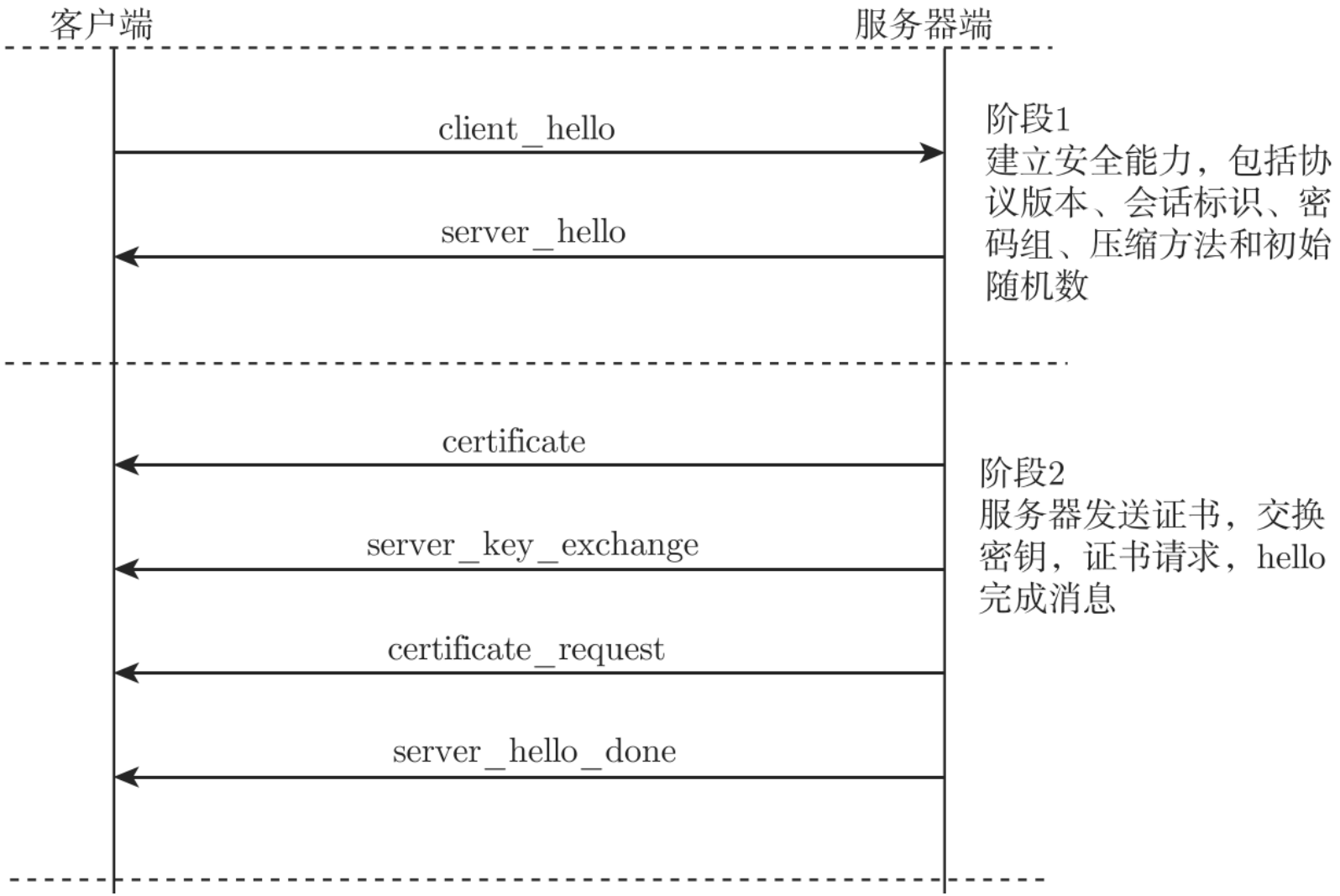
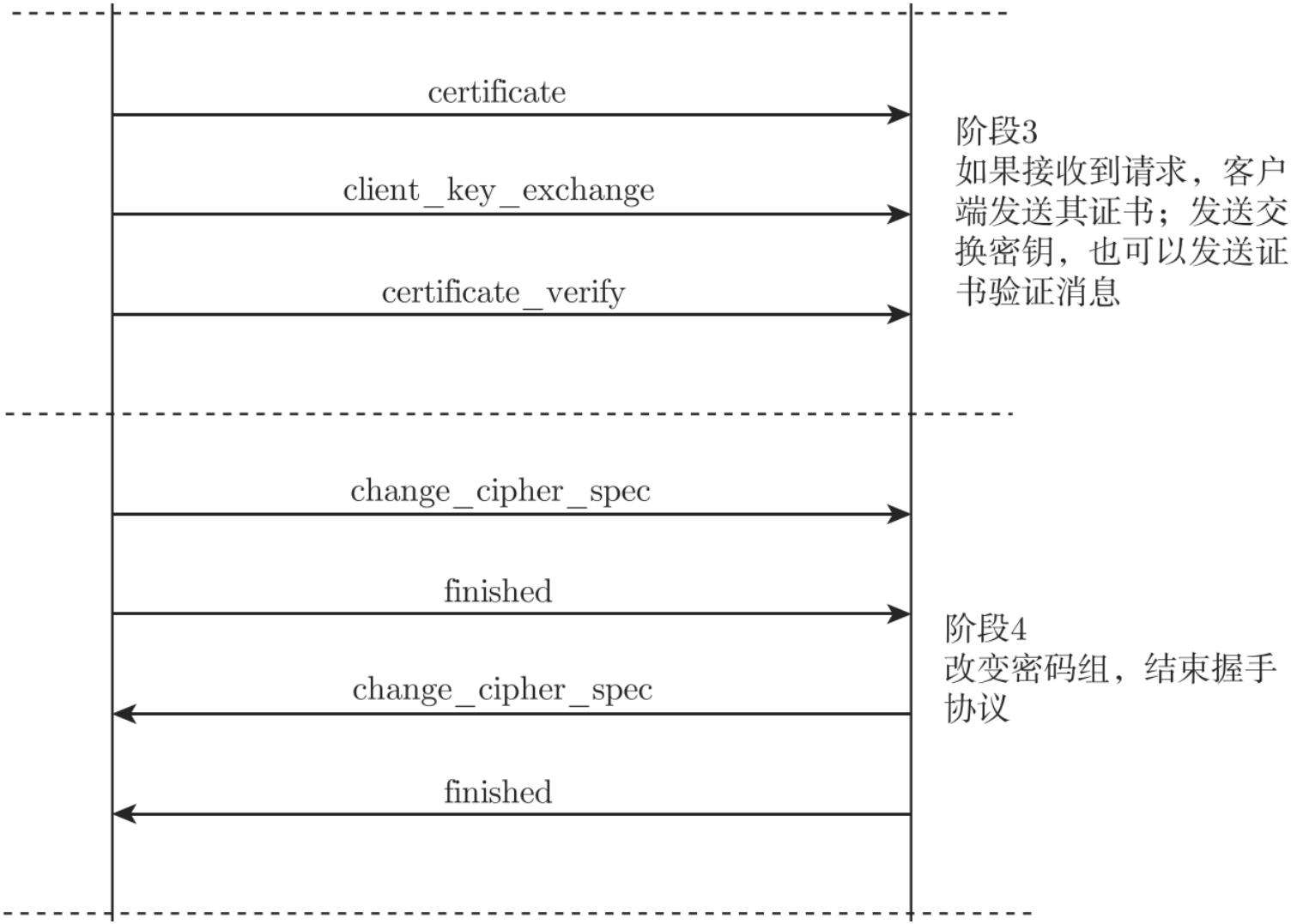


图10-18 握手协议处理过程：阶段3和4



6.TLS协议

- 传输层安全(TLS)是IETF标准的初衷，其目标是成为SSL的互联网标准。TLS v1协议本身基于SSL v3，很多与算法相关的数据结构和规则十分相似。

- 因此，TLS v1与SSL v3的差别并不是非常大，但也存在些许区别，在此不再详述。

如何在自己的C语言程序中使用SSL？

- 参考以下链接：
- https://blog.csdn.net/xs574924427/article/details/17240793

10.4 安全电子交易

- **安全电子交易(secure electronic transaction，SET)协议**是设计用于保护基于信用卡在线支付的电子商务的安全协议，它是由VISA和MasterCard两大信用卡公司于1997年5月联合推出的规范。SET通过制定标准和采用各种密码技术手段，解决了当时困扰电子商务发展的安全问题。目前它已经获得IETF标准的认可，成为**事实上的工业标准**。
- 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中的核心技术主要有公钥加密、数字签名、电子信封、电子安全证书等。

SET提供三种服务

- 目前公布的SET正式文本涵盖了信用卡在电子商务交易中的交易协定、信息保密、资料完整及数字认证、数字签名等。这一标准被公认为全球网际网络的标准，其交易形态将成为未来“电子商务”的规范。

从本质上说，SET提供三种服务。

- (1)为交易各方提供安全的信道。
- (2)通过使用X.509 v3数字证书提供信任。
- (3)由于信息只在需要的时间和地方提供，因而要确保私密性。

10.4.1 SET的需求

(1)**提供支付和订购信息的保密性**

(2)**确保传送数据的完整性**

(3)**持卡人账号认证**：商家需要一种机制确保持卡人是有效账户号码的合法用户。

(4)**为商家提供认证**：持卡人需要能够识别他们将要进行安全交易的商家，能够验证商家与金融机构（清算行）具有允许其接受支付卡的关系。仍然使用数字签名和商家证书来确保商家的认证。

(5)**安全技术**：确保使用最好的安全模式和系统设计技术保护电子交易中所有合法方的利益。

(6)**创建一个不依赖于传输安全机制也不妨碍其使用的协议**：SET专门设计用于安全支付交易。

(7)**在软件和网络提供者之间提供功能设施和互操作性**

SET需要具有以下特性

- (1)**信息保密性**：持卡人账号和支付信息在网络传输过程中是安全的。
- (2)**数据完整性**：持卡人发往商家的支付信息包括订购信息、个人数据和支付指令。保证在传送中不被改动。
- (3)**持卡人账号认证**：SET使得商家能够验证持卡人是否为合法卡账号的合法用户。为此，SET使用带有RSA签名的X.509v3数字证书。
- (4)**商家认证**：SET使得持卡人能验证商家是否与允许接收支付卡的金融机构建立了联系。为此，SET使用带有RSA签名的X.509v3数字证书。
- SET要达到的主要目标是以下方面：

  (1)信息在公共因特网上安全传输。

  (2)订单信息和个人账号信息隔离。

  (3)持卡人和商家相互认证。

10.4.2 SET系统构成

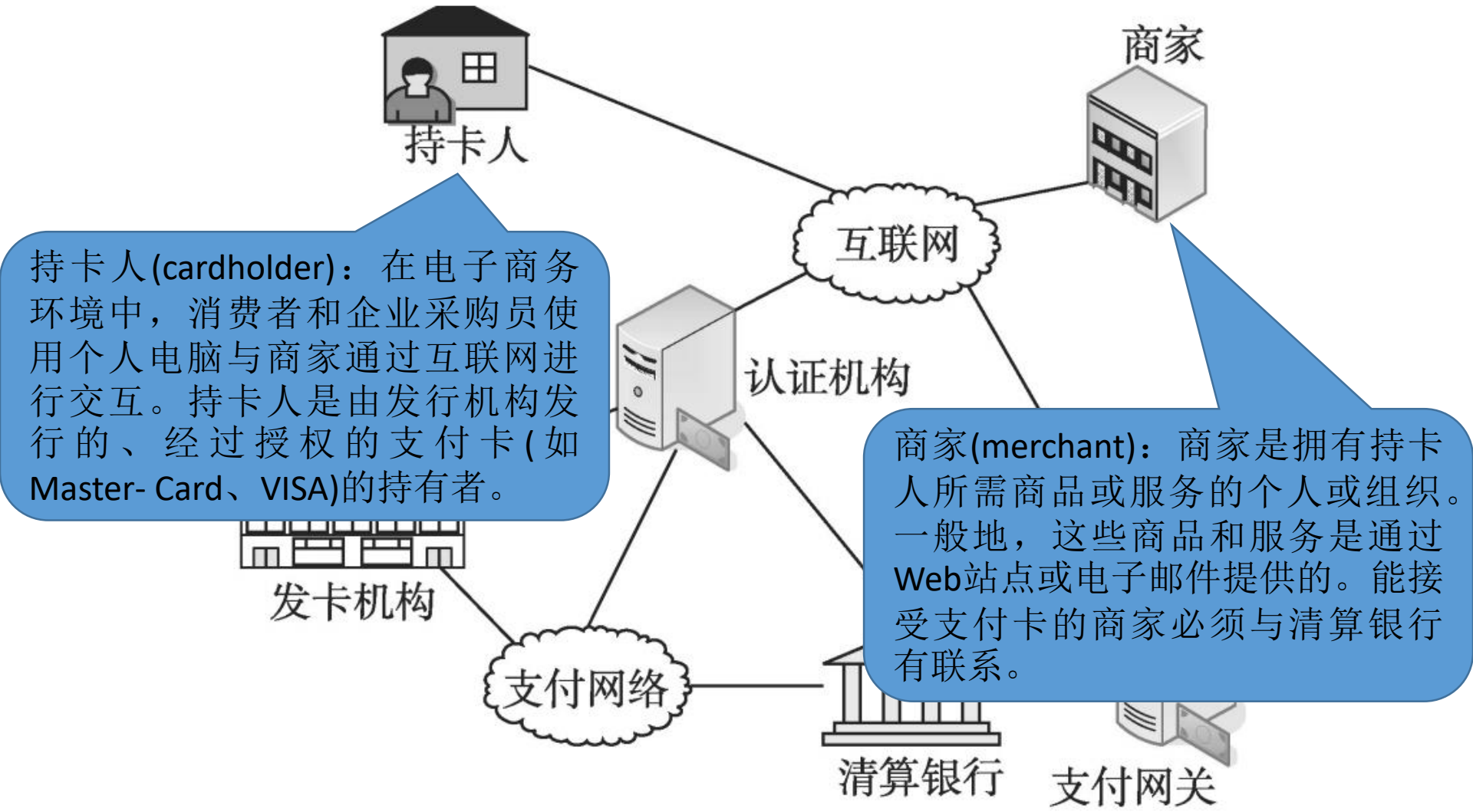


图10-19 SET的组成

清算银行(acquirer)：为商家建立账号、处理支付卡认证和支付的金融机构。商家通常可以接受多种品牌的信用卡，但并不想与所有发卡机构打交道。清算银行向商家提供认证，提供给定卡号是否合法和信用卡的消费限额等信息。清算银行还将支付信息传送到商家的账户中。随后，发卡机构还要为支付网络中的电子资金流动向清算银行提供补偿。

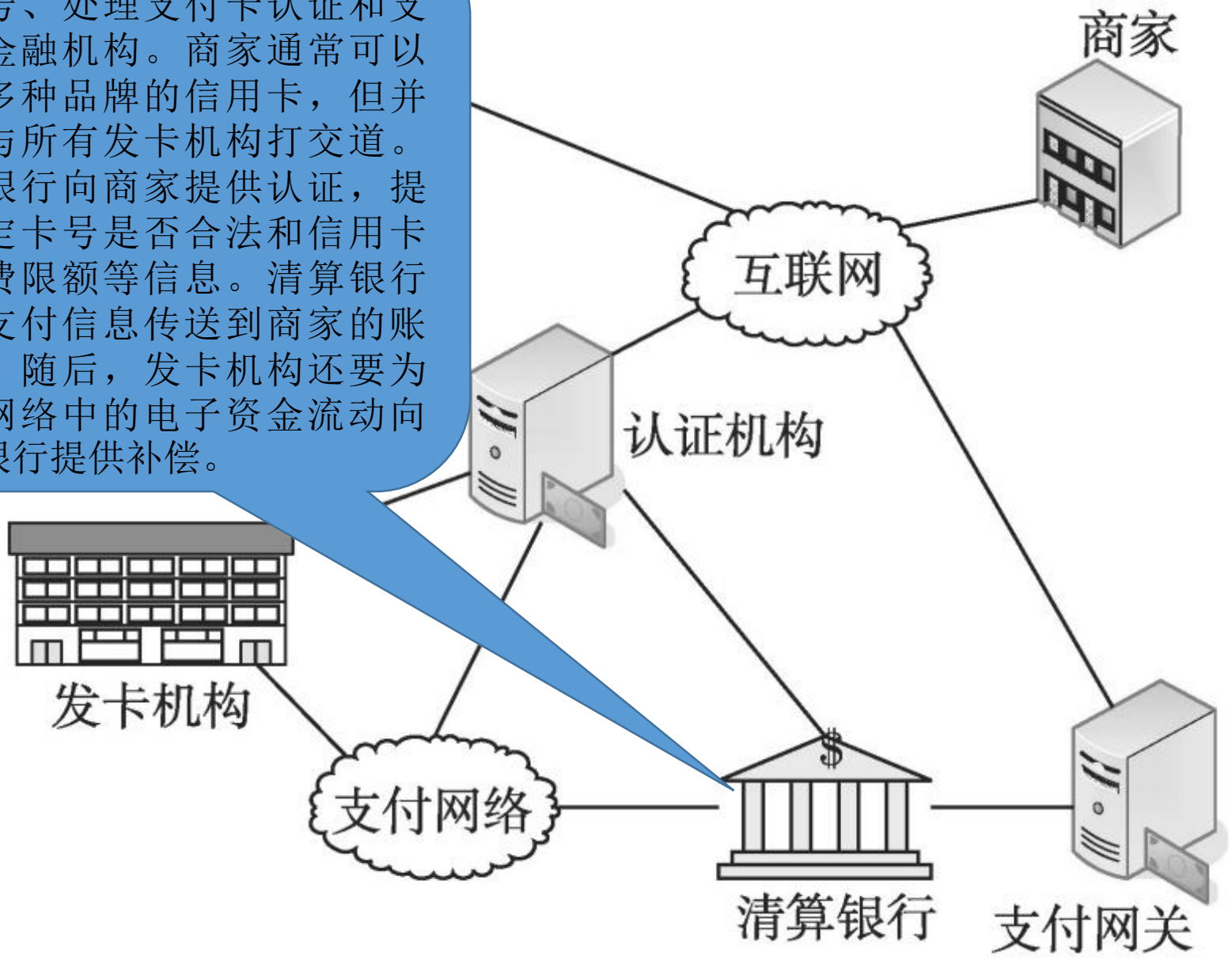


图10-19 SET的组成

支付网关(payment gateway)：由清算银行或指定的第三方提供的功能，处理商家支付信息。它完成众多卡品牌的支付授权服务，并完成清算服务和数据捕获。支付网关是SET和现存的银行卡支付网络的接口，提供认证和支付功能。商家通过互联网使用支付网关交换 SET 信息，而支付网关与清算银行的金融处理系统具有某种直接的连接或网络连接。支付网关以如下方式工作：加密消息，认证交易中的所有参与者，将SET消息转换为与商家销售系统兼容的格式。

认证机构(certification authority，CA)：被信任的，为持卡人、商家和支付网关发行X.509v3公钥证书的实体。SET的成功依赖于，为此目的服务的CA基础设施的存在。如前所述，使用层次CA，使得各方不需要直接被根CA认证。

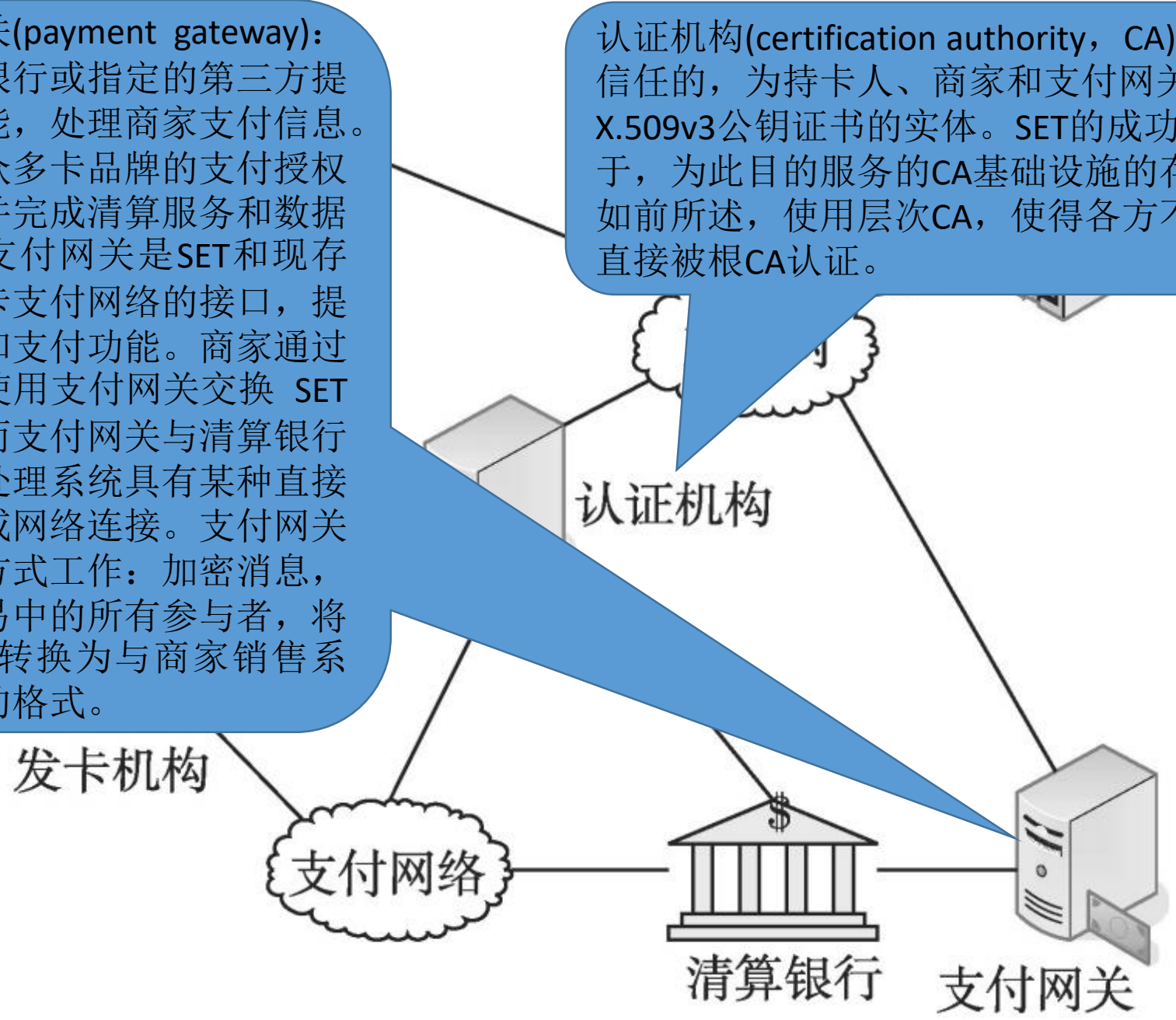


图10-19 SET的组成

基于SET的交易流程

- **(1)顾客开通账号**：顾客从一个支持电子支付和SET的银行获得一个信用卡账号，如 MasterCard或Visa。
- **(2)顾客申请证书**：在通过适当的身份验证后，顾客收到一个银行签发的X.509v3数字证书。证书验证了顾客的RSA公钥和有效期限，并建立了一个由银行担保的用户密钥和对信用卡之间的联系。
- **(3)商家申请证书**：商家在能够接收持卡人的SET支付指令之前必须向某个CA注册并申请证书。接收某品牌信用卡的商家必须拥有两种公钥证书：一个用于签名消息，一个用于密钥交换。商家还需要一个支付网关公钥证书的备份。
- **(4)顾客进行订购**：用户首先浏览商家的Web站点，选择商品。然后，顾客向商家发送一份购买清单，商家发回一个带有各种商品、单价、总金额和订购号的订购单。

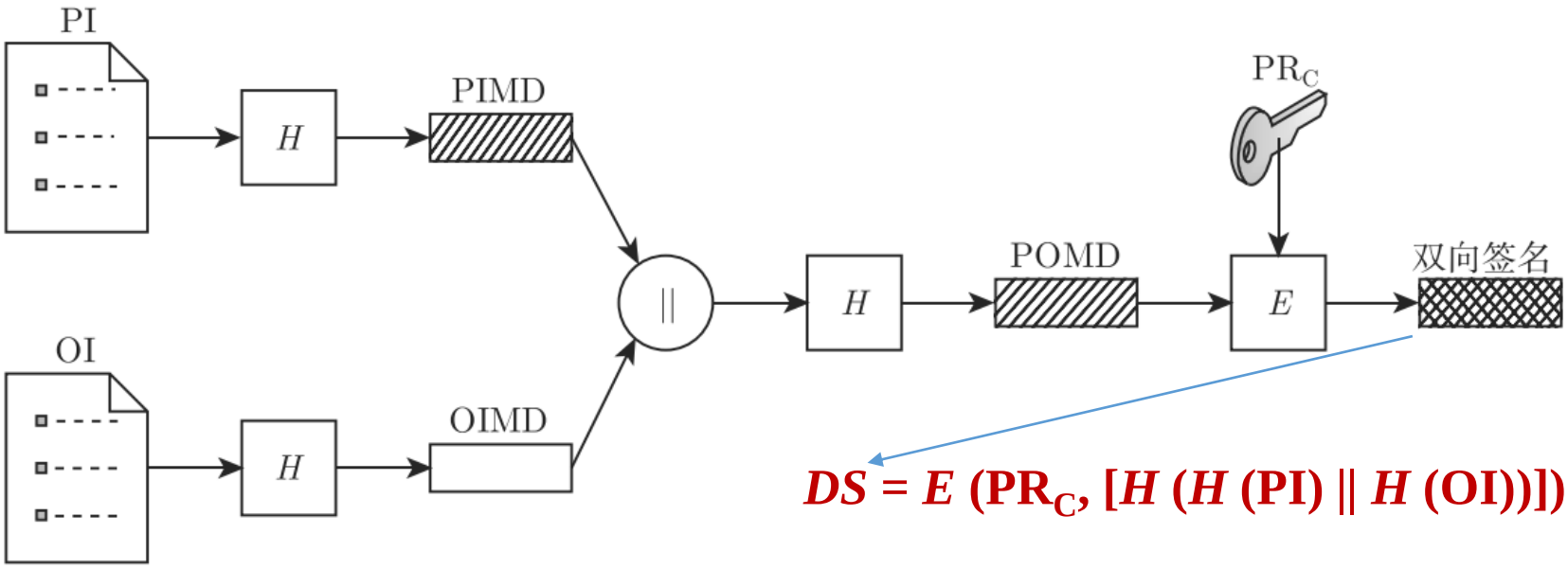
基于SET的交易流程

- **(5)商家被验证**：除了订购单，商家还发给客户一份他自己的证书，使得用户可以验证他正在和一个合法的商家进行交易。
- **(6)发送订购和支付信息**：顾客发送带有其证书的订购和支付信息给商家。其订购信息确认了订购单中要购买的项目。支付信息包括信用卡细节，并用商家无法解密的方法加密。顾客的证书可以使商家验证顾客。
- **(7)商家请求支付认证**：商家将付款信息发给支付网关，请求认证顾客提供的信用卡可以支付此次购买。
- **(8)商家确认订购**：商家向客户发送订购确认消息。
- **(9)商家提供商品或服务**：商家向顾客提供商品或服务。
- **(10)商家请求付款**：此请求发给支付网关，由支付网关处理所有的支付操作。

10.4.3 双向签名

- SET中引进了双向签名机制。双向签名的目的在于将两个接收者不同的消息连接起来。客户想给商家发送订购信息(OI)，给银行发送支付信息(PI)。商家不需要知道客户的信用卡号，银行不需要知道客户订购的细节，这为客户提供了分离这两者的额外保护。
- 然而，必须将这两个部分连接在一起以解决一些可能发生的纠纷。因此，将订购信息和支付信息连接起来，可以使客户证明这笔支付是为了这次订购，而不是为其他商品或服务的支付。
- 假设客户向商家发送了两个消息：一个签名的OI和一个签名的PI，然后由商家将PI传送给银行。如果商家从此客户获得了另一个OI，则商家可以说这个OI是与PI配套的，而不是原来的那个OI。消息连接即可防止此类事件的发生。

SET双向签名



PI —— 支付信息
OI —— 订购信息
H —— 散列函数 (SHA-1)
|| —— 连接符

PIMD —— PI的消息摘要
OIMD —— OI的消息摘要
POMD —— 支付和订购消息的消息摘要
E —— 加密 (RSA)
PR_C —— 顾客的签名私钥

图10-20 SET双向签名

双向签名的验证

- PR_C是用户的签名私钥。现在，假设商家得到了双签名(DS)、OI和PI的数字摘要(PIMD)。由于商家拥有从客户证书得到的客户公钥，使得商家可以计算如下两个值：

$$H(\text{PIMD} \,\|\, H[\text{OI}]) \; ; \; D(\text{PU}_C, \text{DS})$$

- 其中，PU_C是用户的签名公钥。如果这两个值相等，商家即验证了签名。同样，如果银行拥有DS，PI和OI的数字摘要(OIMD)、用户公钥，则银行可以计算：

$$H(H[\text{OI}] \,\|\, \text{OIMD}) \; ; \; D(\text{PU}_C, \text{DS})$$

- 如果两个值相等，银行即验证了签名。

✓(1)商家接收OI并验证签名。

✓(2)银行接收PI并验证签名。

✓(3)客户连接OI和PI，可以证明此连接。

10.4.4 支付处理

表10-2 SET交易类型

持卡人注册	持卡人在向商家发送 SET 消息之前必须到 CA 注册
商家注册	商家在与顾客和支付网关交换 SET 消息之前必须到 CA 注册
支付请求	顾客发给商家的消息，包括给商家的 OI 和给银行的 PI
支付认可	商家和支付网关间交换的消息，验证给定信用卡账号能够支持一次购买
支付获取	允许商家向支付网关申请支付
证书询问状态	如果 CA 无法快速地完成证书请求处理，它将给持卡人或商家发送一个应答，说明将在以后核对。持卡人或商家发送证书询问消息查询证书请求的状态，如果请求被通过，则收到证书
购买询问	允许持卡人在收到购买应答后查询订购处理的状态。注意，此消息不包含如退货等状态，但能表明认证、获取和信用处理等状态
撤销认可	允许商家更正以前的认可请求。如果订购未成，则商家退回所有的认可；如果部分订购未完成 (如退货)，则商家退回部分认可
撤销获取	允许商家更正获取请求中的错误，如店员输入了不正确的交易数据
信用	允许商家在退货或商品在运输过程中损坏时向持卡人账号中发布退还。注意，SET 的信用消息通常是由商家而不是持卡人发送的，商家和持卡人之间的通信使得在 SET 外处理退还
撤销信用	允许商家修正前一个退还请求
支付网关证书请求	允许商家询问网关，得到它的密钥交换和签名证书
批管理	允许商家根据批命令与支付网关交换信息
出错消息	表明由于格式或内容验证问题，接收者拒绝消息

1.购买请求

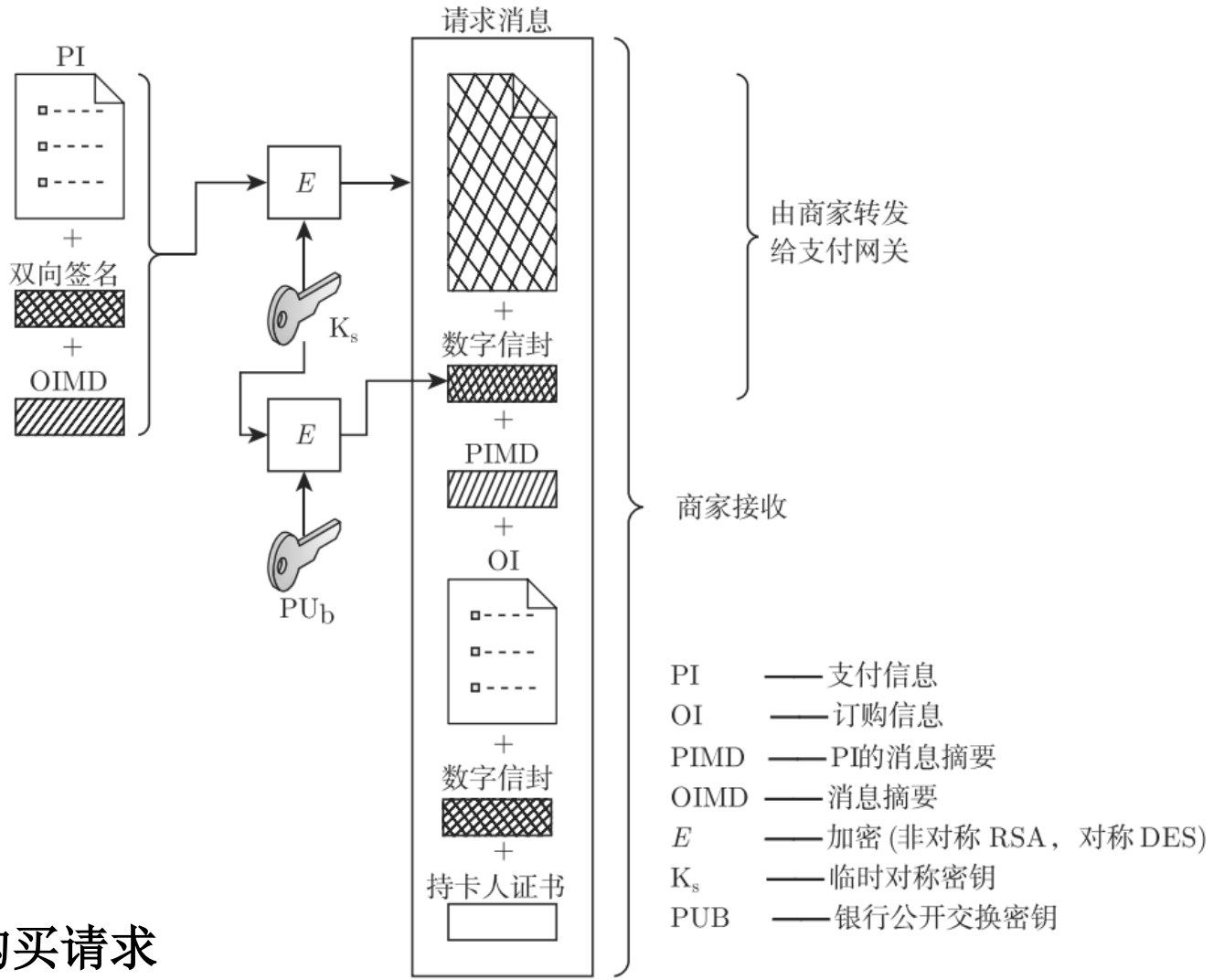


图10-21 购买请求

购买请求验证

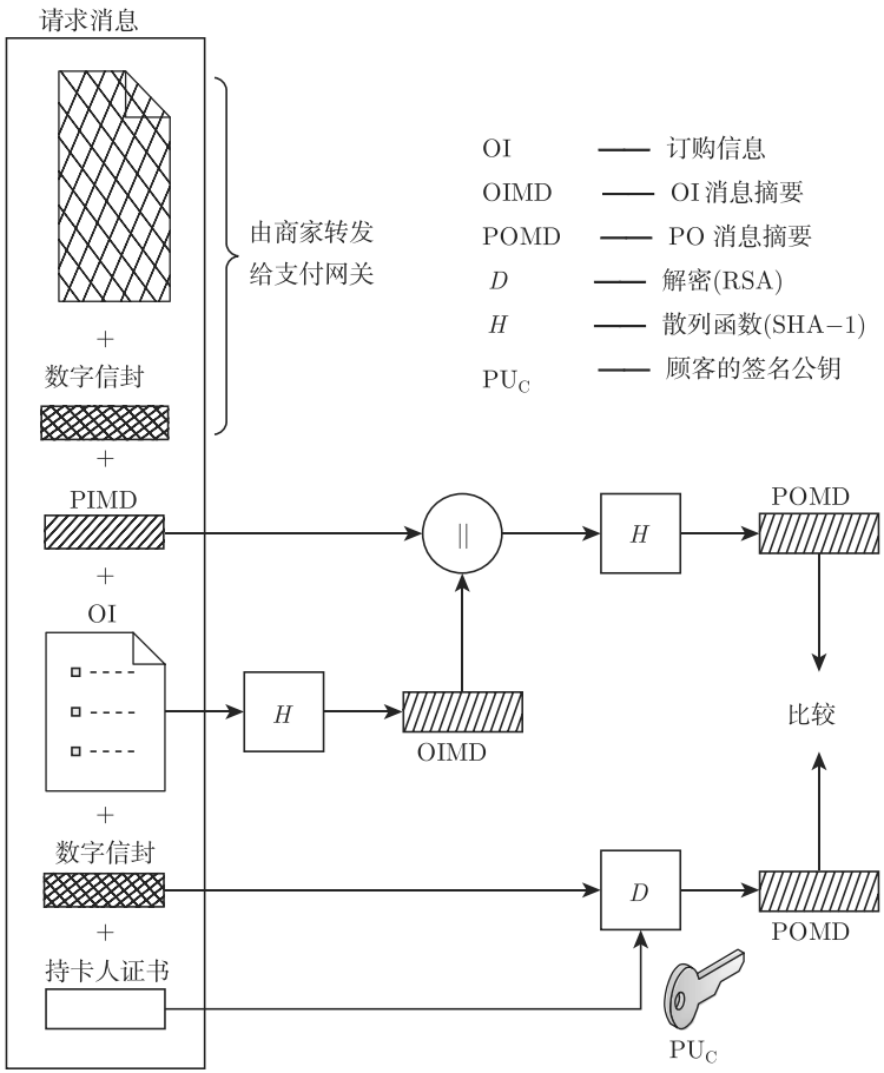


图10-22 购买请求验证

2.支付认可

- 支付授权交换由两个消息组成：认可请求和认可应答。
- 商家向支付网关发送的**认可请求消息包括以下内容。**

1)与购买相关的信息

- 从客户获得的信息，包括以下两种。
  - PI：根据PI和OI计算得到的双向签名，并使用顾客的签名私钥签名；OI消息摘要(OIMD)；数字信封

2)与认可相关的信息

- 由商家生成的信息，包括以下两种。
  - 认证分组：包括使用商家签名私钥签名的交易标识，并使用商家生成的一次性对称密钥加密。数字信封：使用支付网关的公开交换密钥加密一次性密钥形成数字信封。

3)证书

- 包括持卡人签名密钥证书（用于验证双向签名）、商家签名密钥证书（用于验证商家签名）以及商家密钥交换证书（在支付网关的应答中需要）。

支付网关执行的如下任务

- (1)验证所有的证书。
- (2)解密认证分组的数字信封，获得对称密钥，解密认证分组。
- (3)验证认证分组的商家签名。
- (4)解密支付分组的数字信封，获得对称密钥，解密支付分组。
- (5)验证支付分组的双向签名。
- (6)验证从商家接收到的交易标识，与从客户端接收（间接）的PI的交易标识比较。
- (7)请求和接收来自于发卡机构的认证。

支付网关返回的认证应答消息

- 获得发卡机构的认可后，支付网关返回认证应答消息给商家，包含如下元素。
  - **(1)与认证相关的信息：**包含用网关签名私钥签名的认证分组，并用网关生成的一次性对称密钥加密。同时还包含用商家交换密钥的公钥加密的一次性密钥组成的数字信封。
  - **(2)获取标记信息：**此信息用于以后的支付，内容包括签名、加密的获取标记和数字信封。此标记不由商家处理，必须在支付请求中返回。
  - **(3)证书：**网关的签名密钥证书。
- 有了网关的认证，商家即可向顾客提供商品或服务。

3.支付获取

- 为了获得支付款，商家向支付网关请求支付款获取交易，由获取请求和获取应答两个消息组成。
- 对获取请求消息而言，商家对获取请求分组（包括付款金额、交易标识）签名、加密。消息还包括在认可应答消息中收到的被加密的获取令牌、商家的签名密钥和交换密钥的密钥证书。
- 当支付网关接收到获取请求消息时，解密和验证获取请求分组和获取标记。然后验证获取请求与获取令牌的一致性。接着，创建一个通过专用支付网络传送的请求消息，使得资金能够转到商家的账号。然后，网关在获取应答消息中通知商家已支付。
- 获取应答消息包括由网关签名和加密的获取应答分组，还包括网关的签名密钥证书。商家软件存储获取应答，便于和从清算银行获得的支付进行验证。

10.5 安全电子邮件

- 自学PGP的原理
- 参考实验2，了解PGP的应用

第10章作业

- 作业
  - 3.安全服务和安全机制的区别和联系是什么？
  - 5.简述IPSec的两种工作模式。
  - 6.ESP协议和AH协议有哪些不同？
  - 9.SSL记录协议包括哪几个主要步骤？
  - 10.简述SSL握手协议的处理过程。

- 实践（自己研究，不考核）
  - 阅读 http://staff.ustc.edu.cn/~billzeng/ns/ns04.pdf 文档中的IPSec VPN
  - 调研IPSec在VPN中的应用