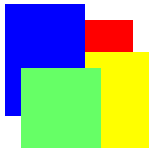


第6章 网络安全加固

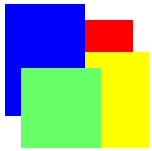
网络层安全加固

董建润

南京邮电大学

关键知识点

- 网络安全加固主要涉及到网络层安全加固技术和应用层安全加固技术。
- 目前较为完整的一类网络层安全加固技术是安全IP技术(IPsec技术)。IPsec涉及到网络层的真实性验证、访问控制、数据保密传送、数据完整传送等技术。
  - 安全IP隧道技术(安全IP网关的互连技术，VPN技术)
- 目前使用较为广泛的一类应用层安全加固技术是安全套接层技术(SSL技术)。SSL涉及到传送层的真实性验证、数据保密传送、数据完整传送技术。
  - HTTPS(安全超文本传送协议：HTTP+SSL)技术



主要内容

- 安全IP概述
- 真实性验证报头(AH)协议
- 封装安全报体(ESP)协议
- 互联网安全关联与密钥管理协议(ISAKMP)
- 互联网密钥交换(IKE)协议

安全IP概述*

- 安全IP(IPsec)在互联网协议(IP)层提供安全服务，也就是在网络层提供安全服务。
- 安全IP提供的安全服务包括：访问控制、数据传递的完整性验证、数据源真实性验证、防范重播分组攻击、数据保密传递、以及有限的数据传递信息保密。
- 这里“有限的数据传递信息保密”是指不泄漏IP分组真实的源地址、目的地址、端口号等协议控制信息。

安全IP的总体组成

- IPsec总体上包括4个组成部分：安全协议，安全关联，密钥管理，以及真实性验证算法与加密算法。
- 为了利用IPsec在IP层提供安全服务，必须选择安全协议、选择安全协议中采用的真实性验证算法或者加密算法，协商真实性验证算法或加密算法采用的密钥，最终建立需要进行IPsec通信的IP结点之间的安全关联。

安全IP中定义的安全协议

- IPsec目前只提供两种安全协议：身份真实性验证报头(AH)协议和封装安全报体(ESP)协议。
- AH协议主要提供的IP层安全服务包括：访问控制、数据传递的完整性验证、数据源真实性验证和防范重播分组攻击。
- ESP协议不仅可以提供AH协议提供的真实性验证类安全服务，还可以提供数据保密传递和有限的数据传递信息保密等功能。

安全关联

- 安全关联(SA)概念是安全IP的基础，AH和ESP都需要使用SA，而互联网密钥交换(IKE)协议的主要功能是建立和维护安全关联。
- 安全关联是两个或者多个实体之间描述如何使用安全服务进行安全通信的一种连接关系，这种关系采用这些实体之间作为合同的一组信息表示。
  - 这组信息是在这些实体之间协商和共享的，有时这组信息本身就称为一个“安全关联”。
- 安全关联是一个单工(单向)连接，它为在该连接上传递的报文提供安全服务。
- SA可以利用AH协议或者ESP协议提供安全服务，但是，一个SA不能同时使用AH和ESP协议。

安全关联的标识

- 一个SA可以由三元组（安全参数索引, IP目的地址, 安全协议标识）唯一标识，
- 安全参数索引(SPI)指向存放该SA已经协商完成的安全参数的数据项，
- IP目的地址指向该SA数据接收方的主机或安全网关，
- 安全协议标识表示SA采用的安全协议，即可以是AH协议标识，或者是ESP协议标识。

安全关联的模式

- SA可以分成两种模式：一种是传送模式，另一种是隧道模式。
- 传送模式的SA是在两个主机之间建立的SA，它仅仅保护IP层之上的报文传递。例如，传送模式的SA可以采用ESP协议对传送层报文进行加密传递。
- 隧道模式的SA是将安全关联应用于IP隧道中。

IP隧道

- IP隧道就是在正常的IP报文外面再封装一个IP报头，使得正常的IP报文先传递到封装的IP报头指定的目的地址，然后拆除封装的IP报头，再按照原来的IP报文指定的目的地址继续传递。

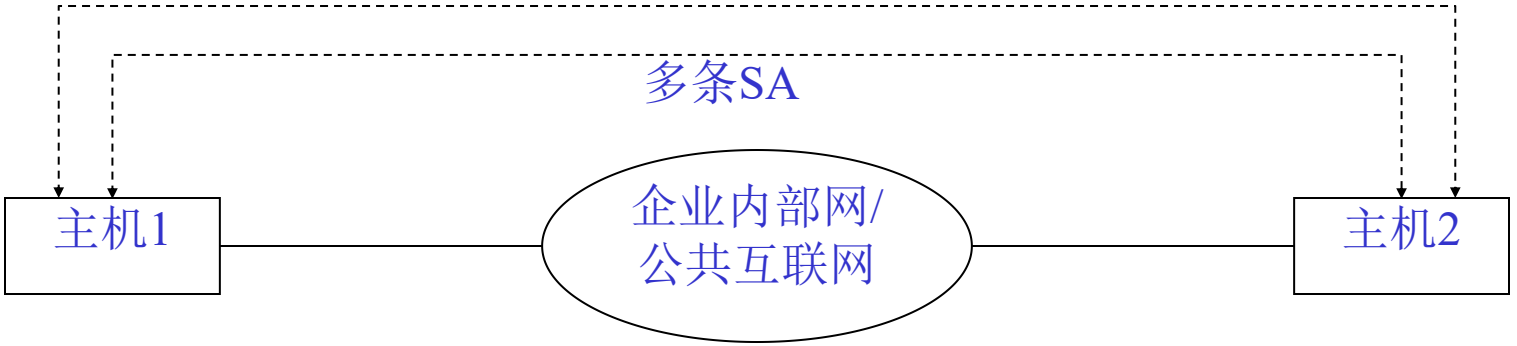
IP隧道示意图

SA组合模式

- 每条SA只能支持一个安全协议。但是，有些应用需要同时支持AH和ESP安全协议。这时，就需要在一对IP网络结点之间建立多条SA(即SA组合)。
- IPsec规定，任何符合IPsec规范的安全IP实现系统中至少必须支持以下4种SA组合模式：

SA组合模式1

- 在两台IP网络主机之间可以建立多条SA(如图6.2所示)，SA可以是传送模式或者隧道模式。这里的主机1和主机2都支持IPsec相关协议。
- 这是虚拟专线的应用模式，课程实验的内容。



SA组合模式1

SA组合模式1(续)

- 在主机1和主机2之间传递的分组报头可以根据使用的IPsec服务和选用的SA的模式采用以下一种形式：

传送模式1：[IP1][AH][Upper]

传送模式2：[IP1][ESP][Upper]

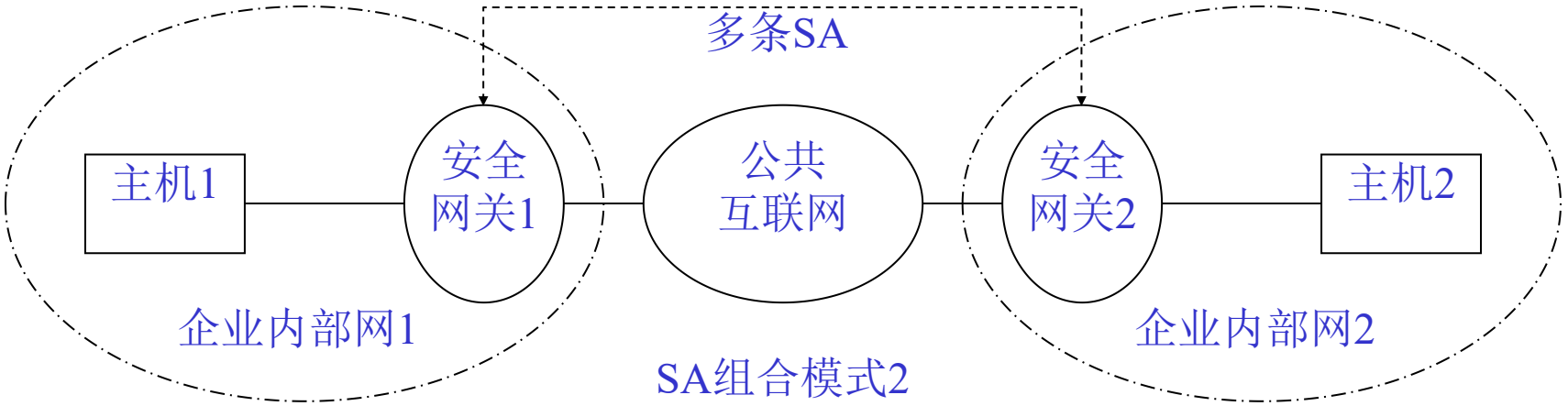
传送模式3：[IP1][AH][ESP][Upper]

隧道模式1：[IP2][AH][IP1][Upper]

隧道模式2：[IP2][ESP][IP1][Upper]

SA组合模式2

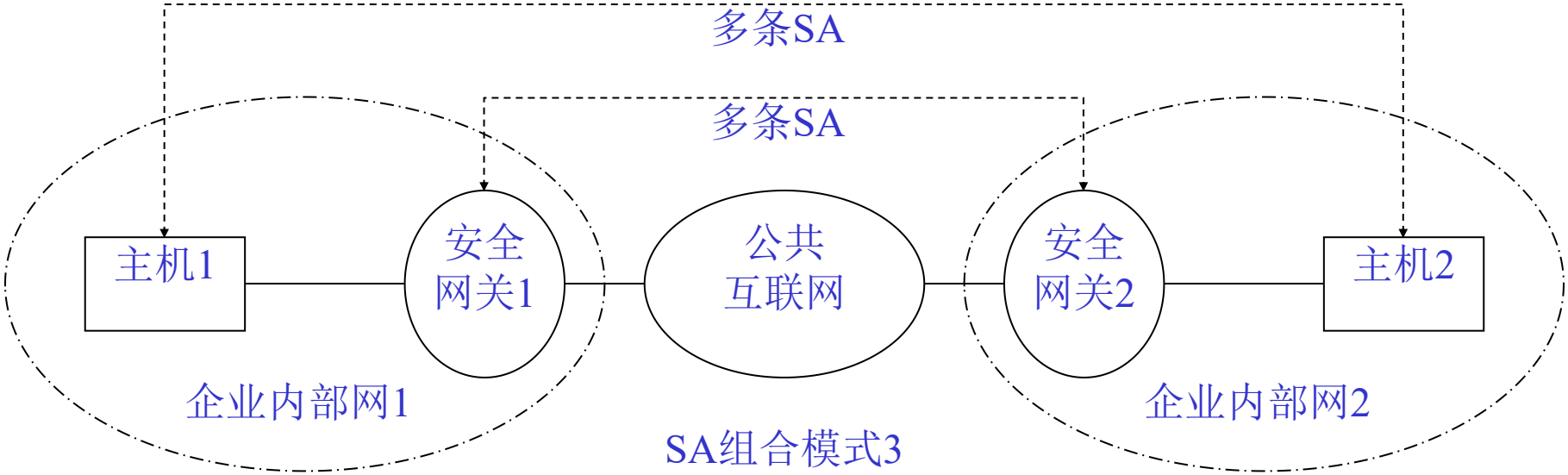
- 这是简单的虚拟专用网(VPN)应用模式，两个企业内部网通过两个安全网关建立的多条SA，实现跨越公共互联网的虚拟内部网。



SA组合模式2

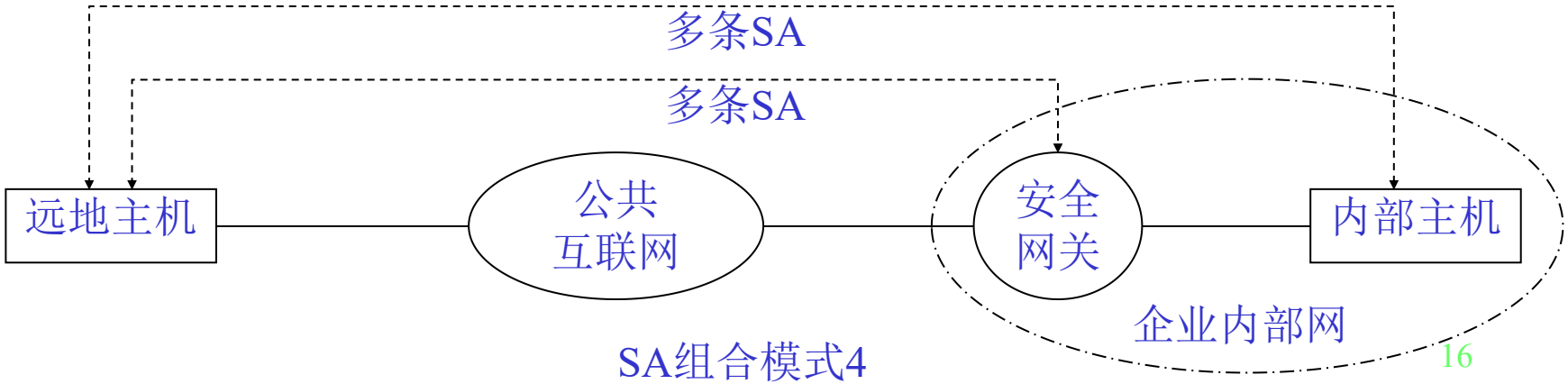
SA组合模式3

- 这是SA组合模式1与SA组合模式2的结合，在SA组合模式2的基础上，增加了虚拟专用网内的多个主机之间的多条SA。



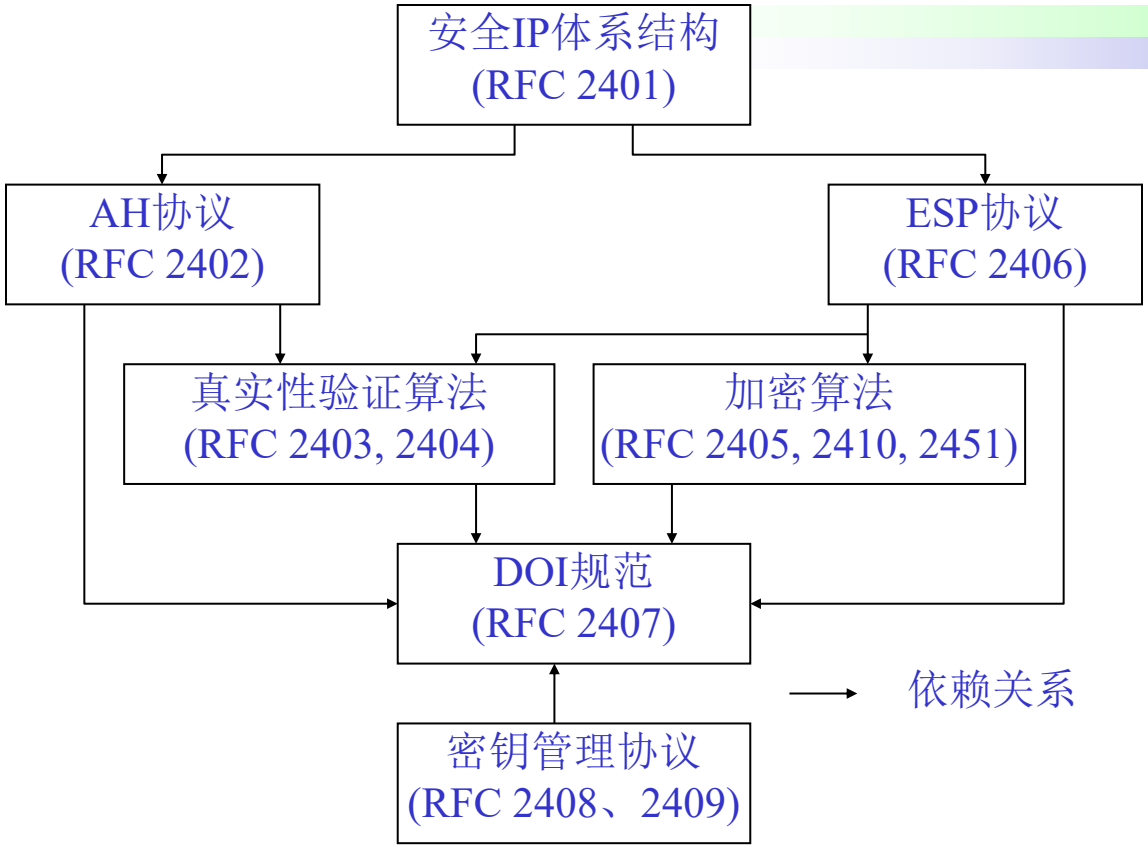
SA组合模式4

- 远地主机首先通过公共互联网与安全网关建立SA连接，然后，再与企业内部网中某个主机建立SA连接——构建虚拟的内部网连接，以及主机之间的安全连接。
- 这是移动办公的应用模式。



SA组合模式4

IPsec协议簇



安全IP协议簇组成结构图

- IPsec由一组IETF定义的IPsec技术标准描述，这组协议称为IPsec协议簇。

真实性验证报头(AH)协议

- 真实性验证报头(AH)协议IPsec中定义的两个安全协议之一。
  - 注：讲义中的“真实性验证报头协议”就是这里的真实性验证报头协议。 “真实性验证”的含义更加准确。
- AH主要对IP报文提供无连接传递的完整性验证以及对数据源的真实性验证，它也可以提供防范IP报文重播攻击的功能。
- AH协议真实性验证的范围包括尽可能多的IP报头的内容，以及IP报文携带的数据。

AH协议报文格式

- AH协议报文包括：下个报头（的协议编号）、报体长度、预留、安全参数索引(SPI)、顺序号和真实性验证数据，这6个AH报文必须的字段。

0　　7 8　　15 16　　31比特

下个报头	报体长度	预留
安全参数索引(SPI)		
顺序编号		
真实性验证数据(长度可变)		

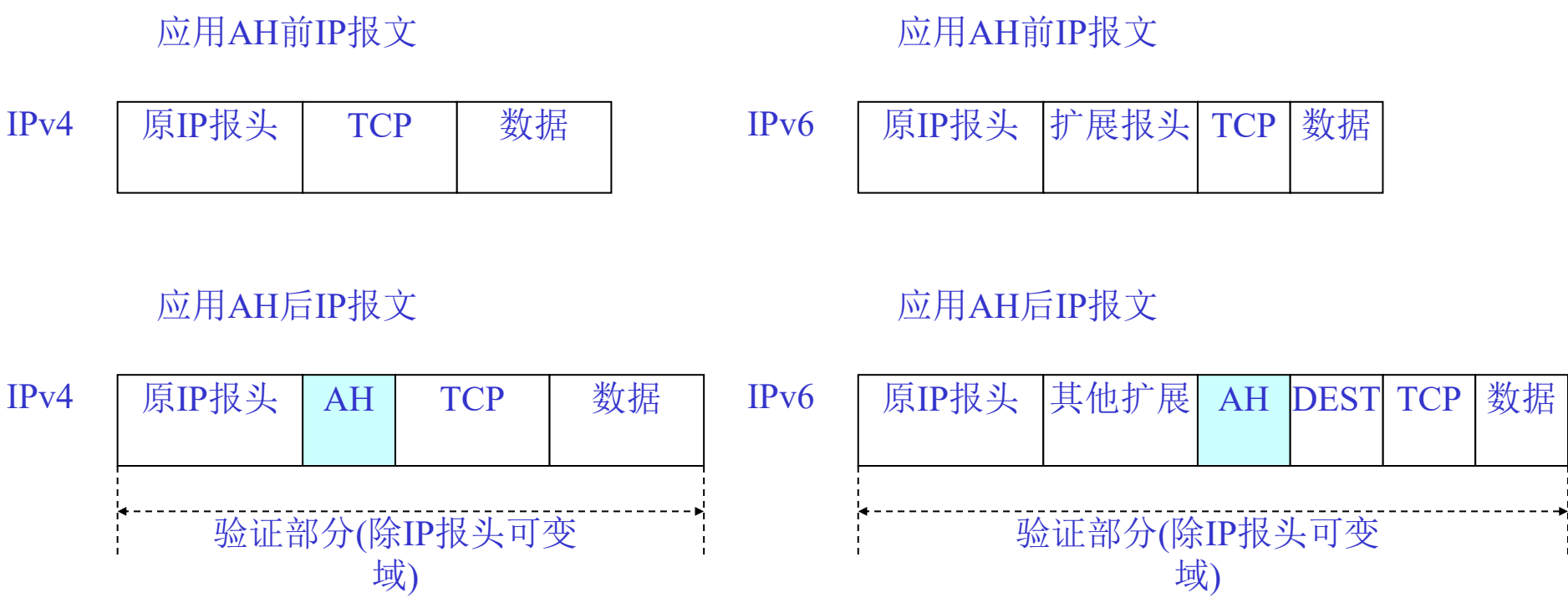
AH协议报头格式

AH协议的处理

- AH协议报文实际上就是一个报头。AH协议编号为51，AH报文将插在IP报头与IP报体之间。
- 根据使用SA的模式不同，AH可有2种使用模式：传送模式和隧道模式。在两种模式中，AH报文的位置有所不同。

AH协议的处理(续1)

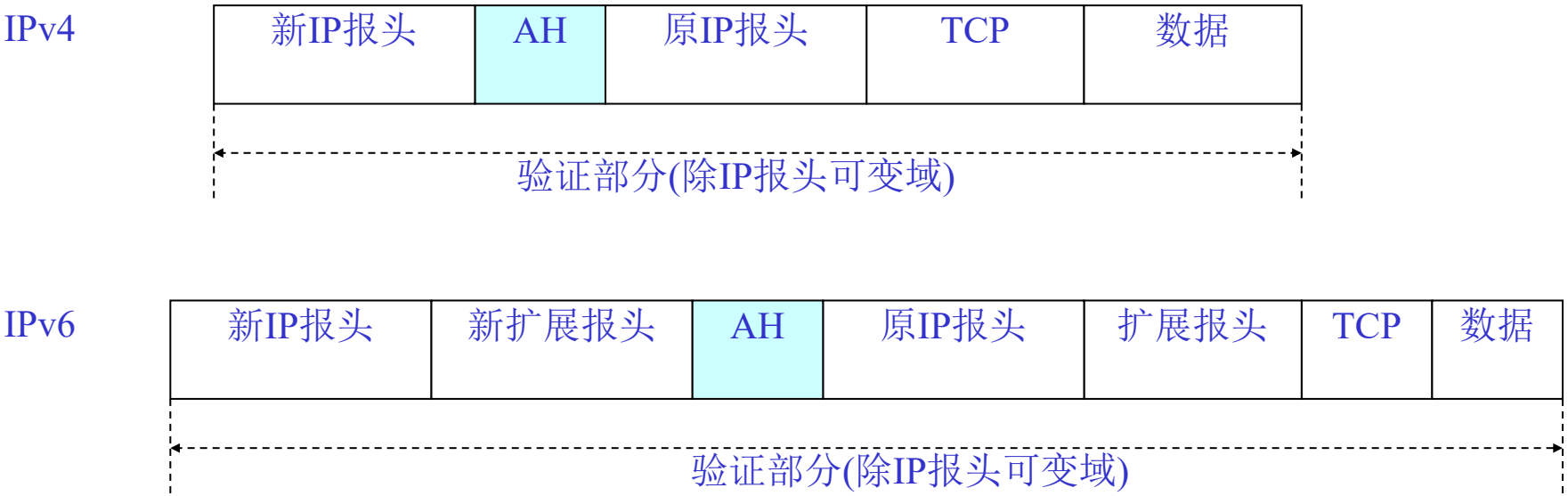
- 传送模式中AH报文的封装格式



传送模式中AH报文的封装格式

AH协议的处理(续2)

- 隧道模式中，AH报文的封装格式：



隧道模式中AH报文的封装格式

报文真实性验证算法

- IPsec采用了以下2种报文真实性验证算法：
- 一种是在RFC 2403中定义的采用MD5作为报文摘要算法，采用HMAC作为报文验证码算法的、适用于AH和ESP协议的真实性验证算法，缩写为HMAC-MD5-96。
- 另一种是在RFC 2404中定义的采用SHA-1作为报文摘要算法，采用HMAC作为报文验证码算法的、适用于AH和ESP协议的真实性验证算法，缩写为HMAC-SHA-1-96。
  - 注：这里的报文真实性验证算法，也就是真实性验证算法

真实性验证算法的验证码长度

- HMAC-MD5-96算法中的MD5算法，产生128比特长度的真实性验证码。在AH和ESP真实性验证的应用中，截取前96比特作为真实性验证数据的操作。
- HMAC-SHA-1-96算法中的SHA-1算法，产生160比特长度的真实性验证码。在AH和ESP真实性验证的应用中，截取前96比特作为真实性验证数据的操作。

真实性验证算法的密钥(保密字)

- 在AH和ESP真实性验证的应用中，HMAC-MD5-96算法中的HMAC算法，必须采用128比特长度的密钥(保密字)。
- 在AH和ESP真实性验证的应用中， HMAC-SHA-1-96算法中的HMAC算法，必须采用160比特长度的密钥(保密字)。
- 这些密钥必须分发到参与AH或ESP真实性验证的IPsec结点。
- 为了防范攻击，建议周期性地更新密钥。

封装安全报体(ESP)协议

- 封装安全报体(ESP)是安全IP技术中定义的两个安全协议之一。
- ESP主要用于对IP报文提供保密传递、无连接传递的完整性验证以及对数据源的真实性验证。ESP也可以提供防范IP报文重播攻击的功能，以及有限度的通信流保密性。
- ESP主要提供对IP报文加密传输的功能，它是专门为对称密钥加密算法设计的安全协议。

ESP协议报文格式

- ESP报文包括安全参数索引(SPI)、顺序编号、报体数据、填充数据、填充数据长度、下个报头、以及真实性验证数据。

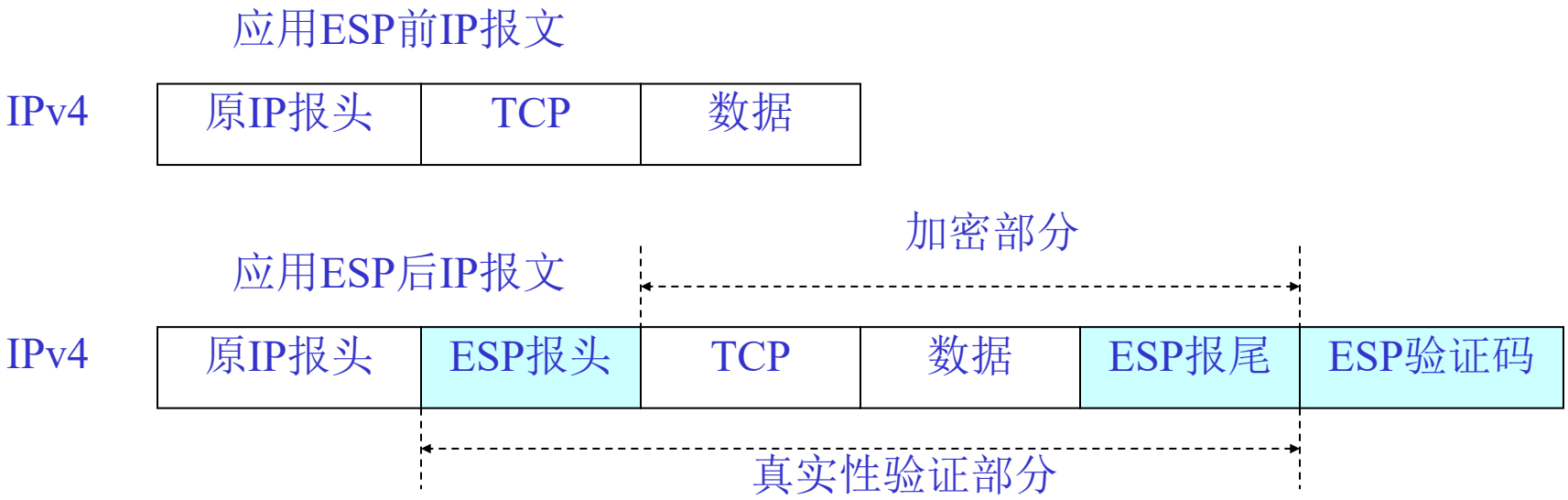
ESP报文格式

ESP协议的处理

- ESP协议编号是50，封装ESP协议的报文需要在“下个报头”字段中设置“50”。
- ESP协议不同于AH协议，它是将需要保护的IP报文(隧道模式)或者IP报文传递的报体(传送模式)封装在自己的“报体数据”字段中。
- IP报文应用ESP协议时，需要考虑ESP报头和报尾在原来IP报文中的位置。

ESP协议的处理(续1)

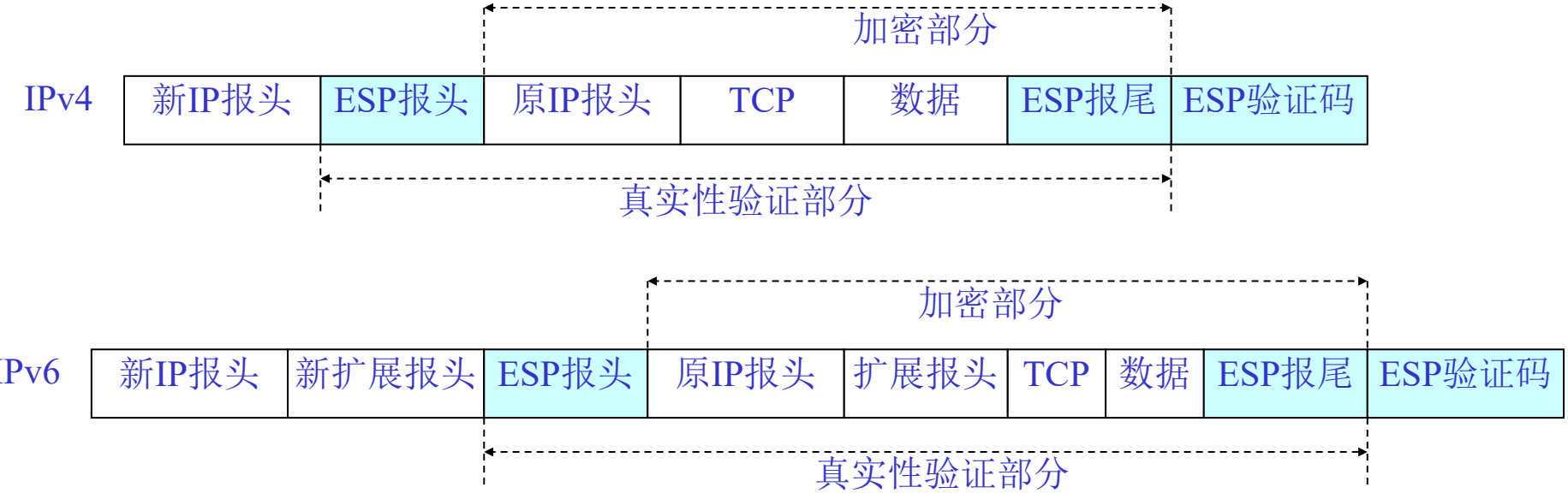
- 与SA的使用模式一样，ESP也有2种使用模式：传送模式和隧道模式。
- 传送模式中，ESP报文对IPv4的封装格式如下：



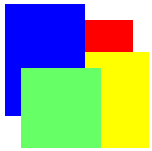
ESP报文的IPv4传送模式封装格式

ESP协议的处理(续2)

- 隧道模式中，ESP报文的封装格式如下：



ESP报文的隧道模式封装格式



ESP协议的加密算法

- ESP协议使用的真实性验证算法与AH协议使用的算法相同。
- 如果ESP协议同时选择了加密功能和真实性验证功能，则必须首先对报文执行加密算法，然后再对加密之后的ESP报文执行真实性验证算法。
- ESP协议是面向对称密钥加密算法设计的安全协议，所以，ESP协议相关的标准加密算法都是对称密钥加密算法。

ESP协议的加密算法(续)

- RFC 2405定义了在ESP协议中采用CBC模式使用DES加密算法的规范，按照该规范使用的加密算法可以简称为DES-CBC算法。
- DES-CBC算法要求每个ESP报文携带CBC模式所需的初始向量IV必须放置在ESP报文的“顺序编号”字段之后，被加密的“报体数据”字段之前。IV长度为64个比特。
- DES-CBC是一种块加密算法，要求块的大小为64个比特。DES-CBC作为一种对称密钥加密算法，其共享密钥的长度为64个比特。

互联网安全关联与密钥管理协议

- 互联网安全关联与密钥管理协议(英文缩写ISAKMP)集成了真实性验证、密钥管理和安全关联的网络安全概念，为互联网上政府、商业和个人通信创建一个安全的环境。
- ISAKMP是在IPsec协议簇中定义的一种密钥管理协议框架，它试图适用于互联网的所有协议层。

ISAKMP概述

- ISAKMP不仅适用于IP协议层的安全通信，也适用于其他所有协议层次的安全通信，例如IPsec、TLS、OSPF等。
  - 这样设计ISAKMP协议的目的是为了提供管理安全关联的统一模式，减少在不同功能层的安全协议之间的差异设计，提高安全关联创建和维护的效率。
- ISAKMP协议定义了用于验证通信对等方身份真实性、创建和管理安全关联、生成密钥、以及减少网络攻击威胁的一组规程。

ISAKMP功能概述

- ISAKMP定义了用于安全关联的多种报体格式，例如交换密钥生成数据和真实性验证数据的报体格式。这些报体格式构成了一个独立于密钥生成技术、加密算法和真实性验证机制的公共框架模型。
- 虽然可以通过密钥交换协议建立安全关联，但是，ISAKMP不同于密钥交换协议，也不同于安全关联建立协议，它仅仅是用于建立、修改和删除SA的一个公共框架模型。

ISAKMP协商能力概述

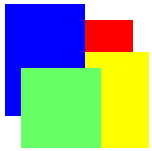
- 不同的网络安全环境需要不同的网络安全关联，ISAKMP就是为了协商这些不同安全需求的安全关联而设计的框架模型。
- ISAKMP支持安全IP和其他安全协议有关不同的加密算法、真实性验证机制和密钥建立算法的协商。
  - ISAKMP支持低层协议面向主机的证书、高层协议面向用户的证书；
  - ISAKMP还支持应用协议、面向会话协议、路由选择协议以及链路层协议要求的独立于具体加密算法和真实性验证机制的安全能力。

ISAKMP适用于不同安全技术

- 作为一种公共框架模型，ISAKMP具有自身的灵活性，它不依赖于任何一种加密算法、真实性验证算法或者安全机制，这样，它可以适用于任何新型的安全技术，同时，也可以通过更新加密算法、真实性验证算法和安全机制，提高自身的安全防御能力。
- ISAKMP中的一个重要思想是：
  - 将真实性验证和密钥交换相结合可以取得更强的安全控制能力；安全关联就是结合了真实性验证和数据保护的一种具体安全控制机制。

ISAKMP的基本要求

- ISAKMP不限定具体的加密算法、密钥产生技术和真实性验证机制，但是，ISAKMP对真实性验证和密钥生成部件有一些基本要求，这样就可以防范“拒绝服务”、“重播”、“中间人”和“连接劫持”攻击。
- 例如，为了减少网络攻击威胁，ISAKMP要求一个基于数字签名的强真实性验证机制，但是，ISAKMP并没有指定某种具体的数字签名算法或证书认证中心。
- 为了在网络实体之间进行安全IP通信，所有实体必须严格遵守“安全关联”的约定。ISAKMP作用就是定义协商这组约定(信息)所需要的报文格式和基本交换过程。



ISAKMP功能

- ISAKMP定义了
  - 一个标准的ISAKMP报头格式、
  - 一组用于安全关联的创建、修改和删除的标准报体格式、以及
  - 一个标准的安全关联创建的两阶段交互过程。
- ISAKMP对于设计和实现互联网环境下的密钥管理协议具有很好的指导作用。

ISAKMP报头格式

- ISAKMP报头包含了维护协议状态、处理报体、以及防范拒绝服务和重播攻击所需要的通用信息。

ISAKMP报头格式

ISAKMP报头格式(续)

- 发起方“甜点(cookie,跟踪文件)”字段和响应方“甜点”字段，用于安全标识ISAKMP的安全关联。
- ISAKMP报文由一个固定格式的报头和一组报体构成。“下个报体”用于标识后续报体类型。
- 大小版本用于标识该报头适用的协议版本范围。
- 交换类型字段指示该ISAKMP报文应用于的交换类型。
- 标志字段指示为ISAKMP交换设置的某些特殊选项。例如加密、提交、和真实性验证标志位。

ISAKMP标准报体格式

- 报体构成了ISAKMP报文的具体处理功能。
- ISAKMP报体类型包括：
  - 无报体
  - 安全关联报体(SA)
  - 建议报体(P)
  - 转换报体(T)
  - 密钥交换报体(KE)、

ISAKMP标准报体格式(续)

- 标识报体(ID)
- 证书报体(CERT)、证书请求报体(CR)
- 哈希报体(HASH)、签名报体(SIG)、一次性数报体(NONCE)
- 通告报体(N)
- 删除报体(D)
- 供货商标识(VID)，等。

ISAKMP交换类型及取值

- ISAKMP交换类型及取值一览表

ISAKMP交换类型	取值
无类型	0
基本型	1
标识保护型	2
真实性验证型	3
自信型	4
消息型	5
ISAKMP未来使用	6 – 31
DOI指定使用	32 – 239
内部使用	240 – 255

标志字段

- 标志字段，长度为1个八位位组(8个比特)，指示为ISAKMP交换设置的某些特殊选项。
- RFC 2408中定义了3个标志位，从低位到高位排序为：加密标志位、提交标志位、真实性验证标志位。标志字段中其他5个标志位在RFC 2408中没有定义，应该设置为“0”。已经定义的3个标志位的具体含义如下：
- 加密标志位(缩写为E)，位于标志字段的0比特位。如果该标志位为“1”，则表示ISAKMP报头后面所有的报体已经按照ISAKMP安全关联指定的加密算法进行加密。

标志字段(续)

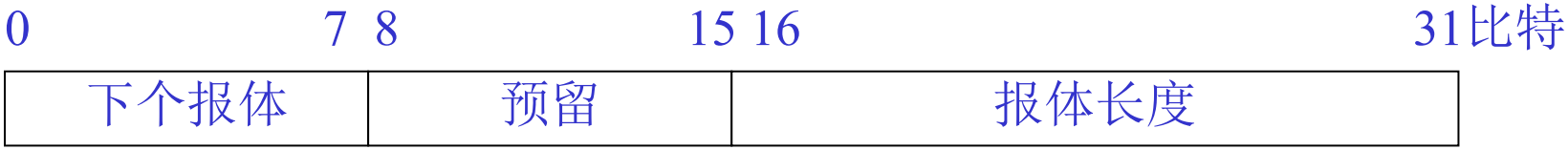
- 提交标志位(缩写为C)，位于标志字段的1比特位。该标志位用于发出密钥交换同步的信号，保证对方在安全关联建立完成之后，才收到密钥材料。如果该标志位为“1”，则接收到该报文的一方必须等待设置该标志位的另一方传来的“已连接”通告报文后，才能启用密钥材料。该标识位可以在ISAKMP两阶段协商中的任何一个阶段设置。
- 真实性验证标志位(缩写位A)，位于标志字段的2比特位。如果该标志位为“1”，则该报头后面的通告报体只进行真实性验证处理，而不进行加密处理。

报文标识符

- 报文标识符字段，长度为4个八位位组(32个比特)，用于标识ISAKMP第二阶段正在协商的安全关联。该字段的数值由第二阶段协商的发起方随机生成。该字段在ISAKMP第一阶段协商时，取值应该为“0”。
- 报文长度字段，长度为4个八位位组(32个比特)，该字段存放以八位位组(8比特)为单位的整个ISAKMP报文的长度，ISAKMP报文包括了ISAKMP报头和所有的报体。

报体通用格式

- 所有的报体都具有一个通用的报头，包括
  - 下个报体字段，长度为1个八位位组(8个比特)，用于指示在该报体的下一个报体的类型。如果该报体是ISAKMP报文的最后一个报体，则该字段取值为“0”。
  - 预留字段，目前尚未定义，该字段取值为“0”。
  - 报体长度，长度为2个八位位组(16个比特)，表示以八位位组(8个比特)为单位的该报体长度。报体包括报体的通用报头和报体的内容。



ISAKMP报体通用报头格式

SA创建的两阶段交互过程

- ISAKMP需要通过两个阶段的报文交互，才能建立针对某个具体安全协议的安全关联。
- 第一个阶段是建立ISAKMP自身的安全关联，称为ISAKMP安全关联；
- 第二个阶段再建立针对某个具体安全协议的安全关联，称为协议安全关联。
- 两阶段协商过程保证了ISAKMP独立于任何具体的安全协议，并且可以适用于任何安全协议(不仅包括AH和ESP协议)的协商过程。

SA创建的两阶段交互的操作

- SA创建的两阶段操作以及字段取值。

编号	操作	发起方 甜点	响应方 甜点	报文 标识符	SPI
1	发起ISAKMP SA协商	X	0	0	0
2	响应ISAKMP SA协商	X	X	0	0
3	发起其他SA协商	X	X	X	X
4	响应其他SA协商	X	X	X	X
5	其他操作(KE, ID等)	X	X	X/0	N/A
6	安全协议(ESP, AH)	N/A	N/A	N/A	X

SA创建的两阶段交互的说明-1

- 表中第1和2项操作属于ISAKMP第一阶段协商ISAKMP 的安全关联操作，在发起ISAKMP安全关联时只出现发起方甜点字段(发起方通用SA标识)，而在响应ISAKMP安全关联时必须同时出现发起方和响应方的甜点字段。
- 表中第3和4项都是属于ISAKMP第二阶段协商其他SA操作，此时交互的ISAKMP报文必须包括发起方和接收方的“甜点”字段，“报文标识符”字段，以及建议报体的“SPI”字段。

SA创建的两阶段交互的说明-2

- 表中第5项操作可以属于ISAKMP第一协商阶段，此时，其报文标识符字段取值为“0”；它也可以属于ISAKMP第二协商阶段，此时，其报文标识符字段必须出现。
- 表中第6项操作是在ISAKMP第二阶段协商完成安全协议SA(例如ESP和AH安全协议SA)之后，进行安全协议(例如ESP和AH)的操作。此时交互的安全协议报文中只需要涉及SPI字段，因为可以通过SPI字段值，查询到已经协商好的SA中所有信息。

甜点字段

- “甜点”字段主要是为了防范“拒绝服务”攻击。ISAKMP协议虽然没有规定具体的“甜点”生成算法，但是，对于对这类算法提出了以下的基本要求：
  - （1）“甜点”必须由某个具体的安全关联的参与方才能生成，无法通过参与方的IP地址或者UPD端口号产生。
  - （2）“甜点”不能由其他实体生成后传递“甜点”发行方，即“甜点”必须由“甜点”发行方利用本地的保密信息生成，并且可以验证该“甜点”的真实性。
  - （3）“甜点”生成算法应该足够快，以便阻止试图消耗ISAKMP服务器或主机资源的“拒绝服务”攻击。

ISAKMP交换类型

- 无论是第一阶段协商，还是第二阶段协商，都采用ISAKMP定义的交换机制，或者采用密钥交换协议定义的交换机制。
- 目前ISAKMP定义了5种缺省的交换类型：基本型、标识保护型、真实性验证型、自信型、以及消息型交换，用于建立和修改安全关联。
- 不同ISAKMP交换类型之间的主要区别是交换报文的次序，以及在单个报文中报体的次序。

基本型交换

- 基本型交换允许同时传递密钥交换信息和真实性验证信息，这样，可以减少报文的交换次数，但是，却无法保护身份标识。基本型交换过程如下：

M1: A → B: HDR, SA, NONCE

M2: B → A: HDR, SA, NONCE

M3: A → B: HDR, KE, ID_{A1}, $AUTH_A$

M4: B → A: HDR, KE, ID_{B1}, $AUTH_B$

标识保护型交换

- 该类型交换将密钥信息的交换与标识信息和真实性验证数据的交换相分离，利用已经协商好的密钥加密标识信息，防范标识信息的泄露。

M1: A → B: HDR, SA

M2: B → A: HDR, SA

M3: A → B: HDR, KE, NONCE

M4: B → A: HDR, KE, NONCE

M5: A → B: HDR*, ID_{A1}, $AUTH_A$

M6: B → A: HDR*, ID_{B1}, $AUTH_B$

真实性验证型交换

- 该类型交换只交换真实性验证数据，对报文进行真实性验证。这样，可以减少计算密钥的开销。采用该交换类型，传输的报文都不进行加密。

M1: A → B: HDR, SA, NONCE

M2: B → A: HDR, SA, NONCE, ID_{B1}, $AUTH_B$

M3: A → B: HDR, ID_{A1}, $AUTH_A$

自信型交换

- 该交换对网络安全环境比较自信，在同一个报文中一次传递安全关联、密钥交换和真实性验证相关的报体。这样，可以减少报文的交换次数，提高交换的效率。但是，这类交换无法保护标识。

M1: A → B: HDR, SA, KE, NONCE, ID_{A1}

M2: B → A: HDR, SA, KE, NONCE, ID_{B1}, $AUTH_B$

M3: A → B: HDR*, $AUTH_A$

消息型交换

- 该类型交换是一种用于安全关联管理的单向消息传递。它可以用于传递通告报体(N)和安全关联删除报体(D)。

M1: A → B: HDR*, N/D

ISAKMP说明

- ISAKMP协议中定义的交换类型实际上并没有构成一个完整的协议，为了真正建立和修改安全关联，还需要定义较为完整的真实性验证和密钥交换协议。
- 互联网密钥交换(IKE)协议就是一种较为完整的安全关联建立和密钥协商协议。
- IKE协议还是采用了ISAKMP定义的ISAKMP报头和报体格式，以及ISAKMP两阶段协商框架结构。

互联网密钥交换协议

- 互联网密钥交换(英文缩写IKE)协议是一种可实现的密钥管理协议，它在保护模式下协商和提供安全关联所需要的经过真实性验证的密钥资料。
- IKE定义的交互模式可以应用于ISAKMP定义的第一阶段和第二阶段的协商，但是这些交互模式只能应用于ISAKMP定义的两种交互阶段中的一个阶段。

IKE交互模式

- IKE定义的“主模式”和“自信模式”用于完成第一阶段ISAKMP安全关联的交互，并且只能用于第一阶段交互。
- 第二阶段是完成某类安全服务协商，例如IPsec安全服务，进行的交互，目的是建立某类安全协议要求的安全关联。第二阶段交互需要协商密钥资料和参数。IKE定义的“快速模式”可以完成第二阶段的交互，并且只能应用于第二阶段的交互。

IKE交互模式(续1)

- IKE定义了应用于第一阶段的两种基本的真实性验证密钥交换模式：主模式和自信模式。
- 这两种模式都是从短期的Diffie-Hellman交换中生成经过真实性验证的密钥资料。主模式是必须实现的，而自信模式是应该实现的。
- 主模式是ISAKMP标识保护型交换的一种实例。自信模式是ISAKMP自信型交换的一种实例。

IKE交换模式(续2)

- IKE定义了应用于第二阶段的密钥交换模式：快速模式。
- 快速模式也是必须实现的一种机制，用于生成最新的密钥资料、协商非ISAKMP的安全服务。
- 快速模式在ISAKMP中没有对应的交换类型，它们是IKE中定义的密钥交换的操作模式。

IKE交换模式(续3)

- IKE定义的“新组模式”既不属于第一阶段，也不属于第二阶段。它是在第一阶段之后建立一个用于未来协商的新组。所以，它属于ISAKMP第一阶段协商之后。
- 加密算法、哈希算法、真实性验证算法、Diffie-Hellman密钥生成数据都是IKE使用的算法和参数，它们是在ISAKMP安全关联中协商的。
- 这些算法和参数仅应用于ISAKMP安全关联中，不一定适用于ISAKMP为其他密钥协商协议建立的安全关联。

IKE的交换协议

- IKE在交换模式的基础上具体定义了基于真实性验证的密钥交换协议。
- 利用主模式和自信模式，IKE可以采用4种不同的真实性验证方法：数字签名、公钥加密真实性验证、改进的公钥加密真实性验证、以及预共享密钥。
- IKE定义的交换协议完全采用ISAKMP定义的报体格式、参数编码、报文超时和重发、以及消息报文。

IKE协议符号定义

- A表示发起方，B表示响应方。注意在RFC 2409中，I表示发起方，R表示响应方。为了保证全书符号尽量统一，这里采用本书在“真实性验证协议”章节中的标记符号。
- HDR表示ISAKMP报头，HDR*表示ISAKMP报头后面的报体被加密。
- SA表示ISAKMP定义的SA报体，SA报体可以带有一个或者多个建议报体。发起方可以提供多个建议报体，而响应方只回复一个被选中的建议报体。在IKE具体交互中，为了简化交互报文的描述，没有明确表示“建议”报体。

IKE协议符号定义(续1)

- <P>表示报体P中内容。例如<SA>表示SA报体的内容。
- CKY_A和CKY_B分别表示在ISAKMP报头中的发起方和响应方“甜点”。
- G^{XA}和G^{XB}分别表示发起方和响应方的Diffie-Hellman的公共值。
- G^{XY}表示Diffie-Hellman算法生成的共享密钥。
- KE表示密钥交换报体，其中包含了Diffie-Hellman交换中需要的公共信息。
- N_A和N_B分别表示ISAKMP发起方和响应方的一次性数报体。

IKE协议符号定义(续2)

- ID_{A1}和ID_{B1}分别表示ISAKMP第一阶段协商过程中ISAKMP安全关联的发起方和响应方的标识报体。
- ID_{A2}和ID_{B2}分别表示第二阶段协商过程中，用户或者应用安全关联的发起方和响应方的标识报体。
- SIG表示数字签名报体。
- CERT表示证书报体。
- HASH表示哈希报体，$HASH_A$和$HASH_B$分别表示发起方和响应方的哈希报体。
- PRF(K, M)是基于密钥K对报文M生成的伪随机函数，通常是基于密钥的哈希函数，用于产生确定性的伪随机输出。该函数可以用于生成密钥和真实性验证。

IKE协议符号定义(续3)

- SKEYID表示从只有参与方知道的保密资料中导出的字符串。
- $SKEYID_E$表示ISAKMP安全关联用于保护报文保密性的密钥资料。
- $SKEYID_A$表示ISAKMP安全关联用于报文真实性验证的密钥资料。
- $SKEYID_D$表示用于导出非ISAKMP安全关联密钥的密钥资料。

IKE交换1：数字签名真实性验证的第一阶段协商

- 原理：该交换协议通过签名双方都可以获得的哈希值进行真实性验证。采用数字签名真实性验证的主模式交换过程如下：

M1: A → B: HDR, SA

M2: B → A: HDR, SA

M3: A → B: HDR, KE, N_A

M4: B → A: HDR, KE, N_B

M5: A → B: HDR*, ID_{A1}, [CERT,] SIG_A

M6: B → A: HDR*, ID_{B1}, [CERT,] SIG_B

IKE交换1(续1)

- M1中的SA包括了多个“建议报体”，而M2中的SA只包括一个B选择的“建议报体”。
- M3和M4中的KE报体包括了Diffie-Hellman密钥生成算法的公共值G^{XA}和G^{XB}，利用这些公共值以及HDR报头中的CKY字段、SA和ID报体值，A和B可以分别计算哈希值$HASH_A$和$HASH_B$，通过签名得到SIG_A和SIG_B。
- 报文M5和M6的报体，即ID、CERT和SIG报体，都是被加密的密文。这两个报文中的CERT报体是可选项，可以选择传递证书报体。

IKE交换1(续2)

- 采用数字签名真实性验证的自信模式交换过程如下：

M1: A → B: HDR, SA, KE, N_A, ID_A

M2: B → A: HDR, SA, KE, N_B, ID_B, [CERT,] SIG_B

M3: A → B: HDR, [CERT,] SIG_A

- 自信模式交换的报体与主模式完全相同，只是每个报文携带的报体组合不同。但是，报体的含义以及在真实性验证中的作用相同。

IKE交换2：公钥加密真实性验证的第一阶段协商

- 原理：双方利用各自私钥加密对方加密的一次性数和标识，构造自己的哈希报体(数字签名)发送给对方，证明自己的身份；验证方通过重构对方的哈希报体验证对方的身份。主模式的交换过程如下：

M1: A → B: HDR, SA

M2: B → A: HDR, SA

IKE交换2(续1)

M3: A → B: HDR, KE, [HASH(1),] $PK_B\{<ID_{A1}>\}$, $PK_B\{<N_A>\}$

M4: B → A: HDR, KE, $PK_A\{<ID_{B1}>\}$, $PK_A\{<N_B>\}$

M5: A → B: HDR*, $HASH_A$

M6: B → A: HDR*, $HASH_B$

- 这里M5和M6中的哈希值：

$HASH_A = PRF(SKEYID, G^{XA} || G^{XB} || CKY_A || CKY_B || <SA_A> || <ID_{A1}>)$

IKE交换2(续2)

$HASH_B = PRF(SKEYID, G^{XB} \| G^{XA} \| CKY_B \| CKY_A \| <SA_A> \| <ID_{B1}>)$

公钥加密中的SKEYID采用以下公式生成：

$SKEYID = PRF(H(<N_A> \| <N_B>), CKY_A \| CKY_B)$，

- 这里H表示哈希函数
- 关键在于采用公钥加密传递密钥材料，通过返回的哈希值向对方验证已经获取了密钥材料。由此证明对方持有该公钥对应的私钥。

IKE交换2(续3)

- 采用公钥加密真实性验证的自信模式交互过程：

M1: A → B: HDR, SA, KE, [HASH(1),] $PK_B\{<ID_{A1}>\}$, $PK_B\{<N_A>\}$

M2: B → A: HDR, SA, KE, $PK_A\{<ID_{B1}>\}$, $PK_A\{<N_B>\}$, $HASH_B$

M3: A → B: HDR, $HASH_A$

- 自信模式交换的报体与主模式基本相同，只是自信模式在交换哈希值时没有进行加密。

IKE交换4：预共享密钥真实性验证的第一阶段协商

- 原理：A和B可以利用双方已经具有的共享密钥生成的保密字和哈希报体进行真实性验证。采用预共享密钥真实性验证的主模式交换过程如下：

M1: A → B: HDR, SA

M2: B → A: HDR, SA

M3: A → B: HDR, KE, N_A

M4: B → A: HDR, KE, N_B

M5: A → B: HDR*, ID_{A1}, $HASH_A$

M6: B → A: HDR*, ID_{B1}, $HASH_B$

IKE交换4(续1)

- IKE交换4的关键验证数据是双方已经具有的共享密钥：
- 共享密钥$SKEYID = PRF(K_{A,B}, <N_A> \| <N_B>)$，这里$K_{A,B}$表示A和B预先共享的密钥。

$HASH_A = PRF(SKEYID, G^{XA} \| G^{XB} \| CKY_A \| CKY_B \| <SA_A> \| <ID_{A1}>)$

$HASH_B = PRF(SKEYID, G^{XB} \| G^{XA} \| CKY_B \| CKY_A \| <SA_A> \| <ID_{B1}>)$

IKE交换4(续2)

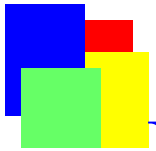
- 采用预共享密钥真实性验证的自信模式交换过程如下：

M1: A → B: HDR, SA, KE, N_A, ID_{A1}

M2: B → A: HDR, SA, KE, N_B, ID_{B1}, $HASH_B$

M3: A → B: HDR, $HASH_A$

- 自信模式中没有对ID报体和HASH报体进行加密，这样，也就无法保护标识。
- 这种模式也只能在交互双方自信比较安全的网络环境下才能使用。



IKE交换5：第二阶段的快速模式

- 快速模式自身不是一个完整的交换过程，它是绑定在第一阶段协商之后的交换过程，作为安全关联的第二阶段协商过程，用于导出密钥资料并且协商针对非ISAKMP安全关联的共享安全策略。
- 在快速模式中交换信息必须被ISAKMP安全关联保护，即除了ISAKMP报头(即HDR)之外所有的报体都必须被加密。

IKE快速模式协商的原理

- 快速模式本质上是一个安全关联的协商过程，也需要传递一次性数报体，用于防范重播报文攻击。在快速模式交换中，也可以携带KE报体，用于为每个快速模式重建一个Diffie-Hellman交换。
- 如果没有在快速模式中指定用户标识符，则快速模式协商的安全关联可以用ISAKMP对等方的IP地址标识。
- 如果指定了用户标识符，则快速模式协商的安全关联采用用户标识符ID_{A2}和ID_{B2}标识。

IKE快速模式的报体和标识

- 快速模式对报文传递的报体顺序有以下要求：HASH报体必须紧跟在ISAKMP报头(即HDR)之后，SA报体必须紧跟在HASH报体之后。
  - 这里HASH报体用于验证报文身份，并且提供该报文是没有过期报文的证明。
- 一个ISAKMP安全关联可能同时有多个快速模式的交换，ISAKMP报头中的报文标识符字段用于标识一个快速模式，快速模式的ISAKMP安全关联由ISAKMP报头中“甜点”字段标识。

IKE快速模式交换的过程

- 快速模式交换过程如下所示：

M1: A → B: HDR*, HASH(1), SA, N_A [, KE] [, ID_{A2}]

M2: B → A: HDR*, HASH(2), SA, N_B [, KE] [, ID_{B2}]

M3: A → B: HDR*, HASH(3)

- 报文M1和M2中的ID_{A2}和ID_{B2}是快速模式协商的安全关联实际对应的发起方用户标识符和响应方用户标识符。

IKE快速模式的报体说明

- HASH(1)是以$SKEYID_A$为密钥，对HDR中报文标识符(M-ID)与所有报体的合并进行哈希计算的值。
- HASH(2)与HASH(1)类似，只是增加了发起方一次性数，用于验证报文M2没有过期。
- HASH(3)也是为了验证报文M3没有过期，其哈希计算的数据由HDR中报文标识符(M-ID)与发起方和响应方的一次性数拼接而成。

IKE快速模式的哈希值计算

- 按照以上快速模式的交换报文，这三个哈希值的计算方法如下：

$HASH(1) = PRF(SKEYID_A, M\text{-}ID \| SA \| N_A [\| KE] [\| ID_{A2} \| ID_{B2}])$

$HASH(2) = PRF(SKEYID_A, M\text{-}ID \| <N_A> \| SA \| N_B [\| KE] [\| ID_{A2} \| ID_{B2}])$

$HASH(3) = PRF(SKEYID_A, M\text{-}ID \| <N_A> \| <N_B>)$

- 以上算式仅仅是针对以上快速模式的交换过程而言，如果交换过程中报体位置发生变化，则以上算式中报体拼接的位置也将发生变化。

IKE快速模式协商多个安全关联

- 快速模式也支持一次交换协商多个安全关联。一个协商两个安全关联的交换过程如下：

M1: A → B: HDR*, HASH(1), SA0, SA1, N_A [, KE] [, ID_{A2}]

M2: B → A: HDR*, HASH(2), SA0, SA1, N_B [, KE] [, ID_{B2}]

M3: A → B: HDR*, HASH(3)

- 这样，通过该快速模式交换，可以建立4个安全关联，SA0和SA1各建立两条相向的安全关联。

IKE交换6：新组模式

- 新组模式交换必须在第一阶段协商之后，当然，新组模式也不属于第二阶段协商。新组模式交换协议只是用于维护某个安全关联，因为从安全角度考虑，某个安全关联组经过一定时间会过期。新组也可以直接在第一阶段中采用主模式协商。新组模式的交换过程如下：

M1: A → B: HDR*, HASH(1), SA

M2: B → A: HDR*, HASH(2), SA

IKE新组模式的哈希值计算

- 这里的HASH(1)和HASH(2)哈希值的计算公式如下：

$$HASH(1) = PRF(SKEYID_A, M\text{-}ID \| SA_A)$$

$$HASH(2) = PRF(SKEYID_A, M\text{-}ID \| SA_B)$$

- 这里SA_A表示发起方A提出的所有建议报体，SA_B表示响应方B选择的一个建议报体。这两个哈希值用于验证报文，防范报文重播攻击。

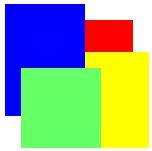
IKE交换7：ISAKMP消息交换

- 该交换协议用于保护ISAKMP的通告或删除消息的交换。如果ISAKMP安全关联已经建立，$SKEYID_A$和$SKEYID_E$已经生成，可以利用以下交换协议安全交换ISAKMP消息：

M1: A → B: HDR*, HASH(1), N/D

- 这里N/D表示或者是ISAKMP的通告(N)报体，或者是删除(D)报体。这里的哈希值HASH(1)计算公式如下：

$HASH(1) = PRF(SKEYID_A, M\text{-}ID \| N/D)$



IKE小结

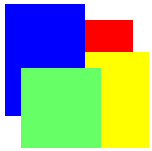
- ISAKMP提供了安全IP的安全关联创建和管理的一个框架性协议。
- 基于ISAKMP框架，IKE提供了安全IP的安全关联创建和管理的一个具体实现的协议。
- IKE提供了七类交换，其中四类交换适用于第一阶段安全关联创建，一类交换适用于第二阶段安全关联创建，二类交换适用于安全关联的管理。

基于IPsec的综合应用题

例题1：假设某个销售人员在外地试图通过公共互联网从公司网络服务器中下载销售资料和文件。请问：

（1）如果该销售人员不采用任何安全技术直接从公司服务器取数据会遇到哪几种安全威胁？

（2）该销售人员考虑采用安全技术，则他至少应该从哪几个方面考虑安全技术？



基于IPsec的综合应用题(续1)

（3）如果他试图保密地传递客户订单，他应该选用何种IPsec中的安全协议？

（4）如果他试图完整地传递客户促销计划，他最好选用哪种IPsec中的安全协议？

（5）如果他选择安全IP技术(IPsec)作为安全防范技术，他如何进行真实性验证？

基于IPsec的综合应用题(续2)

（6）如果公司服务器提供了访问控制机制，需要根据用户标识控制对公司服务器的访问权限，这时他应该选择哪种类型的安全关联建立协议？

（7）假定用户已经获得包括自己私钥和公司服务器公钥的证书，试具体描述这种用于真实性验证和安全关联建立的协议的主要步骤。

基于IPsec的综合应用题(续3)

（1）如果该销售人员不采用任何安全技术直接从公司服务器取数据会遇到哪几种安全威胁？

答：如果不采取安全防范技术，他获取的销售资料可能被窃取，可能被更改，可以被假冒，可能无法访问到公司的服务器。

（2）该销售人员考虑采用安全技术，则他至少应该从哪几个方面考虑安全技术？

答：他至少应该从真实性验证、访问控制和攻击检测三个方面考虑对安全技术的选择。

基于IPsec的综合应用题(续4)

（3）如果他试图保密地传递客户订单，他应该选用何种IPsec中的安全协议？

答：为了保密地传递数据，应用IPsec技术时，必须采用ESP协议。

（4）如果他试图完整地传递客户促销计划，他最好选用哪种IPsec中的安全协议？

答：为了完整地传递数据，应用IPsec技术时，最好采用AH协议。

基于IPsec的综合应用题(续5)

（5）如果他选择安全IP技术(IPsec)作为安全防范技术，他如何进行真实性验证？

答：他为了进行真实性验证，必须首先通过其他安全途径（例如在离开公司之前，直接到公司人力资源部）获得与他相关的用户标识和密钥（可以是公钥也可以是共享密钥）等个人身份数据，然后，在第一次网络连接过程中输入相关个人身份数据。

基于IPsec的综合应用题(续6)

（6）如果公司服务器提供了访问控制机制，需要根据用户标识控制对公司服务器的访问权限，这时他应该选择哪种类型的安全关联建立协议？

答：由于用户标识是系统进行访问控制的依据，所以，在应用IPsec技术创建安全关联时，必须采用具有用户标识保护功能的安全关联创建协议。

基于IPsec的综合应用题(续7)

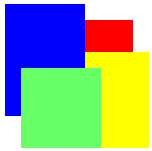
（7）假定用户已经获得包括自己私钥和公司服务器公钥的证书，试具体描述这种用于真实性验证和安全关联建立的协议的主要步骤。

答：运用IKE协议，选用主模式下基于公钥真实性验证的安全关联创建协议如下：

M1: A → B: HDR, SA

M2: B → A: HDR, SA

M3: A → B: HDR, KE, [HASH(1),] $PK_B\{<ID_{A1}>\}$, $PK_B\{<N_A>\}$



基于IPsec的综合应用题(续8)

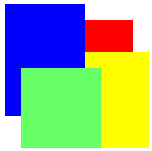
M4: B → A: HDR, KE, $PK_A\{<ID_{B1}>\}$, $PK_A\{<N_B>\}$

M5: A → B: HDR*, $HASH_A$

M6: B → A: HDR*, $HASH_B$

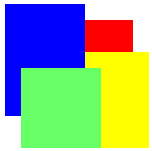
例题分析

- 分析：这是一道综合性应用试题，检验学生全面掌握网络安全知识的水平，以及综合应用网络安全知识的能力。
- 注意：应该从网络安全需求分析，网络安全的技术原理，网络安全技术应用角度分析问题。



重点回顾

- 安全IP基本概念
- 真实性验证报头(AH)协议
- 封装安全报体(ESP)协议
- 互联网安全关联与密钥管理协议
- 互联网密钥交换协议



思考题

(1) 什么是安全IP技术？它由几个部分构成？安全IP协议簇由哪些部分构成？

(2) 什么是安全关联？为什么说安全关联是安全IP的基础？

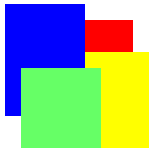
(3) 安全关联具有哪几种操作模式？这几种操作模式分别适用于哪些安全应用环境？

思考题(续1)

(4) 为什么需要组合多个安全关联？安全IP中定义了哪几种安全关联组合模式？这些组合模式分别适用于哪些安全应用环境？

(5) AH安全协议主要提供哪些安全功能？既然ESP也可以提供AH提供的功能，为什么还需要单独设计一个AH安全协议？

(6) AH和ESP安全协议如何防范报文重播攻击？



思考题(续2)

(7) ISAKMP协议是否是只适用于IP层的协议？为什么？这样定义有何优点？有何不足？

(8) ISAKMP协议定义了两阶段安全关联协商的过程，两个安全关联的协商阶段有何不同？这种阶段划分有何好处？

(9) ISAKMP定义了哪几种交换类型？这些交换类型分别适用于哪些安全关联协商过程？

思考题(续3)

(10) IKE协议与ISAKMP协议有何不同？IKE协议究竟提供了什么功能？

(11) IKE定义了哪两种基本的应用于安全关联协商第一阶段的密钥交换模式？这两种密钥交换模式有何不同？如何选择这两种密钥交换模式？

(12) 什么是密钥交换的“快速模式”？它只能适用于哪个阶段的安全关联协商？