网络安全

谢剑刚
广东开放大学

7.1.1 安全威胁

- **计算机网络上的通信面临以下四种威胁：**

01 OPTION 截获 从网络上窃听他人的通信内容。

02 OPTION 中断 有意中断他人在网络上的通信。

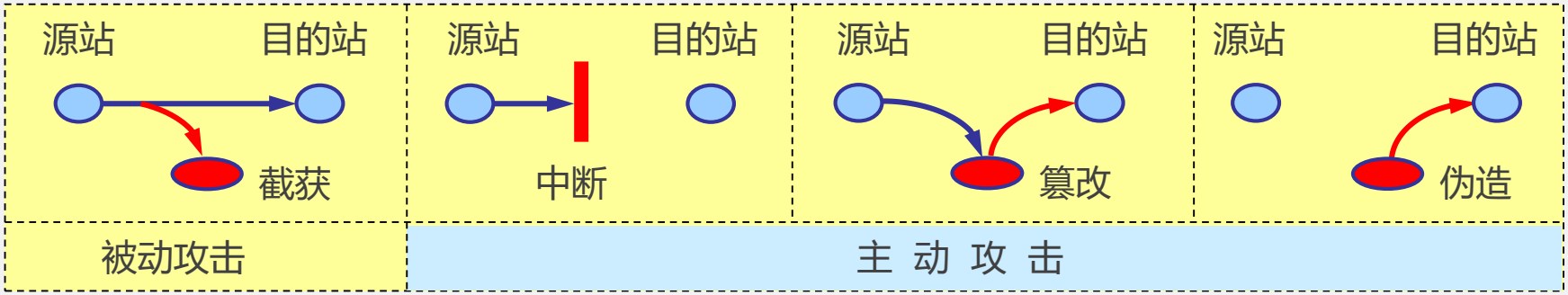
03 OPTION 篡改 故意篡改网络上传送的报文。

04 OPTION 伪造 伪造信息在网络上传送。

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

对网络的被动攻击和主动攻击

- 攻击者只是观察和分析网络中传输的数据流而不干扰数据流本身。
- 主动攻击是指攻击者对传输中的数据流进行各种处理。
  - 更改报文流
  - 拒绝服务攻击
  - 恶意程序攻击



恶意程序(rogue program)

01 OPTION 计算机病毒　会“传染”其他程序的程序，“传染”是通过修改其他程序来把自身或其变种复制进去完成的。

02 OPTION 计算机蠕虫　通过网络的通信功能将自身从一个结点发送到另一个结点并启动运行的程序。

03 OPTION 特洛伊木马　一种程序，它执行的功能超出所声称的功能。

04 OPTION 逻辑炸弹　一种当运行环境满足某种特定条件时执行其他特殊功能的程序。

7.1.2 安全服务

机密性(confidentiality)

确保计算机系统中的信息或网络中传输的信息不会泄漏给非授权用户。这是计算机网络中最基本的安全服务。

报文完整性(message intergrity)

确保计算机系统中的信息或网络中传输的信息不被非授权用户篡改或伪造。后者要求对报文源进行鉴别 。

不可否认性(nonrepudiation)

防止发送方或接收方否认传输或接收过某信息。在电子商务中这是一种非常重要安全服务。

实体鉴别(entity authentication)

通信实体能够验证正在通信的对端实体的真实身份，确保不会与冒充者进行通信。

访问控制(access control)

系统具有限制和控制不同实体对信息源或其他系统资源进行访问的能力。系统必须在鉴别实体身份的基础上对实体的访问权限进行控制。

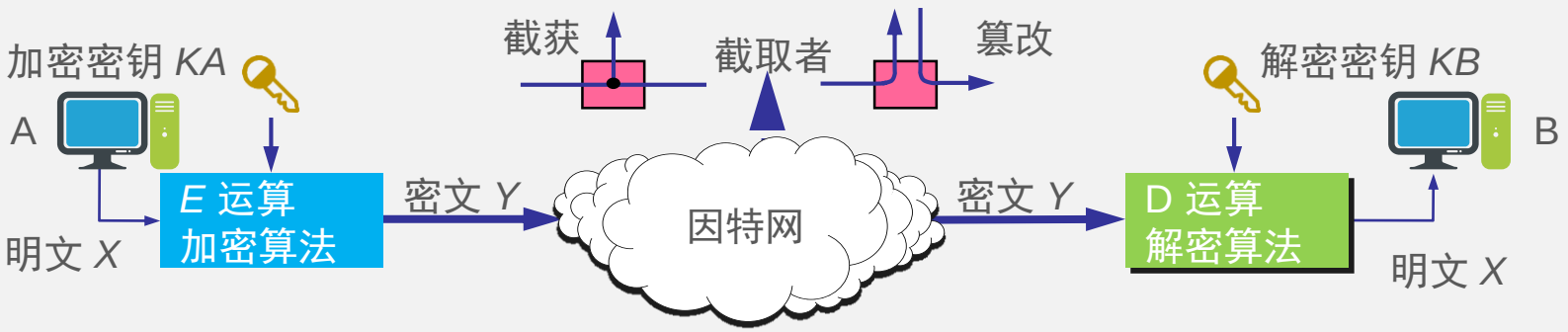
可用性(availability)

确保授权用户能够正常访问系统信息或资源。拒绝服务攻击是可用性的最直接的威胁。

7.2 机密性与密码学

机密性应该是密码学最早的应用领域，但我们在后面几节将会看到密码学技术和鉴别、报文完整性以及不可否认性等是紧密相关的，可以说**密码学是计算机网络安全的基础**。

数据加密的一般模型



$$Y = E_{KA}(X)$$
$$D_{KB}(Y) = D_{KB}(E_{KA}(X)) = X$$

一些重要概念

- 如果不论截取者获得了多少密文，但在密文中都没有足够的信息来唯一地确定出对应的明文，则这一密码体制称为无条件安全的，或称为理论上是不可破的。
- 如果密码体制中的密码不能被可使用的计算资源破译，则这一密码体制称为在计算上是安全的。
- 我们关心的是在计算上（而不是在理论上）是不可破的密码体制。

7.2.1 对称密钥密码体制

- 所谓对称密钥密码体制是一种加密密钥与解密密钥相同的密码体制。
- 在这种加密系统中两个参与者共享同一个秘密密钥，如果用一个特定的密钥加密一条消息，也必须要使用相同的密钥来解密该消息。
- 该系统又称为对称密钥系统。

数据加密标准 DES

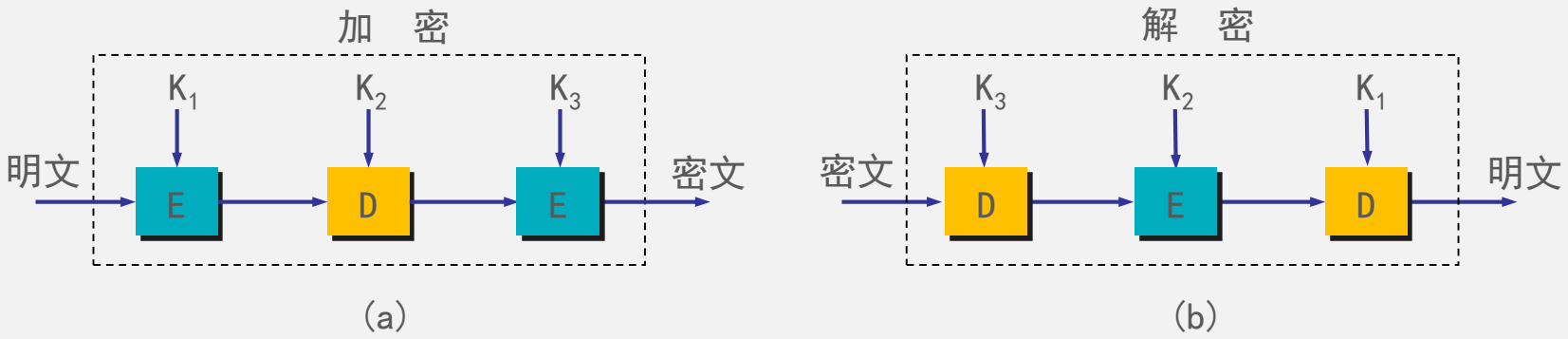
- 数据加密标准 DES 属于常规密钥密码体制，是一种分组密码。
- 数据加密标准DES (Data Encryption Standard)是对称密钥密码的典型代表，由IBM公司研制，于1977年被美国定为联邦信息标准后，在国际上引起了极大的重视。ISO曾把DES作为数据加密标准。
- DES使用的密钥为64位（实际密钥长度为56位，有8位用于奇偶校验）。

DES 的保密性

- DES 的保密性仅取决于对密钥的保密，而算法是公开的。尽管人们在破译 DES 方面取得了许多进展，但至今仍未能找到比穷举搜索密钥更有效的方法。
- DES 是世界上第一个公认的实用密码算法标准，它曾对密码学的发展做出了重大贡献。
- 目前较为严重的问题是 DES 的密钥的长度。
- 现在已经设计出来搜索 DES 密钥的专用芯片。

三重DES

为解决DES密钥太短的问题，人们提出了三重DES。



7.2.2 公钥密码体制

- 公钥密码体制使用不同的加密密钥与解密密钥，是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。
- 公钥密码体制的产生主要是因为两个方面的原因，一是由于常规密钥密码体制的密钥分配问题，另一是由于对数字签名的需求。
- 现有最著名的公钥密码体制是RSA 体制，它基于数论中大数分解问题的体制，由美国三位科学家 Rivest, Shamir 和 Adleman 于 1976 年提出并在 1978 年正式发表的。

加密密钥与解密密钥

- 在公钥密码体制中，加密密钥(即公钥) PK 是公开信息，而解密密钥(即私钥或秘钥) SK 是需要保密的。
- 加密算法 E 和解密算法 D 也都是公开的。
- 虽然秘钥 SK 是由公钥 PK 决定的，但却不能根据 PK 计算出 SK。

公钥算法的特点

发送方用加密密钥 *PK* 对明文 *X* 加密（*E* 运算）后，在接收方用解密密钥 *SK* 解密（*D* 运算），即可恢复出明文：

$$D_{SK}(Y) = D_{SK}(E_{PK}(X)) = X \tag{7-3}$$

解密密钥是接收者专用的秘钥（**私钥**），对其他人都保密。

加密密钥是公开（**公钥**）的，但不能用它来解密，即

$$D_{PK_B}(E_{PK_B}(X)) \neq X \tag{7-4}$$

公钥算法的特点（续）

- 加密和解密的运算可以对调，即

$$E_{PK}(D_{SK}(X)) = D_{SK}(E_{PK}(X)) = X \quad (7\text{-}5)$$

- 在计算机上可容易地产生成对的 *PK* 和 *SK*。
- 从已知的 *PK* 实际上不可能推导出 *SK*，即从 *PK* 到 *SK* 是“计算上不可能的”。
- 加密和解密算法都是公开的。

应当注意

任何加密方法的安全性取决于密钥的长度，以及攻破密文所需的计算量。在这方面，公钥密码体制并不具有比传统加密体制更加优越之处。

公钥密码体制有许多很好的特性，但公钥密码算法比对称密码算法要慢好几个数量级。因此，对称密码被用于绝大部分加密，而公钥密码则通常用于会话密钥的建立。

7.3 完整性与鉴别

01 OPTION
有时，通信双方并不关心通信的内容是否会被人窃听，而只关心通信的内容是否被人篡改或伪造，这就是报文完整性问题。

02 OPTION
报文完整性又称为报文鉴别，既鉴别报文的真伪。

03 OPTION
例如，路由器之间交换的路由信息不一定要求保密，但要求能检测出被篡改或伪造的路由信息。

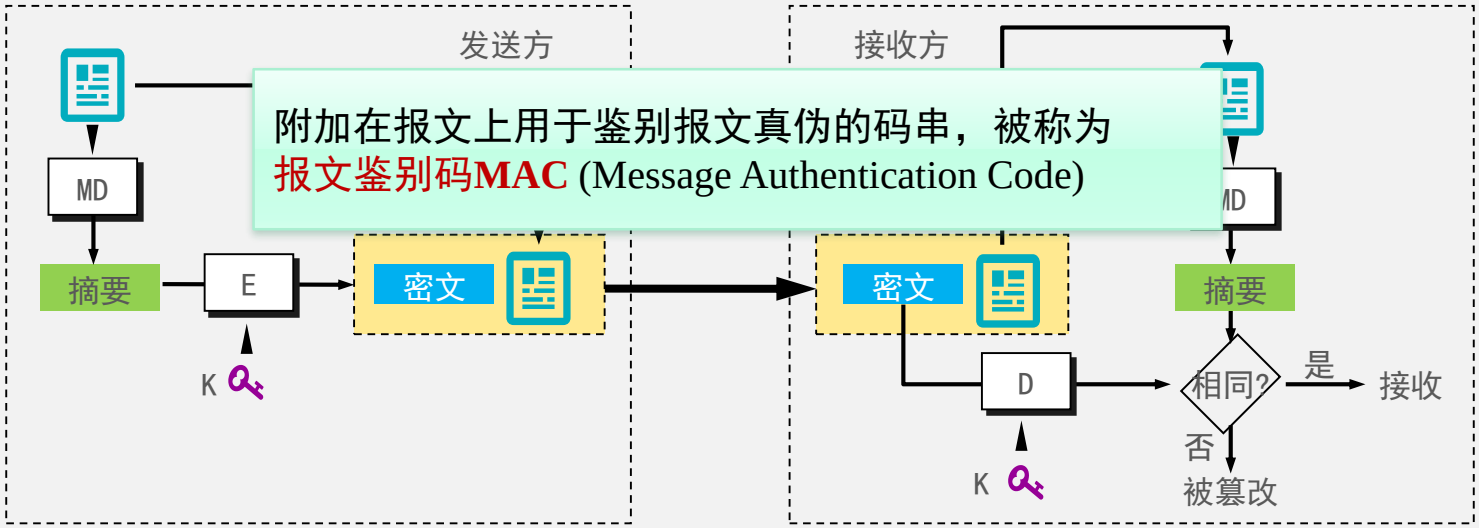
04 OPTION
实体鉴别就是一方验证另一方身份的技术。

7.3.1报文摘要和报文鉴别码

- 使用加密就可达到报文鉴别的目的。但对于不需要保密，而只需要报文鉴别的网络应用，对整个报文的加密和解密，会使计算机增加很多不必要的负担。
- 更有效的方法是使用报文摘要MD (Message Digest)来进行报文鉴别

用报文摘要进行报文鉴别

- 发送方将可变长度的报文m经过报文摘要算法运算后得出固定长度的报文摘要H(m)。
- 然后对H(m)进行加密，得出EK(H(m))，并将其附加在报文m后面发送出去。
- 接收方把EK(H(m))解密还原为H(m)，再把收到的报文进行报文摘要运算，看结果是否与收到的H(m)一样。



密码散列函数

报文摘要和差错检验码都是多对一(many-to-one)的散列函数(hash function)的例子。但要抵御攻击者的恶意篡改，报文摘要算法必须满足以下两个条件：

- 任给一个报文摘要值x，若想找到一个报文y使得H(y) = x，则在计算上是不可行的。
- 若想找到任意两个报文x和y，使得H(x) = H(y)，则在计算上是不可行的。

满足以上条件的散列函数称为**密码散列函数**

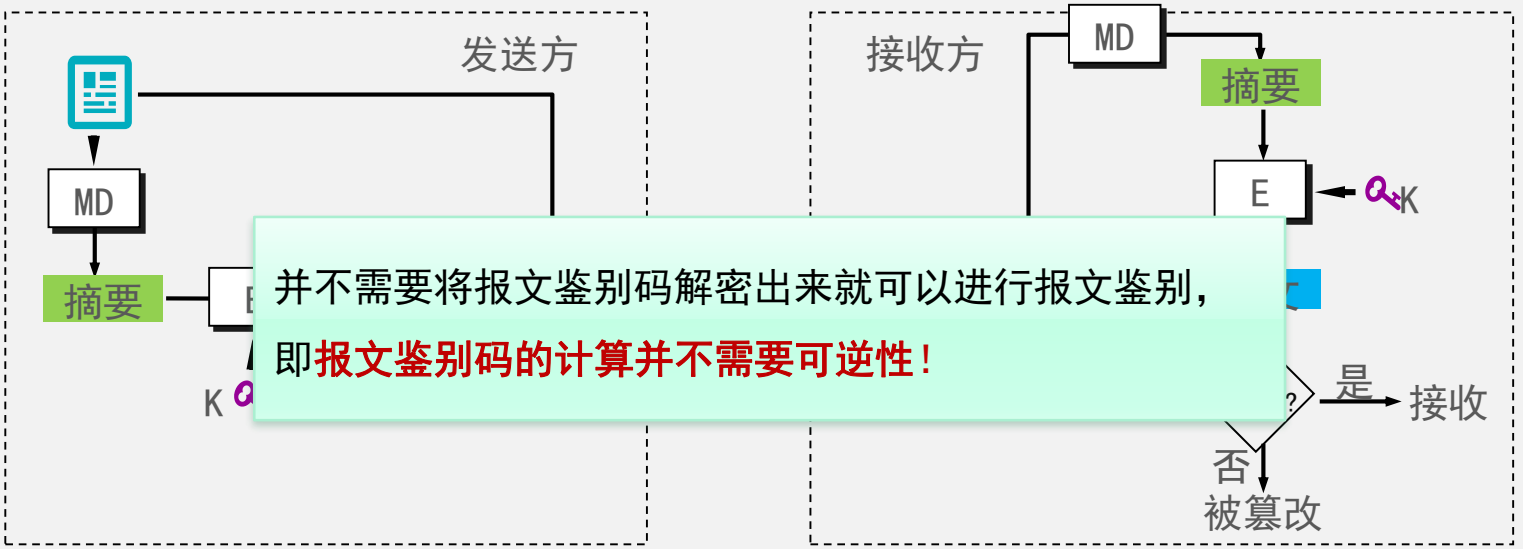
密码散列函数

- 差错检验码通常并不满足以上条件。
- 例如，很容易找到两个不同的字符串：“IOU100.99BOB”和“IOU900.19BOB”的校验和是完全一样的。
- 虽然差错检验码可以检测出报文的随机改变，但却无法抵御攻击者的恶意篡改，因为攻击者可以很容易地找到差错检验码与原文相同的其他报文，从而达到攻击目的。

广泛应用的报文摘要算法

- 目前广泛应用的报文摘要算法有MD5 [RFC 1321]和安全散列算法1(Secure Hash Algorithm, SHA-1)。
- MD5输出128位的摘要，SHA-1输出160位的摘要。
- SHA-1比MD5更安全些，但计算起来比MD5要慢。

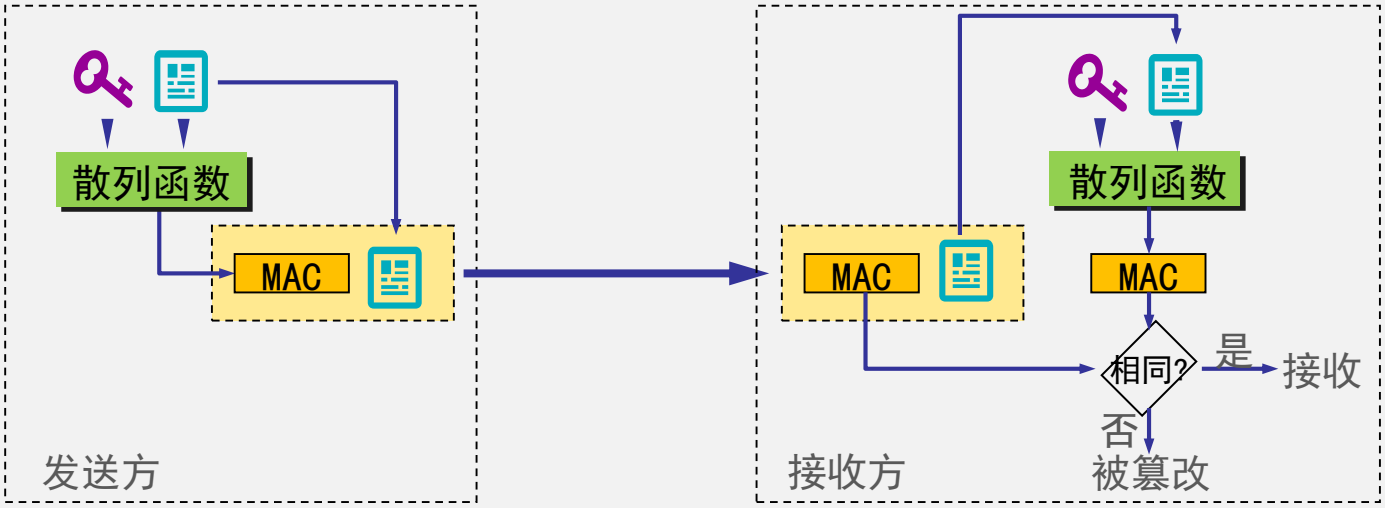
进行报文鉴别并不需要解密



散列报文鉴别码

- 利用密码散列函数无需对报文摘要加密就可以实现对报文的鉴别，前提是双方共享一个称为鉴别密钥的秘密比特串s。
- 发送方计算散列H(m+s)。H(m+s)被称为散列报文鉴别码HMAC (Hashed MAC)。
- 将MAC与报文m一起发送给接收方。接收方利用收到的s和m重新计算MAC，与接收到的MAC进行比较，从而实现鉴别。

散列报文鉴别码HMAC



7.3.2 数字签名

数字签名必须保证以下三点：

(1) 接收方能够核实发送方对报文的数字签名。

(2) 发送方事后不能抵赖对报文的数字签名。

(3) 任何人包括接收方都不能伪造对报文的签名。

现在已有多种实现各种数字签名的方法。但采用公钥算法更容易实现。

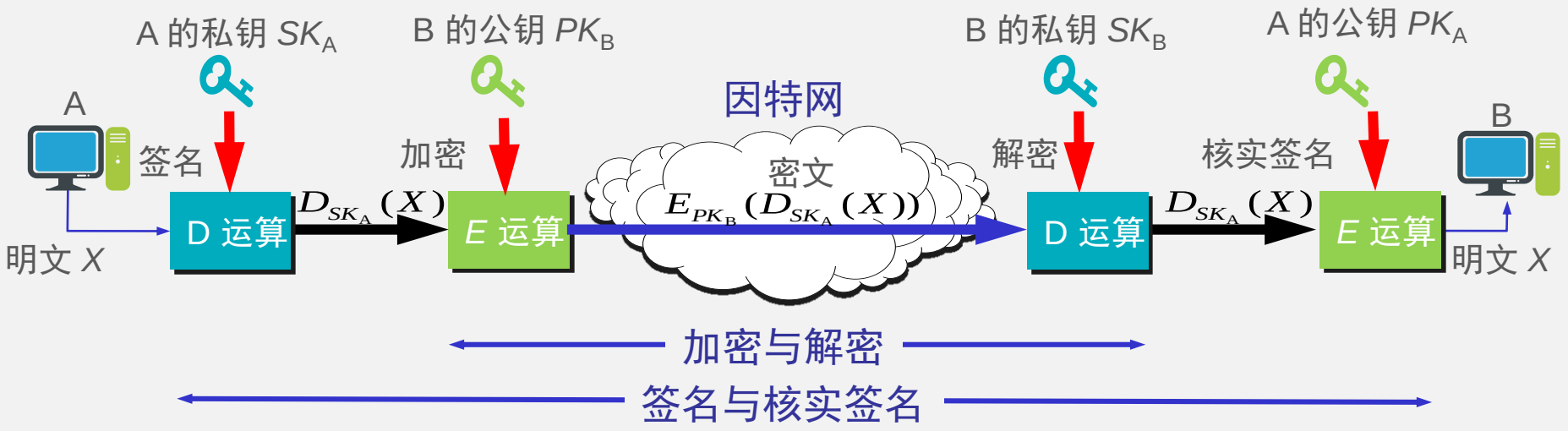
数字签名的实现

- 因为除 A 外没有别人能具有 A 的私钥，所以除 A 外没有别人能产生这个密文。因此 B 相信报文 X 是 A 签名发送的。
- 若 A 要抵赖曾发送报文给 B，B 可将明文和对应的密文出示给第三者。第三者很容易用 A 的公钥去证实 A 确实发送 X 给 B。
- 反之，若 B 将 X 伪造成 X‘，则 B 不能在第三者前出示对应的密文。这样就证明了 B 伪造了报文。

数字签名的实现

公钥密码算法的计算代价非常大，对整个报文进行数字签名是一件非常耗时的事情。更有效的方法是仅对报文摘要进行数字签名。

具有保密性的数字签名



7.3.3 实体鉴别

- **实体鉴别就是鉴别通信对端实体的身份，即验证正在通信的对方确实是所认为的通信实体，这需要使用鉴别协议。**
- **鉴别协议通常在两个通信实体运行其他协议（例如，可靠数据传输协议、路由选择协议或电子邮件协议）之前运行。**

具有保密性的数字签名

- A 发送给 B 的报文的被加密，使用的是对称密钥 K_{AB}。
- B 收到此报文后，用共享对称密钥 K_{AB} 进行解密，因而鉴别了实体 A 的身份。

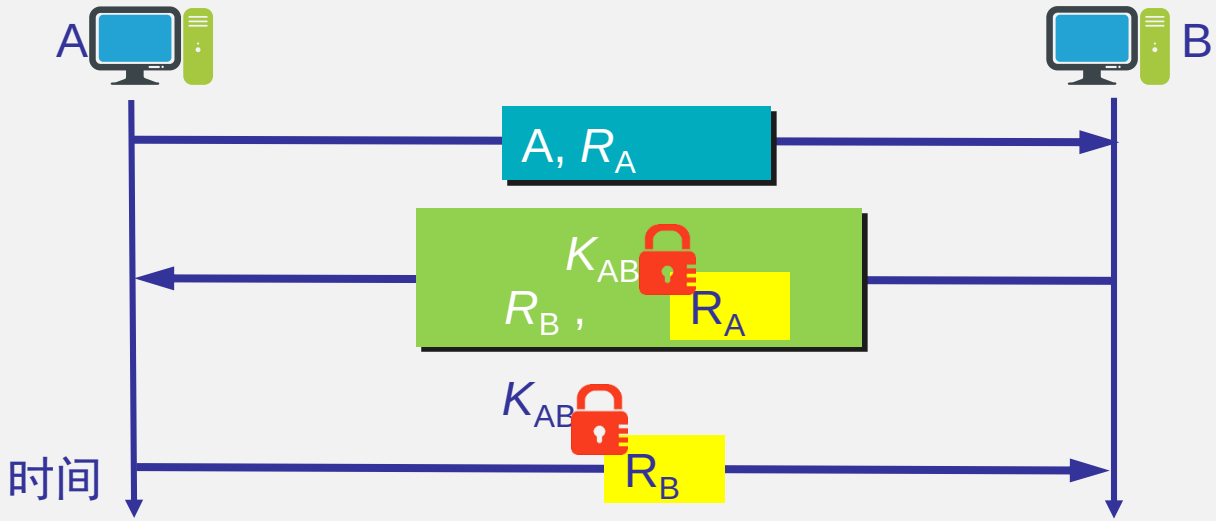
明显的漏洞

- 入侵者 C 可以从网络上截获 A 发给 B 的报文。C 并不需要破译这个报文（因为这可能很花很多时间）而可以直接把这个由 A 加密的报文发送给 B，使 B 误认为 C 就是 A。然后 B 就向伪装是 A 的 C 发送应发给 A 的报文。
- 这就叫做重放攻击(replay attack)。C 甚至还可以截获 A 的 IP 地址，然后把 A 的 IP 地址冒充为自己的 IP 地址（这叫做 IP 欺骗），使 B 更加容易受骗。

使用不重数

为了对付重放攻击，可以使用**不重数**(nonce)。不重数就是一个不重复使用的大随机数，即“**一次一数**”。

使用不重数进行鉴别



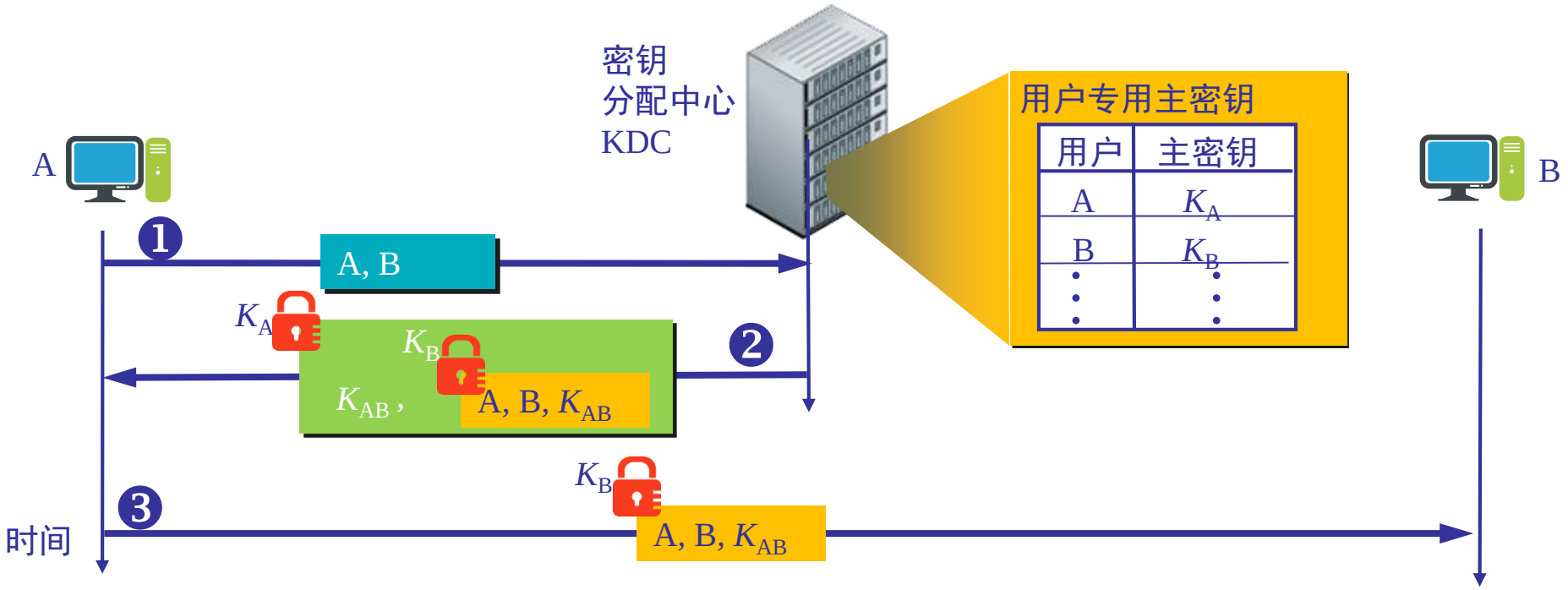
7.4 密钥分发和公钥认证

- 由于密码算法是公开的，密钥系统的安全性依赖于密钥的安全保护。在对称密钥密码体制中，通信双方要共享同一个秘密的密钥，如何将密钥分发到通信的双方是一个需要解决的问题。
- 对于公钥密码体制，虽然不需要共享密钥，公钥可以发布在报纸或网站上，但如何验证该公钥确实是某实体真正的公钥仍然是一个问题。
- 这些问题的解决都可以通过使用一个可信的中介机构得到解决。

7.4.1 对称密钥的分发

- 由于密码算法是公开的，密钥系统的安全性依赖于密钥的安全保护。在对称密钥密码体制中，通信双方要共享同一个秘密的密钥，如何将密钥分发到通信的双方是一个需要解决的问题。
- 对于公钥密码体制，虽然不需要共享密钥，公钥可以发布在报纸或网站上，但如何验证该公钥确实是某实体真正的公钥仍然是一个问题。
- 这些问题的解决都可以通过使用一个可信的中介机构得到解决。

对称密钥的分配

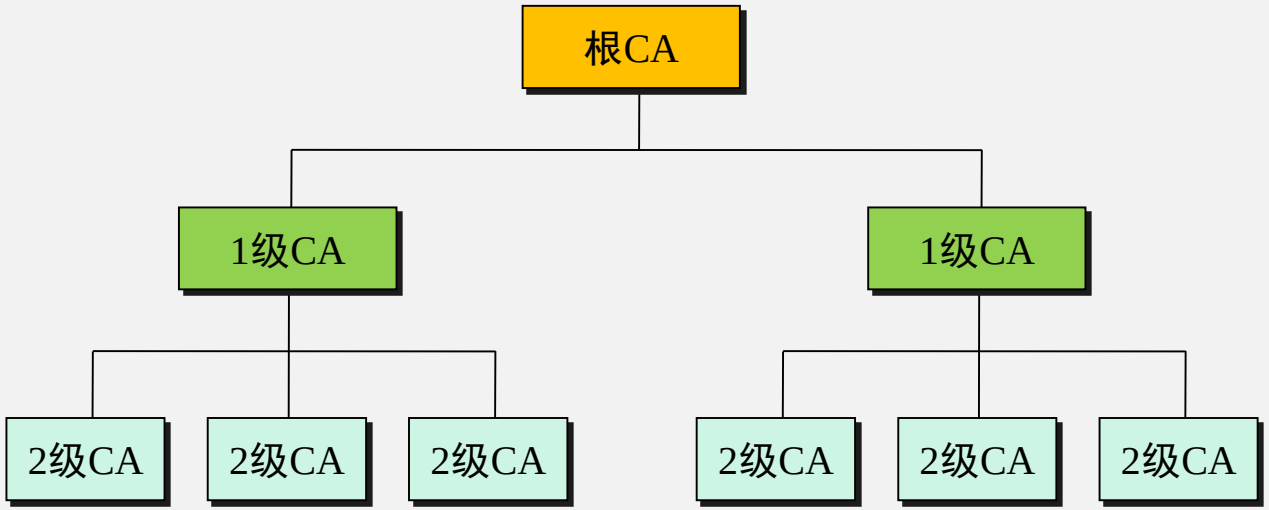

密钥
分配中心
KDC
用户专用主密钥
用户
主密钥
A
K_A
B
K_B
A
B
1
A, B
K_A
K_B
K_{AB} ,
A, B, K_{AB}
2
K_B
A, B, K_{AB}
3
时间

7.4.2 公钥的签发与认证

- 需要有一个值得信赖的机构——即**认证中心**CA（Certification Authority），来将公钥与其对应的实体（人或机器）进行**绑定**(binding)。
- 认证中心一般由政府出资建立。每个实体都有CA发来的**证书**(certificate)，里面有公钥及其拥有者的标识信息。此证书被 CA 进行了数字签名。任何用户都可从可信的地方获得认证中心 CA 的公钥，此公钥用来验证某个公钥是否为某个实体所拥有。有的大公司也提供认证中心服务。

公钥基础设施PKI (Public Key Infrastructure)

- 下级CA的证书由其上级CA签发和认证，所有用户都信任该层次结构中最顶级的CA，但可以信任也可以不信任中间的CA。



7.5 访问控制

7.5.1 访问控制的基本概念

01 OPTION

实施访问控制的依据是用户的访问权限。用户访问权限的授予一般遵循最小特权原则。

02 OPTION

最小特权原则指的是基于用户完成工作的实际需求为用户赋予权限，用户不会被赋予超出其实际需求的权限。

03 OPTION

最小特权原则可以有效防范用户滥用权限所带来的安全风险。

访问控制的基本要素

01 OPTION

主体(subject)指访问活动的发起者。

02 OPTION

客体(object)指访问活动中被访问的对象。

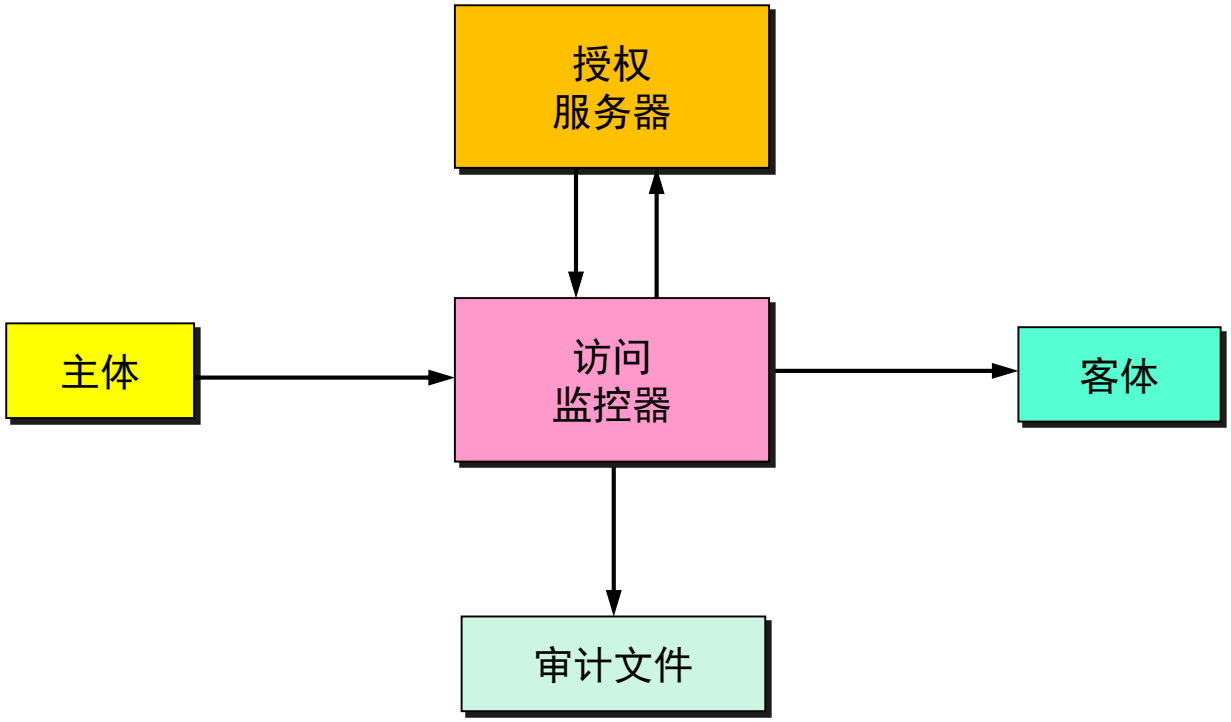
03 OPTION

访问指的是对资源各种类型的使用，例如：读取、修改、创建、删除、执行、发送、接收等操作。

04 OPTION

访问策略体现了系统的授权行为，表现为主体访问客体时需要遵守的约束规则，通常存储在系统的授权服务器中。

访问监控器模型



7.5.2 访问控制策略

- **访问控制策略典型地可分为三类：**

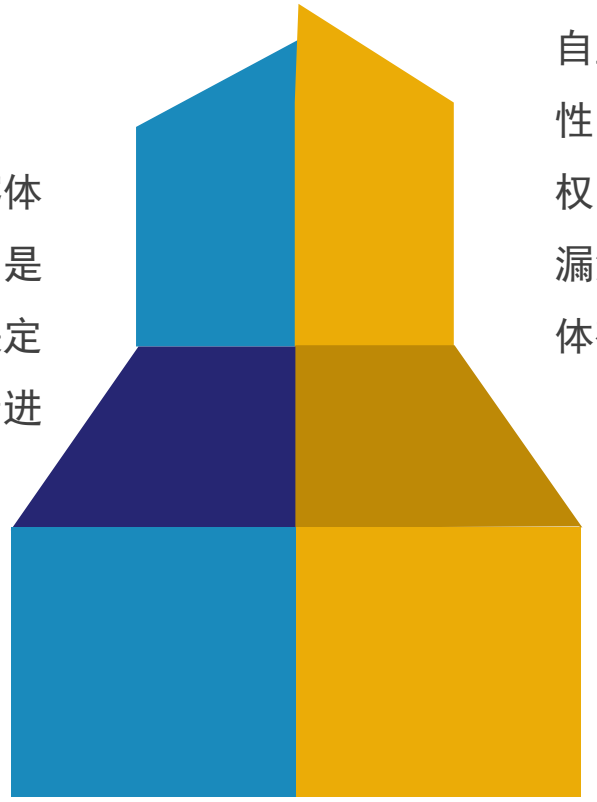
01 OPTION 自主访问控制DAC (Discretionary Access Control)

02 OPTION 强制访问控制MAC (Mandatory Access Control)

03 OPTION 基于角色的访问控制RBAC (Role Based Access Control)

1. 自主访问控制策略

自主访问控制通常基于主客体的隶属关系，“自主”指的是客体的拥有者可以自主地决定其他主体对其拥有的客体所进行访问的权限。



自主访问控制具有很强的灵活性，但是存在一些明显的缺陷：权限管理过于分散，容易出现漏洞；无法有效控制被攻击主体破坏系统安全性的行为。

2. 强制访问控制策略

- **强制访问控制与自主访问控制不同，它不允许一般的主体进行访问权限的设置。**
- **在强制访问控制中，主体和客体被赋予一定的安全级别，普通用户不能改变自身或任何客体的安全级别，通常只有系统的安全管理员可以进行安全级别的设定。**
- **系统通过比较主体和客体的安全级别来决定某个主体是否能够访问某个客体。**

下读和上写是在强制访问控制策略中广泛使用的两项原则：

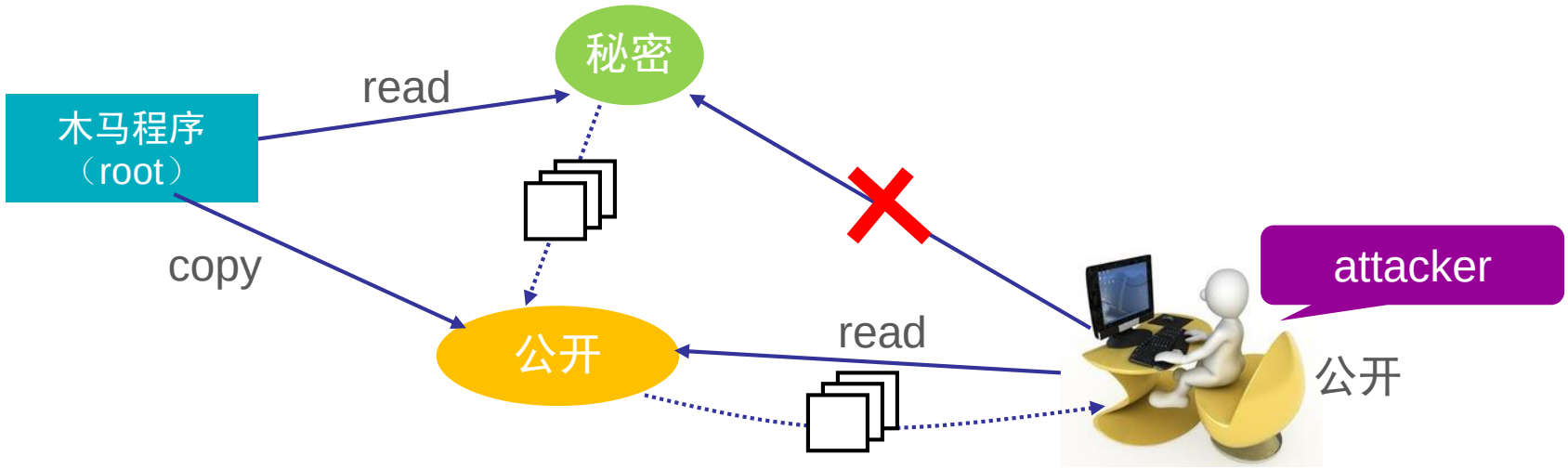
01 OPTION

下读原则：主体的安全级别必须高于或等于被读客体的安全级别，主体读取客体的访问活动才能被允许（向下读）。

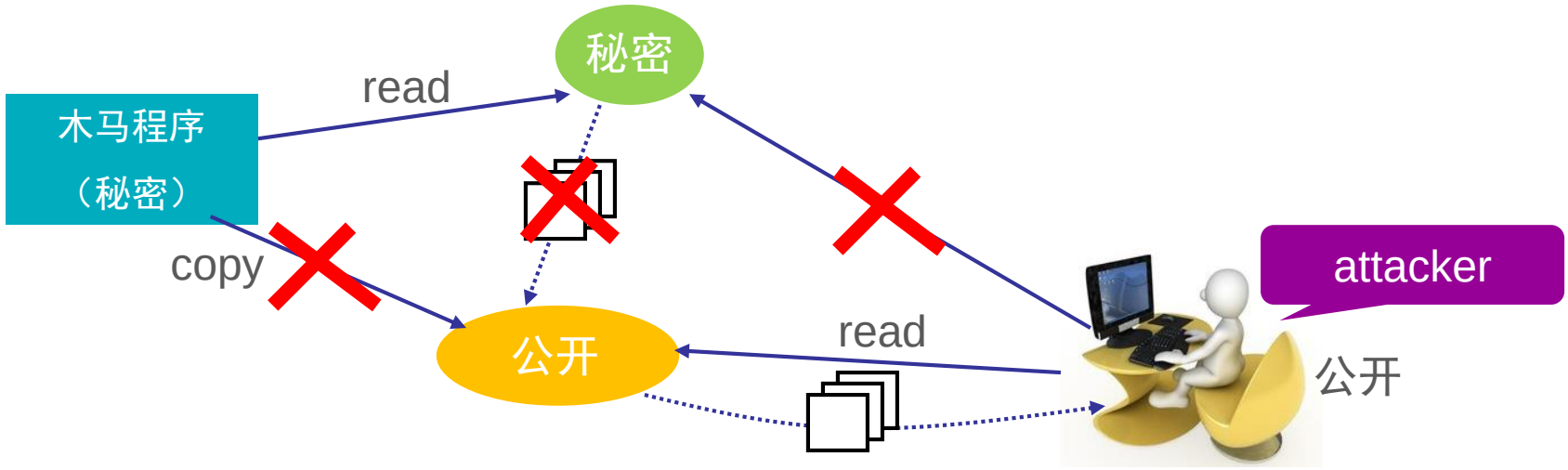
02 OPTION

上写原则：主体的安全级别必须低于或等于被写客体的安全级别，主体写客体的访问活动才能被允许（向上写）。

下读上写原则防止木马窃密攻击



下读上写原则防止木马窃密攻击



3. 基于角色的访问控制策略

01 OPTION

在RBAC中，一个用户可以拥有多个角色，一个角色也可以赋予多个用户。

02 OPTION

一个角色可以拥有多种许可，一种许可也可以分配给多个角色。

03 OPTION

许可指明了对某客体可以进行的访问类型。

7.6 网络各层的安全实例

网络各层都需要安全机制

01 OPTION 物理层：信道加密

02 OPTION 数据链路层：无线局域网链路层加密、接入控制(802.11i)

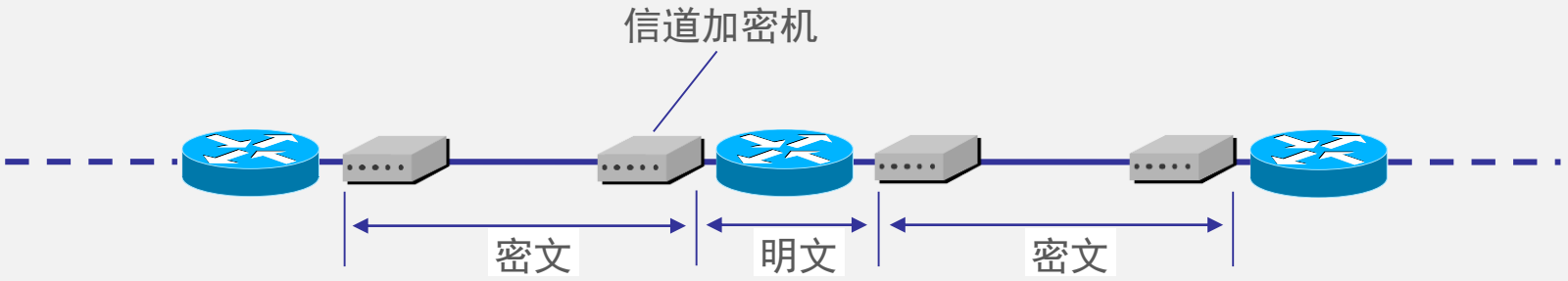
03 OPTION 网络层：主机到主机的数据加密、隧道加密(IPsec)

04 OPTION 运输层：进程间的鉴别、数据加密(SSL/TLS)

05 OPTION 应用层：针对具有网络应用的特定的安全机制(例如：安全电子邮件)

7.6.1 物理层实例：信道加密机

- 使用信道加密技术的一个好处就是对上层协议几乎没有任何影响（即具有很好的透明性），为通过该链路的所有数据提供安全保护。
- 不能保证端到端通信的安全性



7.6.2 数据链路层实例：802.11i

1. 早期无线局域网的安全机制

01 OPTION

SSID匹配　该机制提供了一种无加密的鉴别服务，试图接入无线局域网的终端必须配置与BSS中接入点AP相同的SSID。

02 OPTION

MAC地址过滤　可以为接入点AP设置允许接入或拒绝接入无线局域网的MAC地址列表。

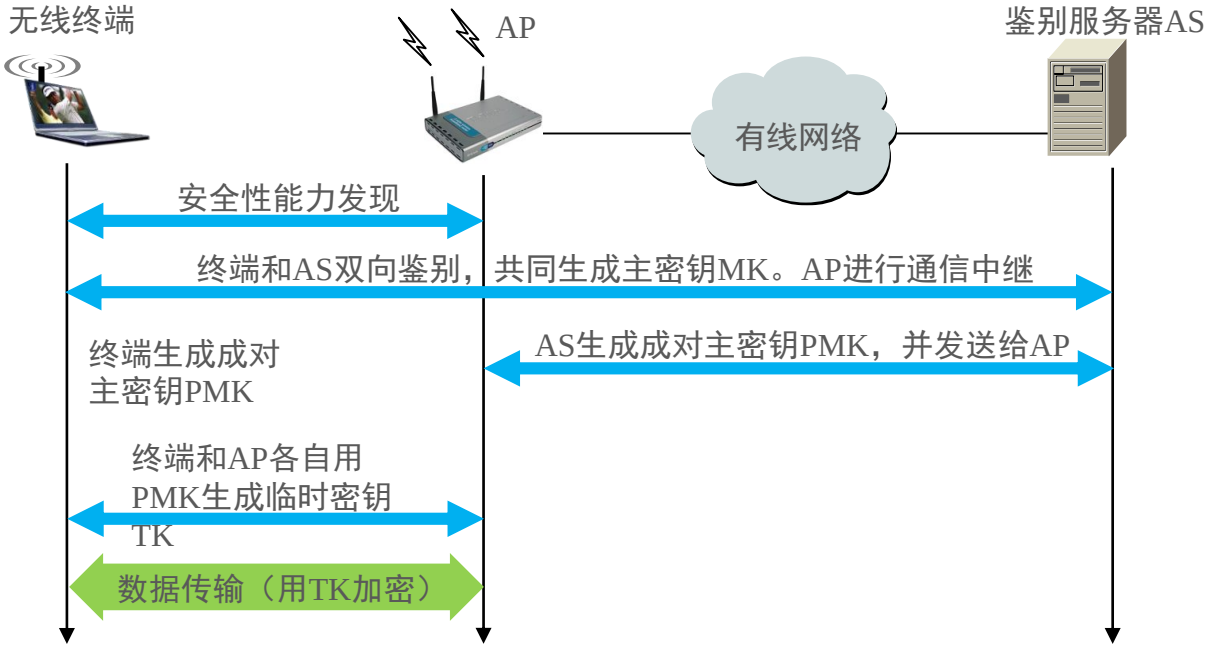
03 OPTION

有线等效保密WEP (Wired Equivalent Privacy) 提供实体鉴别、访问控制、数据加密和完整性检验等。WEP采用对称共享密钥加密技术。

2. IEEE 802.11i

- 具有更强安全性，主要包括一种可扩展的鉴别机制的集合，更强的加密算法，以及一种密钥分发机制。
- IEEE 802.11i的商业名称为WPA2（WiFi Protected Access 2，意思是“无线局域网受保护的接入”的第二个版本）。
- WPA是802.11i的一个子集，在802.11i正式发布前，作为无线局域网安全的过渡标准，代替WEP为802.11无线局域网提供更强的安全性。

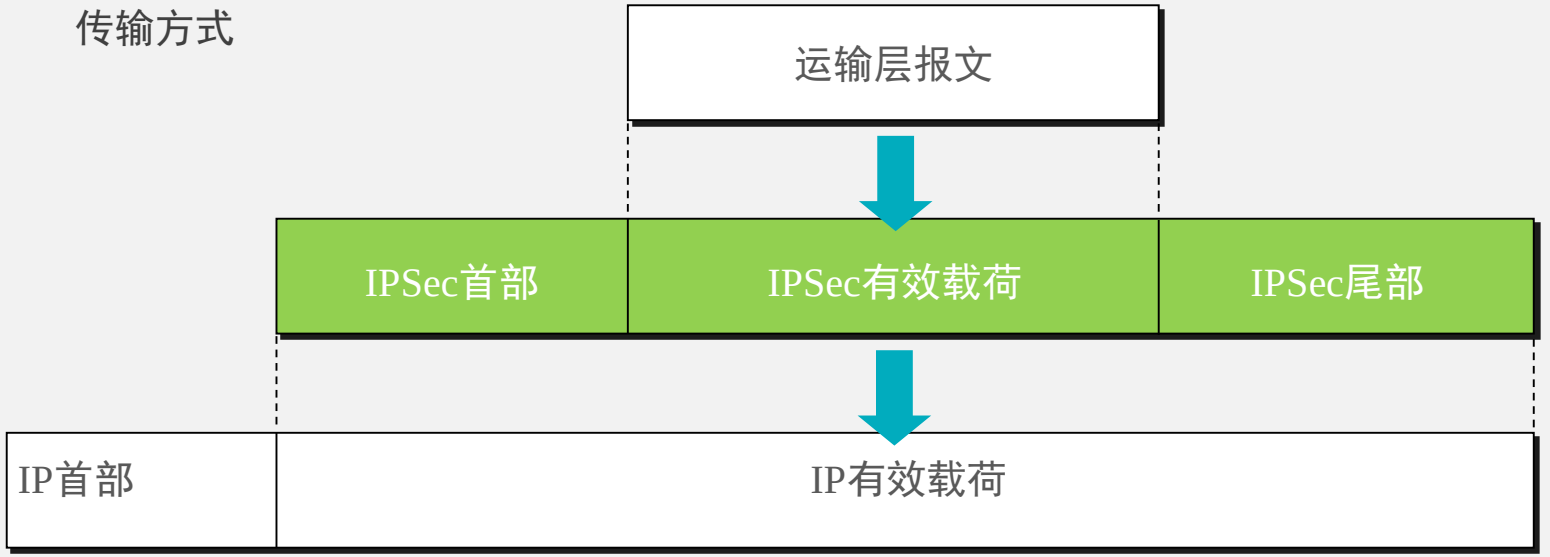
802.11i的基本交互过程



7.6.3 网络层实例：IPsec

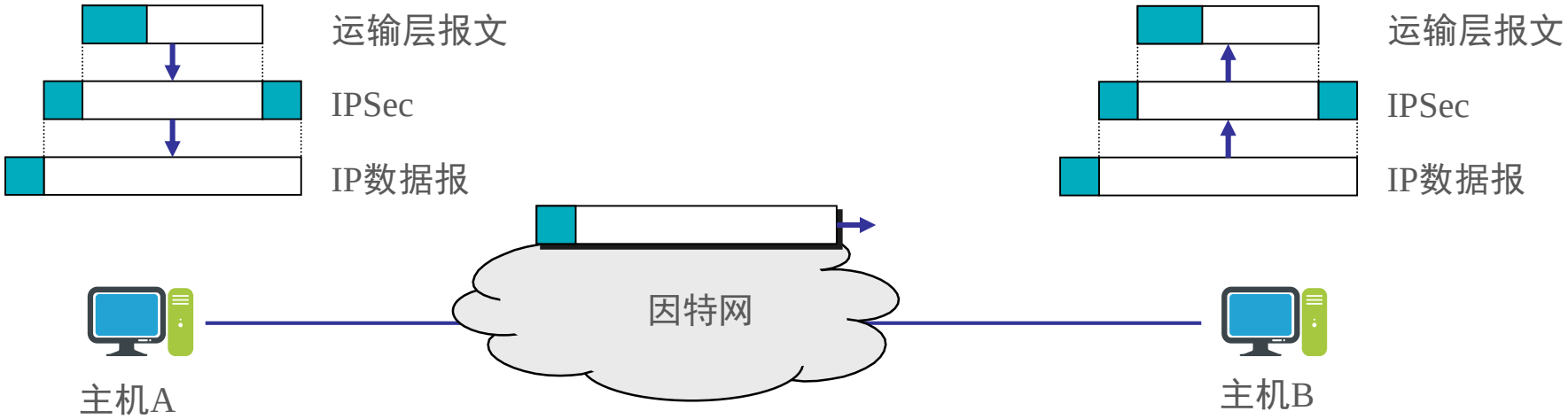
- IPsec是为因特网网络层提供安全服务的一组协议[RFC 2401~2411]。
- IPsec是一个协议名称，是IP Security （意思是IP安全）的缩写。

IPsec 的两种运行方式



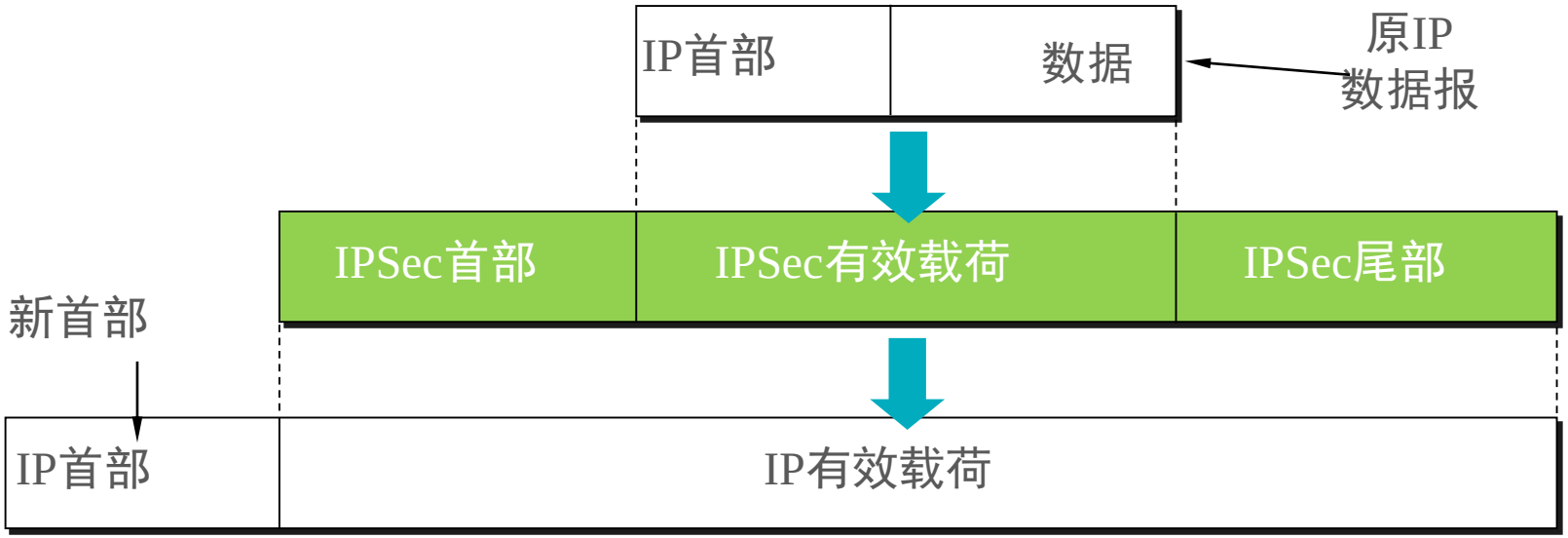
IPsec 的两种运行方式

- **传输方式**



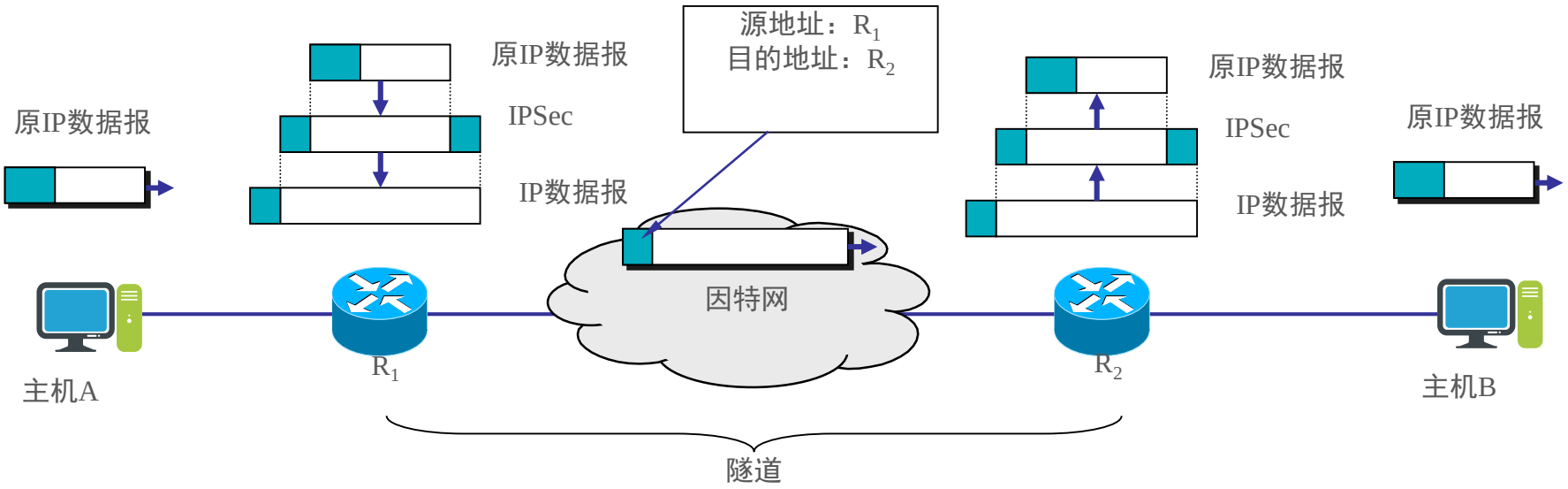
IPsec 的两种运行方式

- **隧道方式**



IPsec 的两种运行方式

- **隧道方式**



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t提供机密性服务。

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机密性服务。

安全关联(Security Association, SA)

- **在两个结点之间用AH或ESP进行通信之前，首先要在这两个结点之间建立一条网络层的逻辑连接，称为安全关联(Security Association, SA)。**
- **通过安全关联，双方确定将采用的加密或鉴别算法以及各种安全参数，并在SA建立时产生一个32位的安全参数索引(Security Parameter Index, SPI)。**

1. 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。

协议 = 51

AH 首部

01 OPTION

下一个首部。标志紧接着本首部的下一个首部的类型（如 TCP 或 UDP）。

02 OPTION

安全参数索引 SPI。标志安全关联。

03 OPTION

序号。AH协议用该序号防止重放攻击。

04 OPTION

鉴别数据(可变)。一个可变长字段，包含一个经过加密或签名的报文摘要。

2. 封装安全载荷 ESP

01 OPTION

使用 ESP 时，IP 数据报首部的协议字段置为 50。当 IP 首部检查到协议字段是 50 时，就知道在 IP 首部后面紧接着的是 ESP 首部，同时在原 IP 数据报后面增加了两个字段，即 ESP 尾部和 ESP 数据。

02 OPTION

在 ESP 首部中有标识一个安全关联的安全参数索引 SPI (32 位)，和序号(32 位)。

03 OPTION

在 ESP 尾部中有下一个首部。ESP 尾部和原来数据报的数据部分一起进行加密，因此攻击者无法得知所使用的运输层协议。

04 OPTION

ESP 鉴别和 AH 中的鉴别数据是一样的。因此，用 ESP 封装的数据报既有鉴别源站和检查数据报完整性的功能，又能提供保密。

在 IP 数据报中的ESP 的各字段

7.6.4 运输层实例：SSL/TLS

网上购物需要的安全服务：

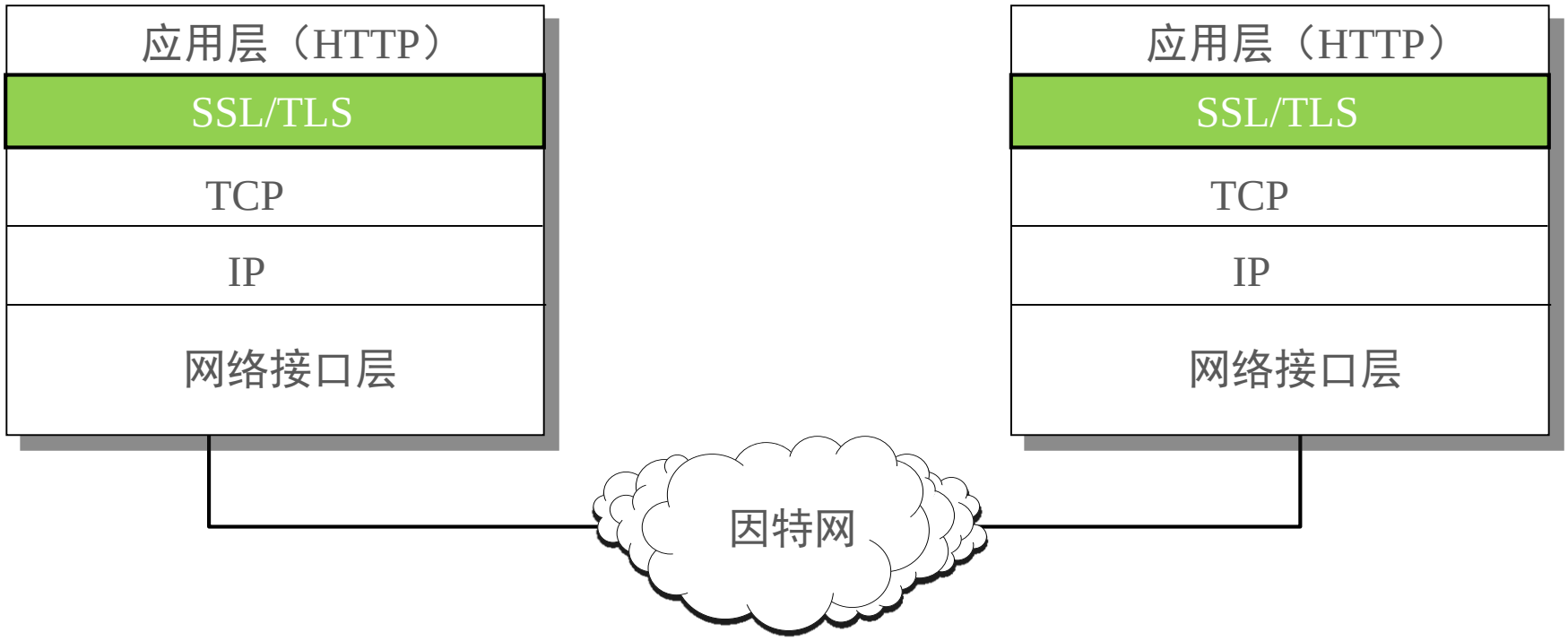
(1) 顾客需要确保服务器属于真正的销售商，而不是属于一个冒充者。

(2) 顾客与销售商需要确保报文的内容在传输过程中没有被更改。

(3) 顾客与销售商需要确保诸如信用卡号之类的敏感信息不被冒充者窃听。

- 运输层安全协议可以提供以上安全服务。
- 现在广泛使用的有两个协议：
  - SSL (Secure Socket Layer)，译为安全套接字层。
  - TLS (Transport Layer Security)，译为运输层安全。
- SSL是Netscape公司在1994开发的，广泛应用于基于万维网的各种网络应用。
- TLS是1995年IETF在SSL 基础上设计的。

SSL/TLS 的位置

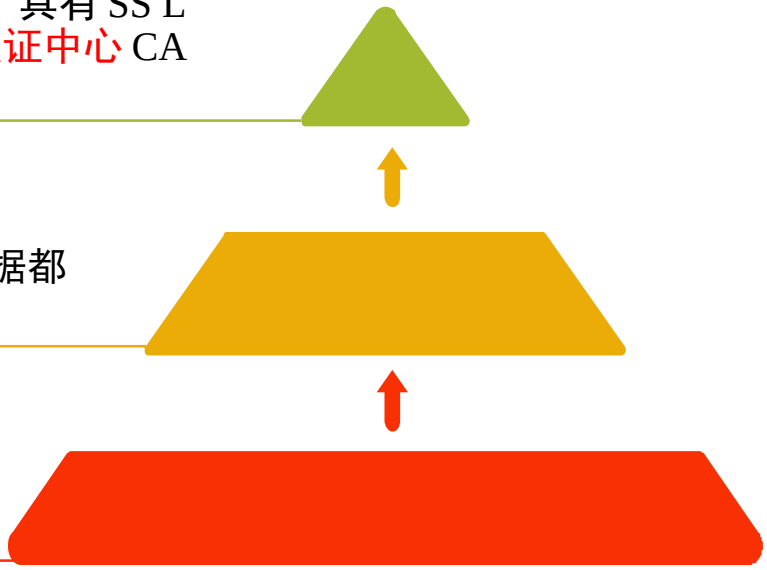


SSL 提供以下三种安全服务

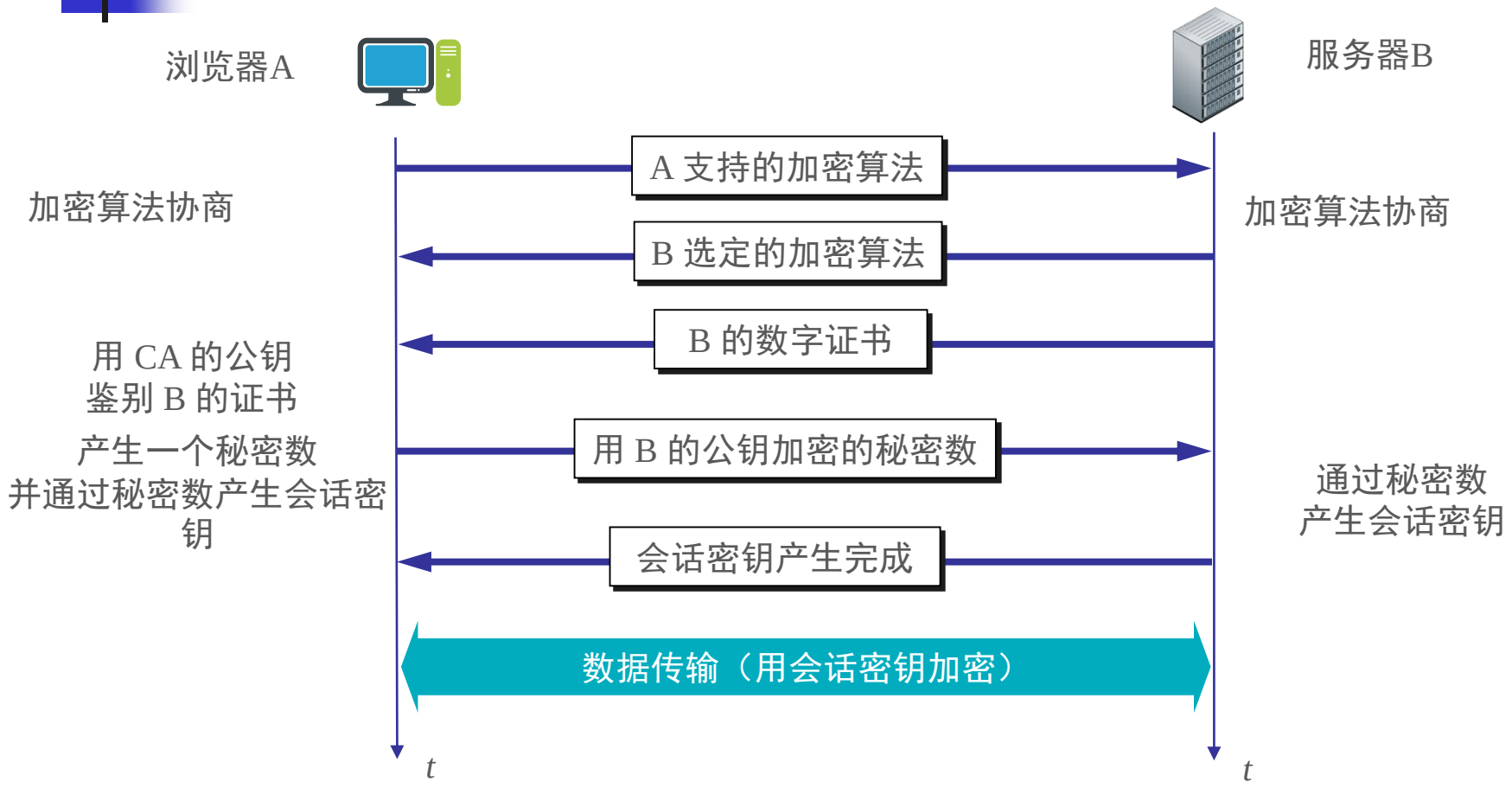
(1) SSL 服务器鉴别　允许用户证实服务器的身份。具有 SS L 功能的浏览器维持一个表，上面有一些可信赖的认证中心 CA (Certificate Authority)和它们的公钥。

(2) 加密的 SSL 会话　客户和服务器交互的所有数据都在发送方加密，在接收方解密。

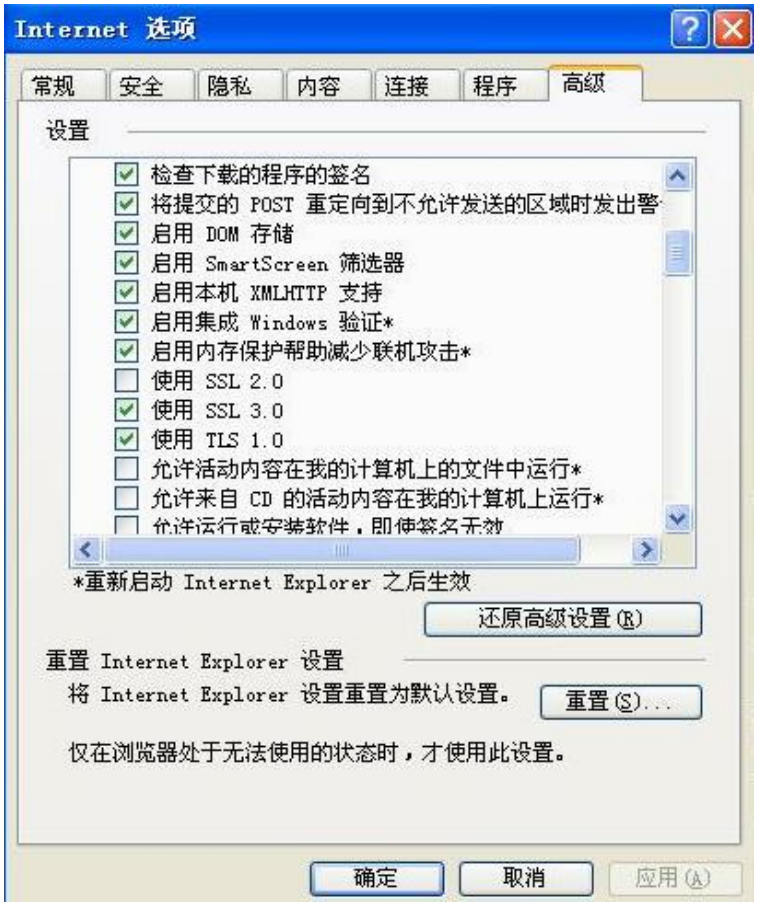
(3) SSL 客户鉴别　允许服务器证实客户的身份。



SSL的基本工作过程


浏览器A
服务器B
A 支持的加密算法
加密算法协商
加密算法协商
B 选定的加密算法
B 的数字证书
用 CA 的公钥
鉴别 B 的证书
产生一个秘密数
并通过秘密数产生会话密钥
用 B 的公钥加密的秘密数
通过秘密数
产生会话密钥
会话密钥产生完成
数据传输（用会话密钥加密）
t
t

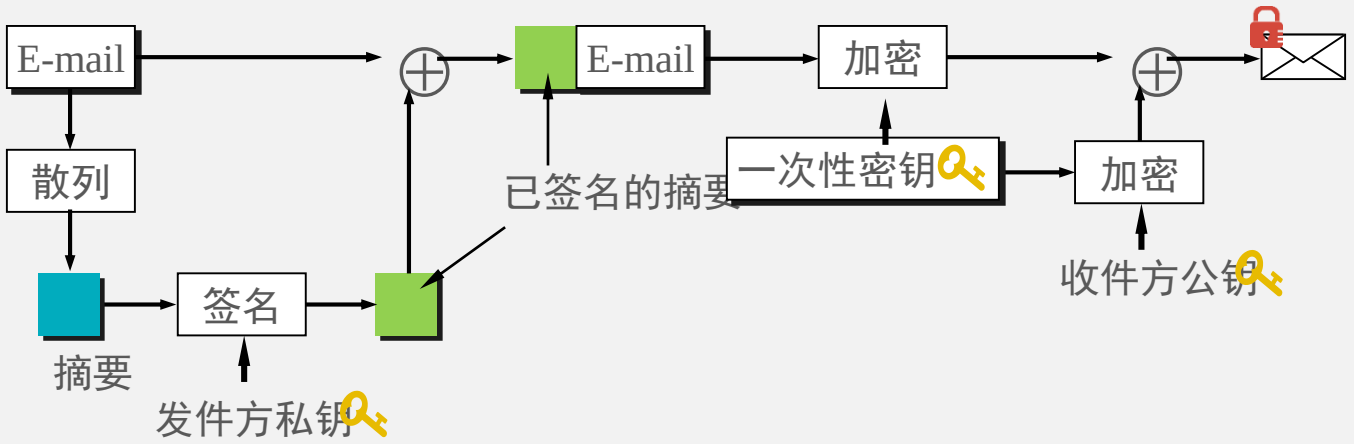
浏览器中的SSL/TLS选项



7.6.5 应用层实例：PGP (Pretty Good Privacy)

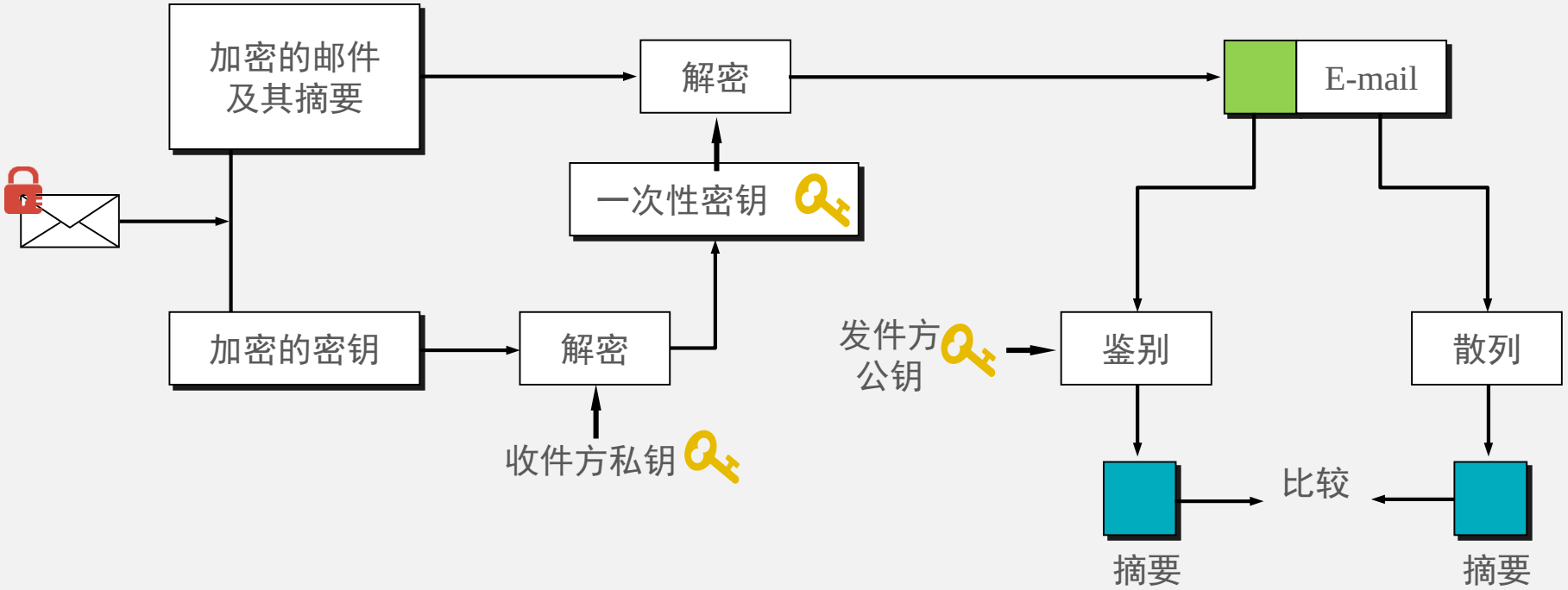
- PGP 是由Phil Zimmermann于1995开发的一个安全电子邮件软件。
- 虽然 PGP 已被广泛使用，但 PGP 并不是因特网的正式标准。
- PGP通过报文摘要和数字签名技术为电子邮件提供完整性和不可否认，使用对称密钥和公钥的组合加密来提供机密性。

PGP发件方处理过程



7.6.5 应用层实例：PGP (Pretty Good Privacy)

PGP发件方处理过程



7.7 系统安全：防火墙与入侵检测

- **恶意用户或软件通过网络对计算机系统的攻击已成为当今计算机安全最严重的威胁之一。**

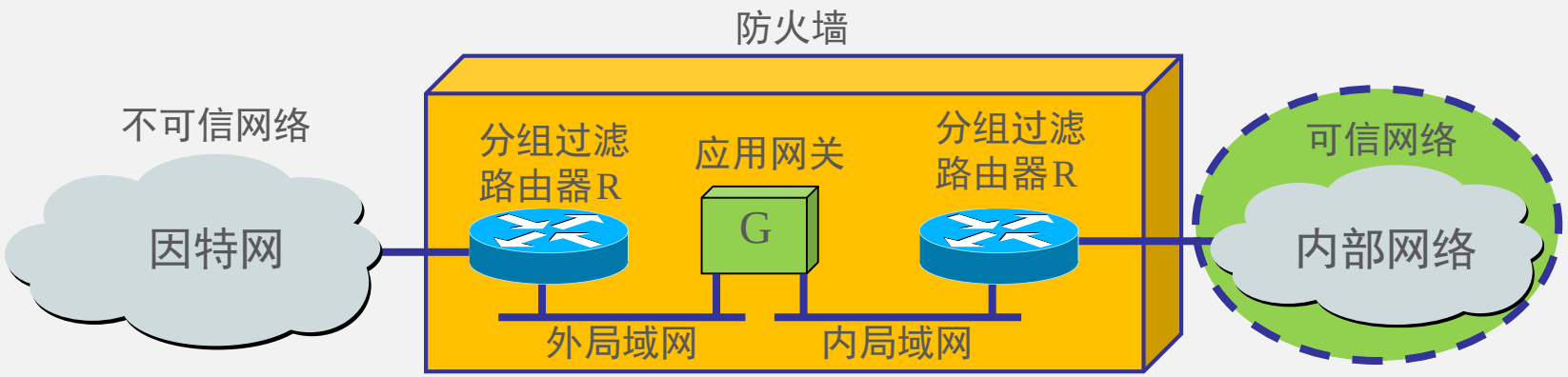
防火墙(firewall)作为一种访问控制技术，通过严格控制进出网络边界的分组，禁止任何不必要的通信，从而减少潜在入侵的发生，尽可能降低这类安全威胁所带来的安全风险。

入侵检测系统(Intrusion Detection System)通过对进入网络的分组进行深度分析与检测发现疑是入侵行为的网络活动，并进行报警以便进一步采取相应措施。

7.7.1 防火墙(firewall)

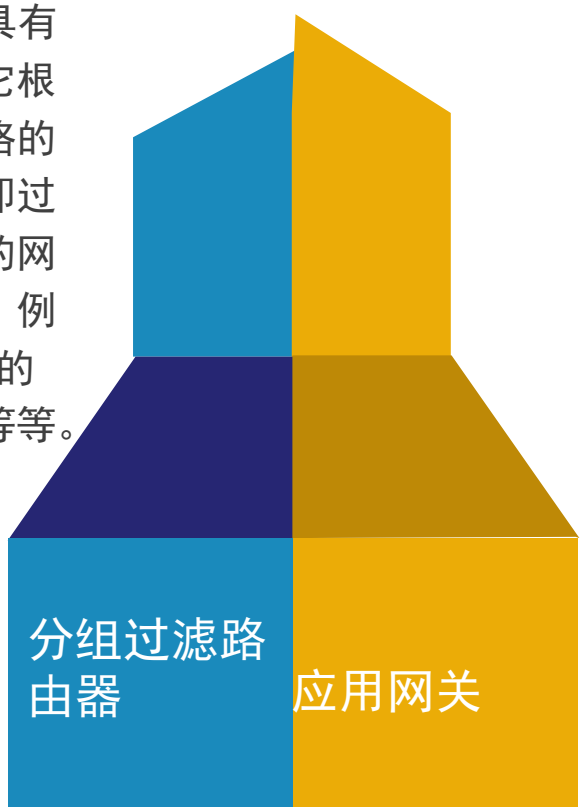
- 防火墙(firewall)是把一个组织的内部网络与其他网络（通常就是因特网）隔离开的软件和硬件的组合。根据访问控制策略，它允许一些分组通过，而禁止另一些分组通过。访问控制策略由使用防火墙的组织根据自己的安全需要自行制订。
- 防火墙内的网络称为“可信网络”(trusted network)，而将外部的因特网称为“不可信网络”(untrusted network)。

防火墙在互连网络中的位置



防火墙技术一般分为两类

分组过滤路由器　是一种具有分组过滤功能的路由器，它根据过滤规则对进出内部网络的分组执行转发或者丢弃（即过滤）。过滤规则基于分组的网络层或运输层首部的信息，例如：源/目的IP地址、源/目的端口、协议类型、标志位等等。



应用网关　在应用层通信中扮演报文中继的角色。一种网络应用需要一个应用网关。在应用网关中可以实现基于应用层数据的过滤和高层用户鉴别。

7.7.2 入侵检测系统

- 防火墙试图在入侵行为发生之前阻止所有可疑的通信。但事实是不可能阻止所有的入侵行为，有必要采取措施在入侵已经开始，但还没有造成危害或在造成更大危害前，及时检测到入侵，以便尽快阻止入侵，把危害降低到最小。这就需要**入侵检测系统**。
- **入侵检测系统**(Intrusion Detection System, IDS) 对进入网络的分组执行深度分组检查，当观察到可疑分组时，向网络管理员发出告警或执行阻断操作（由于IDS的“误报”率通常较高，多数情况不执行自动阻断）。
- IDS能用于检测多种网络攻击，包括网络映射、端口扫描、DoS攻击、蠕虫和病毒、系统漏洞攻击等。

两种入侵检测方法

- **入侵检测方法一般可以分为基于特征的入侵检测和基于异常的入侵检测两种。**

基于特征的入侵检测

- 基于特征的IDS维护一个所有已知攻击标志性特征的数据库。
- 每个特征是一个与某种入侵活动相关联的规则集，这些规则可能基于单个分组的首部字段值或数据中特定比特串，或者与一系列分组有关。
- 当发现有与某种攻击特征匹配的分组或分组序列时，则认为可能检测到某种入侵行为。
- 这些特征和规则通常由网络安全专家生成，机构的网络管理员定制并将其加入到数据库中。

基于异常的入侵检测

- 基于特征的IDS只能检测已知攻击。基于异常的IDS可检测未知攻击。
- 基于异常的IDS通过观察正常运行的网络流量，学习正常流量的统计特性和规律，当检测到网络中流量某种统计规律不符合正常情况时，则认为可能发生了入侵行为。
- 但区分正常流和统计异常流是一个非常困难的事情。至今为止，大多数部署的IDS主要是基于特征的，尽管某些IDS包括了某些基于异常的特性。

7.8 网络攻击及其防范

7.8.1 网络扫描

- **网络扫描技术是获取攻击目标信息的一种重要技术，能够为攻击者提供大量攻击所需的信息。**
- **这些信息包括目标主机的IP地址、工作状态、操作系统类型、运行的程序以及存在的漏洞等等。**
- **主机发现、端口扫描、操作系统检测和漏洞扫描是网络扫描的四种主要类型。**

网络扫描的防范

关闭闲置及危险端口，只打开确实需要的端口。

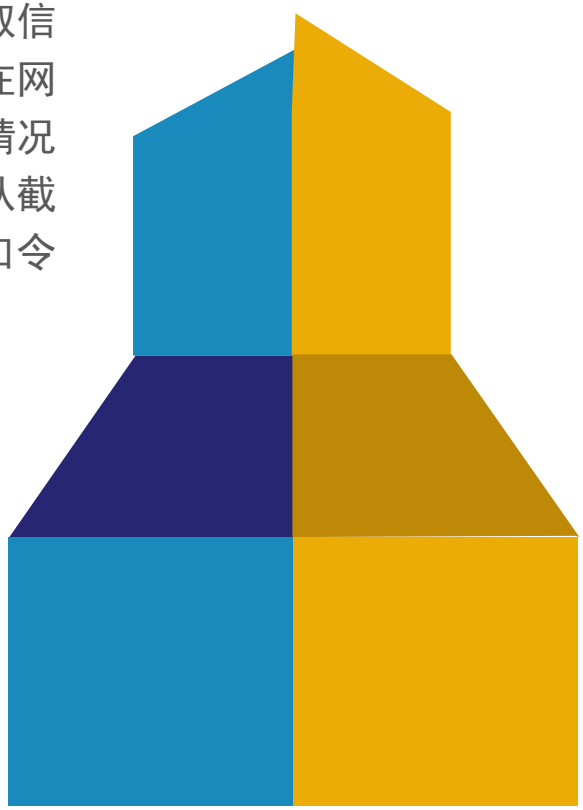
使用NAT屏蔽内网主机地址，限制外网主机主动与内网主机进行通信。

设置防火墙，严格控制进出分组，过滤不必要的ICMP报文。

使用入侵检测系统及时发现网络扫描行为和攻击者IP地址，配置防火墙对该地址的分组进行阻断。

7.8.2 网络监听

网络监听是攻击者直接获取信息的有效手段。如果数据在网络中明文传输（绝大部分情况都是这样），攻击者可以从截获的分组中分析出账号、口令等敏感信息。



攻击者主要采用局域网分组嗅探、交换机毒化攻击、ARP欺骗等攻击手段。

网络监听的防范

01 OPTION 尽量使用交换机，划分更细的VLAN

02 OPTION 为某些交换机端口设置允许学习的源MAC地址数量的上限

03 OPTION 将IP地址、MAC地址与交换机的端口进行静态绑定

04 OPTION 对于要重点保护的主机或路由器使用静态ARP表

05 OPTION 进行数据加密和实体鉴别技术，避免使用Telnet这些不安全的软件

7.8.3 拒绝服务攻击

- 拒绝服务DoS (Denial of Service)攻击是攻击者最常使用的一种行之有效且难以防范的攻击手段
- 是针对系统可用性的攻击，主要通过消耗网络带宽或系统资源导致网络或系统不胜负荷，以至于瘫痪而停止提供正常的网络服务或使服务质量显著降低
- 主要以网站、路由器、域名服务器等网络基础设施为攻击目标，危害极大

分布式拒绝服务攻击

如果处于不同位置的多个攻击者同时向一个或多个目标发起拒绝服务攻击，或者一个或多个攻击者控制了位于不同位置的多台主机，并利用这些主机对目标同时实施拒绝服务攻击，则称这种攻击为分布式拒绝服务DDoS (Distributed Denial of Service)攻击，它是拒绝服务攻击最主要的一种形式。

DoS攻击的防范

以下措施可以部分地减轻DoS攻击所造成的危害，而不能从根本上解决问题。

01 OPTION 利用网络防火墙对恶意分组进行过滤

02 OPTION 在入口路由器进行源端控制

03 OPTION 对路由器流经的IP数据报首部进行自动标记，以追溯攻击源，然后隔离攻击源或采取相应的法律手段

04 OPTION 通过分析分组首部特征和流量特征检测正在发生的DoS攻击，并进行预警

到目前为止，还没有一种完全有效地抵抗DoS攻击的技术和方法，特别是基于大规模流量攻击的DDoS更难防范。

谢谢！