其他内容可访问博客：either fight | or die (yst-10.github.io)

Block3

一. Key Management ---Key Exchange and Certificates

Classes of Keys

Lifetimes

- **Short term keys**
  - (ephemeral keys, session keys)
  - They are generated automatically.
  - Used for one message or session. 用于某一条消息或一条会话
- **Long term keys**
  - Generated explicitly by the users. 由用户显式生成
  - They are used for
    - Authentication
    - Confidentiality (encryption)

Type of service

– Authentication keys

• Public keys may have a long lifetime (decades)　公钥的使用寿命可能很长（几十年）

• Private keys / conventional keys have a shorter lifetime (year or two) 私钥/常规密钥的寿命较短（年或两年）

– Confidentiality keys

• Should have the shortest possible time.　应该有尽可能短的时间

1.Distribution of keys（使用非对称加密的对称密钥分布）

(1)Key Distribution Issues

• Hierarchies of Key Distribution Centres (KDC's) required for large networks, but must trust each other.大型网络需要的密钥分发中心（KDC）的层次结构，但必须相互信任。

• Session key lifetimes should be limited for greater security.为了提高安全性，限制会话密钥使用期。

• Use of automatic key distribution on behalf of users, but must trust system.
代表用户使用自动密钥分配，但必须信任系统。

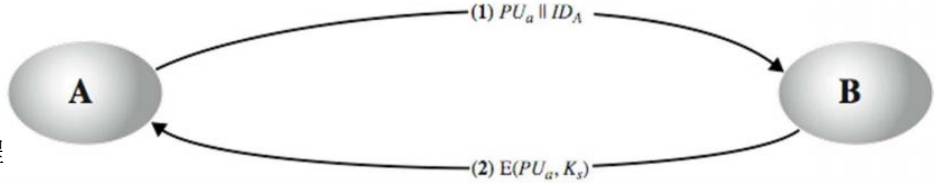
• Use of de-centralised key distribution.使用去集中化的密钥分配

• Controlling key usage.控制密钥使用情况

(2)Simple Secret Key Distribution

– Allows secure communications 允许安全通信

– No keys before/after exist　存在之前/之后没有密钥（生成->丢弃）



<1>过程

1. A generates a public/private key pair {PUa, PRa} and transmits a message to B consisting of PUa and an identifier of A, IDA.

A 生成一个公钥/私钥对{PUa，PRa}，并向 B 发送一个由 PUa 和 IDA，A 的标识符组成的消息。

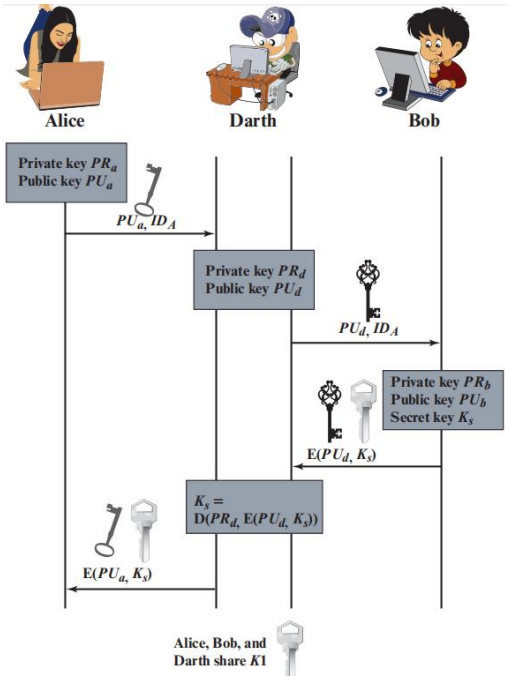
2. B generates a secret key, Ks, and transmits it to A, which is encrypted with A's public key.

B 生成一个密钥 Ks，并将其传输给 A，用 A 的公钥加密。Ks（session key）

3. A computes D(PRa, E(PUa, Ks)) to recover the secret key. Because only A can decrypt the message, only A and B will know the identity of Ks.　　A 计算 D（PRa、E（PUa、Ks））来恢复密钥。因为只有 A 可以解密消息，所以只有 A 和 B 可以知道 Ks 的身份。

4. A discards PUa and PRa and B discards PUa.　　A 丢弃 PUa，PRa 和 B 丢弃 PUa。

<2>man-in-the-middle attack（前面讲过）



1.A generates a public/private key pair {PUa, PRa} and transmits a message intended for B consisting of PUa and an identifier of A, IDA.

A 生成一个公钥/私钥对{PUa，PRa}，并传输一个针对 B 的、由 PUa 和 IDA，A 的标识符组成的消息

2. D intercepts the message, creates its own public/private key pair {PUd, PRd} and transmits PUd } IDA to B.

D 拦截消息，创建自己的公钥/私钥对{PUd，PRd}，并将 PUd||IDA 传输给 B。

3. B generates a secret key, Ks, and transmits E(PUd, Ks).

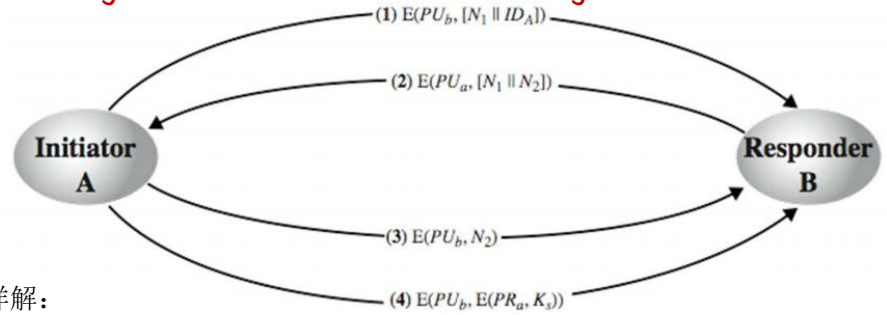
B 生成一个密钥 Ks，并传输 E（PUd、Ks）。

4. D intercepts the message and learns Ks by computing D(PRd, E(PUd, Ks)).　D 通过计算 D（PRd、E（PUd、Ks））来拦截消息并学习 Ks。

5. D transmits E(PUa, Ks) to A　　D 向 A 传输 E（PUa、Ks）

问题：窃听！！！，A,B 正常通信，但 D 也知道 Ks

(3)Secret Key Distribution with Confidentiality and Authentication????



过程详解：

1. A uses B's public key to encrypt a message to B containing an identifier of A(IDA) and a nonce (N1), which is used to identify this transaction uniquely.

A 使用 B 的公钥加密到 B 的消息，其中包含 A（IDA）和临时（N1），用于唯一标识此事务

2. B sends a message to A encrypted with PUa and containing A's nonce (N1) as well as a new nonce generated by B (N2). Because only B could have decrypted message (1), the presence of N1 in message (2) assures A that the correspondent is B.

B 向 A 发送一条用 PUa 加密的消息，其中包含 a 的 nonce（N1）以及由 B（N2）生成的一个新的 nonce。因为只有 B 可以解密消息(1)，所以消息(2)中 N1 的存在保证了 A 的通信者是 B。

3. A returns N2, encrypted using B's public key, to assure B that its correspondent is A.

A 返回 N2，使用 B 的公钥加密，以确保 B 的通信者是 A

4. A selects a secret key Ks and sends M = E(PUb, E(PRa, Ks)) to B. Encryption of this message with B's public key ensures that only B can read it; encryption with A's private key ensures that only A could have sent it.

A 选择一个密钥 Ks 并发送 M = E（PUb，E（PRa，Ks））给 B。用 B 的公钥加密这个消息确保只有 B 可以读取它；用 a 的私钥加密确保只有 A 可以发送它。

5. B computes D(PUa, D(PRb, M)) to recover the secret key.

B 计算 D（PUa、D（PRb、M））来恢复密钥

(4)Hybrid Key Distribution

<1>Retains the use of private KDC. 保留私有 KDC

KDC（密钥分发中心）是负责管理和分发密钥的实体。Hybrid Key Distribution 保留了私有 KDC 的使用，这是传统的密钥管理方式，其中 KDC 负责颁发和管理 session keys

<2>Shares a secret master key with each user. 与每个用户共享一个主密钥

在 Hybrid Key Distribution 中，每个用户与 KDC 共享一个“主密钥”。这个主密钥是一个对称密钥，用于安全地建立通信会话密钥。每个用户与 KDC 之间的通信是通过这个主密钥进行加密和解密的

<3>Distributes session keys using the master key. 使用主密钥的分发会话密钥。

一旦用户与 KDC 建立连接并进行身份验证，KDC 使用主密钥生成并分发会话密钥。会话密钥是为了特定通信会话而产生的临时密钥，用于加密通信内容。

<4>Public-key is used to distribute master keys. 公钥用于分发主密钥。

Especially useful with widely distributed users. 对广泛分布的用户特别有用（允许远程用户以安全方式获得密钥）

<5>Rationale: 理由

Performance.对称密钥加密速度快，主密钥用于生成会话密钥，提高了密钥生成的效率。

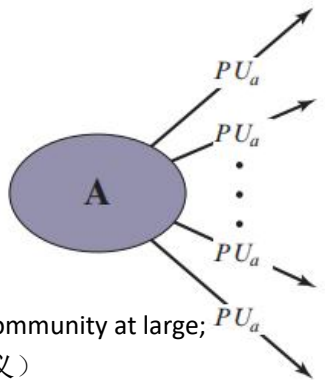
Backward compatibility. 向后兼容性。保留了对称密钥加密系统，同时引入公钥加密以确保安全性，同时保持与传统系统的兼容性。

2.Distribution of Public Keys

• Can be considered as using one of:

– Public announcement. – Publicly available directory.

– Public-key authority. – Public-key certificates.



(1)Public Announcement

• Users distribute public keys to recipients or broadcast to community at large;
用户将公钥分发给收件人或向整个社区进行广播（定义）

– eg. append PGP keys to email messages or post to news groups or email list.

例如，附加到电子邮件或发布到新闻组或电子邮件列表。

• Major weakness is forgery: 主要的弱点是伪造(假装成 A)

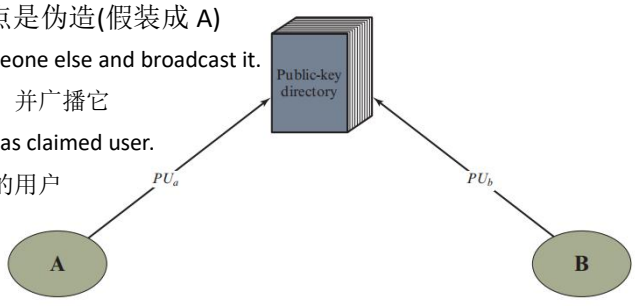
– Anyone can create a key claiming to be someone else and broadcast it.

任何人都可以创建一个自称是别人的钥匙，并广播它

– Until forgery is discovered can masquerade as claimed user.

在发现伪造文件之前，可以伪装成所声称的用户

(2)Publicly Available Directory



<1>Can obtain greater security by registering keys with a public directory.

可以通过在公共目录中注册密钥来获得更大的安全性。

<2>Directory must be trusted with properties:目录必须有以下受信任的性质

– Contains {name, public-key} entries. 包括（name,public-key）项

– Participants register securely with directory. 参与者安全地注册到目录中

– Participants can replace key at any time. 参与者可以随时更换钥匙(either because of the desire to replace a public key that has already been used for a large amount of data, or because the corresponding private key has been compromised in some way)要么是因为希望替换已经用于大量数据的公钥，要么是因为相应的私钥以某种方式受到了损害

– Directory is periodically published. 目录将定期发布

– Directory can be accessed electronically. 目录可以通过电子访问(必须从当局与参与者进行安全、经过验证的通信)

<3>Still vulnerable to tampering or forgery. 仍然容易被篡改或伪造

If an adversary succeeds in obtaining or computing the private key of the directory authority, the adversary could authoritatively pass out counterfeit public keys and subsequently impersonate any participant and eavesdrop on messages sent to any participant. Another way to achieve the same end is for the adversary to tamper with the records kept by the authority.如果对手成功地获得或计算了目录权限的私钥，对手可以权威地传递假冒的公钥，随后模拟任何参与者，并在发送给任何参与者的消息上丢失。另一种达到同样目的的方法是让对手篡改当局保存的记录。

(3)Public-Key Authority 公钥机构许可

<1>Improves security by tightening control over distribution of keys from directory.

通过加强对目录中密钥分配的控制来提高安全性。

<2>Has properties of directory and requires users to know public key for the directory;

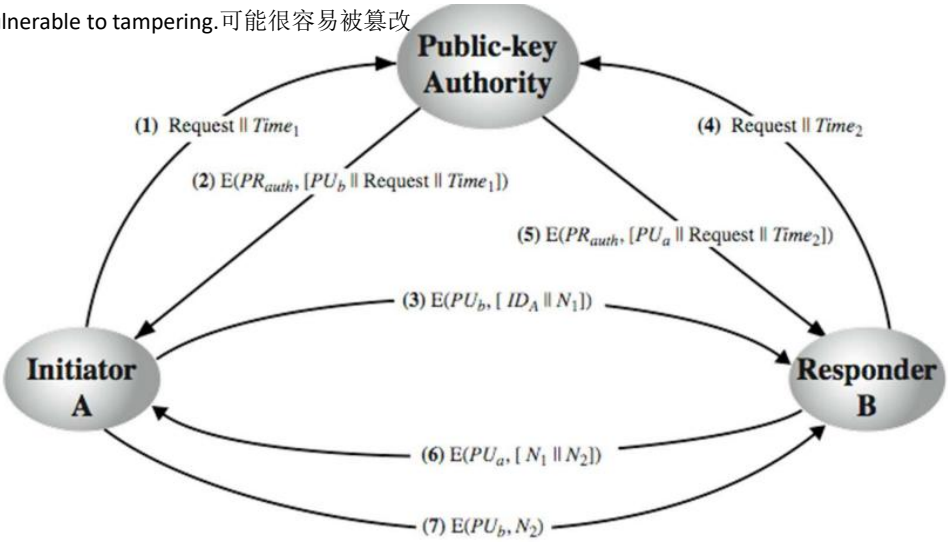
具有目录的属性，并要求用户知道该目录的公钥；

<3>Users interact with directory to obtain any desired public key securely:

用户与目录进行交互，以安全地获得任何所需的公钥：

– Requires real-time access to directory when keys are needed.当需要密钥时，需要实时访问目录

– May be vulnerable to tampering.可能很容易被篡改



<4>过程

1.A sends a timestamped message to the public-key authority containing a request for the current public key of B.

A 向公钥机构发送一个时间戳消息，其中包含对 B 当前公钥的请求。

2. The authority responds with a message that is encrypted using the authority's private key, PRauth. Thus, A is

able to decrypt the message using the authority's public key. Therefore, A is assured that the message originated with the authority. The message includes the following:当局响应一条使用当局的私钥 PRauth 加密的消息。因此，A 能够使用作者身份的公钥来解密消息。因此，A 确信消息源自权威。该消息包括以下内容：

■ B's public key, PUb, which A can use to encrypt messages destined for B

B 的公钥，PUb，A 可以用它来加密发送给 B 的消息

■ The original request used to enable A to match this response with the corresponding earlier request and to verify that the original request was not altered before reception by the authority

原始请求用于使 A 将此响应与相应的早期请求相匹配，并验证在当局收到之前没有更改原始请求

■ The original timestamp given so A can determine that this is not an old message from the authority containing a key other than B's current public key

给出的原始时间戳，以便 A 可以确定这不是来自包含除 B 的当前公钥以外的密钥的权威机构的旧消息

3. A stores B's public key and also uses it to encrypt a message to B containing an identifier of A (IDA) and a nonce (N1), which is used to identify this transaction uniquely. A 存储 B 的公钥，并使用它加密给 B 的消息，其中包含 A（IDA）和 nonce（N1），用于唯一地标识这个转换操作

4, 5. B retrieves A's public key from the authority in the same manner as A retrieved B's public key. At this point, public keys have been securely delivered to A and B, and they may begin their protected exchange. However, two additional steps are desirable: B 从权限中检索 A 的公钥，其方式与 A 检索到的 B 的公钥相同。此时，公钥已经安全地交付给 A 和 B，它们可以开始受保护的交换。然而，还需要另外两个步骤

6. B sends a message to A encrypted with PUa and containing A's nonce (N1) as well as a new nonce generated by B (N2). Because only B could have decrypted message (3), the presence of N1 in message (6) assures A that the correspondent is B. B 向用 PUa 加密的 A 发送一条消息，其中包含 A 的 nonce（N1）以及由 B（N2）生成的一个新的 nonce。因为只有 B 可以解密消息(3)，所以消息(6)中 N1 的存在保证了 A 所对应的信息是 B。

7. A returns N2, which is encrypted using B's public key, to assure B that its correspondent is A.

A 返回 N2，它使用 B 的公钥加密，以确保 B 的对应项是 A。

(4)Public-Key Certificates

<1>Certificates allow key exchange without real-time access to public-key authority.

证书允许密钥交换，而无需实时访问公钥权限

<2>A certificate binds identity to public key.证书会将身份绑定到公钥

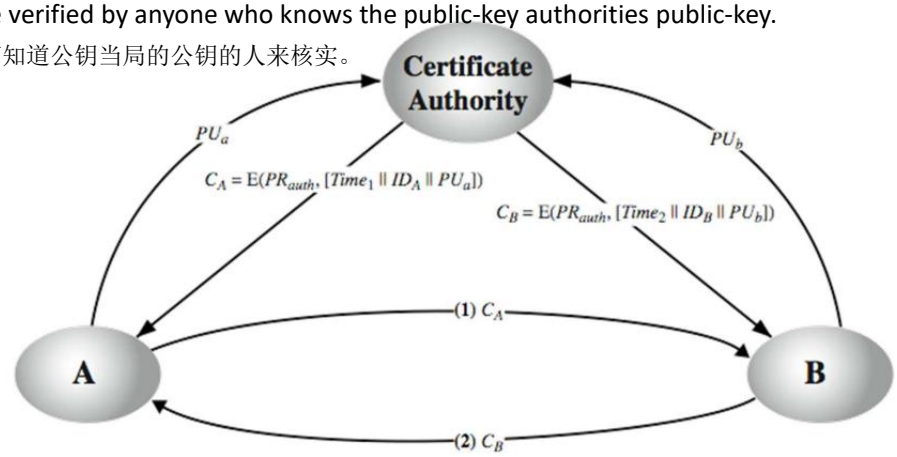
– Usually with other info such as period of validity, rights of use etc.通常与其他信息，如有效期、使用权等

<3>With all contents signed by a trusted Public-Key or Certificate Authority (CA).

包含由受信任的公钥或证书颁发机构（CA）签名的所有内容

<4>Can be verified by anyone who knows the public-key authorities public-key.

可以由任何知道公钥当局的公钥的人来核实。



<5>过程

每个参与者都向 CA 提供公钥请求一个证书，CA 回复 CA = E(PRauth, [Time1|| IDA ||PUa]),

A 可以将证书传递给任何参与者，该参与者可以验证

D(PUauth, CA) = D(PUauth, E(PRauth, [T|| IDA ||PUa])) = (T|| IDA ||PUa)

时间戳 Time 用来知道是否过期，旧的可能被篡改

Summary

– Symmetric key distribution using public-key encryption. • RSA, Diffie-Hellman, ..

– Distribution of public keys. • Announcement, directory, authority, CA.

3. X.509 [Public Key Infrastructure (PKI)]

(1)CA and X.500 history

• X.500 is a series of recommendations that define a directory service. The directory is distributed in several servers. X.500 是定义目录服务的一系列建议。该目录分布在多个服务器中。

• X.500 introduced the Distinguished Name (DN), a guaranteed unique name for everyone on earth. (typical DN component, Country, State, Locality, Organisation, Common Name...)

X.500 引入了区别名称（DN），这是一个保证对地球上每个人的唯一名称。（典型的 DN 组件、国家、州、地区、组织、通用名称……）

• Because of concerns about misuse of the X.500 directory certificates were intended to protect access to the directory. 由于担心滥用 X.500 目录,证书旨在保护对该目录的访问

(2)X.509 Authentication Service X.509 身份验证服务

<1>Part of X.500 directory service standards. 是 X.500 目录服务标准的一部分

<2>**Defines framework for authentication services**. 定义了认证服务的框架

• Directory may store public-key certificates. 目录可以存储公钥证书。

• With public key of user signed by certification authority. 具有由认证机构签名的用户公钥

<3>Also defines authentication protocols. 同时还定义了身份验证协议

<4>X.509 is based in public-key certificates and digital signatures (used S/MIME, IP security, SSL/TLS, SET). X.509 does not dictate which publickey algorithm to use but recommends RSA.

X.509 基于公钥证书和数字签名（使用的 S/MIME、IP 安全、SSL/TLS、SET）。X.509 并不规定使用哪个公钥算法，但推荐 RSA。

<5>X.509 certificates are widely used. X.509 证书被广泛使用。

• have 3 versions.三个版本

(3)X.509 Obtaining a User's Certificate

• Certificates are placed in the directory by a CA or by the user (not by the directory server)

证书由 CA 或用户（而不是由目录服务器）放置在目录中

– Any user with access to the public key of the CA can recover the user public key that was certified.

任何能够访问 CA 公钥的用户都可以恢复已认证的用户公钥。

– Only the certification authority can modify the certificate. Any modification by a third party will be detected.

只有证书颁发机构（CA）可以修改该证书。任何由第三方进行的任何修改将会被检测到。

(4)X.509 The certificate contains:（具体看 5）

Version (V)	(**1**, **2**, or **3**)
Serial Number (SN)	Unique within CA -- identifying certificate
Signature algorithm identifier (AI)	

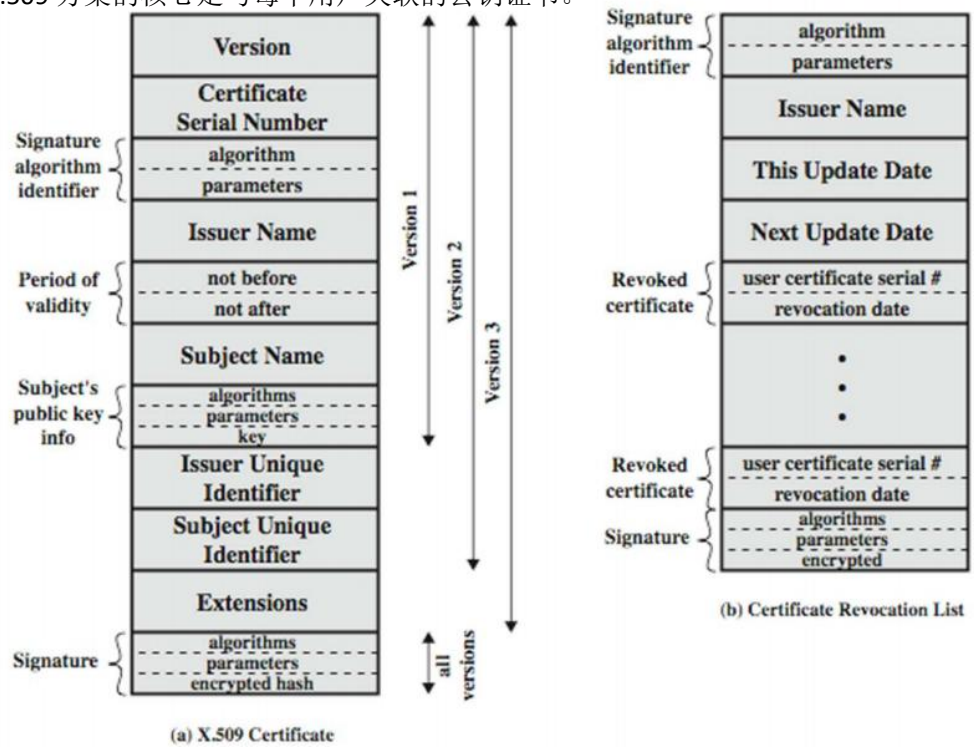
Issuer X.500 name (CA)	
Period of validity (TA)	From - to dates
Subject X.500 name (A)	Name of owner
Subject public-key info (Ap)	algorithm, parameters, key
Issuer unique identifier	v2+
Subject unique identifier	v2+
Extension fields	V3
Signature	.. of hash of all fields in certificate.

• Notation CA<<A>> denotes certificate for A signed by CA　　由 CA 签署的 A 的证书

(5)X.509 Certificates Formats

The heart of the X.509 scheme is the public-key certificate associated with each user.

X.509 方案的核心是与每个用户关联的公钥证书。



<1>Version: Differentiates among successive versions of the certificate format; the default is version 1. If the issuer unique identifier or subject unique identifier are present, the value must be version 2. If one or more extensions are present, the version must be version 3. Although the X.509 specification is currently at version 7, no changes have been made to the fields that make up the certificate since version 3.

区分证书格式的连续版本；默认值为版本 1。如果存在颁发者唯一标识符或主体唯一标识符，则该值必须为版本 2。如果存在一个或多个扩展名，则该版本必须是版本 3。尽管 X.509 规范目前处于版本 7 中，但自版本 3 以来，没有对组成证书的字段进行任何更改。

<2>Serial number: An integer value unique within the issuing CA that is unambiguously associated with this certificate. 与此证书明确关联的发行 CA 中唯一的整数值

<3>Signature algorithm identifier: The algorithm used to sign the certificate together with any associated parameters. Because this information is repeated in the signature field at the end of the certificate, this field has little, if any, utility. 用于与任何相关参数一起签名证书的算法。由于此信息会在证书末尾的签名字段中重复出现，因此此字段几乎没有任何实用程序。

<4>Issuer name: X.500 name of the CA that created and signed this certificate.

发行者名称：创建并签署此证书的 CA 的 X.500 名称。

<5>Period of validity: Consists of two dates: the first and last on which the certificate is valid.

有效期：包括两个日期：该证书有效的第一个和最后一个日期。

<6>Subject name: The name of the user to whom this certificate refers. That is, this certificate certifies the public key of the subject who holds the corresponding private key. （证书持有者）
此证书所引用的用户的名称。也就是说，该证书认证了持有相应私钥的主体的公钥。

<7>Subject's public-key information: The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters.

主体的公钥，加上要使用此密钥的算法的标识符，以及任何相关的参数。

<8>Issuer unique identifier: An optional-bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities. 是 X.509 证书中的一个可选字段，用于在 X.500 名称（通常是颁发者的名字）被用于不同实体的情况下，唯一标识颁发 CA（同一名字也能区分开，用于 CA，区别不同的颁发者）

<9>Subject unique identifier: An optional-bit string field used to identify uniquely the subject in the event the X.500 name has been reused for different entities. 是 X.509 证书中的一个可选字段，用于在 X.500 名称（通常是证书主体的名字）被用于不同实体的情况下，唯一标识证书主体。（同一名字也能区分开，用于持有证书的主体，区分不同的证书拥有者）

<10>Extensions: A set of one or more extension fields. Extensions were added in version 3 扩展：一个或多个扩展字段。扩展已在版本 3 中添加

<11>Signature: Covers all of the other fields of the certificate. One component of this field is the digital signature applied to the other fields of the certificate. This field includes the signature algorithm identifier.
涵盖了该证书的所有其他字段。此字段的一个组成部分是应用于证书的其他字段的数字签名。此字段包括签名算法标识符。

注意：version2 相比于 1 多了<8>,<9>, version3 相比于 2 多了<10>

标准定义一个证书：$CA \ll A \gg = CA\{V, SN, AI, CA, UCA, A, UA, Ap, T^A\}$

Y <<X>> :用户 X 的证书由认证机构 Y 颁发　　Y {I}: I 由 Y 签名。它包括 I 与附加的加密哈希码

V :证书版本　　SN ： serial number of the certificate

AI ： 用于签署证书的算法标识符

UCA ： CA 的可选唯一标识符

UA ： 用户 A 的可选唯一标识符

T^A ： 该证书的有效期

CA ： 证书颁发机构名称

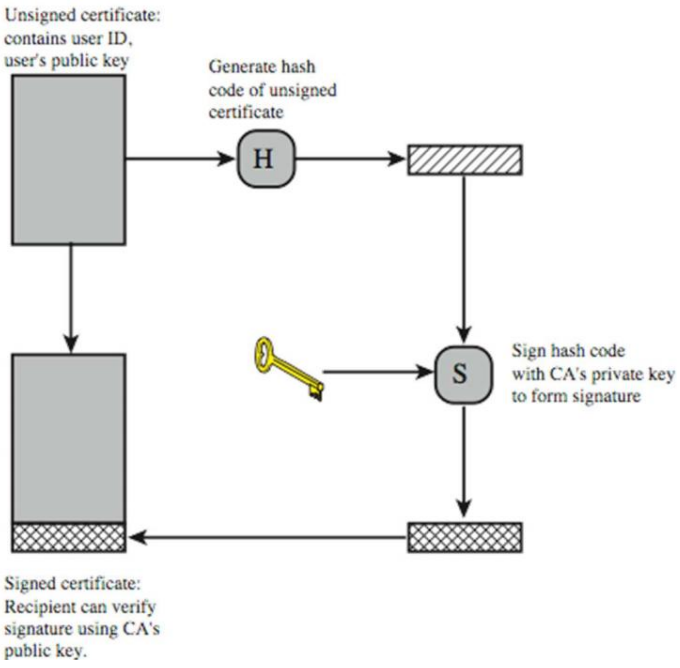
A ： 用户主体名字

Ap ： 用户 A 的公钥

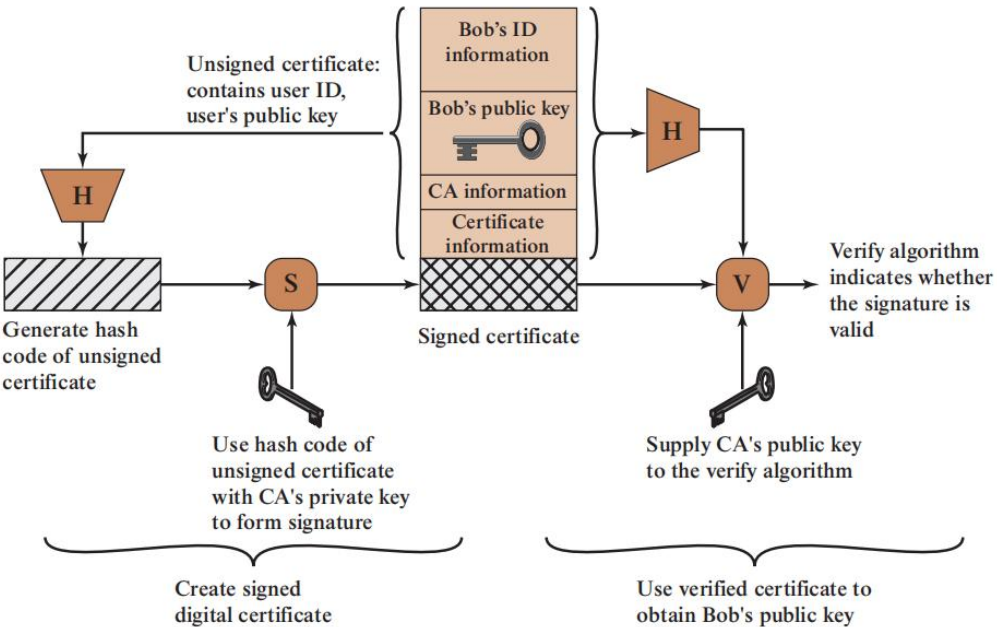
(6)X.509 Version 3

- Additional information fields added in the certificate. 在证书中添加的其他信息字段
  - Email/URL, policy details, usage constraints. 电子邮件/URL，策略细节，使用限制
- Rather than explicitly naming new fields defined a general extension method.
  它不是显式地命名新的字段，而是定义了一个通用的扩展方法
- Extensions consist of: 扩展包括
  - Extension identifier. 扩展标识符
  - Criticality indicator. 临界指标
  - Extension value.扩展值

(7)X.509 Certificate Use



通过计算该信息的哈希值,并使用哈希值和 CA 的私钥生成一个数字签名,从而对该信息进行签名.然后,Bob 可以将此证书广播给其他用户,或者将该证书附加到他签名的任何文档或数据块中.任何需要使用 Bob 的公钥的人都可以保证,Bob 的证书中包含的公钥是有效的,因为该证书是由受信任的 CA 签名的.



(8)Revocation 吊销

<1>Need revocation if:

– User's Private-Key has been compromised 用户的私钥已被泄露

– Certification Authority has been compromised 证书颁发机构已经被泄露了

– User is no longer certified by this Authority 用户不再由本授权机构认证

Reasons for this include that the subject's name has changed, the certificate is superseded, or the certificate was not issued in conformance with the CA's policies.其原因包括：主题的名称已经更改，证书已被取代，或者证书没有按照 CA 的政策颁发。

<2>Certificate Revocation List (CRL) 证书撤销清单（CRL）

<3>Users should check certificates with CA's CRL. 用户应该使用 CA 的 CRL 来检查证书。

(9)Authentication Procedures

• If A and B were to exchange information using two keys issued from different Certification Authorities (CAs)?如果 A 和 B 要使用来自不同的认证机构（ca）颁发的两个密钥来交换信息？

– In X509: 过程

• User A sends B a key, which was issued by CA_A 用户 A 向 B 发送一个密钥，它是由 CAA 发行

• User B receives it, but does not know (or trust) CAA , hence requests CAB to supply a certificate of CAA . 用户 B 收到它，但不知道（或信任）CAA，因此请求 CAB 提供 CAA 的证书

• CAB supplies B with a certificate of CAA , signed with CAB . CAB 向 B 提供与 CAB 签署的 CAA 证书。

– This is applied in exchange of emails, websites, etc. 这适用于交换电子邮件、网站等。

– You might have noticed Internet browsers sometime ask for your judgement to permission to enter a website as the certificate is not recognised!你可能已经注意到，互联网浏览器有时会要求你的判断，允许进入一个网站，因为证书不被识别！

(10)CA Hierarchy

<1>If both users share a common CA then they are assumed to know its public key.

如果两个用户共享一个共同的 CA，那么就假设他们知道它的公钥。

<2>Otherwise CA's must form a hierarchy. 否则，CA 必须形成一个层次结构

<3>Use certificates linking members of hierarchy to validate other CA's.

使用链接层次结构成员的证书来验证其他 CA。

Each CA has certificates for clients (forward) and parent (backward).

每个 CA 都有客户端（前）和父（后）的证书

<4>Each client trusts parents certificates. 每个客户端都信任父证书

<5>Enable verification of any certificate from one CA by users of all other CAs in hierarchy.

允许由层次结构中所有其他 CA 的用户对来自一个 CA 的任何证书进行验证

<6>A has used a chain of certificates to obtain B's public key. In the notation of X.509, this chain is expressed as A 使用了一个证书链来获取 B 的公钥。在 X.509 的符号中，这个链被表示为

$$X_1 \ll X_2 \gg X_2 \ll B \gg$$

In the same fashion, B can obtain A's public key with the reverse chain:（X 是 CA 机构）

$$X_2 \ll X_1 \gg X_1 \ll A \gg$$

更多：$X_1 \ll X_2 \gg X_2 \ll X_3 \gg \ldots X_N \ll B \gg$

<7>The connected circles indicate the hierarchical relationship among the CAs; the associated boxes indicate certificates maintained in the directory for each CA entry. The directory entry for each CA includes two types of certificates: 连接的圆圈表示 CA 之间的层次关系；关联的框表示每个 CA 条目的目录中维护的证书。每个 CA 的目录条目包括两种类型的证书：

Forward certificates: *Certificates of X generated by other CAs* 前向证书：由其他 CAs 生成的 X 证书(例如，如果你有一个证书是由 CA1 颁发的，而另一个证书是由 CA2 颁发的，后者是 CA1 的子证书，那么 CA2 颁发的证书就可以被称为 CA1 的前向证书。)

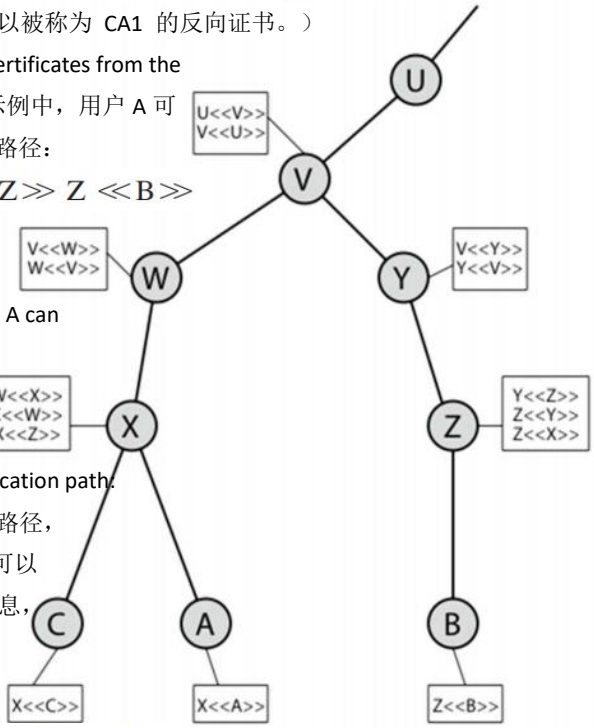
Reverse certificates: *Certificates generated by X that are the certificates of other CAs*

反向证书：由 X 生成的、属于其他 ca 的证书的证书（例如，如果一个用户 X 颁发了一个证书给 CA1，证实 CA1 对用户 X 的某些权限，那么这个证书可以被称为 CA1 的反向证书。）

1.In this example, user A can acquire the following certificates from the directory to establish a certification path to B:在本示例中，用户 A 可以从该目录中获取以下证书，以建立到 B 的认证路径：

$$X \ll W \gg W \ll V \gg V \ll Y \gg Y \ll Z \gg Z \ll B \gg$$

2.When A has obtained these certificates, it can unwrap the certification path in sequence to recover a trusted copy of B's public key. Using this public key, A can send encrypted messages to B. If A wishes to receive encrypted messages back from B, or to sign messages sent to B, then B will require A's public key, which can be obtained from the following certification path: 当 A 获得了这些证书时，它可以按顺序展开证书路径，以恢复 B 的公钥的受信任副本。使用此公钥，A 可以向 B 发送加密消息。如果 A 希望从 B 接收加密消息，或对发送给 B 的消息进行签名，则 B 将需要 A 的公钥，可以从以下认证路径获得：



$$Z \ll Y \gg Y \ll V \gg V \ll W \gg W \ll X \gg X \ll A \gg$$

"the use of an X.509 hierarchy to mutually verify clients certificates"

B 可以从目录中获得这组证书，或者 A 可以提供它们 作为它传递给 B 的最初信息的一部分。

二. Example of a User Authentication and Access Control Application

1.User Authentication and Authentication Protocols

<1>User Authentication is the process of verifying an identity claimed by or for a system entity. 是验证由系统实体或为系统实体声明身份的过程。

<2>User Authentication Has two steps:
– Identification - specify identifier 标识
– Verification - bind entity (person) and identifier 验证 -绑定实体（人员）和标识符
<3>User Authentication Distinct from message authentication 不同于消息身份验证
<4>Authentication Protocols Used to convince parties of each other’s identity and to exchange session keys.
用来说服双方了解对方的身份，并交换会话密钥。
<5>May be one-way or mutual. 可以是单向的或相互的
<6>Key issues are:关键问题是
– Confidentiality – to protect session keys. 保密性——用以保护会话密钥
– Timeliness – to prevent replay attacks. 及时性-以防止重放攻击

2.Identity Management

(1)Federated Identity Management 联合身份管理

联合身份管理是一种跨越不同组织、企业或系统边界的身份管理方法。它允许用户在多个不同实体的网络中使用相同的身份验证凭据，而无需在每个系统中单独创建或维护帐户信息。

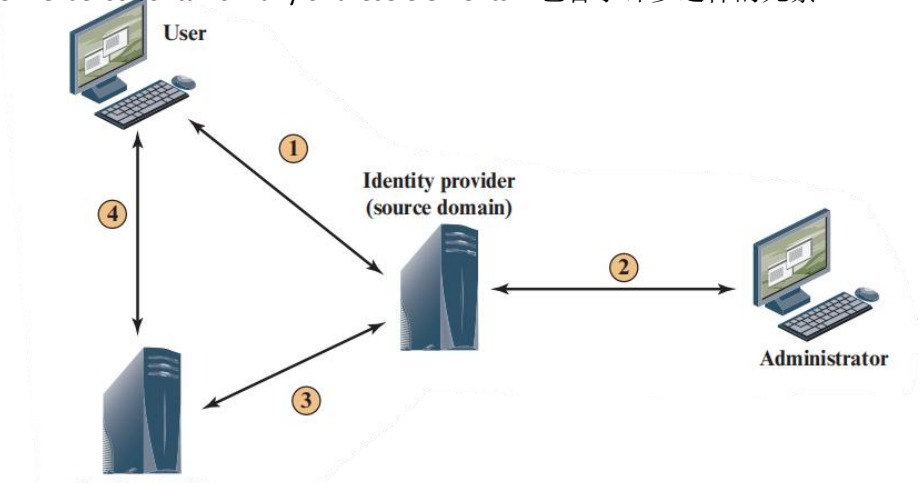
主要特点和目标包括：

- **跨组织边界：** 联合身份管理旨在跨越不同实体或系统之间的边界。它使用户能够在多个组织或系统中使用相同的身份验证标识，而不是每个地方都需要单独的帐户。
- **单点登录（SSO）：** 用户只需一次登录即可访问所有参与的系统，避免了多次登录不同系统的麻烦，提高了用户体验和便利性。
- **安全和标准性：** 身份验证和授权方法需要被标准化和保障安全性，以确保在不同实体之间共享身份信息时的安全性和完整性。
- **权限控制和管理：** 提供对用户权限和访问控制的集中管理。通过联合身份管理，组织可以更好地管理和控制对不同系统的访问权限。
- **互操作性：** 联合身份管理系统需要与不同的系统和应用程序进行交互，并能够处理不同的身份验证和授权机制，以实现不同系统之间的互操作性。

<1>Use of common identity management scheme 使用通用身份管理方案
• Across multiple enterprises & numerous applications 跨多个企业和众多的应用程序
• Supporting many thousands, even millions of users 支持数千名用户，甚至数百万名用户
<2>Principal elements are: 主要要素
• Authentication, authorisation, accounting, provisioning, workflow automation, delegated administration, password synchronisation, self-service password reset, federation

- **认证（Authentication）：** 确认用户身份的过程。
- **授权（Authorization）：** 决定用户可以访问哪些资源或数据。
- **计费（Accounting）：** 跟踪和记录用户访问和使用资源的情况。
- **配置管理（Provisioning）：** 管理用户对系统和资源的访问权限。
- **工作流自动化（Workflow Automation）：** 通过自动化流程简化和优化工作流程。
- **委派管理（Delegated Administration）：** 分配给其他人进行部分管理权限的过程。
- **密码同步（Password Synchronization）：** 确保用户在不同系统中使用相同的密码。
- **自助密码重置（Self-Service Password Reset）：** 用户可以自行重置密码而不需要管理员介入。
- **联合（Federation）：** 不同系统之间共享身份验证信息和访问权限。

<3>Kerberos contains many of these elements 包含了许多这样的元素



①End user's browser or other application engages in an authentication dialogue with identity provider in the same domain. End user also provides attribute values associated with user's identity.
最终用户的浏览器或其他应用程序与同一域中的身份提供程序进行身份验证对话。最终用户还提供了与用户标识相关联的属性值。

②Some attributes associated with an identity, such as allowable roles, may be provided by an administrator in the same domain.与标识相关联的一些属性，如允许的角色，可能由同一域中的管理员提供。

③A service provider in a remote domain, which the user wishes to access, obtains identity information, authentication information, and associated attributes from the identity provider in the source domain.
用户希望访问的远程域中的服务提供者，从源域中的身份提供者获取身份信息、身份验证信息和关联的属性。

④Service provider opens session with remote user and enforces access control restrictions based on user's identity and attributes.服务提供商打开与远程用户的会话，并根据用户的身份和属性强制执行访问控制限制。

(2)Standards Used

<1>Security Assertion Markup Language (SAML) 安全断言标记语言

• XML-based language for exchange of security information between online business partners

基于 xml 的语言，用于在在线业务合作伙伴之间交换安全信息

<2>Part of OASIS (Organisation for the Advancement of Structured Information Standards) standards for federated identity management 作为 OASIS 标准的一部分

• e.g. WS-Federation for browser-based federation

<3>Need a few mature industry standards 需要一些成熟的行业标准

(3)Summary

<1>Kerberos

– **Definition**: Kerberos is an authentication service designed for use in a distributed environment.

Kerberos 是一种设计用于在分布式环境中使用的身份验证服务。

– **Uses**: It makes use of a trusted third-party authentication service that enables clients and servers to establish authenticated communication.

它利用一个受信任的第三方身份验证服务，使客户端和服务器能够建立经过身份验证的通信

<2>Federated Identity Management is a relatively new concept dealing with the use of a common identity management scheme across multiple enterprises and numerous applications and supporting many thousands, even millions of users.联合身份管理是一个相对较新的概念，处理跨多个企业和多个应用程序使用通用身份管理方案，并支持成千上万甚至数百万用户。

– Kerberos contains many of these elements.

3.Kerberos

(1)定义

• Kerberos is an authentication service which addresses the following problem:

Kerberos 是一种可以解决以下问题的身份验证服务

In an open distributed environment in which users want to access services on servers distributed throughout the network, how can the servers Restrict the access to authorised users, and Authenticate requests for service. 在一个用户希望访问分布在整个网络中的服务器上的服务的开放的分布式环境中，服务器如何限制对授权用户的访问，并对服务请求进行身份验证。

(2)Threats 威胁

<1>**Impersonation**: A user gains access to a particular workstation and pretends to be another user operating from that workstation.冒充：一个用户可以访问一个特定的工作站，并假装是从该工作站操作的另一个用户。

<2>**Workstation "Impersonation"**: A user modifies the network address of a workstation so that the request sent by the modified workstation appear to be from the "impersonated" workstation. 工作站冒充：用户修改工作站的网络地址，使修改后的工作站发送的请求似乎是来自"冒充的"工作站。

<3>**A user eavesdrop on information exchanges and use a replay attack to gain entrance to a server** (or disrupt operations).用户窃听信息交换，并使用重播攻击来获得进入服务器（或中断操作）。

(3)Kerberos Approach

<1>Kerberos provides a centralised authentication server that authenticates

Kerberos 提供了一个可进行身份验证的集中身份验证服务器

功能 to authenticate

– User to servers

– Servers to users

- Network Authentication Protocol
- Developed at MIT in the mid 1980s.
- Available as open source or in supported commercial software.

<2>Kerberos uses conventional encryption (DES). There are two versions of Kerberos:

Kerberos 使用了传统的加密技术（DES）（只依赖于对称（传统）加密，不使用 public-key 加密）。

– Version 4: Is the 'original' Kerberos as versions 1-3 were internal development versions. This version still exists in many applications.是"原始的"Kerberos，因为版本 1-3 是内部开发版本。这个版本仍然存在于许多应用程序中

– Version 5: Corrects some of the security deficiencies found in version 4.

纠正了在版本 4 中发现的一些安全缺陷

(4)Motivation

• For the authentication of dedicated user workstations (clients) and distributed or centralised servers we can do the following: 对于专用用户工作站（客户端）和分布式或集中服务器的身份验证（组成的体系结构），我们可以执行以下操作：（有三种安全方式）

<1>Rely on clients to assure identify of its user(s) and rely on each server to enforce the security policies (based on ID). 依赖于客户端来确保其用户的身份，并依赖于每个服务器来强制执行安全策略（基于 ID)。

<2>Require that client systems authenticate themselves to servers. Trust the client system concerning the identity of the user. 要求客户端系统对服务器进行自身身份验证。但就其用户的身份信任客户端系统

<3>Require the user to prove identity for each service invoked. Require that servers prove their identity to clients (The Kerberos Approach)要求用户为被调用的每个服务证明其身份。还要求服务器向客户机证明它们的身份。

注意：在小的封闭环境中<1><2>足够，但是，在一个支持与其他机器的网络连接的更开放的环境中，需要第三种方法来保护位于服务器上的用户信息和资源。Kerberos 支持该方法，Kerberos 采用 distributed client/server architecture，并使用一个或多个 Kerberos 服务器来提供身份验证服务。

(5)Requirements

<1>**Secure**: Should cope with external attacks. 应对外部攻击

<2>**Reliable**: Kerberos should be highly reliable and should employ distributed server architecture. One system able to back up another. Kerberos 应该是高度可靠的，并且应该采用分布式服务器架构。一个系统能够备份另一个系统。

<3>**Transparent**: Apart from the password, a user should not be aware of the authentication is taking place. 透明的：除了需要密码外，用户不应该知道正在进行的身份验证

<4>**Scalable**: As the network grows, there should be a method which allows such growth.

可扩展性：随着网络的增长，应该有一种方法来允许这种增长。

(6)Simple Authentication

<1>**A simple authentication is when a new student wants to use the university library**. Before it can use the library 一个简单的身份验证是当一个新学生想使用大学图书馆。在它可以使用之前需要：

– The student identifies himself/herself with the university administration.

这个学生认为自己属于大学的管理部门。

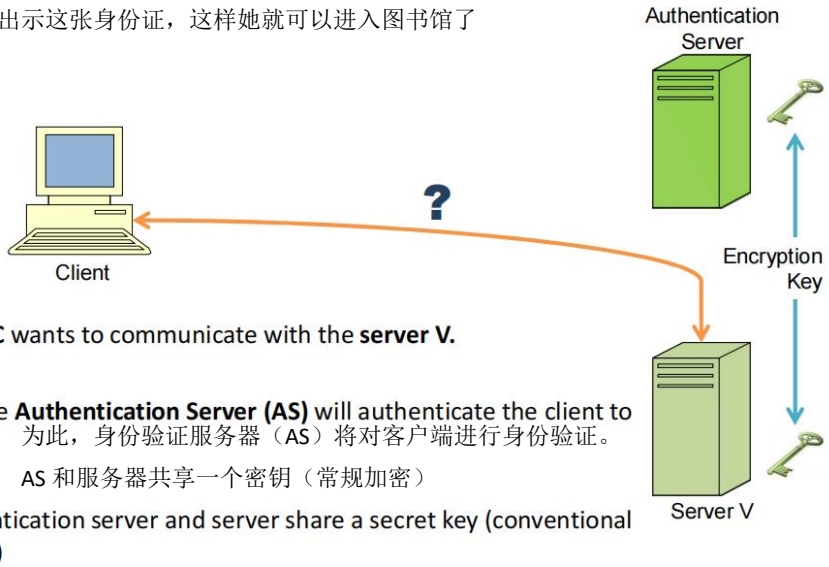
– The administration check the students details. If a valid student, then it provides him/her with a student ID card.

行政部门会检查学生的详细资料。如果是一个有效的学生，那么它会给他/她一张学生身份证

– The student goes to the library and shows this ID card so she/h has access to the library.

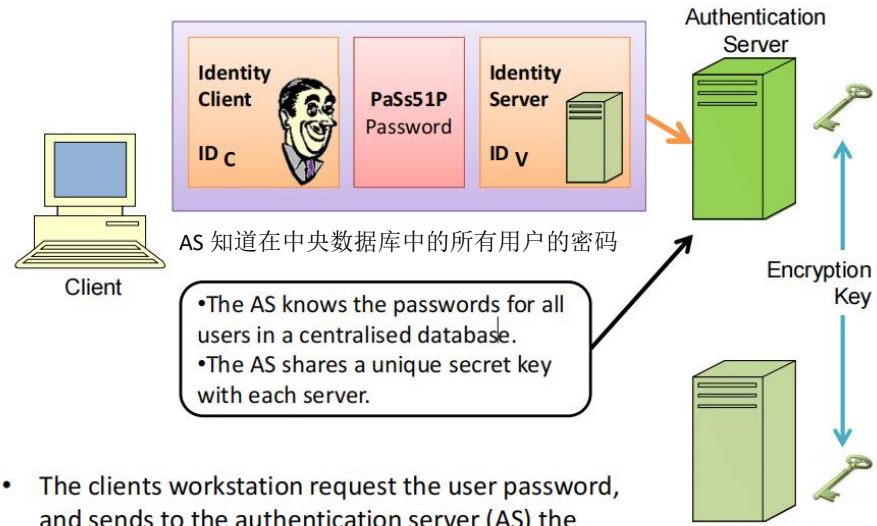
学生去图书馆，出示这张身份证，这样她就可以进入图书馆了

<2>过程



- The **client C** wants to communicate with the **server V.**
- To do so the **Authentication Server (AS)** will authenticate the client to the server. 为此，身份验证服务器（AS）将对客户端进行身份验证。

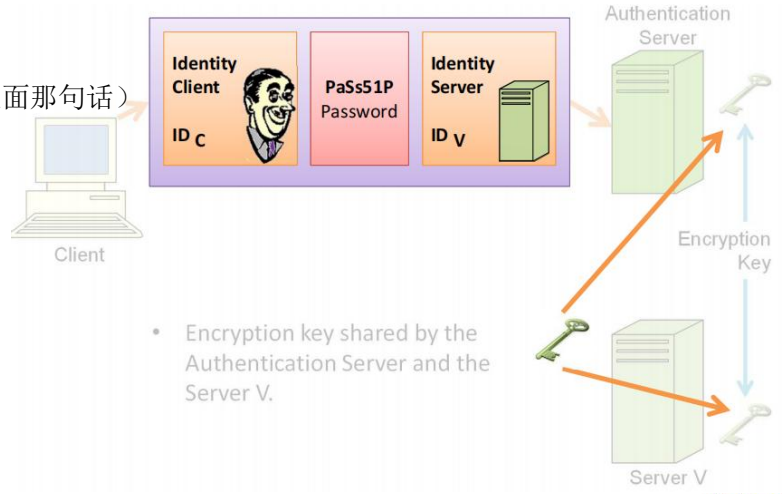
  AS 和服务器共享一个密钥（常规加密）
- The Authentication server and server share a secret key (conventional encryption)



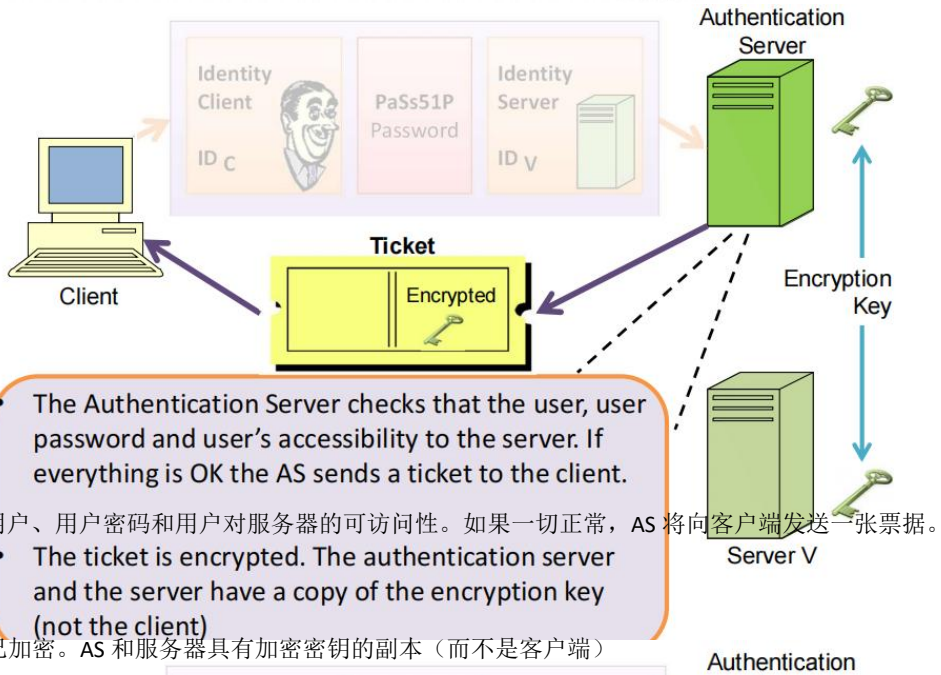
- The clients workstation request the user password, and sends to the authentication server (AS) the

AS 与每个服务器共享一个唯一的密钥

客户端工作站请求用户密码，并将用户 ID、用户密码和服务器 ID 发送给身份验证服务器（AS）

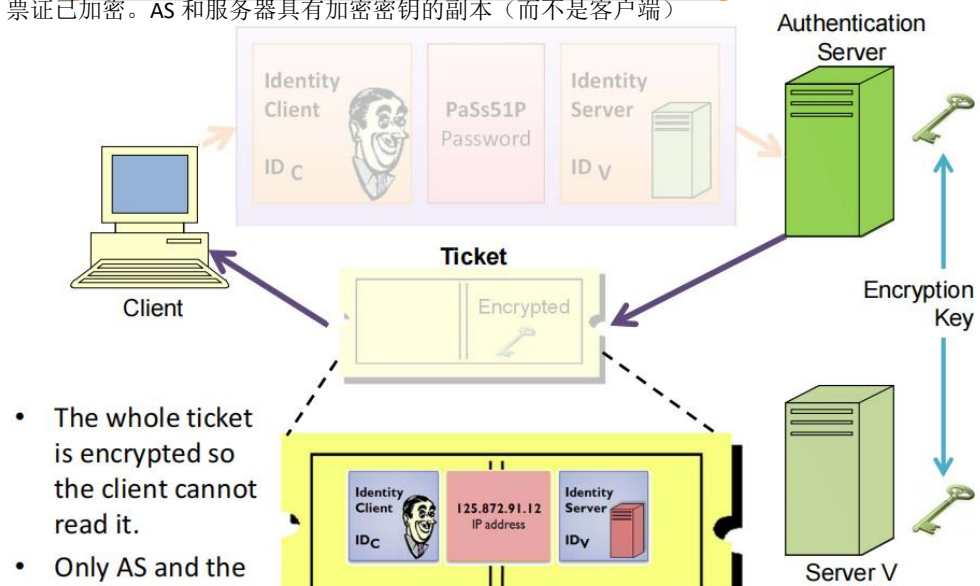


（解释上面那句话）



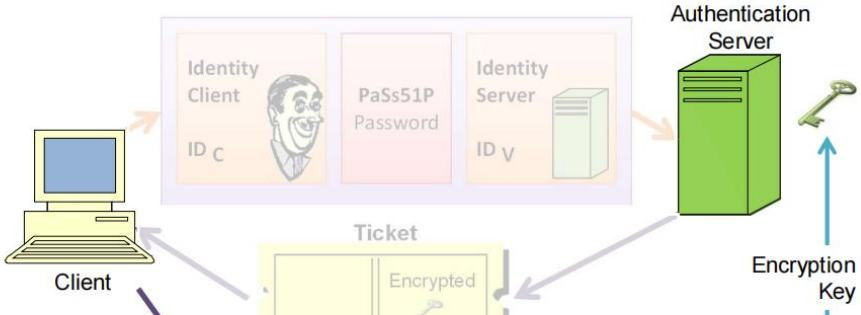
AS 将检查用户、用户密码和用户对服务器的可访问性。如果一切正常，AS 将向客户端发送一张票据。

票证已加密。AS 和服务器具有加密密钥的副本（而不是客户端）



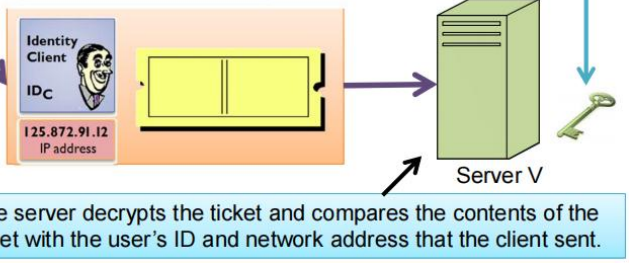
整个票证都是加密的，因此客户端无法读取它

只有 AS 和服务器 V 可以读取票据



客户端为了获得对服务器 V 的访问权限，会将其 ID、工作站地址和票证发送给服务器。

- The client, to gain access to the server V, sends to the server its ID, the address of the workstation and the ticket.



服务器对票证进行解密，并将票证的内容与客户端发送的用户 ID 和网络地址进行比较

<3>Simple Authentication Dialogue

(1) C → AS: $ID_C \| P_C \| ID_V$

(2) AS → C: $Ticket$

(3) C → V: $ID_C \| Ticket$

$Ticket = E(K_v, [ID_C \| AD_C \| ID_V])$

C = client
AS = authentication server
V = server
ID_C = identifier of user on C
ID_V = identifier of V
P_C = password of user on C
AD_C = network address of C
K_v = secret encryption key shared by AS and V

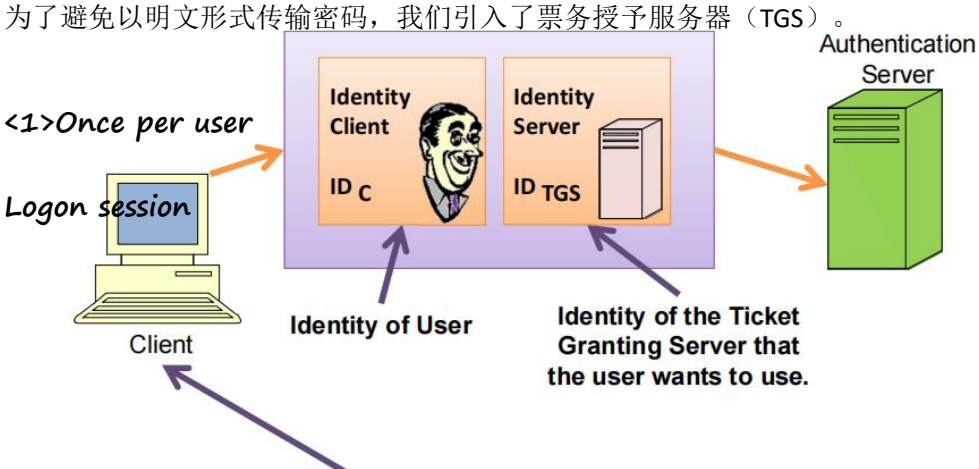
<4>Problems（中途拦截地址）

- Try to minimise the number of times a user enters a password. 尽量减少用户输入密码的次数。
- Plaintext transmission of the password.密码的明文传输

(7)More Secure Authentication

To avoid transmitting the password as plaintext we introduce the Ticket Granting Server (TGS).
为了避免以明文形式传输密码，我们引入了票务授予服务器（TGS）。

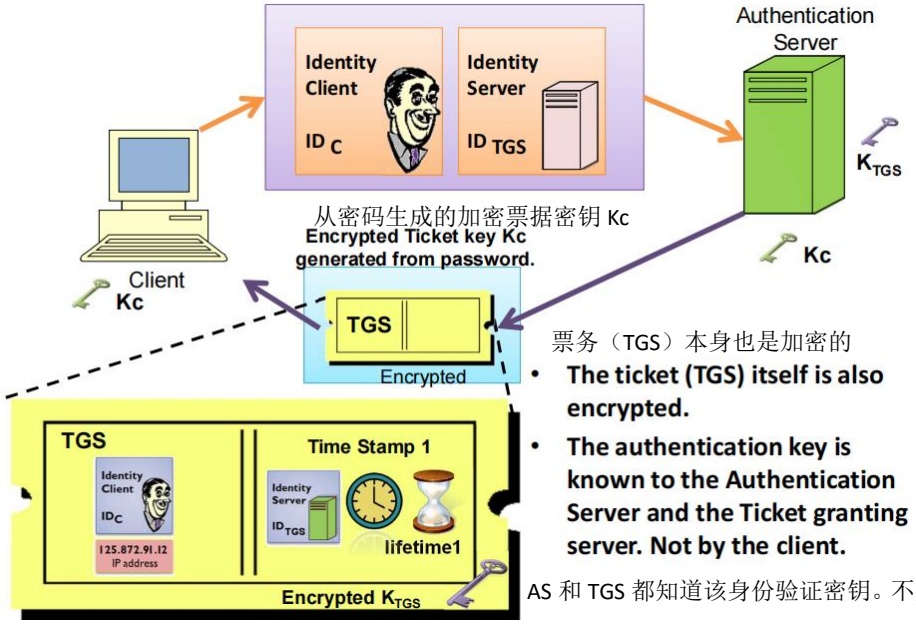
<1>Once per user



用户要使用的 TGS 的标识

客户端请求身份验证服务器（AS）代表用户授予票务授予票单。

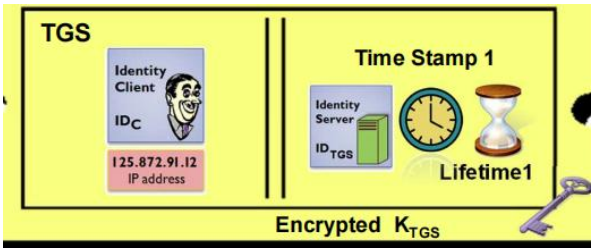
Once per user logon 每次用户登陆一次



票务（TGS）本身也是加密的

- **The ticket (TGS) itself is also encrypted.**
- **The authentication key is known to the Authentication Server and the Ticket granting server. Not by the client.**

AS 和 TGS 都知道该身份验证密钥。不是客户提供的。



• AS sends the ticket-granting service (TGS) ticket, the whole ticket is double encrypted First with using a key known to AS and the ticket granting server, then using a key generated by the password.

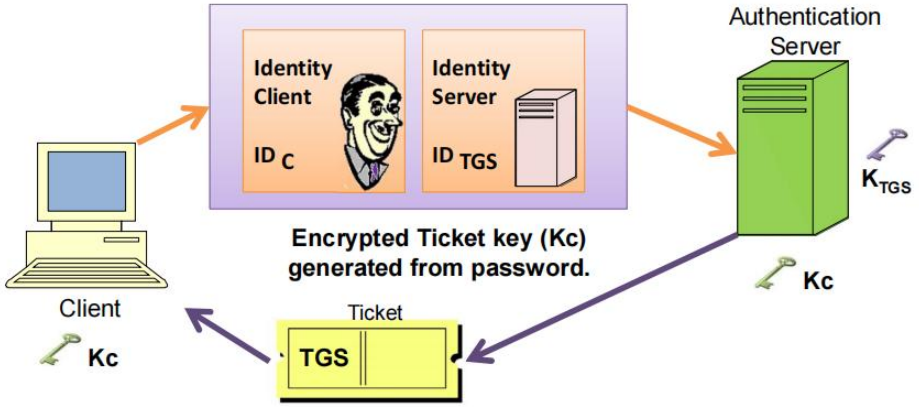
AS 发送票授予服务（TGS）票，整个票进行双重加密。首先使用 AS 已知的密钥和票务授予服务器，然后使用由密码生成的密钥。

• The encryption key Kc is generated from the password of the user (AS knows the password). Notice that the password never transmitted.

加密密钥 Kc 由用户的密码生成(AS 知道密码）。请注意，密码从未传递。

• The ticket contains an IP address, a time stamp and a lifetime.

票据包含一个 IP 地址、一个时间戳和一个生命周期。

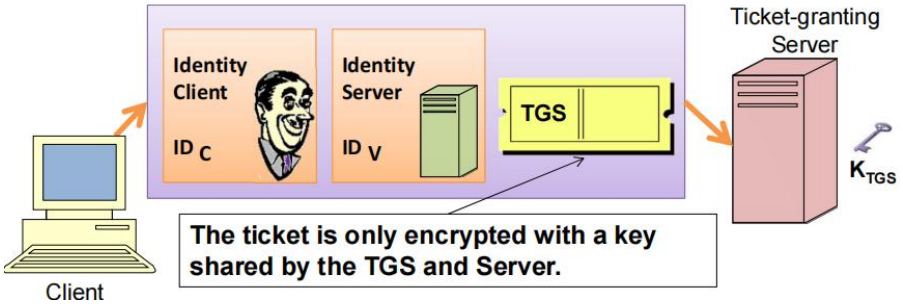


- **The client ask the users for his/her password, generates the key Kc, and recovers the TGS ticket.**

客户端向用户查询其密码，生成密钥 Kc，并恢复 TGS 票据。

AS 和 User 之间的身份验证使用 Kc 完成。

<2>Once per type of service



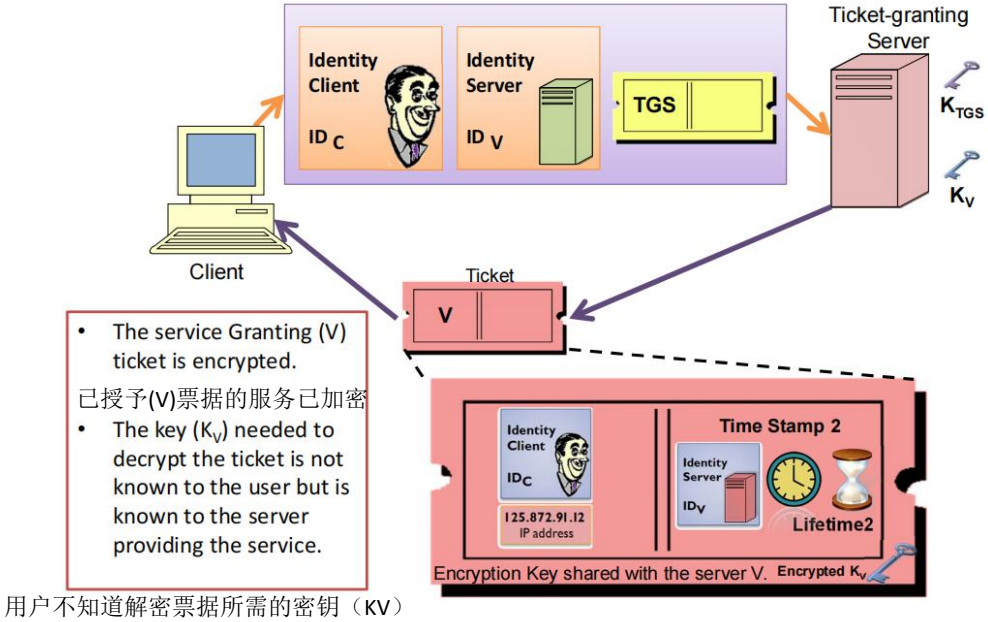
• The client request from Ticket Granting Service a service-granting ticket.

客户端向 TGS 请求一个服务授予的票据

• It sends the user's ID, the desire service ID and the ticket-granting ticket.

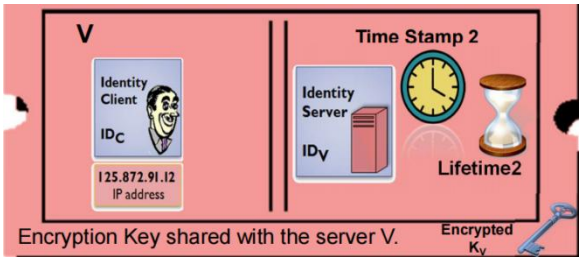
它发送用户的 ID、服务 ID 和授予票据

• The TGS decrypts the ticket-granting ticket (using KTGS). Authenticates the user (comparing the incoming information and ticket information) and checks if the user has access to the requested server. TGS also checks if the lifetime has not expired. TGS 解密票据（使用 KTGS）。对用户进行身份验证（比较输入的信息和票据信息），并检查用户是否可以访问所请求的服务器。TGS 还将检查该生命周期是否过期。



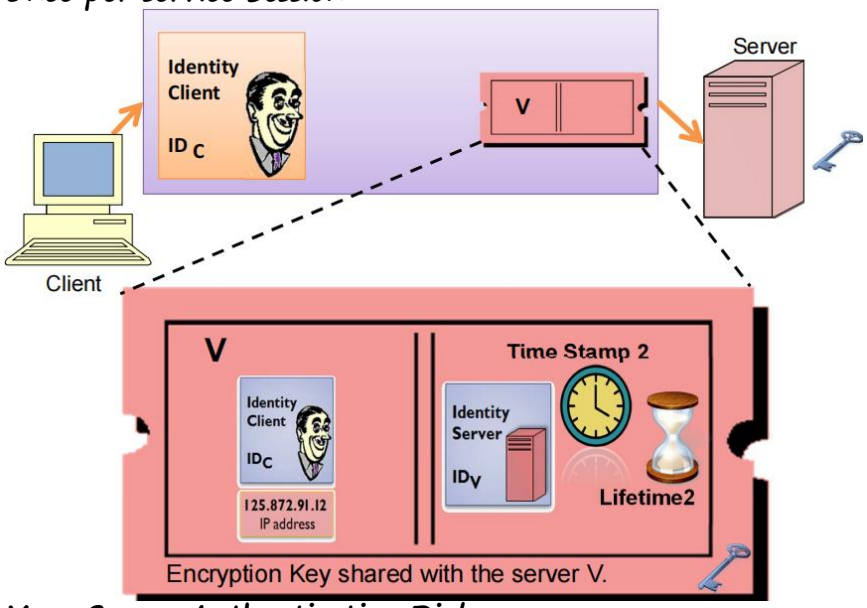
用户不知道解密票据所需的密钥（KV）

但提供该服务的服务器知道它



• The service-granting ticket (V) is encrypted. The encryption key KV is known by the service granting server and the server.
服务授予票据(V)已被加密。加密密钥 KV 由服务授予服务器和服务器所知道
• The ticket contains a time stamp and lifetime.该票据包含一个时间戳和一个生命周期

<3>Once per service Session



<4>More Secure Authentication Dialogue

Once per user logon session:

(1) $C \rightarrow AS: \quad ID_C \| ID_{tgs}$
(2) $AS \rightarrow C: \quad E(K_c, Ticket_{tgs})$

Once per type of service:

(3) $C \rightarrow TGS: \quad ID_C \| ID_V \| Ticket_{tgs}$
(4) $TGS \rightarrow C: \quad Ticket_v$

Once per service session:

(5) $C \rightarrow V: \quad ID_C \| Ticket_v$

$$Ticket_{tgs} = E(K_{tgs}, [ID_C \| AD_C \| ID_{tgs} \| TS_1 \| Lifetime_1])$$
$$Ticket_v = E(K_v, [ID_C \| AD_C \| ID_v \| TS_2 \| Lifetime_2])$$

This new scenario satisfies the two requirements of only one password query per user session and protection of the user password.

<5>Problems

• Lifetime of the ticket
– Short lifetimes means the user has to type password often.短意味着用户必须经常输入密码
– Long lifetimes means that the user has greater opportunity to replay.

长意味着用户有更大的机会被重放攻击。

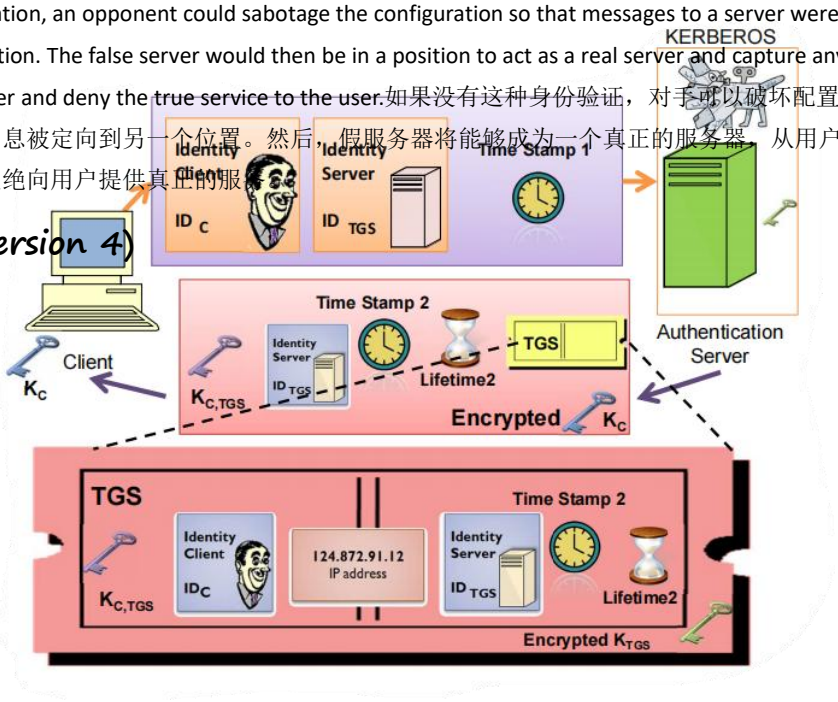
所以针对以上要求！A network service (the TGS or an application service) must be able to prove that the person using a ticket is the same person to whom that the ticket was issued.

网络服务（TGS 或应用程序服务）必须能够证明使用票证的人是签发票证的同一个人

• Server does not authenticate to users. (Why is this a problem?)服务器不向用户进行身份验证

Without such authentication, an opponent could sabotage the configuration so that messages to a server were directed to another location. The false server would then be in a position to act as a real server and capture any information from the user and deny the true service to the user.如果没有这种身份验证，对手可以破坏配置，以便发送到服务器的消息被定向到另一个位置。然后，假服务器将能够成为一个真正的服务器，从用户那里获取任何信息，并拒绝向用户提供真正的服务。

(8)Kerberos (version 4)



<1>The client requests access to TGS. It sends the user's ID, the TGS ID and a time-stamp.

客户端请求访问 TGS。它发送用户的 ID、TGS ID 和一个时间戳。

<2>AS responds with an encrypted message. The encryption key is derived from the user's password. The message contains a copy of the session key $K_{C,TGS}$ (the key is generated by AS and used by the client and TGS) and a ticket. The ticket contains a copy of this session key.

AS 以一条加密的消息进行响应。加密密钥来源于用户的密码。该消息包含会话密钥 KC、TGS（该密钥由 AS 生成并由客户端和 TGS 使用）和票据的副本。该票据包含此会话密钥的副本。

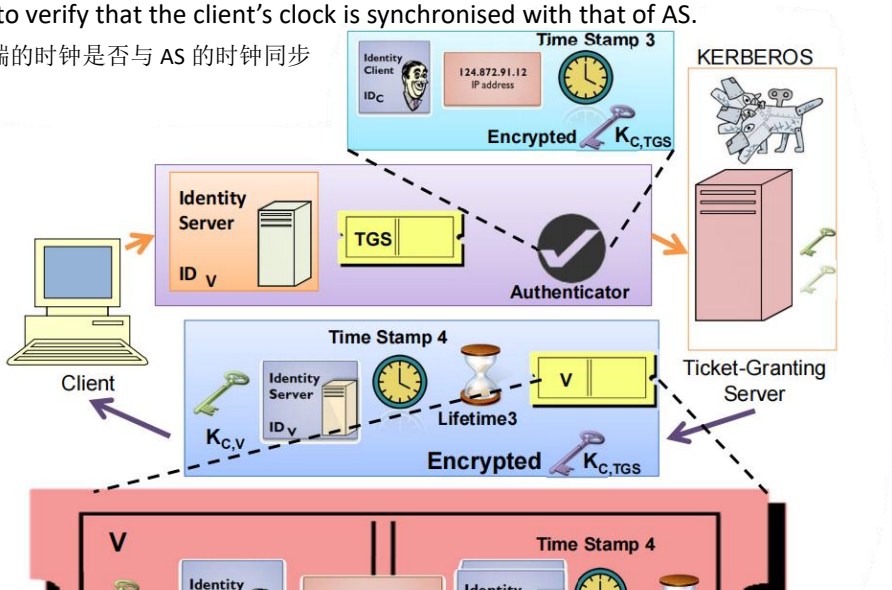
<3>The ticket is encrypted. The key for the ticket (d) encryption is known to AS and TGS (not the client).票证已加密。AS 和 TGS（而不是客户端）知道票据(d)加密的密钥。

<4>The session key shared by the client and TGS is used by the client to prove its' identity to TGS.

客户端和 TGS 共享的会话密钥被客户端用来向 TGS 证明其身份。

<5>The time stamp is to verify that the client's clock is synchronised with that of AS.

时间戳是为了验证客户端的时钟是否与 AS 的时钟同步



<6>The client request from TGS a service-granting ticket. It sends the user's ID, the desire service ID, the ticket-granting ticket and an authenticator. The authenticator has a very short lifetime and is used to authenticate the user.客户端请求 TGS 一个服务授予票据。它发送用户的 ID、愿望服务 ID、票据授予票证和身份验证器。身份验证器的使用寿命很短，可用于对用户进行身份验证。

<7>The TGS, decrypts the authenticator using the session key $K_{C,TGS}$ and compares the user's name, address from the authenticator with the ones of the ticket, the ticket is decrypted first. (The authenticator says "at time T3 , I hereby use $K_{C,TGS}$). TGS 使用会话密钥 KC、TGS 解密身份验证器，并将用户名、来自验证器的地址与票据中的地址进行比较，首先解密票据。（认证者说："在 T3 时刻，我在此使用 KC，TGS）。"

<8>The reply of TGS includes a new client-server session key (generated by TGS) plus the user's ID, the service-granting ticket and a time-stamp. All these information is encrypted using the session key shared by the TGS and the client. TGS 的回复包括一个新的客户端-服务器会话密钥（由 TGS 生成）加上用户的 ID、服务授予票证和一个时间戳。所有这些信息都使用 TGS 和客户端共享的会话密钥进行加密。

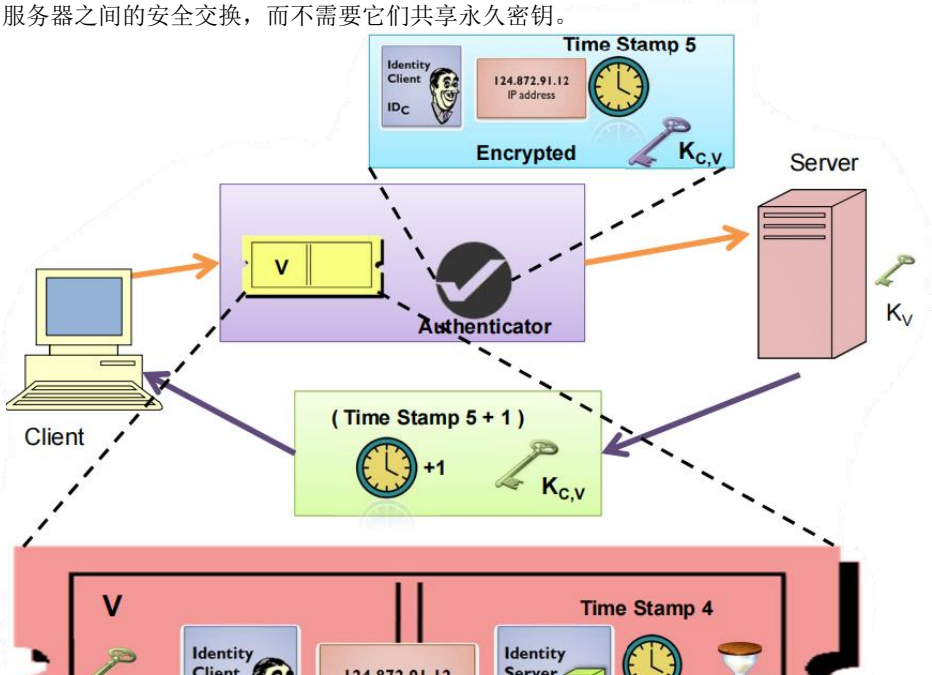
<9>The service-granting ticket is encrypted. The key is known to the server and TGS (not the client). 服务授予票据已被加密。服务器和 TGS（而不是客户端）都知道该密钥。

<10>The ticket-granting ticket assures TGS that this user has been authenticated by AS. 票据授予票据向 TGS 保证该用户已通过 AS 进行了身份验证。

<11>The authenticator is generated by client to validate the ticket Assures TGS that the ticket presenter is the same as the client whom the ticket was issued.身份验证器由客户端生成，以验证票据，确保 TGS 的票证呈现者与发出票据的客户端相同。

<12>The session key shared by client and TGS protects the contents of the message. Is used by TGS to decrypt the authenticator, thereby authenticating the request. 由客户端和 TGS 共享的会话密钥可以保护消息的内容。被 TGS 用来解密身份验证器，从而进行身份验证请求。

<13>A copy of the session key accessible to client. Used for secure exchange between the client and server without requiring them to share a permanent key.客户端可访问的会话密钥的副本。用于客户机和服务器之间的安全交换，而不需要它们共享永久密钥。



<14>The client requests access to the server. It sends the service-granting ticket and an authenticator. 客户端请求访问该服务器。它发送服务授予票据和一个身份验证器

<15>The authenticator contains the user's ID, the address and a time stamp. The authenticator is encrypted with the client-server session key. 身份验证器包含用户的 ID、地址和时间戳。身份验证器使用客户端-服务器会话密钥进行加密。

<16>The server authenticates the information by comparing the contents of the ticket and the content of the authenticator. 服务器通过比较票据的内容和身份验证器的内容来对信息进行身份验证

<17>The ticket is decrypted using the key that is shared by the server and the TGS.
使用服务器和 TGS 共享的密钥解密票据。

<18>If mutual authentication is required, the server sends the time-stamp plus one. This message is encrypted with the session key
如果需要相互身份验证，则服务器将发送时间戳加上 1。此消息使用会话密钥进行加密

<19>Kerberos v4 structure

- A basic third-party authentication scheme 一个基本的第三方认证方案
- Have an Authentication Server (AS) 具有身份验证服务器（AS）
  – Users initially negotiate with AS to identify self 用户最初与 AS 协商以确定自我身份
  – AS provides a non-corruptible authentication credential (ticket granting ticket TGT)
  AS 提供不可损坏的认证凭据（票据授予票证 TGT)
- Have a Ticket Granting server (TGS) 拥有一个票务授予服务器（TGS）
  – Users subsequently request access to other services from TGS on basis of users TGT
  用户随后根据用户 TGT 请求从 TGS 访问其他服务
- Using a complex protocol using DES 使用使用 DES 的复杂协议

<20>Kerberos v4 Dialogue

(1) $C \rightarrow AS \quad ID_c \| ID_{tgs} \| TS_1$

(2) $AS \rightarrow C \quad E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) $C \rightarrow TGS \quad ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) $TGS \rightarrow C \quad E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) $C \rightarrow V \quad Ticket_v \| Authenticator_c$

(6) $V \rightarrow C \quad E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

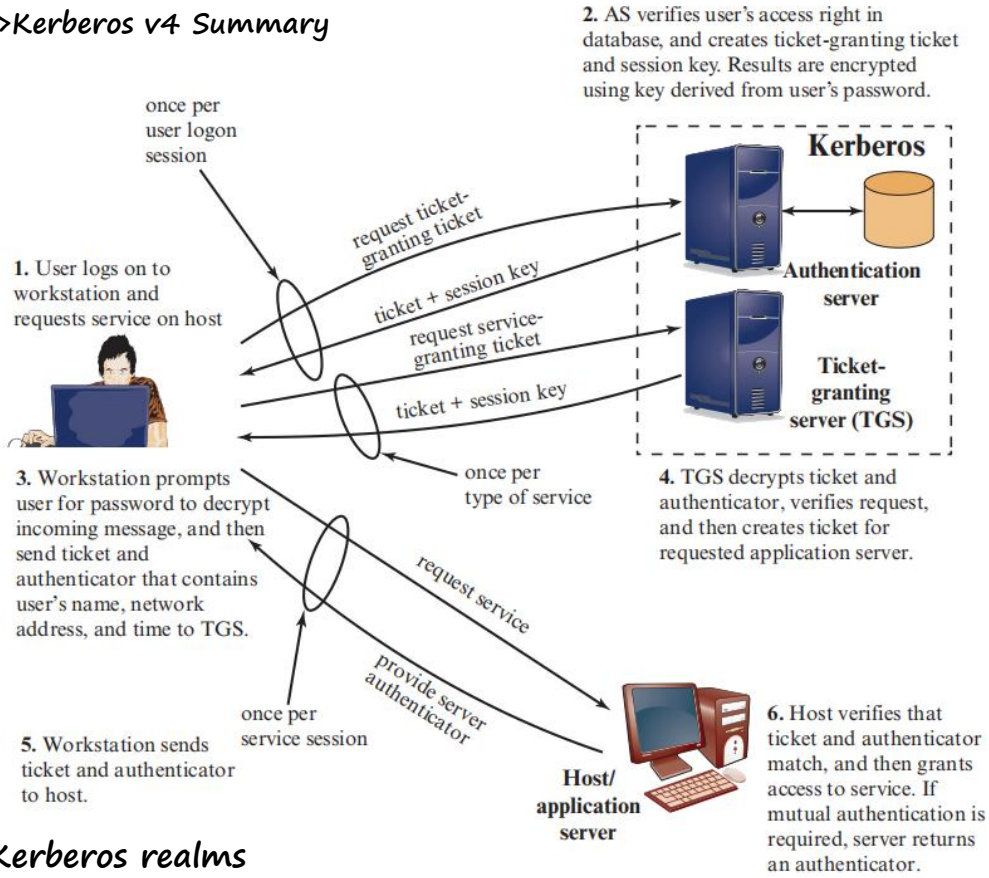
$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$

(c) Client/Server Authentication Exchange to obtain service

C = Client
AS = authentication server
V = server
IDc = identifier of user on C
IDv = identifier of V
Pc = password of user on C

ADc = network address of C
Kv = secret encryption key shared by the TGS and V
TS = timestamp
|| = concatenation

<21>Kerberos v4 Summary



(9)Kerberos realms

<1> Kerberos Environment（全服务环境）要求两点

• Consist of a Kerberos server, a number of clients, and a number of application servers. This environment is called realm. With the following:

由 Kerberos 服务器、许多客户端和许多应用程序服务器组成。这个环境被称为领域。使用以下内容：

– The Kerberos server must have the ID and password of all users. All users are registered with the Kerberos server. Kerberos 服务器必须具有所有用户的 ID 和密码。所有用户都已在 Kerberos 服务器上注册。

– The Kerberos server must share secret keys with each server. All servers are registered with the Kerberos server. Kerberos 服务器必须与每个服务器共享密钥。所有服务器都已在 Kerberos 服务器上注册

<2>Kerberos realms

– For inter-realm authentication the Kerberos server in each realm shares a secret key with the server in the other realm. The two Kerberos server are registered with each other.

对于跨领域的身份验证，每个领域中的 Kerberos 服务器与另一个领域中的服务器共享一个密钥。两个 Kerberos 服务器相互注册。

(1) $C \rightarrow AS$: $ID_c \| ID_{tgs} \| TS_1$

(2) $AS \rightarrow C$: $E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

(3) $C \rightarrow TGS$: $ID_{tgsrem} \| Ticket_{tgs} \| Authenticator_c$

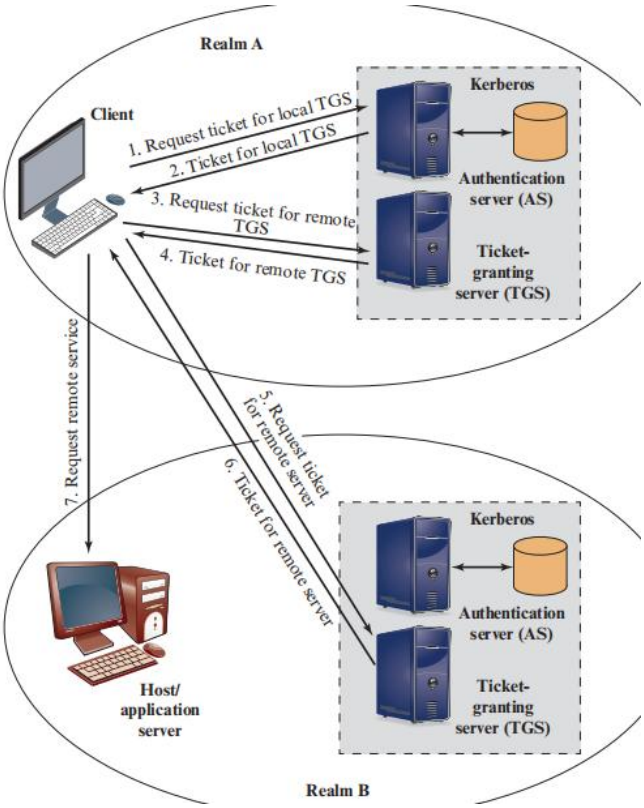
(4) $\text{TGS} \rightarrow \text{C}$: $E(K_{c,tgs}, [K_{c,tgsrem} \| ID_{tgsrem} \| TS_4 \| Ticket_{tgsrem}])$

(5) $\text{C} \rightarrow \text{TGS}_{\text{rem}}$: $ID_{vrem} \| Ticket_{tgsrem} \| Authenticator_c$

(6) $\text{TGS}_{\text{rem}} \rightarrow \text{C}$: $E(K_{c,tgsrem}, [K_{c,vrem} \| ID_{vrem} \| TS_6 \| Ticket_{vrem}])$

(7) $\text{C} \rightarrow \text{V}_{\text{rem}}$: $Ticket_{vrem} \| Authenticator_c$

The ticket presented to the remote server (Vrem) indicates the realm in which the user was originally authenticated. The server chooses whether to honor the remote request. 提供给远程服务器（Vrem）的 ticket 指示对用户最初进行身份验证的领域。服务器将选择是否接受远程请求。



<3>One problem presented by the foregoing approach is that it does not scale well to many realms. If there are N realms, then there must be N(N - 1)/2 secure key exchanges so that each Kerberos realm can interoperate with all other Kerberos realms.
上述方法提出的一个问题是，它不能很好地扩展到许多领域。如果有 N 个领域，那么必须有 N 个（N - 1）/2 个安全的密钥交换，这样每个 Kerberos 领域都可以与所有其他 Kerberos 领域互操作。

(10)Kerberos version 5

<1>Developed in mid 1990's
<2>Specified as Internet standard RFC 1510
<3>Provides the following improvements over version 4

– Environmental

- Any encryption technique can be used (not only DES)可以使用任何加密技术（而不仅仅是 DES)
- Different network address type can be used (not only IP)可以使用不同的网络地址类型（而不仅仅是 IP）
- Unambiguous byte ordering 明确的字节排序
- Longer ticket lifetimes 更长的票据寿命

• Authentication forwarding 身份验证向前

• Inter-realm authentication.领域间身份验证

– Technical

• Avoid double encryption 避免双重加密

• CBC mode of operation instead of PCBC. CBC 的操作模式，而不是 PCBC。

• Sub-session keys for client and server (better security) 针对客户机和服务器的子会话密钥（更好的安全性）

• Improvements against password attacks. 改进以对抗密码攻击

<4>Kerberos v5 Dialogue

(1) C → AS $Options \| ID_c \| Realm_c \| ID_{tgs} \| Times \| Nonce_1$

(2) AS → C $Realm_C \| ID_C \| Ticket_{tgs} \| E(K_c, [K_{c,tgs} \| Times \| Nonce_1 \| Realm_{tgs} \| ID_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS $Options \| ID_v \| Times \| Nonce_2 \| Ticket_{tgs} \| Authenticator_c$

(4) TGS → C $Realm_c \| ID_C \| Ticket_v \| E(K_{c,tgs}, [K_{c,v} \| Times \| Nonce_2 \| Realm_v \| ID_v])$

$Ticket_{tgs} = E(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$

$Ticket_v = E(K_v, [Flags \| K_{c,v} \| Realm_c \| ID_C \| AD_C \| Times])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| Realm_c \| TS_1])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V $Options \| Ticket_v \| Authenticator_c$

(6) V → C $E_{K_{c,v}}[TS_2 \| Subkey \| Seq\ \#]$

$Ticket_v = E(K_v, [Flag \| K_{c,v} \| Realm_c \| ID_C \| AD_C \| Times])$

$Authenticator_c = E(K_{c,v}, [ID_C \| Relam_c \| TS_2 \| Subkey \| Seq\ \#])$

(c) Client/Server Authentication Exchange to obtain service

Realm: Indicates realm of user

Options: Used to request that certain flags be set in the returned ticket

Times: Used by the client to request the following time settings in the ticket:

—**from**: the desired start time for the requested ticket

—**till**: the requested expiration time for the requested ticket

—**rtime**: requested renew-till time

Nonce: A random value to be repeated in message (2) to assure that the response is fresh and has not been replayed by an opponent

Subkey: The client's choice for an encryption key to be used to protect this specific application session. If this field is omitted, the session key from the ticket ($K_{c,v}$) is used.

客户端选择了一个用于保护此特定应用程序会话的加密密钥。如果省略此字段，则会使用票据中的会话键（Kc、v）。

Sequence number: An optional field that specifies the starting sequence number to be used by the server for messages sent to the client during this session. Messages may be sequence numbered to detect replays.

一个可选字段，用于指定服务器在此会话期间发送给客户端的消息所使用的起始序号。消息可以用序列编号来检测回放。

(11)Summary • Kerberos

– **Definition**: Kerberos is an authentication service designed for use in a distributed environment.

Kerberos 是一种设计用于在分布式环境中使用的身份验证服务

– **Uses**: It makes use of a trusted third-party authentication service that enables clients and servers to establish authenticated communication.

它利用一个受信任的第三方身份验证服务，使客户端和服务器能够建立经过身份验证的通信。

三. IP Security Security at the IP layer

• There are many application-specific security mechanism in a number of application areas, e.g. Electronic mail (S/MIME,PGP), client/server (Kerberos), Web access (Secure Socket Layer) etc.

在许多应用程序领域中有许多特定于应用程序的安全机制，例如电子邮件（S/MIME、PGP）、客户端/服务器（Kerberos）、Web 访问（安全套接字层）等。

• Security at the IP level (IPSec) can ensure security not only for applications that have security mechanisms but for many security-ignorant application. IP 级的安全性（IPSec）不仅可以确保具有安全机制的应用程序的安全性，而且还可以确保许多不依赖安全的应用程序的安全性

1. IPSec

(1)

• IP security is built into the IP layer. IP 安全性被内置到 IP 层中

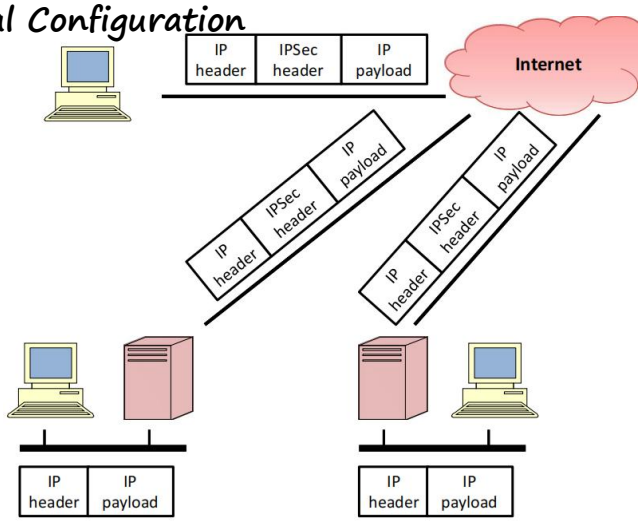
• IPSec can encrypt and/or authenticate all traffic at the IP authentication. Comprised of two pairs: IPSec 可以在 IP 身份验证中加密和/或身份验证所有流量。由两对组成：

– IPSEC proper (authentication and encryption) IPSEC 正确的（身份验证和加密）

– IPSEC key management IPSEC 密钥管理

• Required for IPv6, optional for IPv4. IPv6 需要，IPv4 可选。

(2)IPSec Typical Configuration



• An organisation keeps LANs at dispersal locations.一个组织将局域网保持在分散的位置。

• The IPSec protocols operate in networking devices (routers, Firewalls).

IPSec 协议在网络设备（路由器、防火墙）中运行

• Applications 应用 （1）中黄色部分是原因

– Secure LAN and WAN connectivity i.e. a VPN in college. 安全的局域网和广域网连接，即在大学里的 VPN。

– Secure remote access. 安全的远程访问

– Secure communication with other organisations. 确保与其他组织的安全沟通。

– E-commerce security.电子商务安全。

•IPsec encompasses three functional areas: authentication, confidentiality, and key management.

(3)IPSec Benefits

• Combined with a Firewall or router it provides strong security to all traffic crossing the perimeter.结合防火墙或路由器，它为所有越过周边的交通提供了强大的安全性。

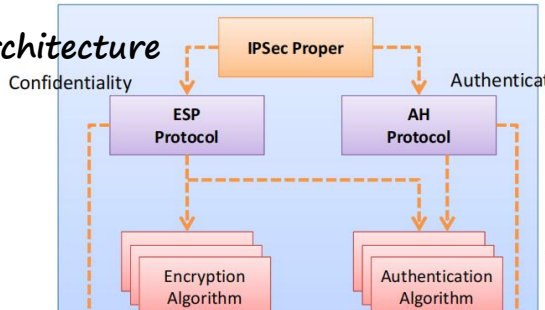
• IPSec in a Firewall is resistant to bypass if all traffic from the outside must use IP and the Firewall is the only gate from the Internet.如果防火墙中的所有外部流量都必须使用 IP，并且防火墙是来自互联网的唯一门，那么该防火墙中的 IPSec 将无法绕过。

• IPSec is below the transport layer (TCP, UDP), hence is transparent to applications.

IPSec 位于传输层以下（TCP，UDP）之下，因此对应用程序是透明的

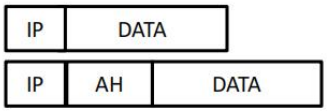
• IPSec is transparent to end users. IPSec 对最终用户是透明的。

(4)IPSec Architecture

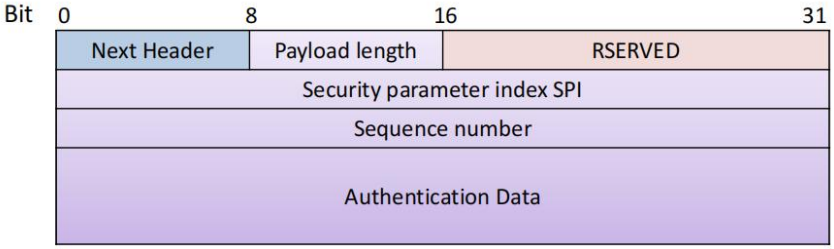


- Encapsulate Security Payload (ESP)
- Authentication Header (AH)

<1>Authentication Header (AH)



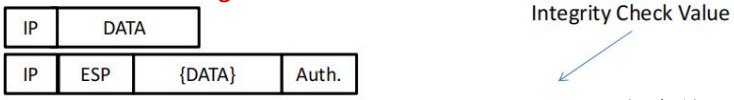
• Integrity protection only. 完整性保护
• Inserted in the datagram 插入数据报
– Integrity check value (ICV) is 96-bit HMAC. 完整性检查值（ICV）为 96 位 HMAC
– Authenticates entire datagram; 验证整个数据报
  • Mutable fields (time-to-live, IP checksums) are ignored before the AH is added.
    在添加 AH 之前，将忽略可变字段（实时时间、IP 校验和）



AH is an extension header to provide message authentication. Because message authentication is provided by ESP, the use of AH is deprecated. It is included in IPsecv3 for backward compatibility but should not be used in new applications. AH 是一个提供消息身份验证的扩展头。因为消息认证是由 ESP 提供的，所以不赞成使用 AH。它包含在 IPsecv3 中，是为了向后兼容，但不应该在新的应用程序中使用。

<2>Encapsulating Security Payload (ESP)

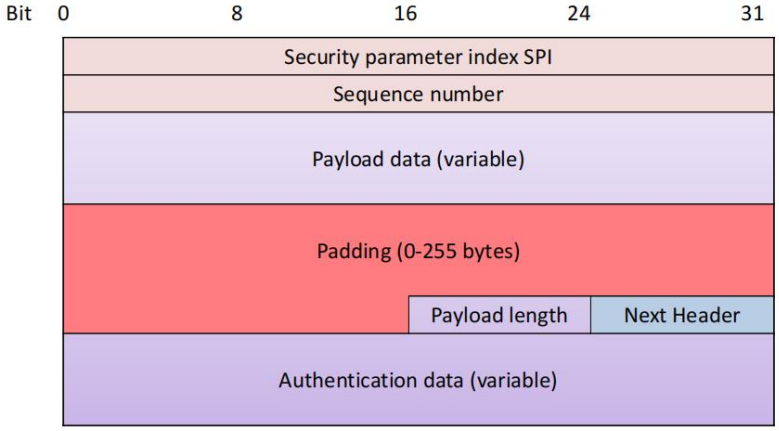
• Provides authentication (optional) and confidentiality 提供身份验证（可选）和机密性
• Inserted in the datagram



Contains sequence numbers and optional ICV as for AH. 包含关于 AH 的序列号和可选的 ICV。
• Encryption protects payload 加密保护有效载荷
• Authentication protects header and encryption 身份验证可保护报头和加密

■ **Security Parameters Index (32 bits)**: Identifies a security association.

■ **Sequence Number (32 bits):** A monotonically increasing counter value; this provides an anti-replay function, as



discussed for AH.一个单调递增的计数器值；这提供了一个反重放函数，如对 AH 所讨论的

■ **Payload Data (variable):** This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.

这是一个受加密保护的传输级段（传输模式）或 IP 数据包（隧道模式）。

■ **Padding (0–255 bytes):** The purpose of this field is discussed later.

■ **Pad Length (8 bits)**: Indicates the number of pad bytes immediately preceding this field.

指示紧邻此字段前面的 pad 字节数。

■ **Next Header (8 bits)**: Identifies the type of data contained in the payload data field by identifying the first header in that payload (e.g., an extension header in IPv6, or an upper-layer protocol such as TCP).

通过识别有效负载中的第一个头（例如 IPv6 中的扩展头或例如 TCP 的上层协议）来识别有效负载数据字段中包含的数据类型。

■ **Integrity Check Value (variable)**: A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field.

一个可变长度的字段（必须是一个 32 位字的整数），其中包含通过 ESP 数据包计算的完整性检查值减去身份验证数据字段

<3>IPSec Algorithms

• Encryption: DES in CBC mode　　CBC 模式下的 DES

• Authentication: HMAC/MD5 and HMAC/SHA (truncated to 96 bits)

Later versions added optional DOI-dependent algorithms 后来的版本添加了可选的依赖于 doi 的算法

• TDES • Blowfish • CAST-128 • IDEA • RC5

<4>Domain of Interpretation (DOI)

• The Internet Security Association and Key Management Protocol (ISAKMP) defines a framework for security association management and cryptographic key establishment for the Internet. This framework consists of defined exchanges, payloads, and processing guidelines that occur within a given Domain of Interpretation (DOI). This document defines the Internet IP Security DOI (IPSEC DOI), which instantiates ISAKMP for use with IP when IP uses ISAKMP to negotiate security associations.（ISAKMP）为互联网定义了一个安全协会管理和密码密钥建立的框架。这个 框架由发生在给定的解释领域（DOI）内的已定义的交换、有效负载和处理准则组成。本文档定义了互联网 IP 安全 DOI（IPSEC DOI），它实例化了 ISAKMP，以便在 IP 使用 ISAKMP 协商安全关联时与 IP 一起使用。

• Contains values to relate the different specifications of the protocol

包含用于关联协议的不同规范的值

– Identifiers for encryption and authentication algorithms 用于加密和身份验证算法的标识符

– Operational parameters, key lifetimes, key exchange etc.操作参数、钥匙寿命、钥匙交换等

(5)IPSec Services

	AH	ESP	
	AH	ESP encryption	ESP encryption with authentication
Access control	✓	✓	✓
Connectionless integrity	✓		✓
Data origin authentication	✓		✓
Rejection of replayed packets	✓	✓	✓
Confidentiality (encryption)		✓	✓
Limited traffic flow confidentiality		✓	✓

IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. Two protocols are used to provide security: an authentication protocol designated by the header of the protocol, Authentication Header (AH); and a combined encryption/ authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP).

(6)Security Association (SA)

<1>

• A one-way relationship between sender and receiver that describes a security service.
发送方和接收方之间描述安全服务的单向关系。

• For two-way exchange of data, two SAs are needed, from sender-to-receiver and receiver-to-sender.对于数据的双向交换，需要两个 sa，从发送者到接收者和接收者到发送者。

<2>SAs are defined by three parameters

Security Parameters Index (SPI)：A label (bit string) to identify the security association 用于标识安全关联的标签（位字符串）A 32-bit unsigned integer assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed. 分配给此 SA 且仅具有局部意义的 32 位无符号整数。SPI 是在 AH 和 ESP 头中携带的，使接收系统能够选择处理接收包的 SA

IP Destination Address：Only unicast This is the address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router.这是 SA 的目标端点的地址，它可以是最终用户系统或网络系统，如防火墙或路由器。

Security Protocol Identifier：AH or ESP

<3>Parameters which characterise the nature of a given SA

- Sequence Number Counter
- Sequence Counter Overflow
- Anti–Replay Window
- AH Information
- ESP Information
- Lifetime of this Security Association
- IPSec Protocol Mode: tunnel or transport
- Path MTU (maximum transmission unit)

1. Sequence Number Counter（序列号计数器）：在IPsec中，序列号计数器用于追踪发送的数据包顺序，以便检测和防止重放攻击。
2. Sequence Counter Overflow（序列计数器溢出）：指当序列号计数器达到其最大值时发生的情况。这可能会导致安全漏洞，因此需要采取预防措施。
3. Anti-Replay Window（抗重放攻击窗口）：用于确定可以接受的旧数据包的范围，以便检测和拒绝已经被截获并重新传输的数据包，从而防止重放攻击。
4. AH Information（认证标头信息）：指定IPsec认证标头的相关信息，用于验证数据包的完整性和真实性。
5. ESP Information（封装安全载荷信息）：指定IPsec封装安全载荷的相关信息，用于对数据包进行加密和认证。
6. Lifetime of this Security Association（安全关联的生存期）：指定安全关联（SA）的有效期，即在此时间段内，协议将为通信提供的安全性参数。
7. IPSec Protocol Mode: tunnel or transport（IPSec协议模式：隧道或传输）：指定了IPSec的工作模式，隧道模式用于整个IP包的加密和认证，而传输模式只对IP包的载荷进行加密和认证。
8. Path MTU (maximum transmission unit)（路径最大传输单元）：指在IPsec通信中，指定了可通过的最大传输单元大小，以避免数据包被分片引起的问题。

(7)Anti-Replay Service

<1>To disrupt in some way, the attacker obtains a copy of an authenticated packet and re–transmit the packet to its intended destination.

为了以某种方式破坏，攻击者获得经过验证的包的副本，并将包重新发送到预期的目的地。

– Sequence Number used to stop this attack 用于阻止此攻击的序号

– Packets are numbered (using a counter) as they are sent 数据包在发送时进行编号（使用计数器）

– If sequence number greater than 2^64 – 1 then terminate SA and start again

如果序列号大于 2^64–1，则终止 SA 并重新开始

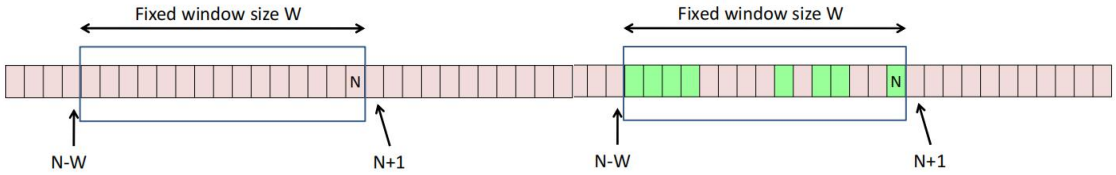
– As IP is connectionless and unreliable, use a sliding window to overcome these IP limitations.由于 IP 是无连接的和不可靠的，所以使用滑动窗口来克服这些 IP 的限制。

<2>

• Sender implements a window of size W. 发送方实现了一个大小为 W 的窗口

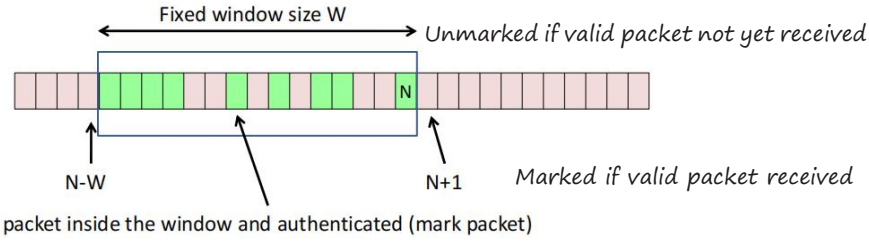
• Right edge of the window represents highest sequence number N.窗口的右边表示最高的序列号 N

• Left edge of the window is N – W 左边是 N-M



default of W = 64

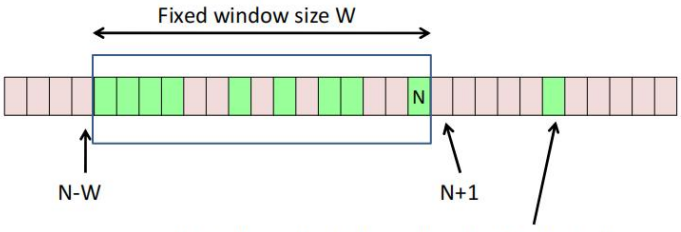
第一种在窗口内



packet inside the window and authenticated (mark packet)

窗口内的包和经过认证的包（标记包）

第二种右侧



new packet to the right of the window (authenticated)

位于窗口右侧的新数据包（已通过身份验证）

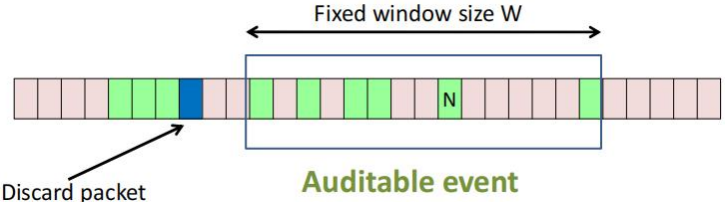
Slide the window so that this new packet is its right edge

滑动窗口，使此新数据包成为其右边缘

第三种左侧

New packet to the left of the window (or authentication failure)

位于窗口左侧的新数据包（或身份验证失败）



A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination.

重播攻击是指攻击者获得经过身份验证的数据包的副本，然后将其传输到预期的目标

(8)Tunnel and Transport mode

<1>

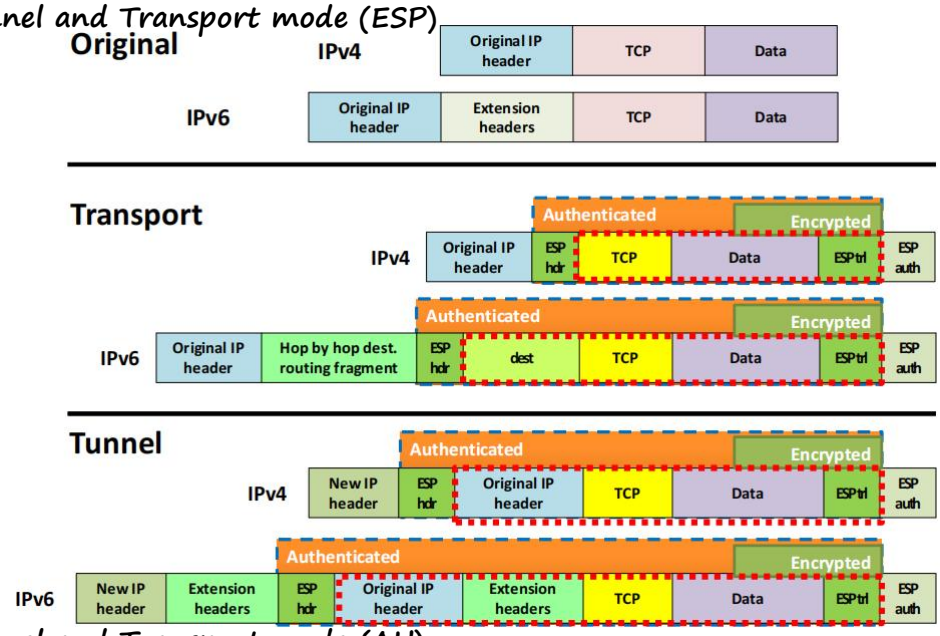
Processing

- Use Security Parameter Index (SPI) to look up security association (SA).
  使用安全参数索引（SPI）来查找安全关联（SA）
- Perform authentication check using SA 使用 SA 执行身份验证检查
- Perform encryption/decryption of authenticated data using SA
  使用 SA 对经过身份验证的数据进行加密/解密

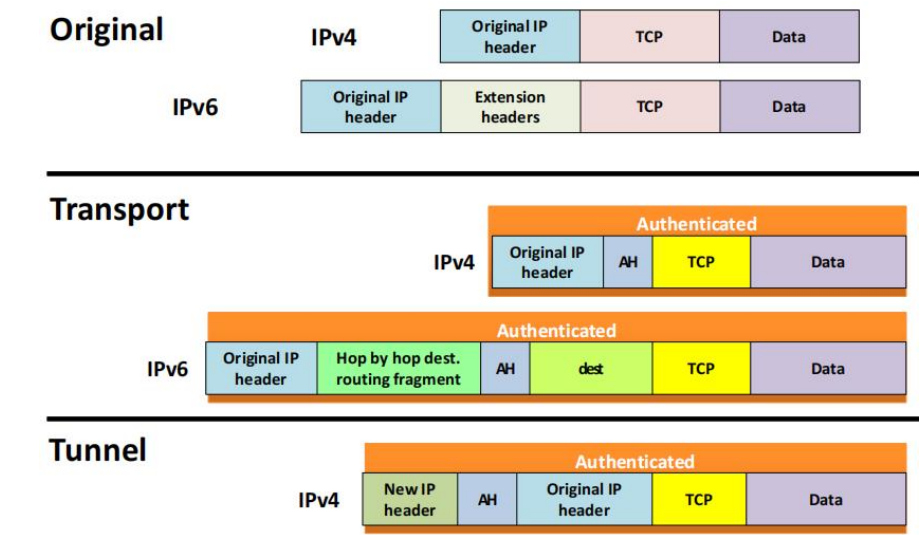
Operates in two modes:

- Tunnel Mode: protects entire packet. 保护整个数据包
- Transport Mode: protects payload. 保护有效载荷

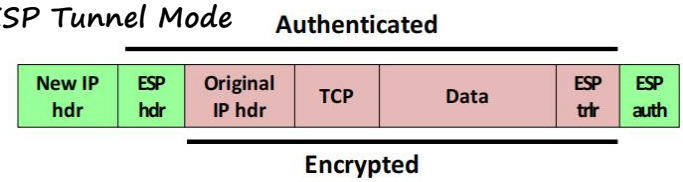
<2>Tunnel and Transport mode (ESP)



<3>Tunnel and Transport mode (AH)



<4>ESP Tunnel Mode

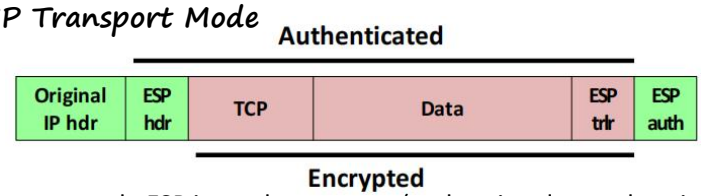


• In tunnel mode ESP can be used to set up a virtual private network.
在 tunnel 模式下，可以使用 ESP 建立一个虚拟专用网。

• Host on the internet networks use the Internet transport of data but do not interact with other Internet-based hosts.互联网网络上的主机使用互联网传输数据传输，但不与其他基于互联网的主机交互

• Tunnel mode operation provides protection against traffic analysis 隧道模式运行可防止交通分析

<5>ESP Transport Mode



• In transport mode ESP is used to encrypt (and optional to authenticate) the data carried by IP.
在传输模式下，ESP 用于加密 IP 携带的数据（可选地用于身份验证）

• The entire transport-level segment plus the ESP trailer are encrypted.
整个运输级段和 ESP 拖车都被加密了。

• Transport mode operation provides confidentiality.传输模式操作提供了机密性。

• Transport mode operation may be summarized as follows. 总结 Transport 模式：

①. At the source, the block of data consisting of the ESP trailer plus the entire transport-layer segment is encrypted and the plaintext of this block is replaced with its ciphertext to form the IP packet for transmission. Authentication is added if this option is selected. 在源处，由 ESP 拖车和整个传输层段组成的数据块被加密，该块的明文被替换为其密文，以形成用于传输的 IP 包。如果选择了此选项，则将添加身份验证。

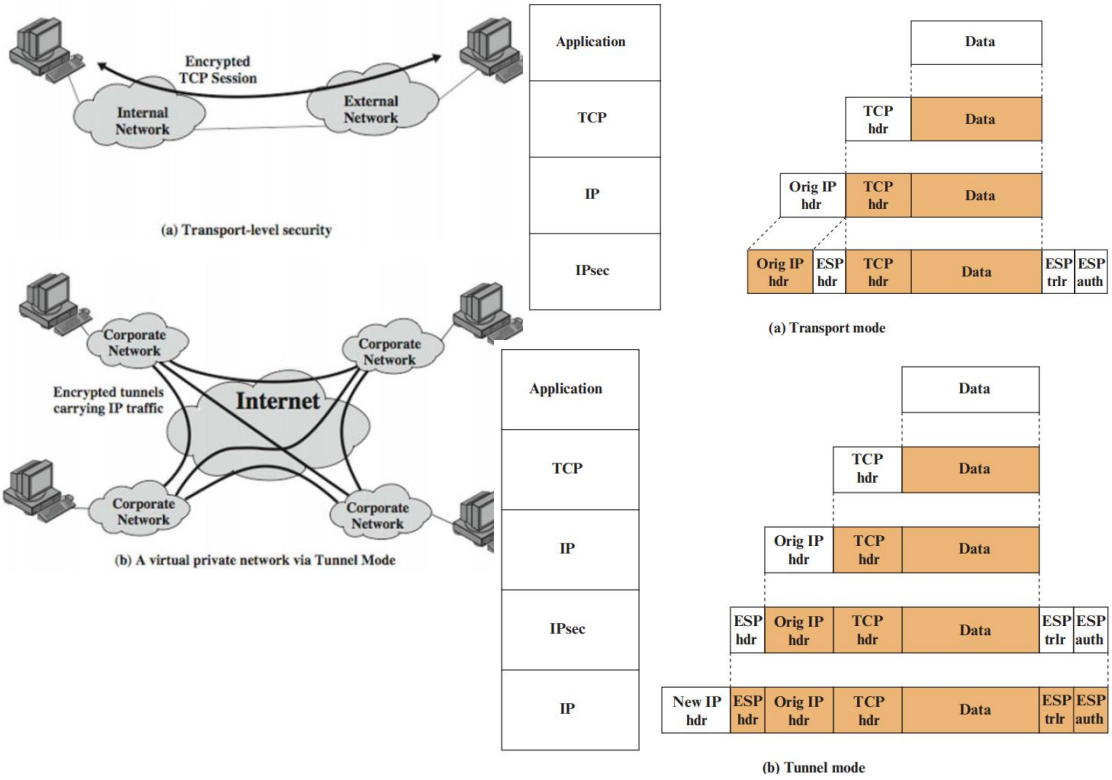
②. The packet is then routed to the destination. Each intermediate router needs to examine and process the IP header plus any plaintext IP extension headers but does not need to examine the ciphertext. 然后，将数据包路由到目的地。每个中间路由器需要检查和处理 IP 头和任何明文 IP 扩展头，但不需要检查密文。

③. The destination node examines and processes the IP header plus any plaintext IP extension headers. Then, on the basis of the SPI in the ESP header, the destination node decrypts the remainder of the packet to recover the plaintext transport-layer segment. 目标节点检查和处理 IP 头和任何明文 IP 扩展头。然后，根据 ESP 报头中的 SPI，目标节点对数据包的其余部分进行解密，以恢复明文传输层段。

• Transport mode operation provides confidentiality for any application that uses it, thus avoiding the need to implement confidentiality in every individual application. One drawback to this mode is that it is possible to do traffic analysis on the transmitted packets.传输模式操作为使用它的任何应

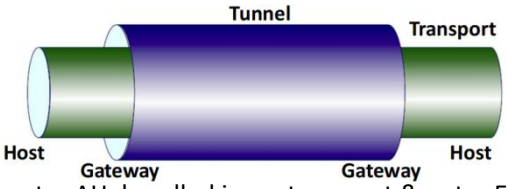
	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.

用程序提供机密性，从而避免了在每个单独的应用程序中实现机密性。这种模式的一个缺点是可以对传输的数据包进行流量分析。



(9)Combining Security Associations

- SA's can implement either AH or ESP　一个 SA 可以实现 AH 或 ESP
- To implement both need to combine SA's　要想实现两个需要结合 SA
  - Form a security association bundle 形成一个安全关联捆绑包（要求）
  - May terminate at different or same endpoints 可以在不同的或相同的端点上终止（要求）
  - Combined by 两种结合方法
    - Transport adjacency
    - Iterated tunneling



- Combining authentication & encryption
  - ESP with authentication, bundled inner ESP & outer AH, bundled inner transport & outer ESP
    带认证的 ESP，捆绑内部 ESP 和外部 AH，捆绑内部运输和外部 ESP
- Example
  - Authentication between host (without encryption). 主机之间的身份验证（没有加密）
- AH-transport between hosts 主机之间的 AH 传输

– Confidentiality when transversing the WAN. ESP-tunnel between gateways.穿越 WAN 时的机密性。网关之间的 esp 隧道。

Case 1. All security is provided between end systems that implement IPsec. For any two end systems to communicate via an SA, they must share the appropriate secret keys. Among the possible combinations are 在实现 IPsec 的终端系统之间提供了所有的安全性。对于任何两个终端系统通过 SA 进行通信，它们必须共享适当的密钥。可能的组合中有

a. AH in transport mode

b. ESP in transport mode

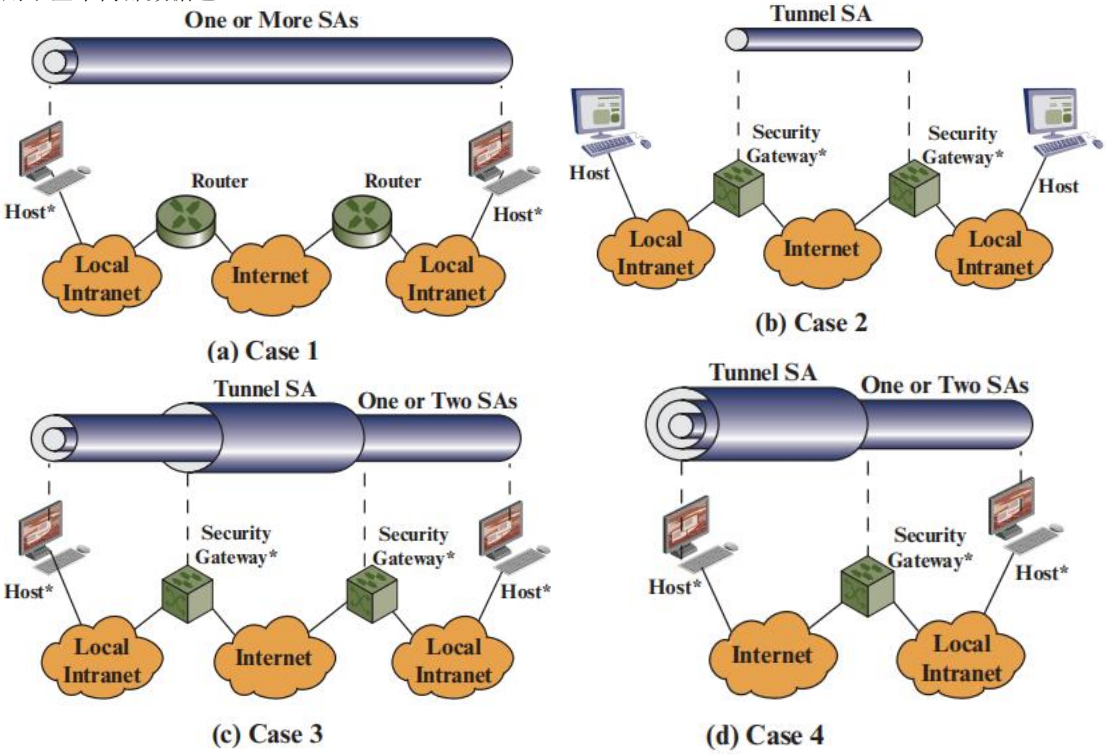
c. ESP followed by AH in transport mode (an ESP SA inside an AH SA)

在传输模式下，ESP 之后是 AH（AHSA 内的 ESPSA）

d. Any one of a, b, or c inside an AH or ESP in tunnel mode

在隧道模式下的 AH 或 ESP 中的 A、b 或 c 中的任何一个

Case 2. Security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPsec. This case illustrates simple virtual private network support. The security architecture document specifies that only a single tunnel SA is needed for this case. The tunnel could support AH, ESP, or ESP with the authentication option. Nested tunnels are not required, because the IPsec services apply to the entire inner packet.仅在网关（路由器、防火墙等）之间提供安全性。而且没有主机实现 IPsec。本例说明了简单的虚拟专用网支持。安全体系结构文档指定在此情况下只需要一个隧道 SA。该隧道可以支持 AH、ESP 或 ESP 的认证选项。不需要嵌套的隧道，因为 IPsec 服务将应用于整个内部数据包。



Case 3. This builds on case 2 by adding end-to-end security. The same combinations discussed for cases 1 and 2 are allowed here. The gateway-to-gateway tunnel provides either authentication, confidentiality, or both for all traffic between end systems. When the

gateway-to-gateway tunnel is ESP, it also provides a limited form of traffic confidentiality. Individual hosts can implement any additional IPsec services required for given applications or given users by means of end-to end SAs. 这是建立在案例 2 的基础上的，通过添加端到端安全性。这里允许对案例 1 和情况 2 讨论相同的组合。网关到网关隧道为端系统之间的所有通信提供身份验证、机密性或两者。当网关到网关的隧道是 ESP 时，它还提供了一种有限的流量保密形式。单个主机可以通过端到端 SAs 实现给定应用程序或给定用户所需的任何额外的 IPsec 服务。

Case 4. This provides support for a remote host that uses the Internet to reach an organization's firewall and then to gain access to some server or workstation behind the firewall. Only tunnel mode is required between the remote host and the firewall. As in case 1, one or two SAs may be used between the remote host and the local host. 这为远程主机提供了支持，它使用互联网到达组织的防火墙，然后访问防火墙后面的某些服务器或工作站。在远程主机和防火墙之间，只需要使用隧道模式。与情况 1 一样，可以在远程主机和本地主机之间使用一个或两个 sa。

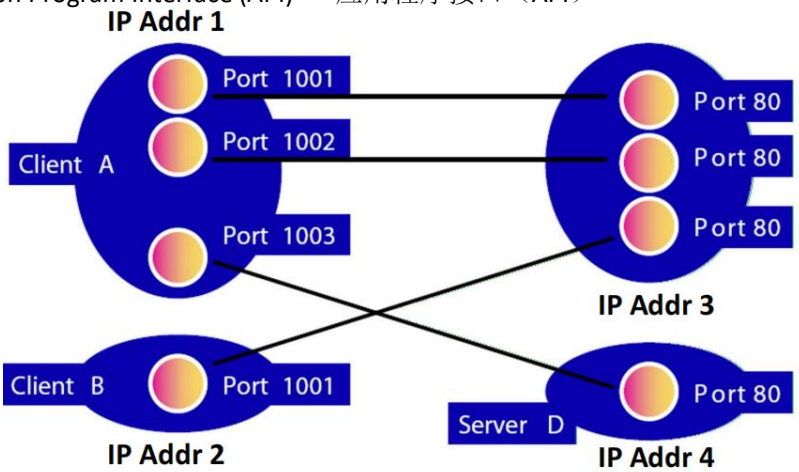
(10)Socket

<1>

• A Socket is a communication end point 套接字是一个通信终点

• Applications communication using a socket 应用程序使用套接字进行通信

• Application Program Interface (API) 应用程序接口（API）



<2>A socket is defined in the operating system as a structure.套接字在操作系统中被定义为一种结构

– **Family**: defines the protocol group: IPv4, IPv6... 定义协议群组

– **Type**: defines the type i.e. stream, datagram, or raw socket 定义了以下类型

– **Protocol**: usually set to zero for TCP and UDP 对于 TCP 和 UDP，通常设置为零

– **Local socket address**: defines the local socket address, a structure of type sockaddress
定义本地套接字地址，一种类型为索地址的结构

– **Remote socket address**: defines the remote socket address, a structure of type sockaddress
定义远程套接字地址，一种索地址类型的结构

<3>IPSec: Packet or Socket

IPsec policy can be configured in per-packet, or per-socket manner:

IPsec 策略可以按每个数据包或每个套接字的方式进行配置：

– **Per-packet**: configured into the kernel just like packet filters. You can specify like ‘‘encrypt outgoing packets if I'm sending to 10.1.1.0/24’’. This works well when you are running an IPsec

router. 就像数据包过滤器一样，被配置到内核中。你可以指定像“加密传出的数据包，如果我正在发送到10.1.1.0/24”。当你在运行一个 IPsec 路由器时，这工作得很好。

– **Per-socket**: configured via setsockopt(2) for a certain socket. You can specify like ‘‘encrypt outgoing packets from this socket’’. This works well when you would like to run IPsec-aware server program. 通过设置(2)配置。您可以指定像“从这个套接字加密传出的数据包”。当您想运行 ipsec 感知的服务器程序时，这工作得很好。

(11)Key Management

<1>

• Key management involves the determination and distribution of secret keys
密钥管理涉及到秘密密钥的确定和分发

• The distribution of keys can be manual or automatic. 钥匙的分配可以是手动的或自动的。

• Oakley Key Determination Protocol: is a key exchange protocol (improved Diffie– Hellman)
Oakley 密钥确定协议：是密钥交换协议（改进的 Diffie– Hellman）

• Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for key management and provides the specific protocol support.互联网安全协会和密钥管理协议（ISAKMP）为密钥管理提供了一个框架，并提供了特定的协议支持。

<2>Oakley

• Is a key exchange protocol, based on Diffie-Hellman key exchange

• Exchange messages containing any of 交换包含以下任何内容的消息

– Client/Server cookies 客户端/服务器 Cookie

– Diffie-Hellman information

– Offered/chosen security parameters 已提供的/已选择的安全参数

– Client/Server ID’s

until both sides are satisfied.

Oakley is very open–ended, with many variations possible, ex
Oakley 是非常开放的，有许多可能的变化，例如

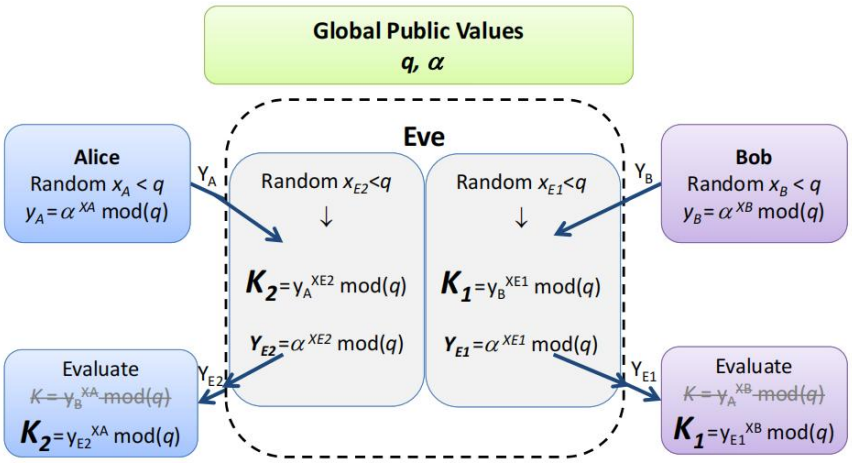
– Speed vs thoroughness

– New session vs re-key

– Identification vs anonymity

– Diffie–Hellman vs shared secrets vs Public Key -based exchange

<3>Man-in-the-middle attack



<4>Oakley Authentication

• Digital Signature: Authentication is done by signing a mutually obtainable hash. Each party encrypts the hash with its private key.

通过签名一个相互可获得的 hash 来完成身份验证。每一方都用其私钥加密 hash。

• Public–key encryption

• Symmetric–key encryption

<5>Oakley Characteristics

• Use of cookies to thwart clogging attacks 使用 cookies 来阻止阻塞的攻击

• Specify the global parameters of the Diffie–Hellman algorithm

指定迪分-希尔曼算法的全局参数

• Uses nonce to ensure against replay attacks 使用 nonce 来确保防止重放攻击

• Exchange of Diffie–Hellman public key values

• Authenticates the Diffie–Hellman exchange to thwart man-in-the-middle attack

(12)ISAKMP(Internet Security Association and Key Management Protocol)

• NSA–designed protocol to exchange security parameters (but not establish key)

NSA 设计的协议来交换安全参数（但不建立密钥

– Protocol to establish, modify and delete IPSec security association 建立、修改和删除 IPSec 安全关联的协议

– General framework for exchanging cookies, security parameters, key management and identification

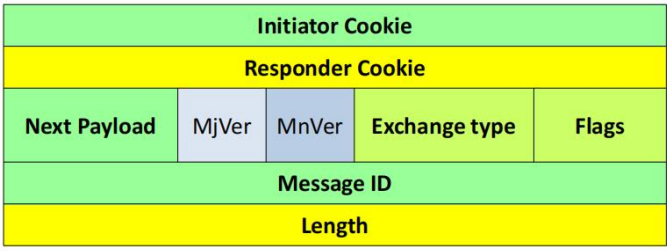
交换 Cookie、安全参数、密钥管理和识别的通用框架

– Details left to other protocols

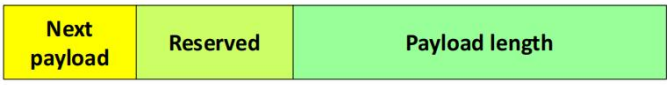
• Two phases:

1. Establish secure, authenticate channel (SA) 建立安全的身份验证通道（SA）

2. Negotiate security parameters (KMP)协商安全参数（KMP）



ISAKMP header



Generic payload header

(13)ISAKMP / Oakley

• They merged so

– ISAKMP provides the protocol framework

– Oakley provides the security mechanism

Combined version clarifies both protocols, resolve ambiguities.

四. Firewalls

1.FireWalls

(1)简介

• A Firewall protects a local system/network from network–based security threats, at the same time allows access to the outside world (WAN, Internet). 防火墙可保护本地系统/网络免受基于网络的安全威胁，同时还允许访问外部世界（广域网、互联网）

• A Firewall is needed because by all networks

– Internet connectivity is not an option 互联网连接不是一个选择

– Internet access creates a security threat to the local network 互联网接入对本地网络造成了安全威胁

– It is not economical to equip each PC, server, etc. with strong security features

装备每台个人电脑、服务器等并不经济。具有强大的安全功能

• The Firewall is inserted between the premises network and the Internet.
防火墙被插入到办公场所网络和互联网之间

• The Firewall establishes a controlled link and security wall between the premises and the Internet.防火墙在房屋和互联网之间建立了一个受控制的链接和安全墙

• The Firewall may be one or more computer systems.

• All traffic from inside to outside and vice versa must pass through the Firewall.

所有从内到外的交通工具，反之亦然，都必须通过防火墙。

• Only authorised traffic will be allowed to pass. 只有经授权的交通工具才能通行

• The Firewall itself is immune to penetration. 防火墙本身不受渗透的影响

(2)Firewall Characteristics

• **Firewall also provides**
  – Service Control
  – Direction Control
  – Use Control
  – Behaviour Control

(3)Firewall Limitations

• The Firewall cannot protect against attacks that bypass the Firewall.
防火墙无法防止绕过防火墙的攻击

• The Firewall does not protect against internal attacks.防火墙并不能防止内部攻击

• The Firewall cannot protect against computer viruses.防火墙无法防止计算机病毒感染

(4)Other common Firewall Services

• Encrypted Authentication 加密身份验证

• VPN to avoid expensive leased lines VPN，以避免昂贵的租用线路

• Virus Scanning 病毒扫描

• Content Filtering (added to the proxy server) 内容筛选（已添加到代理服务器）

• Other ..

2.Firewall Protection Methods

• **Packet Filtering**

– Rejects unauthorised TCP/IP packets or connection attempts.

拒绝未经授权的 TCP/IP 数据包或连接尝试

• **Application-Level Gateway**

– Acts as a relay of application-level traffic. 充当应用程序级流量的中继器

• **Circuit-Level Gateway**

– AKA Network Address Translation (NAT) AKA 网络地址转换（NAT）

– Translates the addresses of internal hosts in order to hide them from the outside world.

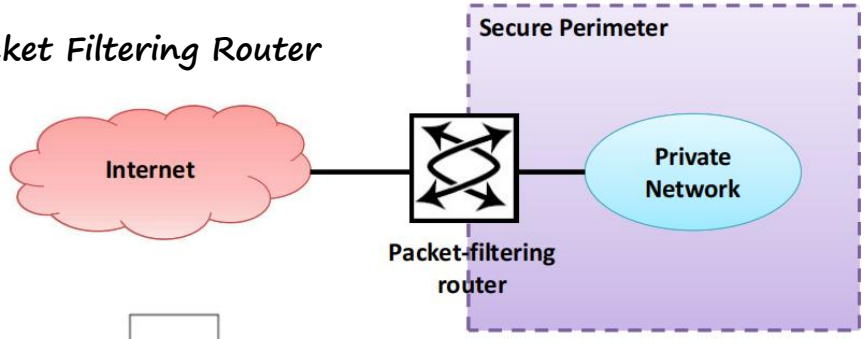
翻译内部主机的地址，以使它们远离外部世界

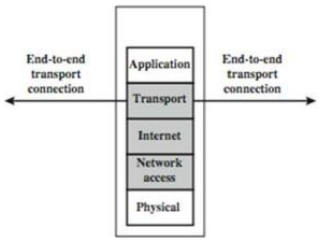
• **Proxy Services**

– Makes high level application level connections to external hosts on behalf of the internal hosts to completely isolate the internal form external hosts.

代表内部主机进行到外部主机的高级应用程序级连接，以完全隔离内部形式的外部主机。

(1)Packet Filtering Router





<1>

• Filters the IP packets, forwarding or discarding them depending on a list of rules.

过滤 IP 数据包，并根据规则列表转发或丢弃它们

• The rules are based on IP fields and transport header (TCP, UDP).

这些规则基于 IP 字段和传输标头（TCP、UDP）。

• Filters packets in both directions. 在两个方向上过滤数据包

Action	Outhost	Port	Theirhost	Port	comment
Block	*	*	Dave	*	We don't trust him
Allow	OUR-GW	25	*	*	Connection to our mailer port
:	:	:	:	:	:

<2>Disadvantages:

– Difficulty setting up rules and no authentication. 难以设置规则，并且没有身份验证

– IP addresses of hosts on the protected side of the filter can be readily determined by observing the packet traffic on the unprotected side of the filter

通过观察过滤器未受保护侧的数据包流量，可以很容易地确定过滤器受保护侧的主机的 IP 地址

– Filters cannot check all of the fragments of higher level protocols (like TCP) as the TCP header information is only available in the first fragment.

过滤器不能检查更高级别的协议的所有片段（如 TCP），因为 TCP 报头信息只在第一个片段中可用。

– Filters are not sophisticated enough to check the validity of the application level protocols imbedded in the TCP packets

过滤器还不够复杂，无法检查嵌入在 TCP 数据包中的应用程序级协议的有效性

<3>Some attacks:

– IP address spoofing　IP 地址欺骗

• Fake resource address to be trusted 要受信任的假资源地址

→Add filters on router to block 在路由器上添加过滤器来阻止

– Source routing attacks　源路由攻击

• Attacker sets a route other than default 攻击者设置了一个除默认值以外的路由

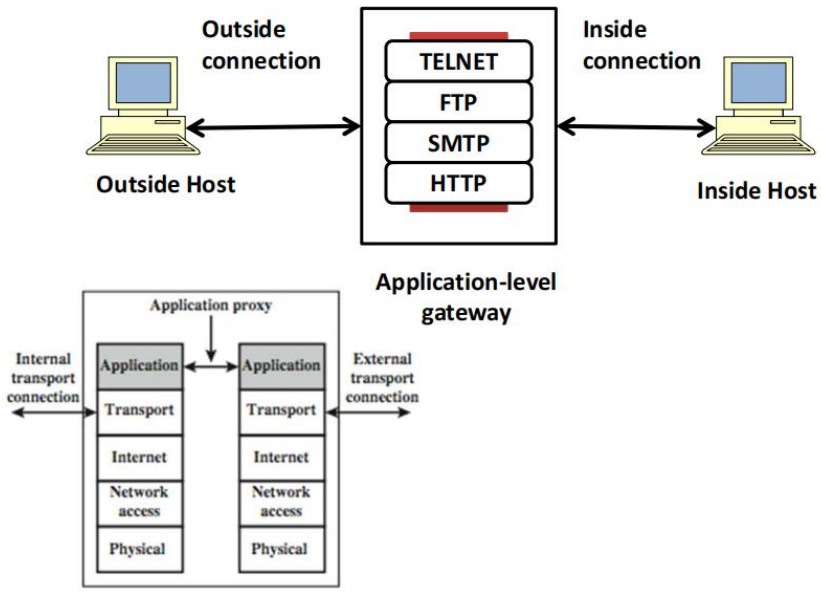
→Block source routed packets 阻止源路由数据包

– Tiny fragments attacks 小碎片攻击

• Split header info over several tiny packets 在几个小数据包上分割报头信息

→Either discard or reassemble before check 在检查前先丢弃或重新组装

(2)Application-level Gateway



• An application-level gateway (or proxy server), acts as a relay of application level traffic.

应用程序级网关（或代理服务器），充当应用程序级流量的中继。

• A user contacts the gateway to access some service, provides details of the service, remote host & authentication details, contacts the application on the remote host and relays all data between the two endpoints. 用户联系网关以访问某些服务，提供服务的详细信息、远程主机和身份验证的详细信息，联系远程主机上的应用程序，并在两个端点之间中继所有数据。

• If the gateway does not implement the proxy code for a specific application, then it is not supported and cannot be used.

如果网关没有为特定的应用程序实现代理代码，则它不受支持，也不能使用。

• Some services naturally support proxying, whilst others are more problematic.

有些服务自然会支持代理，而另一些服务则更有问题

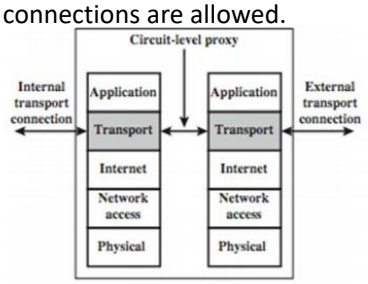
• Application-level gateways tend to be more secure than packet filters, &can log and audit traffic at application level.

应用程序级网关往往比数据包过滤器更安全，并且可以在应用程序级别记录和审计流量。

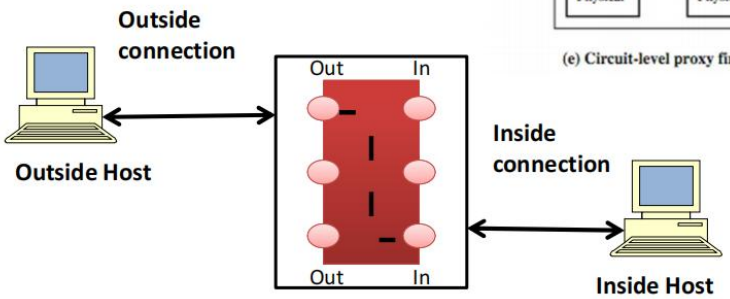
• They are more secure than packets filters as only scrutinise a few allowable applications.
它们比数据包过滤器更安全，因为只仔细检查少数允许的应用程序。
• Disadvantage:
– Additional processing overhead for each connection.每个连接的额外处理开销

(3)Circuit-level Gateway

• It does not permit an end-to-end TCP connection, but rather relays them.
它不允许端到端 TCP 连接，而是中继它们。
• It opens two connections between
– Itself and inner host 本身和内部主机
– Itself and outside host 本身和外部主机
• Security function consist of determining which connections are allowed.
安全功能包括确定允许使用哪些连接。



(e) Circuit-level proxy firewall



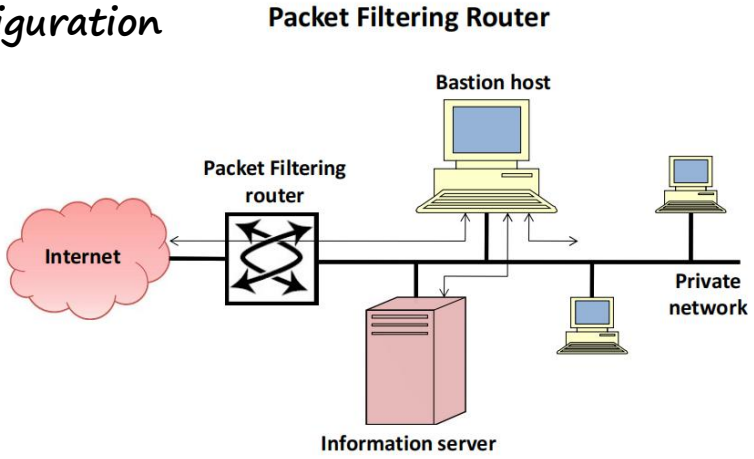
Circuit-level gateway

(4)Bastion Host

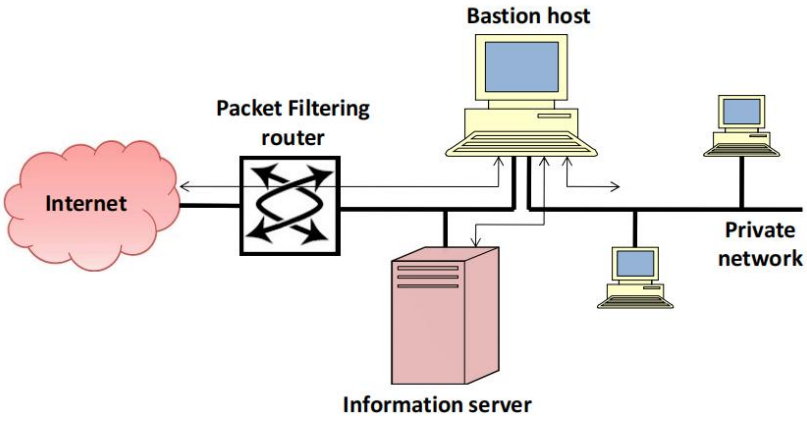
• Is a critical strong point in the network's security. 是网络安全方面的一个关键的强项
• It serves as a platform for application–level or circuit–level gateway.
可作为应用程序级或电路级网关的平台
• Its hardware executes a secure version of its operating system (trusted system)
其硬件执行其操作系统的安全版本（可信系统）
• Before the user is allowed access the bastion host can require authentication of the user
在允许用户访问之前，堡垒主机可能需要对用户进行身份验证
• Only "essential" services are installed, like proxy Telnet, DNS, FTP, . . .
只安装"基本"服务，如代理 Telnet、DNS、FTP、……
• **The proxy 代理**
– Supports only a subset of the application's command set 仅支持该应用程序的命令集的一个子集
– Access to only some of the host systems 仅访问部分主机系统
– Keeps audits 保持审计
– Small software package 小型软件包
– Independent of other proxies 独立于其他代理
– No disk access 没有磁盘访问
– Run as non-privileged user 以非特权用户身份运行

3.Firewall configuration

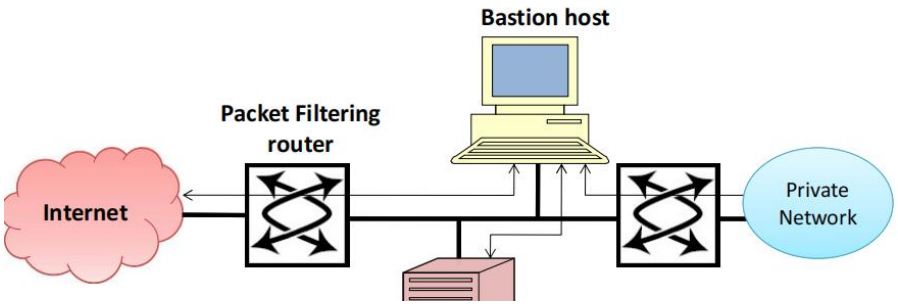
(1)

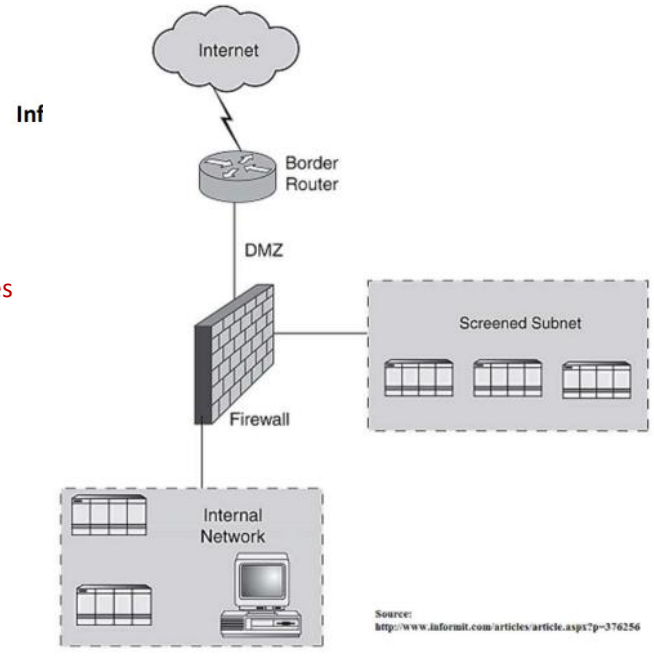


Dual Homed Bastion Host



Screened Subnet Firewall





Inf

• De-Militarised Zones and Screened Subnets 非军事化区域和屏蔽子网

– DMZ and screened subnet refer to a small network containing public services connected directly to and offered protection by the firewall or other filtering device.DMZ 和屏蔽子网是指包含

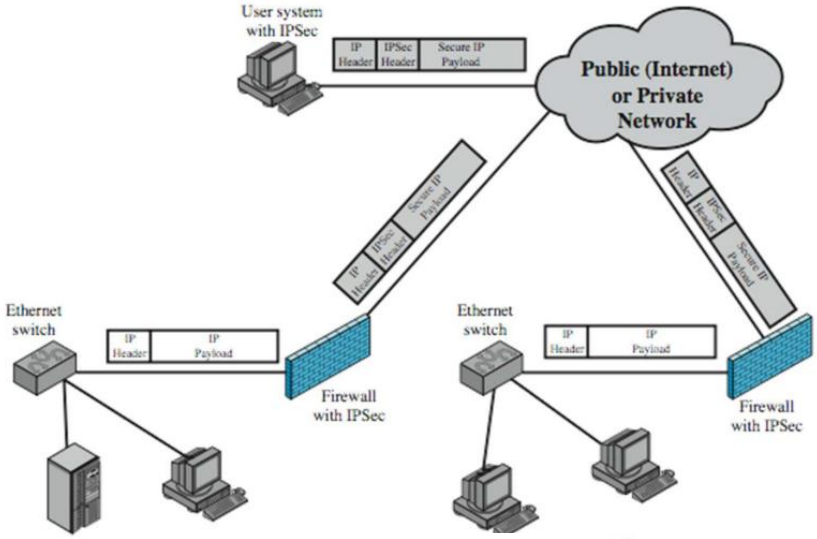
直接连接到防火墙或其他过滤设备并提供保护的公共服务的小型网络。

– A firewall or a comparable traffic-screening device protects a screened subnet that is directly connected to it. 防火墙或类似的流量筛选设备保护直接连接到它的屏蔽子网

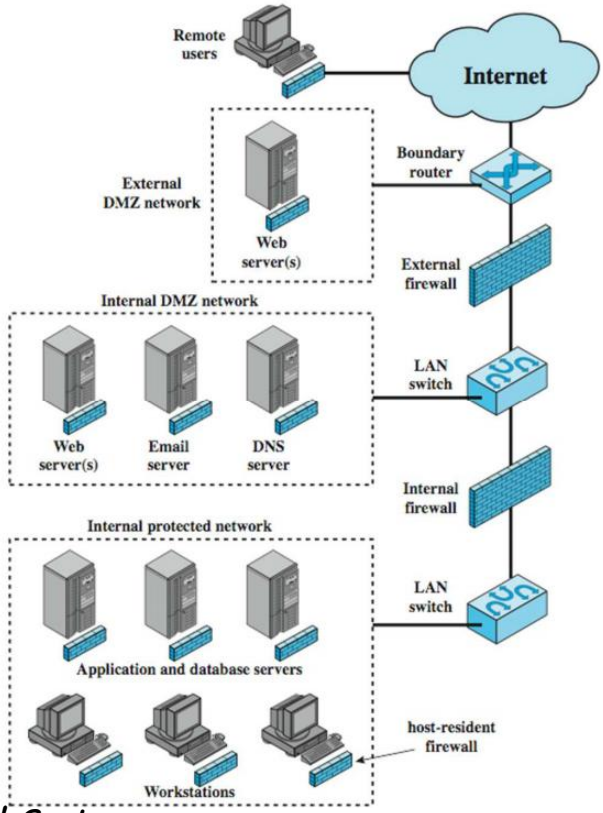
– A DMZ is in front of a firewall, whereas a screened subnet is behind a firewall.

DMZ 在防火墙的前面，而被屏蔽的子网在防火墙的后面。

(2)Virtual Private Networks



(3)Distributed Firewalls



(4)Bastion Host and Trusted Systems

• To protect data or resources on the basis of level security (confidential, secret, top secret, ultra . .) 基于级别安全来保护数据或资源

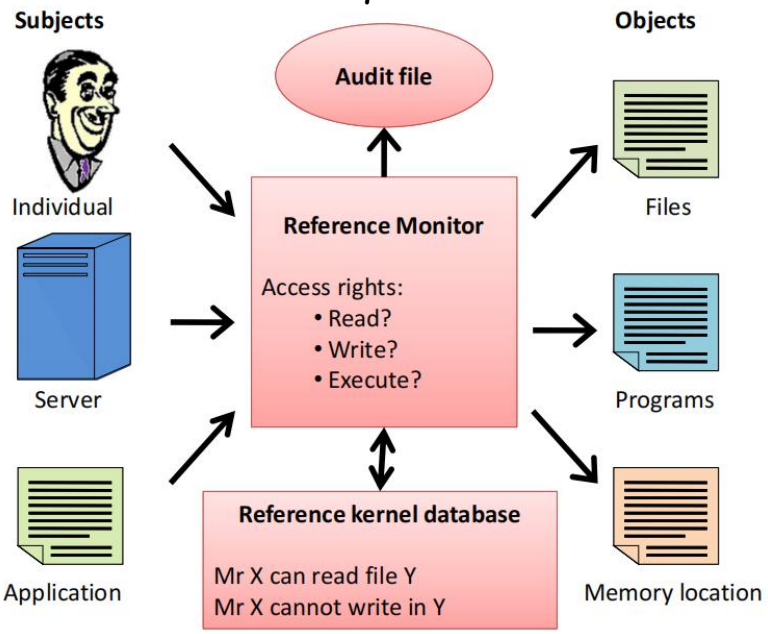
• Example

– In a company, the strategic planning is only available to corporate officers and the financial data only accessible to administration officers.
在公司中，战略规划只面向公司官员访问，而财务数据只面向管理人员访问。

(5)Trusted Systems: Multilevel Security

• The system enforces the following rules 该系统将强制执行以下规则
– No read up (simple security property): A subject can only read an object of less or equal security level. 不读取（简单安全属性）：主题只能读取小于或等于的对象保密等级
– No write down (*–property): A subject can only write into an object of greater or equal security level. 无写入（*-属性）：主题只能写入大于或等于安全级别的对象

(6)Reference Monitor Concept



(7)Trusted Systems

• Properties of the Reference Monitor
– Complete mediation.
– Isolation.
– Verifiability.