《网安》习题&重点

Ex&Key 0

1.What is your opinion about the difference of computer security, network security and information security?

(1)Network security is network equipment and network attacks.

(2)Computer security is virus Trojan horse and password protection.

(3)Information security includes network security and computer security.

2.What is cyberspace security?What is the relation between cyberspace and sea, land, air and space?

(1)Cyberspace security refers to the virtual information space created by computers. Cyberspace is not only the living environment of people, but also the living environment of network information.Therefore, cyberspace security is the basic requirement of people and information to cyberspace.

(2)Cyberspace is the fifth largest sovereign space alongside land, sea, air and sky.

3.Except these topics, what do you think this course should included?

(1)Symmetrical encryption and message confidentiality

(2)Public key cryptography and message authentication

(3)Malicious Software

(4)Intruder

习题&重点〇

1.您对计算机安全、网络安全和信息安全的区别有何看法？

(1)网络安全是网络设备和网络攻击。

(2)计算机安全是病毒木马和密码保护。

(3)信息安全包括网络安全和计算机安全。

2.什么是网络空间安全？网络空间与海、陆、空、空间之间的关系是什么？

(1)网络空间安全是指由计算机创建的虚拟信息空间。网络空间既是人的生存环境，也是网络信息的生存环境，因此网络空间安全是人和信息对网络空间的基本要求。

(2)网络空间（cyberspace）是与陆、海、空、天并列的第五大主权空间。

3.除了这些主题，你认为本课程应该包括哪些内容？

对称加密和消息机密性、公钥密码和消息认证、恶意软件、入侵者

Ex&Key U1

1.Please explain the network security objectives with your own words.

(1)Confidentiality：Guarantee personal privacy and private information.

(2)Integrity:Prevent improper modification and destruction of information.

(3)Availability：Ensure people timely and reliably access and use information.

(4)Authenticity:Information can be verified and trusted.

(5) Accountability:The behavior of each entity can be uniquely tracked.

(6) Nonrepudiation：Provide the basis and means for investigation of network security issues, and ensure that information actors can not deny their actions.

2.Point out the most important network security challenge. Why you think it is the most important one?

(1)Data security concerns caused by the "Internet +" era.

(2)Recently, many Internet enterprises that go to sea have been surrounded, chased and intercepted, and their opponents are making a big fuss about data security and privacy. This requires that all staff, including business directors, accurately understand the importance of data security and privacy protection, establish corresponding culture, organization, process and technology, and release the value of data to the maximum extent while effectively controlling risks.

3.Describe the meaning and types of passive attack and active attack briefly.

(1) The essence of passive attack is to eavesdrop or monitor data transmission, and the target of the attacker is to obtain the transmitted data information. The two forms of passive attack are message content disclosure attack and traffic analysis attack;

(2) Active attack includes rewriting of data stream and adding of error data stream. Active attacks can be divided into four categories: counterfeiting, replay, message rewriting and denial of service.

4.Please explain the principle of network communication security model.

Both parties of the transaction must cooperate to exchange messages through some type of interconnection network. A logical information channel can be established by defining a route from the information source to the information destination and a certain protocol used between two information subjects on the interconnection network.

(1) To ensure the confidentiality and authenticity of information, it is necessary to provide the following security technologies:

• Perform security-related transformations on the information to be sent, such as message encryption, and scramble the message to make it unreadable to the attacker; Establish an additional code on the message content to verify the identity of the sender;

• The two subjects share secret information that is not known by the attacker. For example, the encryption key used in message exchange, which scrambles messages before transmission and recovers messages after reception.

(2) In order to achieve secure transmission, a trusted third party is also needed, for example, the third party distributes secret information to two subjects and hides the information from the attacker; The third party needs to arbitrate the serious dispute between the two parties about information transmission.

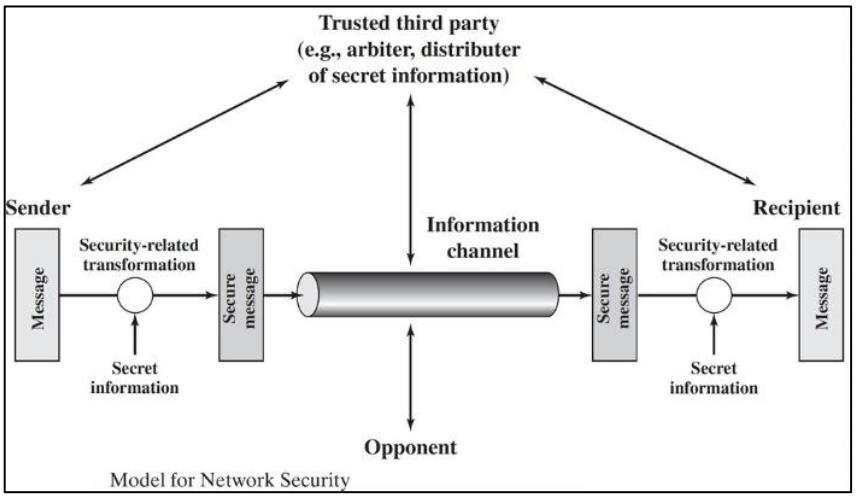
This model shows that there are four basic tasks for designing specific security services:

(1) An algorithm is designed to perform security-related transformations, and the algorithm is not broken by attackers;

(2) Using this algorithm to generate secret information;

(3) Develop methods to distribute and share secret information;

(4) Specify the protocol used by the two principals to obtain specific security services.



Model for Network Security

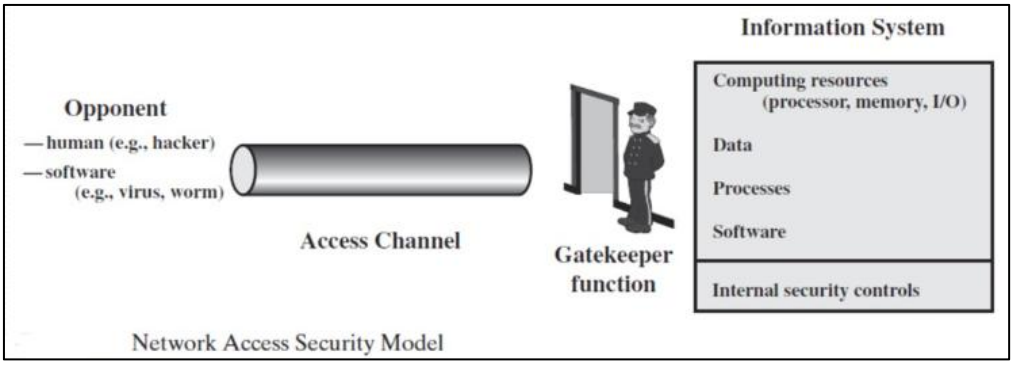
5.Please explain the principle of network access security model.

In the network access security model, the following two categories are used to solve harmful access:

(1) The first is the gatekeeper function, which includes the password-based login process and denies all access except authorized use;

(2) The second type is screening logic, which is used to detect and reject attacks such as worms and viruses.

Once any harmful software or user gets access, the second line of defense, namely internal security control, can monitor and analyze the stored information to detect the existence of harmful intruders.



Network Access Security Model

6.SummaryU1

(1)There are passive attacks and active attacks of network security.

(2)Confidentiality, Integrity, Availability,Authenticity, Accountability,Nonrepudiation are the major objectivesof network security.

(3)Access control, encryption, signature,padding, audit are basic network security mechanisms.

(4)GB/T and GM/T are the standards we should comply during our working.

习题&重点 U1

1.请用自己的语言解释网络安全目标。

(1)保密性：保证个人隐私和私人信息。

(2)完整性：防止信息的不当修改和破坏。

(3)可用性：确保人们及时、可靠地访问和使用信息。

(4)真实性：信息可以被验证和信任。

(5)可计量性：可以唯一地跟踪每个实体的行为。

(6)不可否认性：为调查网络安全问题提供基础和手段，并确保信息参与者不会否认其行为。

2.指出最重要的网络安全挑战。为什么你认为这是最重要的?

(1)“互联网+”时代引发的数据安全担忧。

(2)最近，许多出海的互联网企业遭到围追堵截，对手在数据安全和隐私问题上大做文章。这要求包括业务主管在内的所有员工准确理解数据安全和隐私保护的重要性,建立相应的文化、组织、流程和技术，在有效控制风险的同时最大限度地释放数据的价值。

3.简述被动攻击和主动攻击的含义和类型。

(1)被动攻击的本质是窃听或监视数据传输，攻击者的目标是获取传输的数据信息。被动攻击的两种形式是消息内容泄露攻击和流量分析攻击；

(2)主动攻击包含数据流的改写和错误数据流的添加。主动攻击可划分为 4 类：假冒、重放、改写消息和拒绝服务。

4.请说明网络通信安全模型的原理。

事务的双方必须合作通过某种类型的互连网络进行消息交换,可以通过在互连网络上定义一条从信息源到信息目的地之间的路由以及两个信息主体之间使用的某种协议来建立一条逻辑信息通道。

(1)保证信息机密性、真实性需要提供包含以下方面安全性的技术：

•对将要发送的信息进行与安全相关的转换，例如消息加密，打乱消息使得它对于攻击者不可读；建立消息内容上的附加码，用于验证发送方的身份；

•两个主体共享不被攻击者所知的秘密信息。例如消息交换中使用的加密密钥，它在传输之前打乱消息并且在接收之后恢复消息。

(2)为了达到安全传输还需要可信的第三方，例如第三方分发给两个主体秘密信息并对攻击者隐藏这些信息；第三方需要对两个主体之间关于信息传输认真的纷争进行仲裁。

这个模型表明，设计特定的安全服务有以下 4 个基本任务：

(1)设计算法用于执行安全相关的转换，并且该算法不被攻击者击破；

(2)用该算法生成秘密信息；

(3)开发方法用于分发和共享秘密信息；

(4)指定两个主体使用的协议，以便获得特定的安全服务。

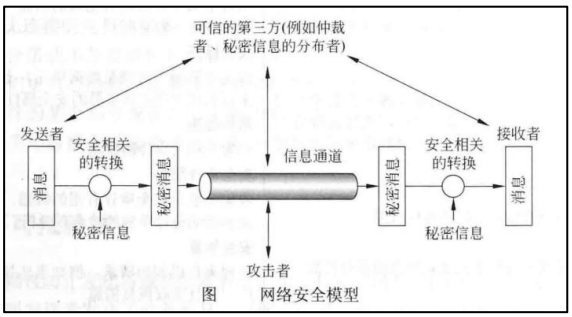


图　网络安全模型

5.请说明网络访问安全模型的原理。

网络访问安全模型中有以下两大范畴用于解决有害访问：

(1)第一类是看门人功能，它包含基于口令的登录过程，拒绝除授权用户外的所有访问；

(2)第二类是屏蔽逻辑，用来检测和拒绝蠕虫、病毒等攻击。

一旦任何一个有害的软件或者用户获得访问权，第二道防线，即内部安全控制就能监视和分析存储的信息来检测有害入侵者的存在。

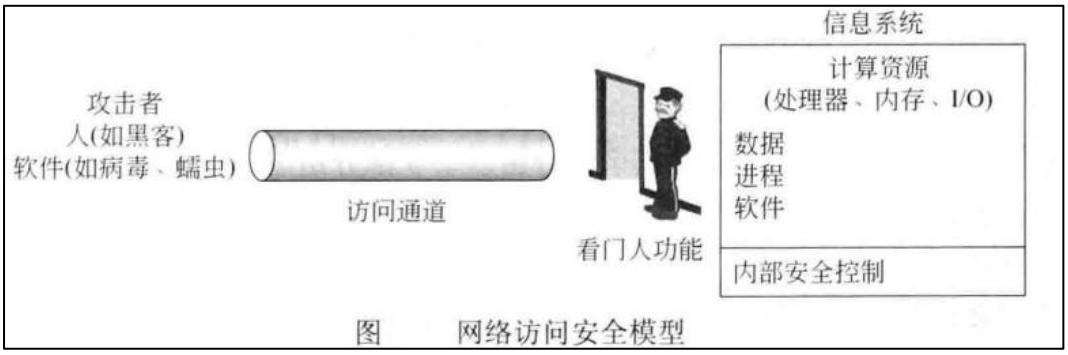


图　　网络访问安全模型

6.总结 U1

(1)网络安全有被动攻击和主动攻击。

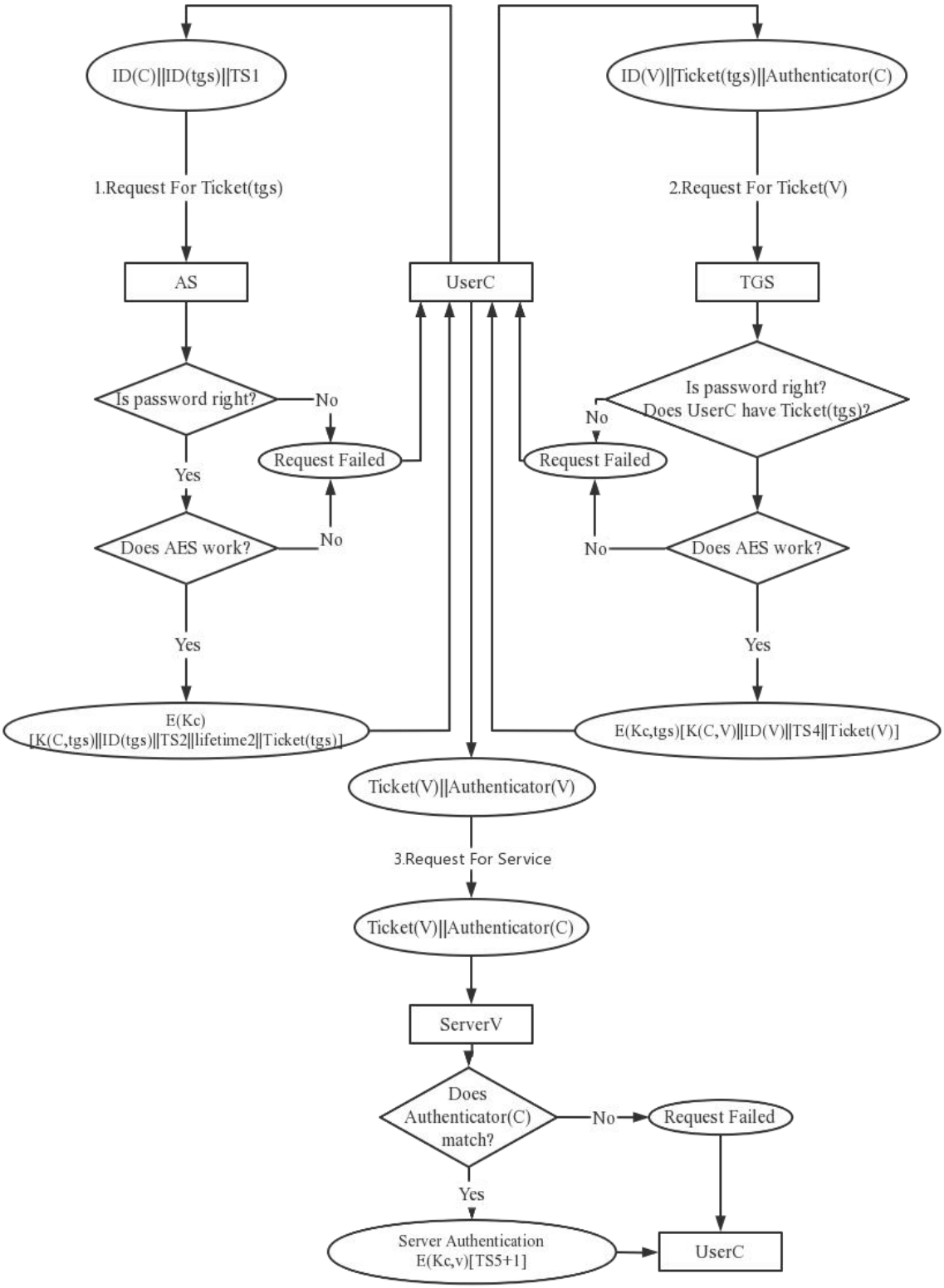
(2)保密性、完整性、可用性、真实性、责任性和不可否认性是网络安全的主要目标。

(3)访问控制、加密、签名、填充和审计是基本的网络安全机制。

(4)GB/T 和 GM/T 是我们在工作过程中应该遵守的标准。

Ex&KeyU2

1.Please design a procedure for server C to authenticate user U and generate session key to protect the communication between S and U when there is only AES or SM4 available.



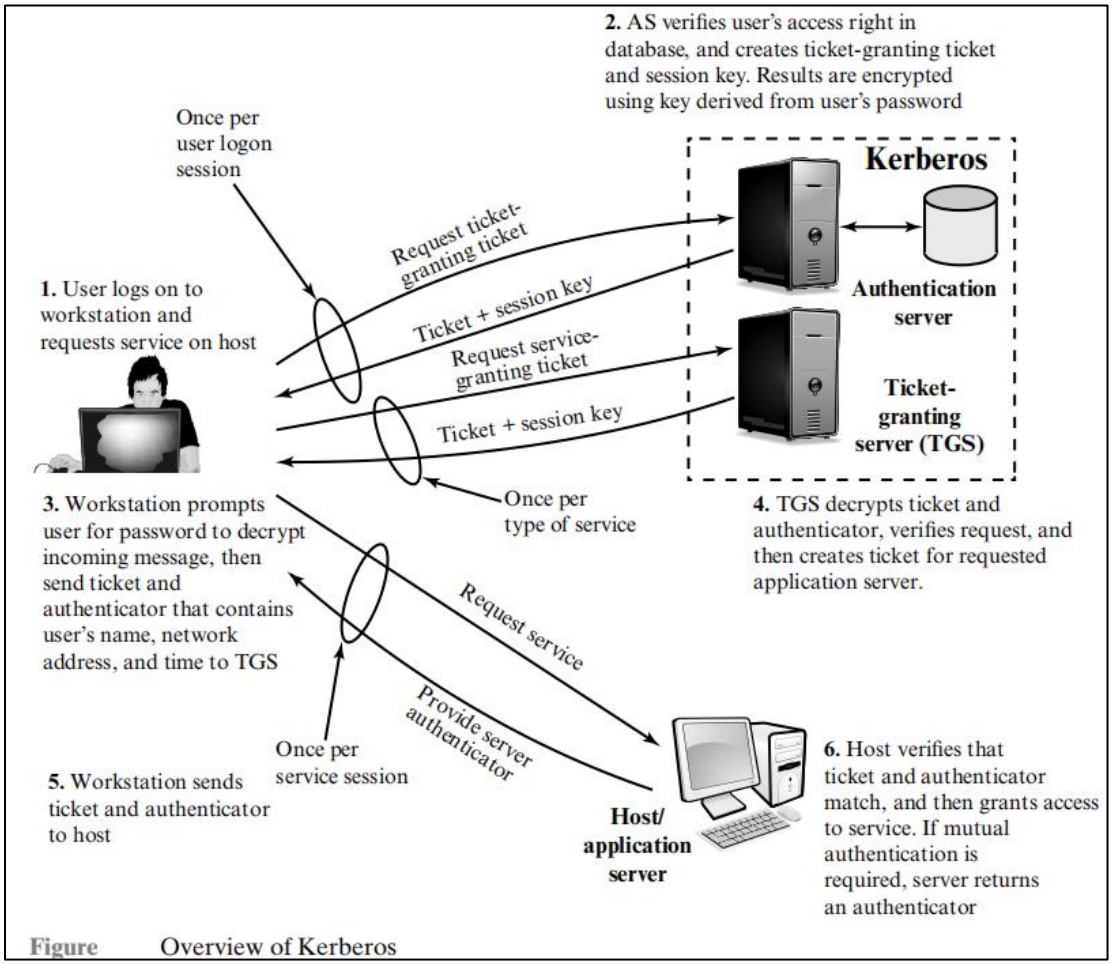


Figure Overview of Kerberos

2.What types of keys are used by the Key Distribution Center (KDC)? Please briefly describe the procedure.

• Types of keys:

(1)permanent key(master key, mk)

(2)session key

• Procedure:

(1)A and B connect to KDC with their own master key such as mkA,mkB;

(2)KDC generates the session key;

(3)KDC encrypts the key with mkA of A to skA and send it to A;

(4)KDC encrypts the key with mkB of B to skB and send it to B.

3.A and B have used a key before. Describe the process of using the key to form a new key and restore it briefly.

• enckey=enc(k,skey)

• k=dec(enckey,skey)

4.Points in public key distribution of secret key.

(1)Symmetric key distribution needs pre-shared key.

(2)Diffie-Hellman key exchange provides no authentication.

(3)Public key distribution of secret key

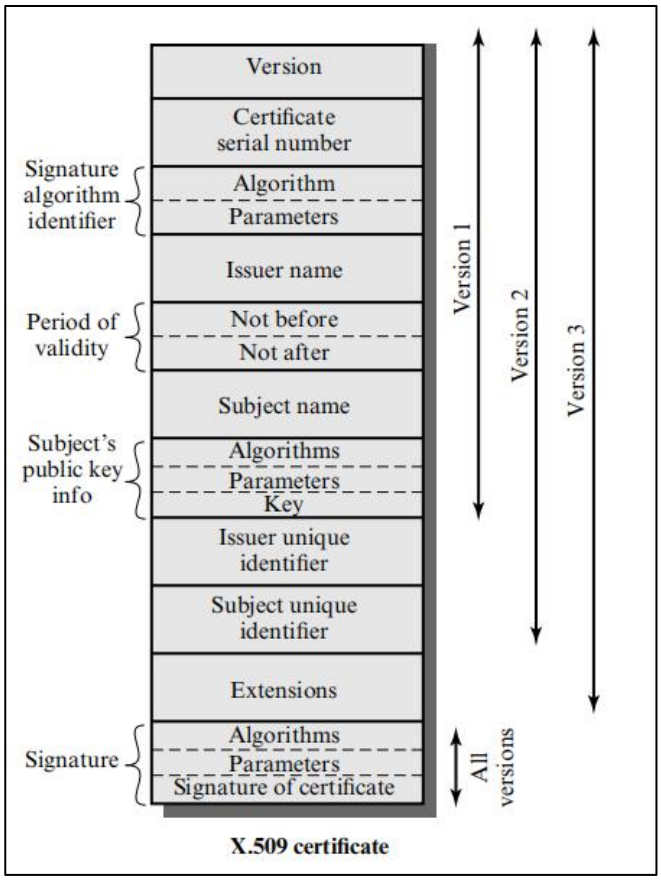
- esk=enc(pkU, sk)——Encrypt a key with the recipient's public key and send it to the recipient.
- U can, and only u can do sk=dec(skU, esk).
- But U and pk must be bound to make sure that pkU is really of U.

5.What is the function and content of the public key certificate? What is the format of X.509 certificate?

(1) Function: bind user's ID and public key

(2) Content: public key, user ID, signature data of authentication center

(3) X.509 certificate format:



6.Noun interpretation：

(1)CA:Certification Authority

(2)RA:Registration Authority

(3)CRL:Certificate Revocation List

7.SummaryU2

(1)Symmetric key distribution needs pre-shared secret.

(2) Kerberos is a KDC that consists of AS and TGS.AS grants ticket for accessing TGS, and TGS grants tickets for accessing application servers.

(3)Public key distribution can do authentication at the same time.
(4)Certificate is used to bind user and public key.
(5)The principal objective of PKI is to enable secure,convenient, and efficient acquisition of public keys.
(6)Identity management is an approach to provide access to resources.

习题&重点 U2

1.当只有 AES 或 SM4 可用时，请为服务器 S 设计一个程序来验证用户 C 并生成会话密钥以保护 S 和 C 之间的通信。

Table Summary of Kerberos Version 4 Message Exchanges

(1) C → AS $ID_c \| ID_{tgs} \| TS_1$

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

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

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

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

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

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

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

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

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

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

(6) V → C $E(K_{c,v}, [TS_5 + 1])$(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

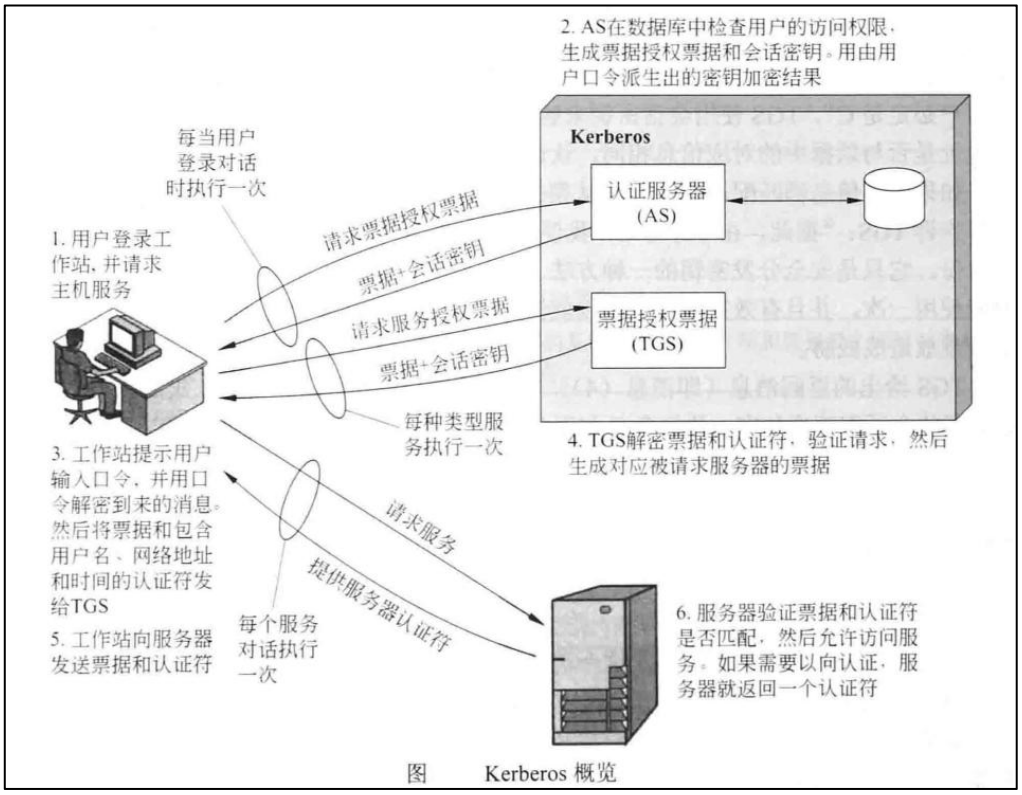


图 Kerberos 概览

2.密钥分发中心(KDC)用到的密钥有哪些类型？请简述操作过程。

• 类型：

(1)永久密钥

(2)会话密钥

• 操作过程：

(1)A 和 B 使用自己的主密钥（如 mkA、mkB）连接到 KDC；

(2)KDC 生成会话密钥；

(3)KDC 用 A 的 mkA 将密钥加密成 skA 并发送给 A；

(4)KDC 用 B 的 mkB 将密钥加密成 skB 并将其发送给 B。

3.A 和 B 之前使用过一个密钥，简述利用该密钥形成新密钥以及还原的过程。

• enckey=enc(k,skey)

• k=dec(enckey,skey)

4.基于公钥密码算法的密钥分发中需要注意的点

(1)对称密钥分发需要预共享密钥

(2)Diffie-Hellman 密钥交换不提供身份验证

(3)密钥的公钥分发：

• esk=enc(pkU,sk)——用接收者的公钥加密一个密钥发给接收者

• U 可以，而且只有 U 可以做到 sk＝dec(skU,esk)

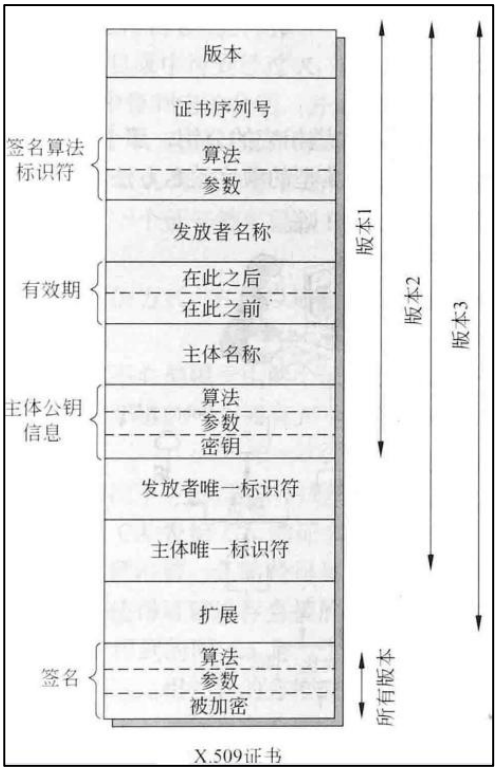
• 但 U 和 pk 必须确保 pkU 是真实的

5.公钥证书的功能和内容是什么？X.509 证书的格式是怎么样的？

(1)功能：绑定用户 ID 和公钥

(2)内容：公钥、用户 ID、认证中心的签名数据

(3)X.509 证书的格式：



6.名词解释：
(1)CA:认证中心
(2)RA:注册中心
(3)CRL:证书撤销列表

7.总结 U2
(1)对称密钥分发需要预共享密钥。
(2)Kerberos 是一个 KDC，由 AS 和 TGS 组成。AS 授予访问 TGS 的票证，TGS 授予访问应用程序服务器的票证。
(3)公钥分发可以同时进行身份验证。
(4)证书用于绑定用户和公钥。
(5)PKI 的主要目标是实现安全、方便和高效地获取公钥。
(6)身份管理是一种提供资源访问的方法。

Ex&KeyU3

1.Explain the principle of IEEE802.1x from the viewpoint of its architecture (port-based).

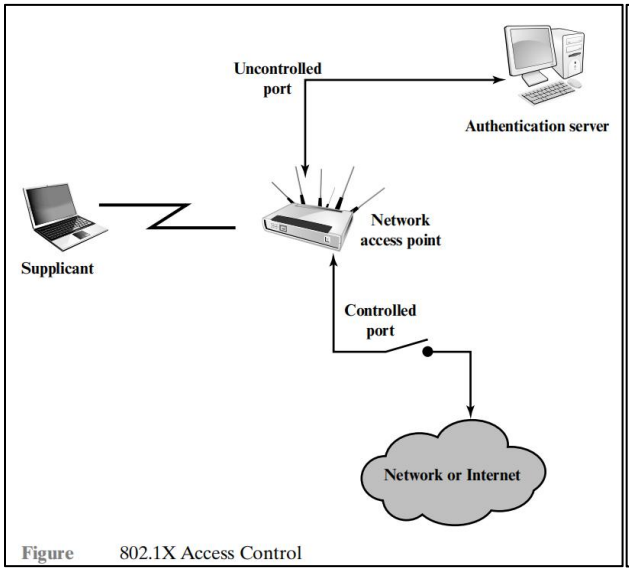


Figure 802.1X Access Control

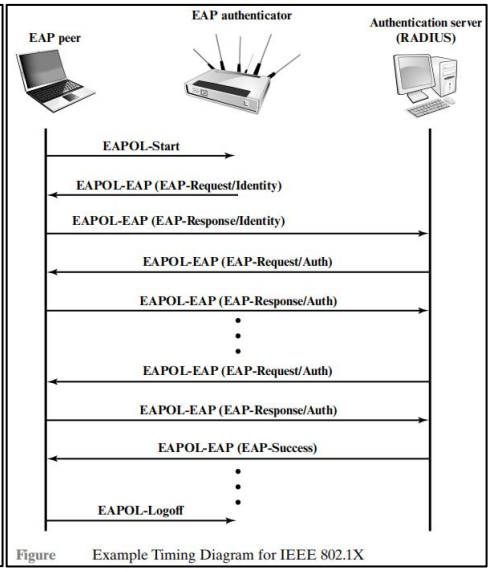


Figure Example Timing Diagram for IEEE 802.1X

IEEE802.1x uses the concept of controlled port and uncontrolled port.

• Uncontrolled ports ignore the authentication status of the requester, that is, whether the requester is authorized or not, he can communicate with the authentication server.

• The controlled port can communicate with other systems on the network only when the current requester is authorized to exchange. The specific process is as follows:

(1) The requester sends the EAPOL-Start packet to the network to determine whether there is an authenticator in the network, and if there is one, notify the authenticator that the request is ready;

(2) The authenticator sends the EAP request identity information to the requester, which is encapsulated in the EAPOL-EAP package;

(3) The requester sends the EAP response identity information to the authentication server AS through the uncontrolled port;

(4) The AS sends the EAPOL-EAP package to send the EAP request authentication information to the requester, and the requester sends the EAP response authentication information to the AS, and so on until the AS sends the EAP success message to the requester to allow the requester to access the network;

(5) Once the decision is made to allow the requester to access the network, the authenticator uses the EAP-key package to send the key to the requester;

(6) The requester holds the key and connects to the LAN or Internet through the controlled port, and communicates with it;

(7) After the communication, the requester sends the EAP-Logoff package to the authenticator, indicating that it wants to disconnect from the network.

2.What are the types of cloud computing deployment models?

(1) Public cloud

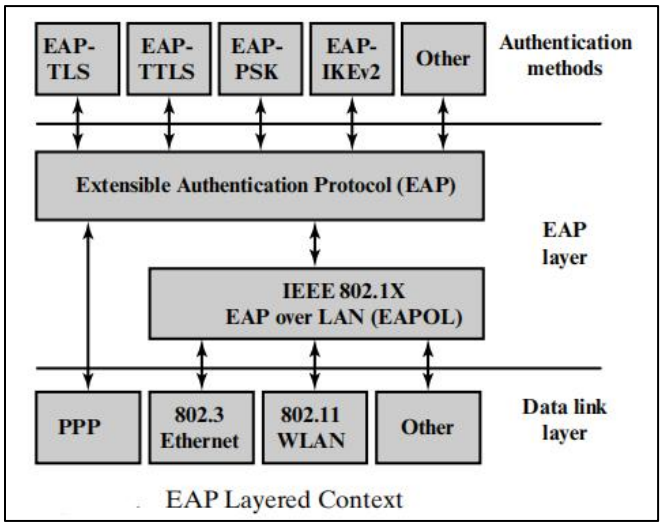
(2) Private Cloud

(3) Community cloud

(4) Hybrid cloud

3.What is EAP?What is the framework like?

EAP is extensible authentication protocol. The layered context is as follows:



EAP Layered Context

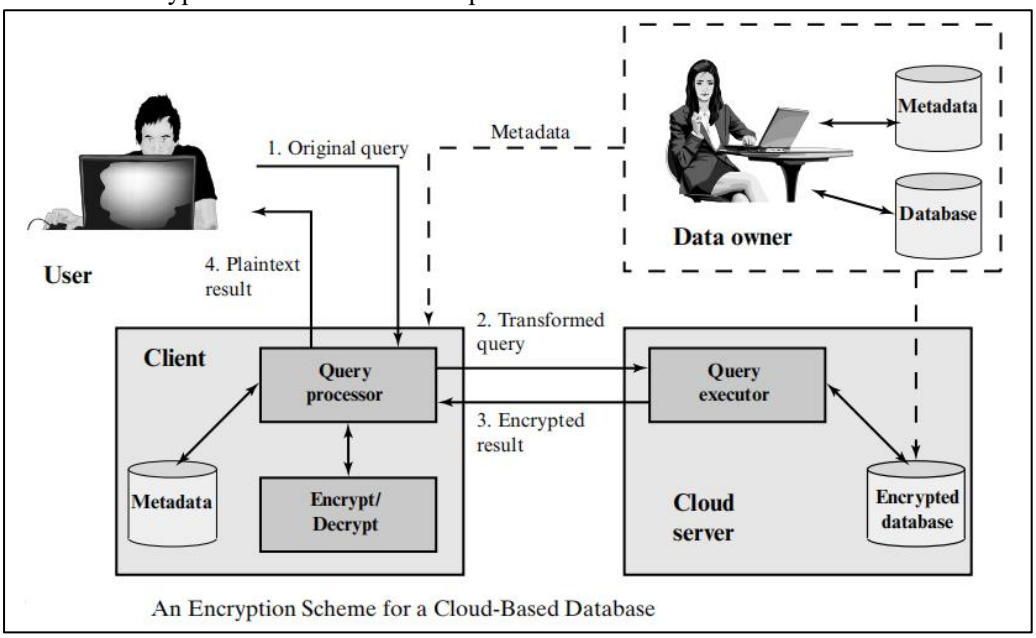
4.Register a free public cloud computing service. What is the model of the serviceyou get?

(1)Software as a service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser.

(2)Platform as a service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.

(3)Infrastructure as a service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which caninclude operating systems and applications.

5.What is the encryption mode of cloud data protection?



An Encryption Scheme for a Cloud-Based Database

6.What is the concept of SecaaS?

SecaaS means Security as a Service.

7.SummaryU3

(1)Network access control(NAC) based on authentication.

(2)IEEE 802.1x, employing extensible authentication protocol(EAP), is a framework for NAC.

(3)IaaS, PaaS and SaaS are service models of cloud computing(CC); public cloud, private cloud,community cloud are deployment models of CC;consumer, provider, auditor, broker and carrier are roles of CC.

(4)Abuse, malicious insider, data leakage, insecure interface are major risks of CC.

(5)Data encryption is necessary in CC.

习题&重点 U3

1.从架构（基于端口）的角度解释 IEEE802.1x 的原理。

IEEE802.1x 使用了受控端口和未受控端口的概念。

未受控端口会忽略请求者的认证状态，即无论请求者是否获得授权，他都可以和认证服务器通信。

受控端口只有在当前请求者被授权允许进行交换时，才可以在请求者与网络上的其他系统通信。具体过程如下：

(1)请求者向网络发出 EAPOL-Start 包，判断该网络中是否存在认证者，如果存在，则通知该认证者请求已经准备好；

(2)认证者向请求者发送 EAP 请求身份标识信息，该信息被封装在 EAPOL-EAP 包中；

(3)请求者通过未受控端口向认证服务器 AS 发送 EAP 应答身份标识信息；

(4)AS 发送 EAPOL-EAP 包向请求者发送 EAP 请求认证信息，请求者向 AS 发送 EAP 应答认证信息，如此往复直到 AS 向请求者发送 EAP 成功消息允许请求者接入网络；

(5)一旦决定允许请求者接入网络，认证者使用 EAP-key 包向请求者发送密钥；

(6)请求者持有密钥并通过受控端口连接到 LAN 或 Internet，并与其通信；

(7)通信结束后，请求者向认证者发送 EAP-Logoff 包，表示希望与网络断开连接。

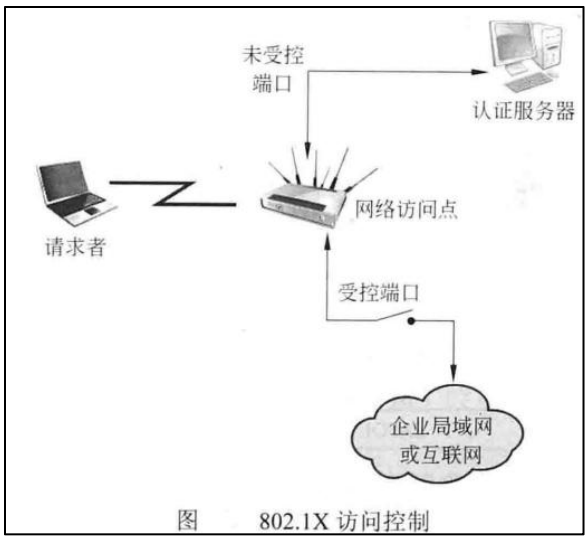


图　802.1X 访问控制

图　IEEE 802.1X 时序示意图

2.云计算部署模型有哪些类型？

(1)公有云

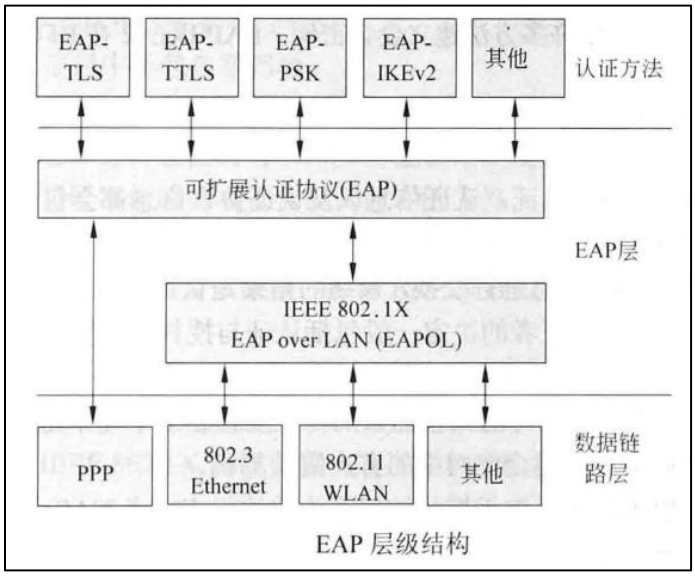
(2)私有云

(3)社区云

(4)混合云

3.EAP 是什么？框架是什么样的？

EAP 是可扩展认证协议。层级结构如下：



EAP 层级结构

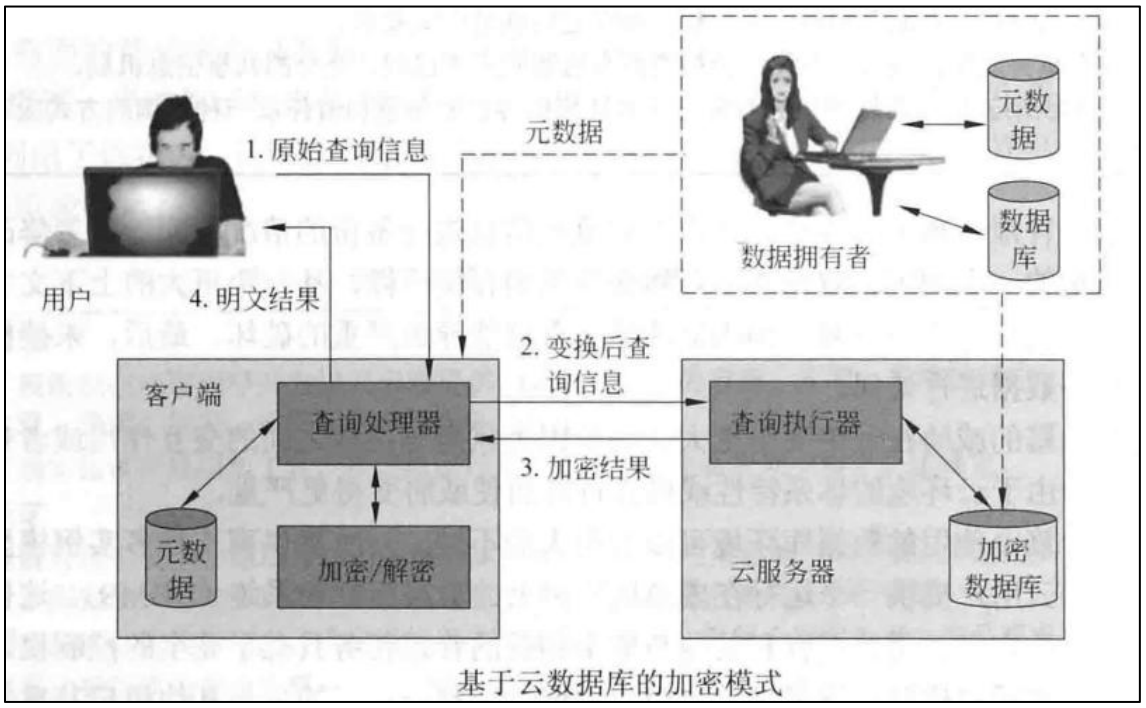
4.注册免费的公共云计算服务。您获得的服务模式是什么？

(1)软件即服务（SaaS）：向消费者提供的功能是使用在云基础设施上运行的提供商应用程序。应用程序可通过诸如 Web 浏览器之类的瘦客户端接口从各种客户端设备访问。

(2)平台即服务（PaaS）：向消费者提供的功能是将消费者使用提供商支持的编程语言和工具创建或获取的应用程序部署到云基础设施上。

(3)基础设施即服务（IaaS）：提供给消费者的功能是提供处理、存储、网络和其他基础计算资源，消费者可以在这些资源中部署和运行任意软件，包括操作系统和应用程序。

5.云端数据保护的加密模式是什么样的？



基于云数据库的加密模式

6.SecaaS 的概念是什么？

SecaaS 是 Security as a Service，意思是安全即服务。

7.总结 U3

(1)基于认证的网络访问控制（NAC）。

(2)IEEE 802.1x 采用可扩展认证协议（EAP），是 NAC 的框架。

(3)IaaS、PaaS 和 SaaS 是云计算（CC）的服务模型；公共云、私有云、社区云是 CC 的部署模型；消费者、提供者、审计员、经纪人和承运人是 CC 的角色。

(4)滥用、恶意内幕、数据泄露、界面不安全是 CC 的主要风险。

(5)CC 中需要数据加密。

Ex&KeyU4

1.What is the difference between TKIP and CCMP?

(1) TKIP only needs to make software changes to the equipment supported by WEP. CCMP is set to enable the new version of IEEE 802.11 equipment equipped with hardware to support this mechanism;

(2) TKIP adds information integrity field after the data domain of 802.11 MAC frame to ensure information integrity, and CCMP uses message authentication code to ensure information integrity;

(3) TKIP uses RC4 stream cipher algorithm to encrypt MAC protocol data unit and information integrity field to ensure data confidentiality, and CCMP uses AES's CTR cipher block mode for data encryption.

2.Develop a program to encrypt data stream byte by byte using AES or SM4 in CTR mode. You can select programing language and platform freely.

3.Key

(1)IEEE 802.11 is the standard of wireless network, and some of it involves network security; IEEE 802.11i is the standard of wireless network security, and WAPI is the standard of wireless network security in China.

(2)Wi-Fi(Wireless Fidelity)， Wi-Fi Alliance

(3)The Wi-Fi Alliance has developed certification procedures for IEEE 802.11 security standards,referred to as Wi-Fi Protected Access (WPA). The most recent version of WPA,known as WPA2, incorporates all of the features of the IEEE 802.11i WLAN security specification.

4.IEEE 802.11 Terminology

(1)Access point (AP): Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.

(2)Station(STA): Any device that contains an IEEE 802.1 1 conformant MAC and physical layer.

(3)Basic service set (BSS): A set of stations controlled by a single coordination function.

(4)Extended service set (ESS): A set of one or more interconnected BSSs and integrated L ANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.

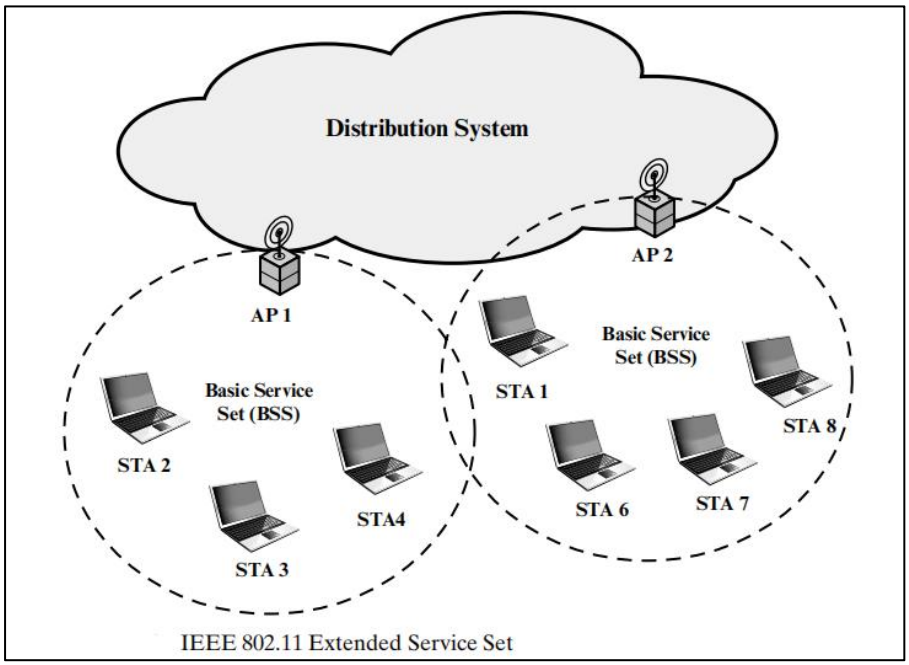
(5)Distribution system (DS): A system used to interconnect a set of BSSs and integrated L ANS to create an ESS.

5.Key2

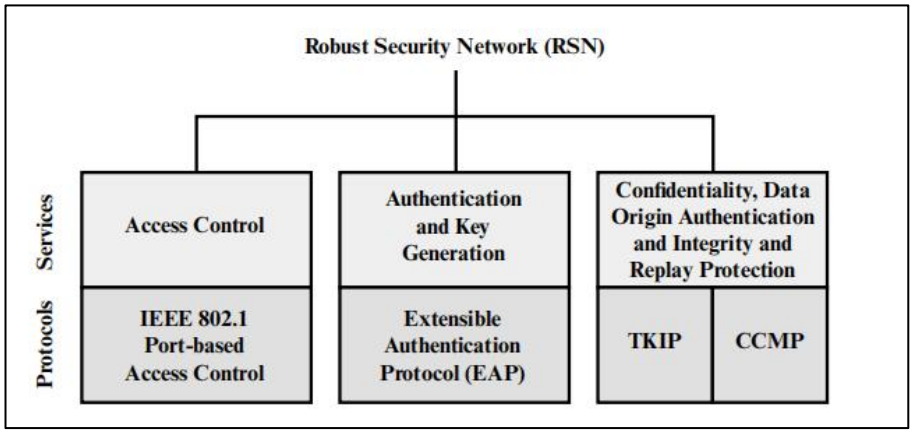
(1)In IEEE 802.11 access and security service is defined as WEP(Wired Equivalent Privacy).

(2)IEEE 802.11i extends and enhances WEP, and the final form is RSN (robust and secure network).

6.What is the composition and architecture model of IEEE 802.11 network?



7.What is the structure of RSN?



8.Key3

(1)TKIP uses RC4 stream cipher algorithm, which is suitable for communication; CCMP uses AES block cipher algorithm into CTR stream cipher algorithm and CBC-MAC hash cipher algorithm.

9.SummaryU4

(1)WIFI alliance developed WPA and WPA2,the certification procedures, to incorporate IEEE 802.11 and IEEE 802.11i.

(2)WLAN consists of STAs and AP.

(3)IEEE 802.11i employs 802.1x to do authentication, supports TKIP and CCMP.

(4)TKIP is based on RC4.

(5)CCMP makes use of AES.

习题&重点 U4

1.TKIP 和 CCMP 之间的区别是什么？

(1)TKIP 只需要对 WEP 支持的设备进行软件改变，CCMP 是为了让新版本的由硬件装备的 IEEE 802.11 设备支持该机制而设置的；

(2)TKIP 在 802.11 MAC 帧的数据域后增加信息完整性字段保证信息完整性，CCMP 利用消息身份验证代码来确保信息完整性；

(3)TKIP 通过 RC4 流密码算法来加密 MAC 协议数据单元和信息完整性字段来确保数据机密性，CCMP 使用 AES 的 CTR 密码块模式进行数据加密。

2.开发一个程序，在 CTR 模式下使用 AES 或 SM4 逐字节加密数据流。您可以自由选择编程语言和平台。

3.重点 1

(1)IEEE 802.11 是无线网络的标准，有一部分涉及网络安全；IEEE 802.11i 完全是无线网络安全方面的标准，WAPI 是我国的无线网络安全标准。

(2)相关概念：Wi-Fi(Wireless Fidelity)，Wi-Fi Alliance

(3)最近，Wi-Fi 联盟为 IEEE 802.11 安全标准制订了认证系统，称为 Wi-Fi 网络安全存取(WPA)。最新版本的 WPA 是 WPA2，整合了 IEEE802.11i 无线局域网安全规范的各种特色。

4.IEEE 802.11 术语

(1)接入点(AP)：具有站点功能并通过无线介质为相关站点提供对分发系统访问的任何实体。

(2)站点(STA)：包含符合 IEEE 802.1 1 的 MAC 和物理层的任何设备。

(3)基本服务集(BSS)：由单个协调功能控制的一组站。

(4)扩展服务集(ESS)：一组一个或多个互连的 BSS 和集成的 L AN，在与这些 BSS 中的一个相关联的任何站点作为单个 BSS 出现在 LLC 层。

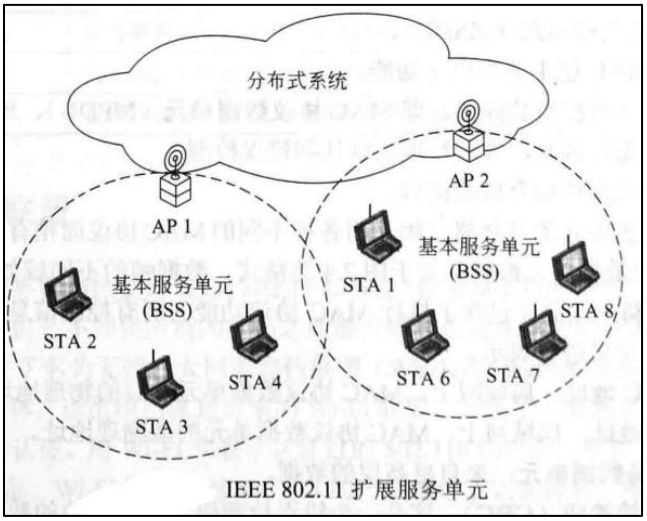
(5)分配系统(DS)：用于互连一组 BSS 和集成 L ANS 以创建 ESS 的系统。

5.重点 2

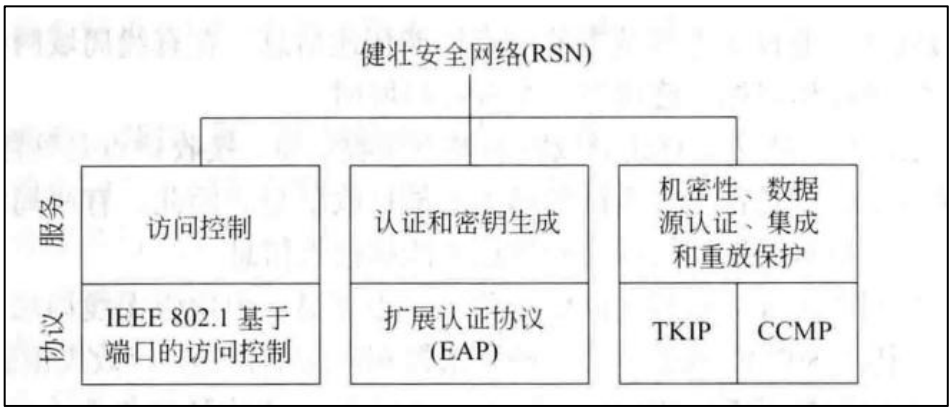
(1)在 IEEE 802.11 中，接入和安全服务被定义为 WEP（有线等效隐私）。

(2)IEEE 802.11i 对 WEP 进行扩展增强，最终形式为 RSN（健壮安全网络）。

6.IEEE 802.11 网络组成与架构模型是什么样的？



7.RSN 的结构是什么样的？



8.重点 3

(1)TKIP 使用 RC4 流密码算法，适用于通信；CCMP 将 AES 分组密码算法用成 CTR 流密码算法和 CBC-MAC 哈希密码算法

9.总结 U4

(1)WIFI 联盟开发了 WPA 和 WPA2 认证程序，以结合 IEEE 802.11 和 IEEE 802.11i。

(2)WLAN 由 STA 和 AP 组成。

(3)IEEE 802.11i 采用 802.1x 进行认证，支持 TKIP 和 CCMP。

(4)TKIP 基于 RC4。

(5)CCMP 使用 AES。

Ex&KeyU5

1.What are the advantages of IPSec?

(1) When IPSec is used in routers and firewalls, it provides strong security for all traffic flows through its boundaries.

(2) IPSec in the firewall can prevent bypass when all external traffic must use IP.

(3) IPSec is under the transport layer (TCP, UDP), so it is transparent to all applications.

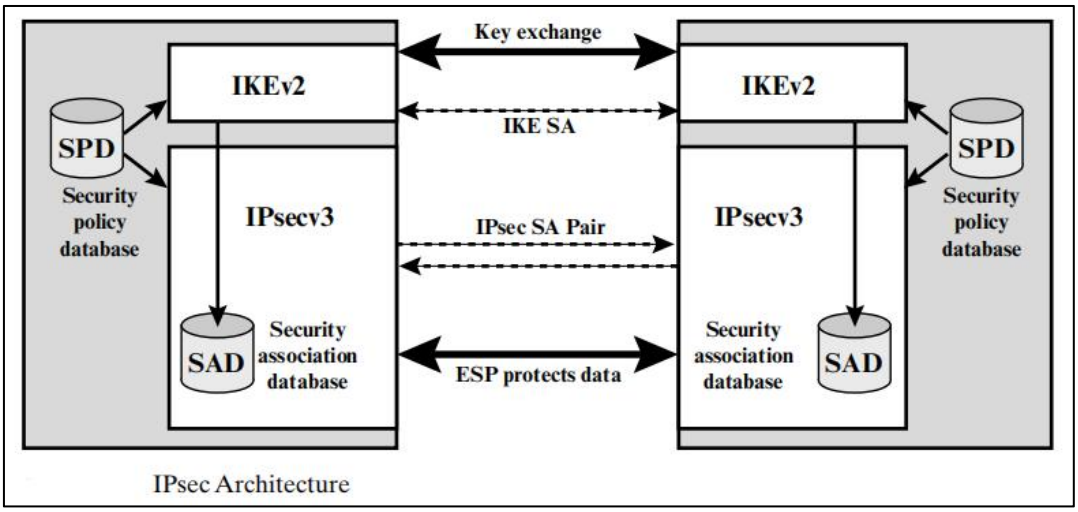
(4) IPSec can be transparent to end users.

(5) If necessary, IPSec can provide security for individual users.

2. What is the structure of IPSec?

(1)IPSec provides access control,confidentiality, integrity, anti-replay.

(2)IKE, SPD and SAD are components of IPSec.

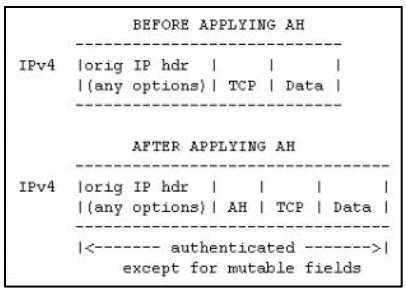


3.Functions and structure of packet of AH protocol

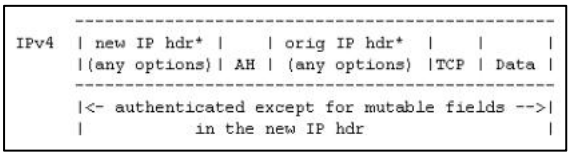
(1)Functions:Data Source Verification,Anti-Replay

(2)Structure of packet

• Transport Model



• Tunnel Model

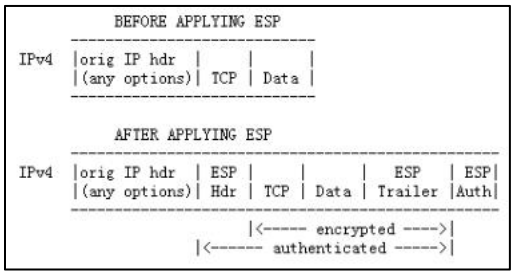


4.Functions and structure of packet of ESP protocol

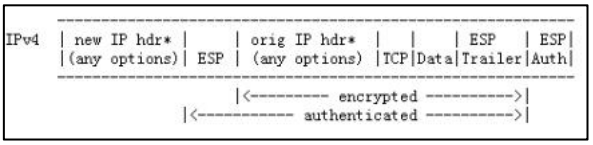
(1)Functions:Confidentiality,Data Source Verification,Anti-Replay

(2)Structure of packet

• Transport Model



• Tunnel Model



5.Comparing with AH and ESP

(1)Authentication of AH is more secure than that of ESP, for AH extends its authentication to the external IP header.

(2)For ESP, tunnel mode is more secure than transfer mode but requires more bandwidth,and the funtions of ESP includes the functions of AH.

6.SummaryU5

(1)IPSec provides access control,confidentiality, integrity, anti-replay.

(2)IKE, SPD and SAD are components of IPSec.

(3)IPSec support transport and tunnel modes.

(4)There are AH and ESP in IPSec, and AH is more secure than ESP in authentication.

(5)AES and SHA are used in IPSec.

习题&重点 U5

1.IPSec 的优点有哪些？

(1)当在路由器和防火墙中使用 IPSec 时，它对通过其边界的所有通信流提供了强安全性。

(2)防火墙内的 IPSec 能在所有的外部流量必须使用 IP 时阻止旁路。

(3)IPSec 位于传输层(TCP、UDP)之下，所以对所有的应用都是透明的。

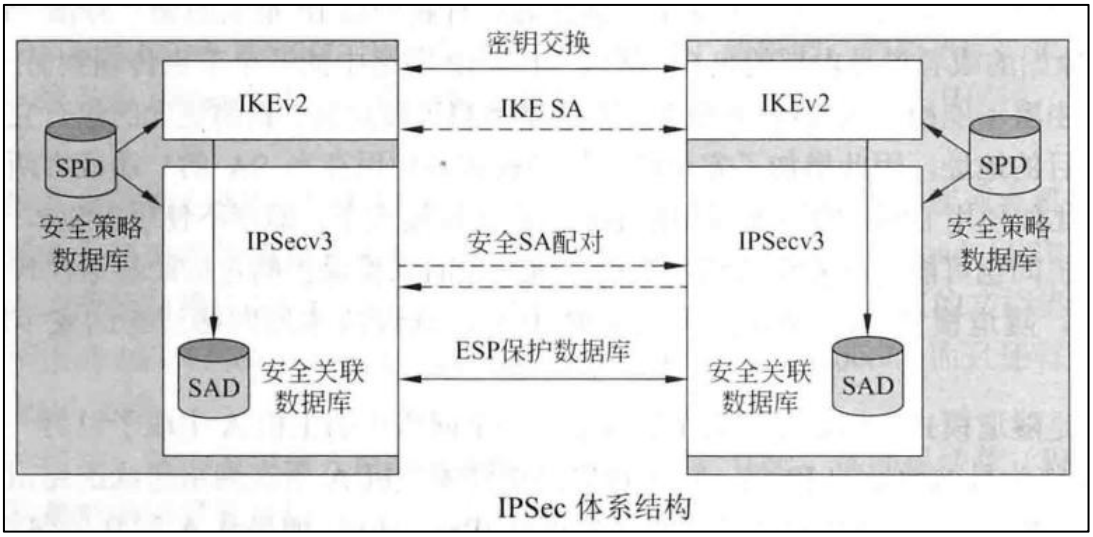
(4)IPSec 可以对终端用户是透明的。

(5)若有必要，IPSec 能给个人用户提供安全性。

2.IPSec 的结构是什么样的？

(1)IPSec 提供访问控制、保密性、完整性和防重放。

(2)IKE、SPD 和 SAD 是 IPSec 的组成部分。

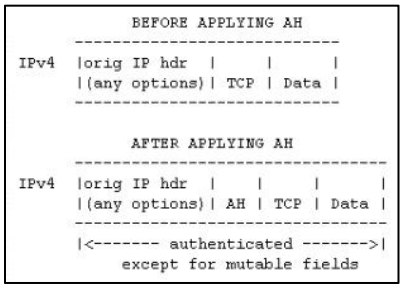


3.AH 协议的功能和包的结构

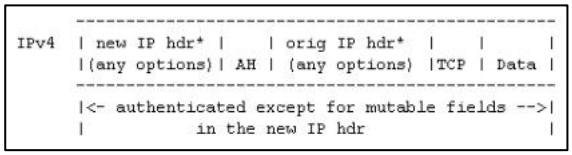
(1)功能：数据源验证，反重放

(2)结构：

• 传输模型



• 隧道模式

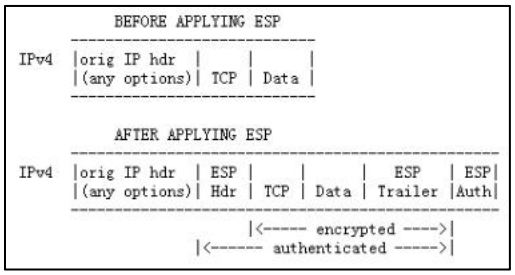


4.ESP 协议的功能和包的结构

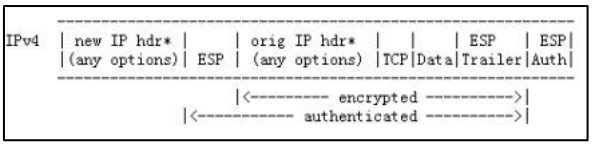
(1)功能：保密，数据源验证，反重放

(2)结构：

• 传输模型



• 隧道模式



5.AH 协议和 ESP 协议的比较

(1)AH 的认证比 ESP 更安全，因为 AH 扩展了额外 IP 报头的认证。

(2)对于 ESP，隧道模式比传输模式更安全，但需要更多带宽，并且 ESP 的作用包含了 AH 的作用。

6.总结 U5

(1)IPSec 提供访问控制、保密性、完整性和防重放。

(2)IKE、SPD 和 SAD 是 IPSec 的组成部分。

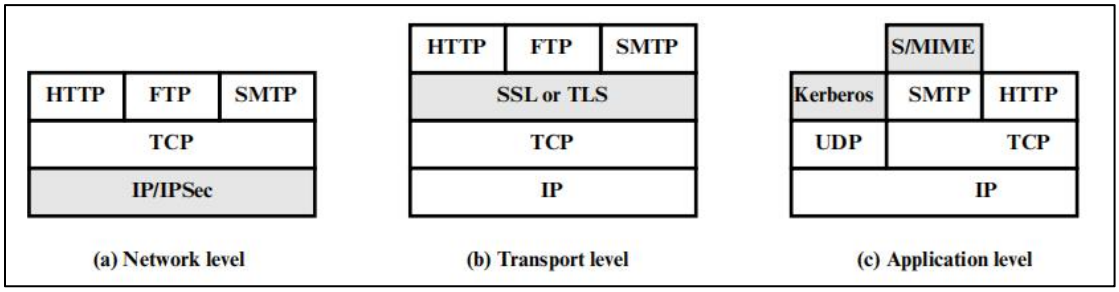
(3)IPSec 支持传输和隧道模式。

(4)IPSec 中有 AH 和 ESP，并且 AH 在认证方面比 ESP 更安全。

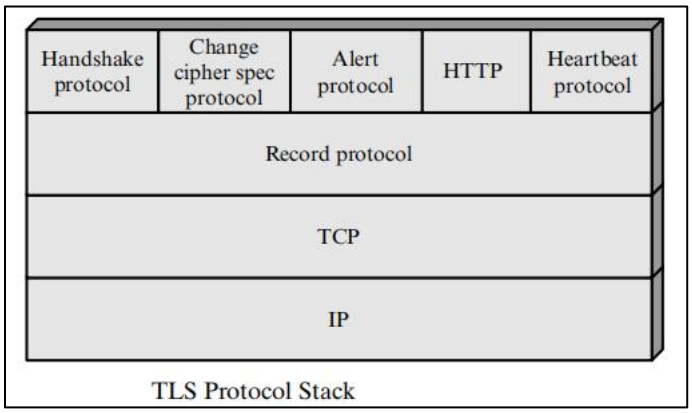
(5)IPSec 中使用 AES 和 SHA。

Ex&KeyU6

1.Protocol Location



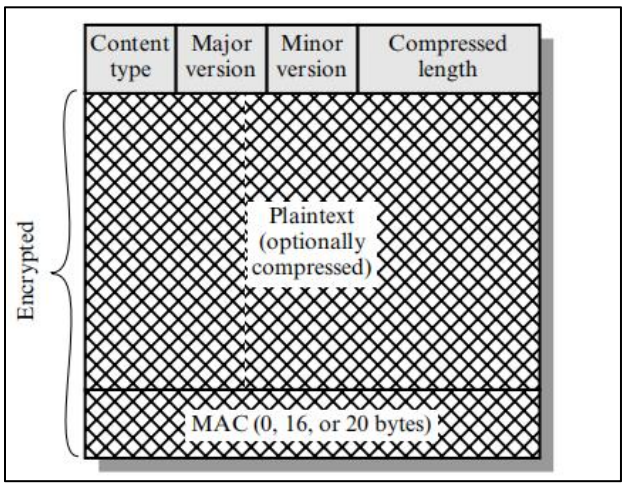
2.SSL Protocol Stack



3.Functions,packet structure,content types and options of SSL Record Protocol

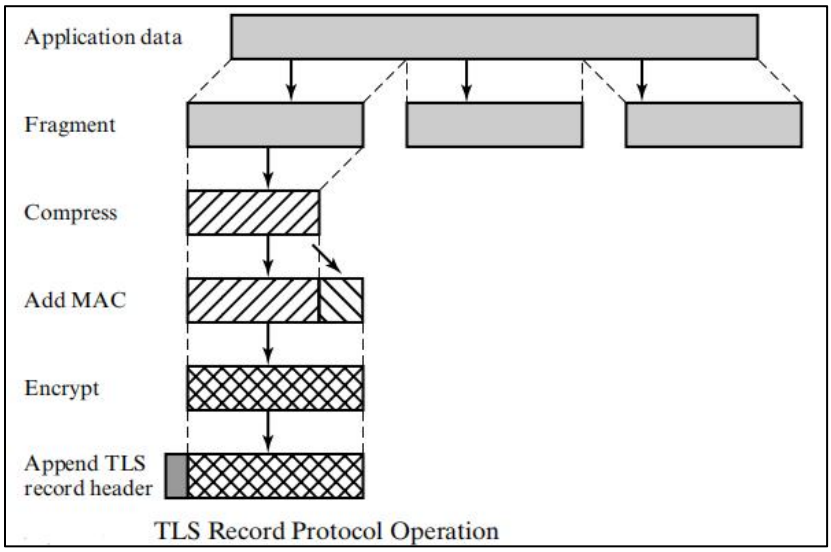
(1)Functions:Confidentiality,Message integrity

(2)Packet Structure:



(3)Content Types:charge-cipher-spec,alert,handshake,application_data

(4)Options:



TLS Record Protocol Operation

Compression and encryption cannot be exchanged because the encrypted data is random and cannot be compressed.

4.Cryptographic computations

(1)Master secret creation

• pre_master_secret——generated by the client,encrypted with the server's public RSA key and sended to the server(Digital Envelope)

• master_secret

```
master_secret =
   PRF(pre_master_secret, "master secret", ClientHello.random || ServerHello
.random)
```

(2)Generation of cryptographic parameters——part of key_block generated from master_secret

5.HTTPS

(1)Data Encrypted:URL,Content of http,Header of http

(2)After HTTP uses SSL, all content transportted will be encrypted.

6.SummayU6

(1)Web needs CIA.

(2)Https provides CIA for Web by employing SSL/TLS.

(3)SSL includes record, handshake, change cipher spec and alert protocol.

(4)A SSL session can serve multiple connections.

(5)Record protocol operation includes application fragment, compress, add MAC, encrypt and append SSL record header.

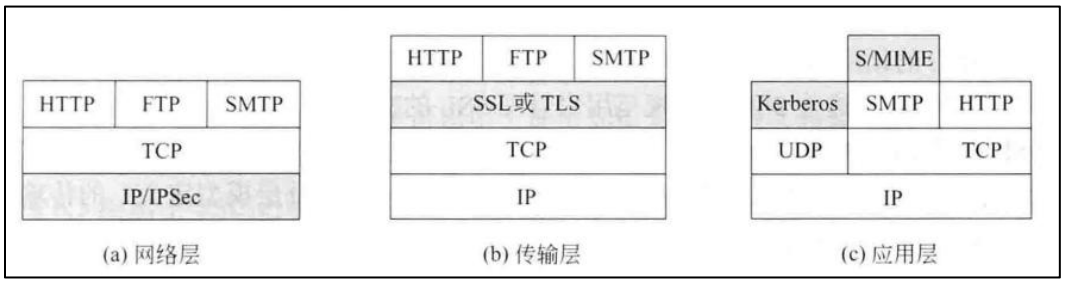
(6)There are pre_ master_ secret, master_ secret and key_ block in SSL.

(7)SSH includes transport layer, user authentication and connection protocol.

(8)SSH supports channel of session, x11 and port forwarding.

习题&重点 U6

1.协议层面



2.SSL 协议栈

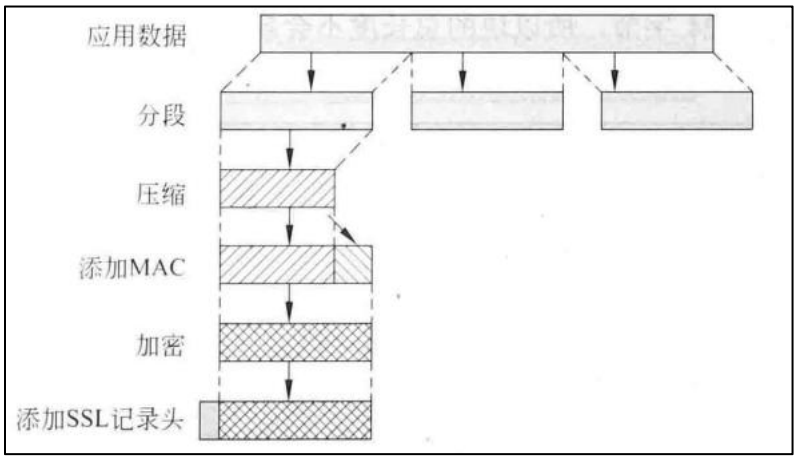
3.SSL 记录协议的功能、包的结构、内容类型、运行流程

(1)功能：机密性、消息完整性

(2)包的结构：

(3)内容类型：修改密码规格、警报、握手、应用程序数据

(4)运行流程：



压缩和加密不能交换，因为加密后的数据具有随机性，无法压缩。

4.密钥计算

(1)主密钥创建

• 预备主密钥——由客户端生成然后用服务器的 RSA 公钥加密并发给服务器(数字信封)

• 主密钥

```
master_secret =
   PRF(pre_master_secret, "master secret", ClientHello.random ‖ ServerHello
.random)
```

(2)生成加密参数——主密钥生成的密钥块的一部分

5.HTTPS

(1)加密的数据：URL，文件的内容，浏览器表单

(2)HTTP 使用 SSL 后，传输的所有内容都会被加密。

6.总结 U6

(1)网络需要中央情报局。

(2)Https 通过使用 SSL/TLS 为 Web 提供 CIA。

(3)SSL 包括记录、握手、更改密码规范和警报协议。

(4)SSL 会话可以提供多个连接。

(5)记录协议操作包括应用程序片段、压缩、添加 MAC、加密和附加 SSL 记录头。

(6)SSL 中有 pre-mastersecret、mastersecret 和 keyblock。

(7)SSH 包括传输层、用户身份验证和连接协议。

(8)SSH 支持会话通道、x11 和端口转发。

Ex&KeyU7

1.What are the main components of E-mail?

(1)Message User Agent (MUA)

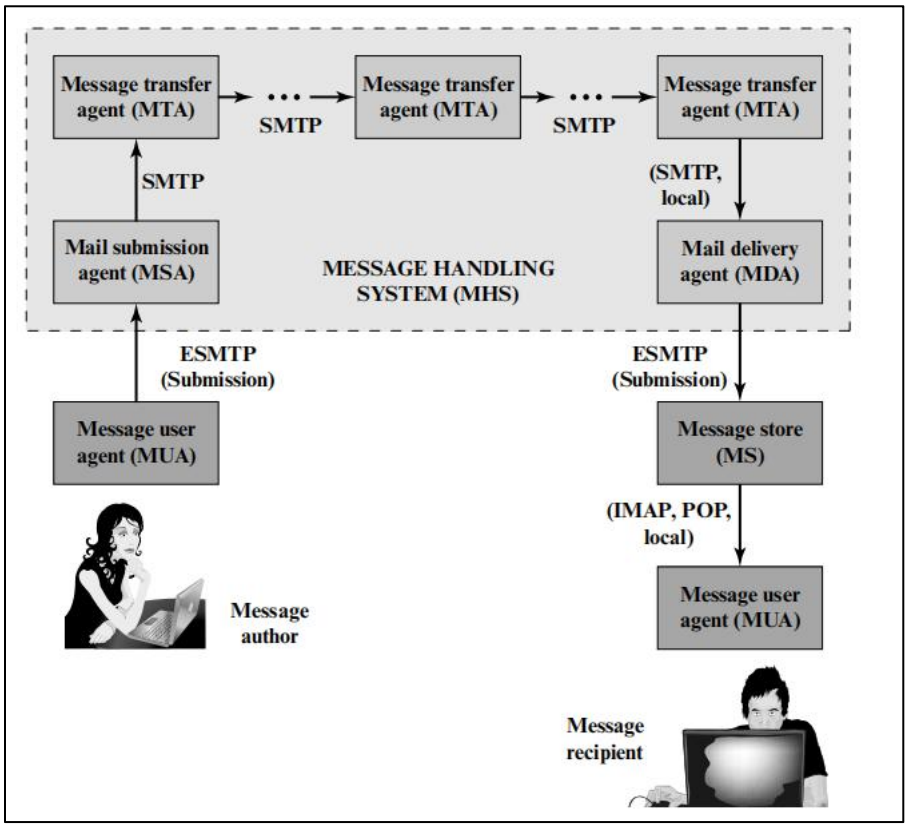
(2)Mail Submission Agent (MSA)

(3)Message Transfer Agent (MTA)

(4)Mail Delivery Agent (MDA)

(5)Message Store (MS)

2.What's the structure of E-mail?



3.What protocols are used in the E-mail structure?What are their own functions?

(1)Simple Mail Transfer Protocol (SMTP):

• Move messages from source to destination by the Internet.

• SMTP encapsulates an e-mail message in an envelope and is used to relay the encapsulated messages from source to destination through multiple MTAs.

Attention:

• Extended SMTP (ESMTP) is often used to refer to these later versions of SMTP.

• SMTP is a text- based client-server protocol.

(2)Mail Access Protocols(MAP):

• Transfer information between mail servers.

• Post Office Protocol(POP 3)

• Post Office Protocol (POP3) allows an e-mail client (user agent) to download an e-mail from an e-maill server (MTA).

•POP3 user agents connect via TCP to the server (typically port 110). After authorization, the

UA can issue POP3 commands to retrieve and delete mail.

• Internet Mail Access Protocol(IMAP)

• Internet Mail Access Protocol (IMAP) also enables an e-mail client to access mail on an e-mail server.

• IMAP also uses TCP, with server TCP port 143.

• IMAP provides stronger authentication than POP3 and provides other functions not supported by POP3.

4.What's the relation between IMAP protocol and POP3 protocol?

(1) Both can allow the UA to access the mail on the email server, and both use TCP protocol.

(2) The server TCP port used by POP3 is 110, and the server TCP port used by IMAP is 143.

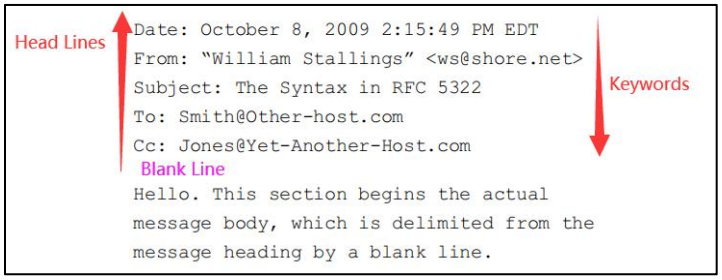
(3) After authorization, the UA can issue the POP3 command to retrieve and delete messages; MAP provides stronger authentication than POP3 and provides other functions that POP3 does not support.

5.E-mail Formats

(1)RFC 822

From RFC 822 to RFC 5322,the e-mail format becomes from simple to complex,from unnormal to normal.

(2)RFC 5322



(3)MIME (RFCs 2045 through 2049)

• Five new message **header fields** are defined, which provide information about the body of the message.

• A number of **content formats** are defined, thus standardizing representations that support multimedia electronic mail.

•**Transfer encodings** are defined that enable the conversion of any content format into a form that is protected from alteration by the mail system.

Attention:MIIME supports all kinds of mail,but cannot solve security problems.

6.What message content types have been added to MIME by Secure/Multipurpose Internet Mail Extension (S/MIME)?

• Data: Refers to the inner MIME-encoded message content, which may then be encapsulated in a SignedData,EnvelopedData, or CompressedData content type.

• SignedData: Used to apply a digital signature to a message.

• EnvelopedData: This consists of encrypted content of any type and encryption keys for one or more recipients.

• CompressedData: Used to apply data compression to a message.

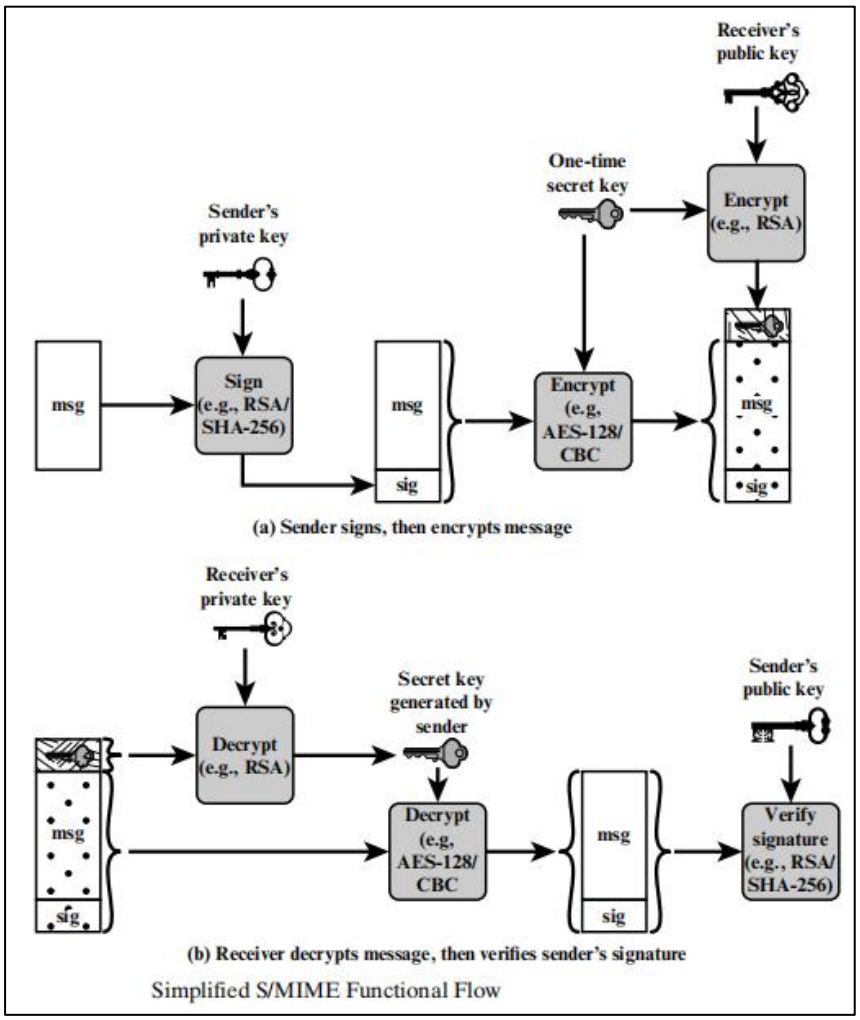
7.What are the functions of SignedData,EnvelopedData and Clear Signing?

(1)SignedData:Used for data signature of messages to ensure integrity and source authentication

(2)EnvelopedData:Encapsulate content and encrypt message to ensure confidentiality

(3)Clear Signing:Store unprocessed delay information, ensure compatibility, and support software that does not support S/MIME

8.Describle the functional flow of S/MIME that ensures the confidentiality and authentication.



Simplified S/MIME Functional Flow

9.SummaryU7

(1)SMTP, POP3 and IMAP are protocols used in email system.

(2)MIME defines the format for email.

(3)S/MIME extends MIME by providing content types such as SignedData, EnvelopedData, CompressedData, etc.

习题&重点 U7

1.电子邮件体系的主要组件有哪些？

(1)消息用户代理 (MUA)

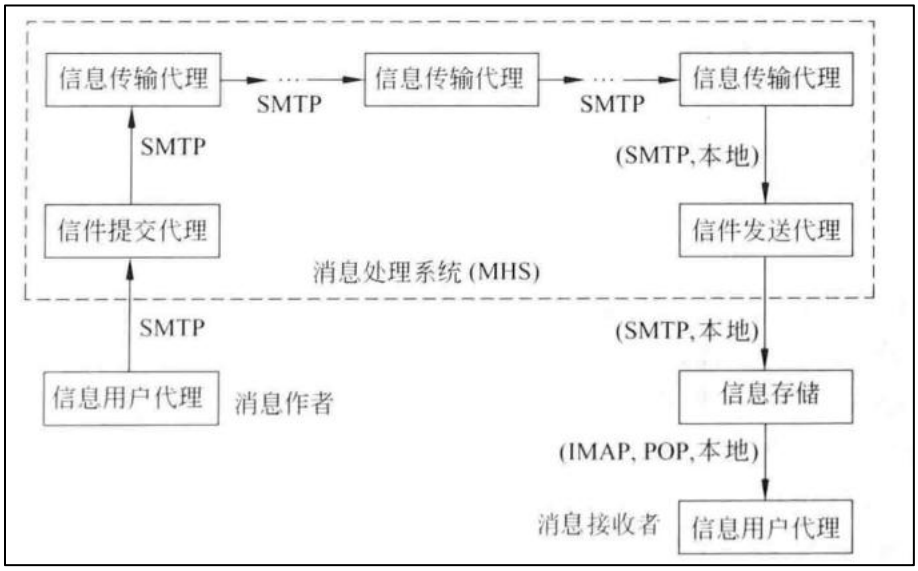
(2)邮件提交代理 (MSA)

(3)邮件传输代理 (MTA)

(4)邮件传递代理(MDA)

(5)信息存储(MS)

2.电子邮件体系的架构是什么样的？



3.电子邮件体系中用到了哪些协议，各有什么作用？

(1)简单的邮件传输协议 (SMTP)：

• 把消息通过互联网从源地移动到目标地

• SMTP 将电子邮件封装在信封中，用于通过多个 MTA 将封装的邮件从源转发到目标。

注：

• 扩展 SMTP（ESMTP）通常用于指代这些较新版本的 SMTP。

• SMTP 是一种基于文本的客户端-服务器协议。

(2)邮件访问协议（MAP）：

• 在邮件服务器之间传输信息

• 邮局协议（POP 3）

• 邮局协议（POP3）允许电子邮件客户端（用户代理）从电子邮件服务器（MTA）下载电子邮件。

• POP3 用户代理通过 TCP 连接到服务器（通常是端口 110）。授权后，UA 可以发出 POP3 命令来检索和删除邮件。

• Internet 邮件访问协议（IMAP）

•Internet 邮件访问协议（IMAP）也允许电子邮件客户端访问电子邮件服务器上的邮件。

• IMAP 还使用 TCP 协议，服务器 TCP 端口是 143。

• IMAP 提供了比 POP3 更强的身份验证，并提供了 POP3 不支持的其他功能。

4.IMAP 协议和 POP3 协议之间的关系？

(1)两者都能让 UA 访问电子邮件服务器上的邮件，都使用 TCP 协议

(2)POP3 使用的服务器 TCP 端口是 110，IMAP 使用的服务器 TCP 端口是 143

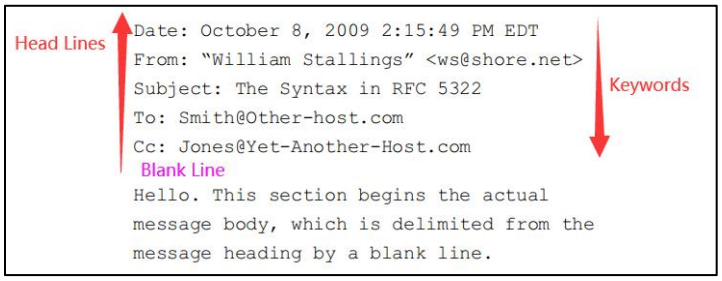
(3)授权后，UA 可以发出 POP3 命令来检索和删除邮件；MAP 提供了比 POP3 更强的身份验证，并提供了 POP3 不支持的其他功能

5.邮件格式

(1)RFC 822

从 RFC 822 到 RFC 5322，电子邮件格式从简单到复杂、不规范到规范。

(2)RFC 5322



(3)MIME (RFCs 2045 through 2049)

- 定义了五个新的消息**头字段**，它们提供了有关消息主体的信息。
- 定义了许多**内容格式**，从而使支持多媒体电子邮件的表示标准化。
- **传输编码**被定义为允许将任何内容格式转换为不受邮件系统更改的形式。

注意：MIIME 支持各种邮件，但不能解决安全问题。

6.安全/多用途互联网邮件扩展(S/MIME)在 MIME 上增加了哪些消息内容类型？

- 数据：指内部 MIME 编码的消息内容，然后可以将其封装为签名数据、封装数据或压缩数据内容类型。
- 签名数据：用于对消息进行数据签名。
- 封装数据：包含任何类型的加密内容和一个或多个收件人的加密密钥。
- 压缩数据：用于对消息应用数据压缩。

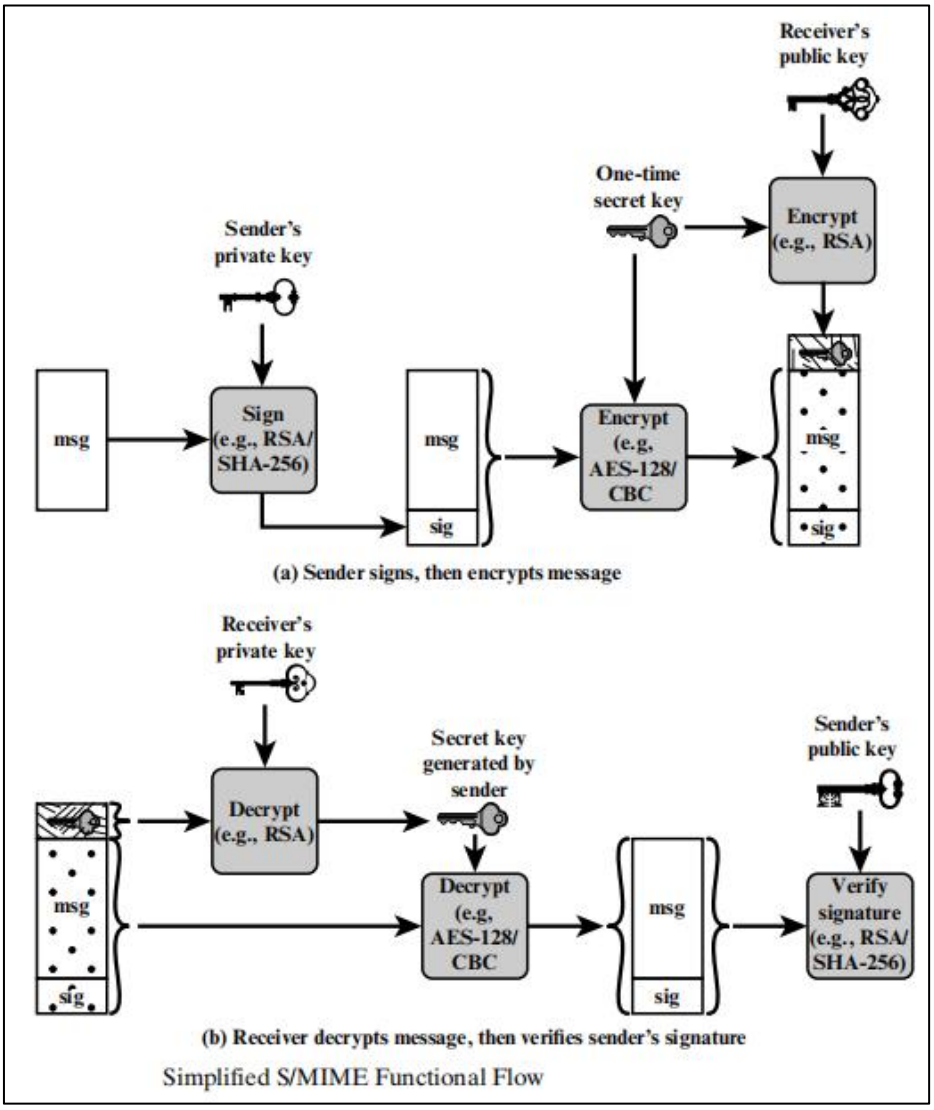
7.签名数据、封装数据和明确签名的作用是什么？

(1)签名数据：对消息进行数据签名，保证完整性，用于来源认证

(2)封装数据：封装内容，加密消息，保证机密性

(3)透明签名：存放未处理的延时信息，保证兼容性，支持那些不支持 S/MIME 的软件

8.描述 S/MIME 保证机密性和认证的功能流的过程。



9.总结 U7

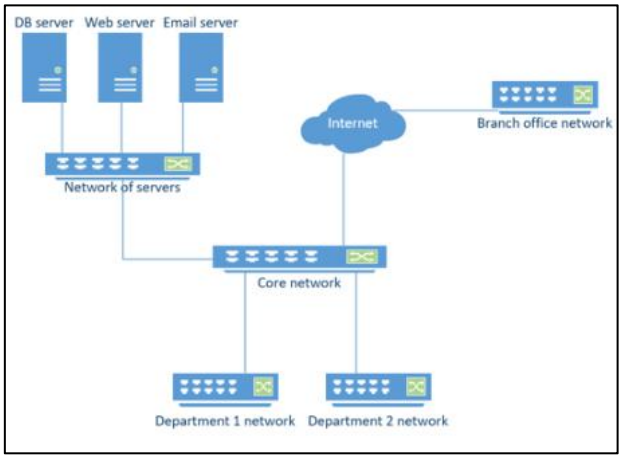
(1)SMTP、POP3 和 IMAP 是电子邮件系统中使用的协议。

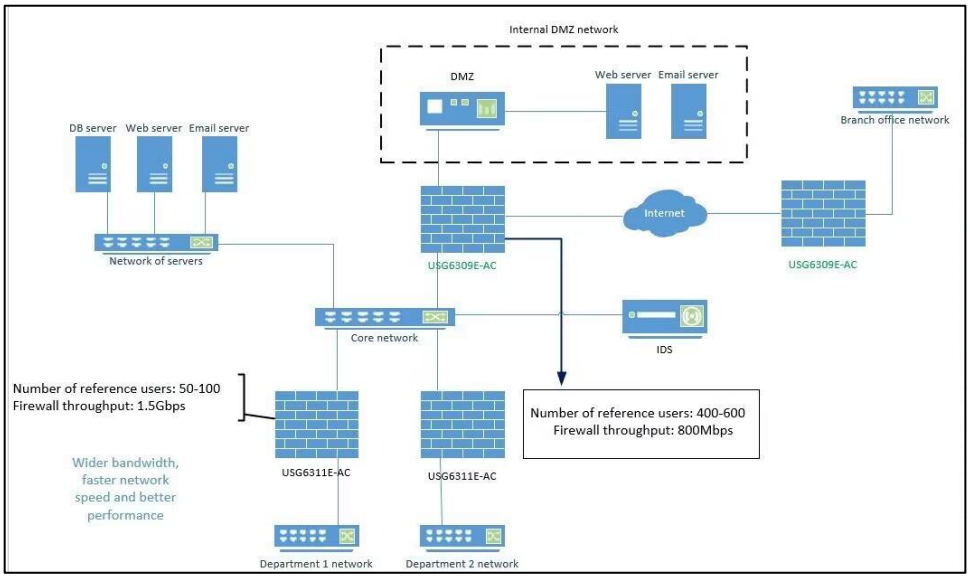
(2)MIME 定义电子邮件的格式。

(3)S/MIME 通过提供 SignedData、EnvelopedData、CompressedData 等内容类型来扩展 MIME。

Ex&KeyU8

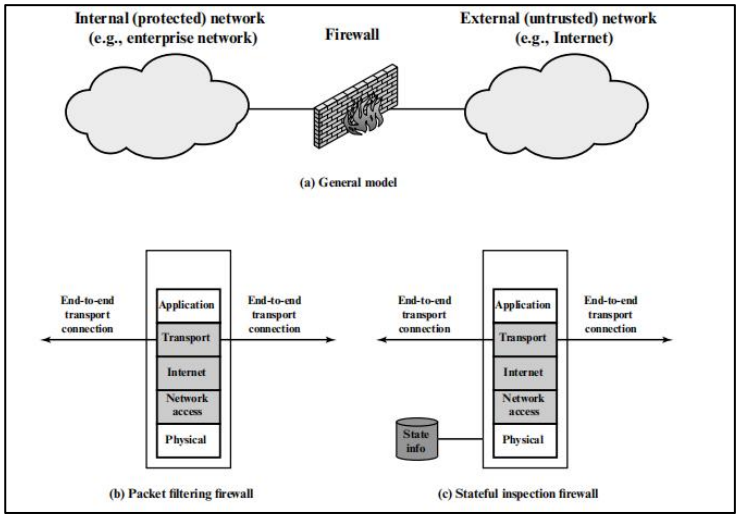
1.Design a protection solution of the network by deploying network security devices. The topology of the protected network, model and key parameters of security devices should be given.





2.The type and model of firewall

Packet Filtering Firewall,Stateful Inspection Firewall,Application Proxy Firewall,Circuit-level Proxy Firewall



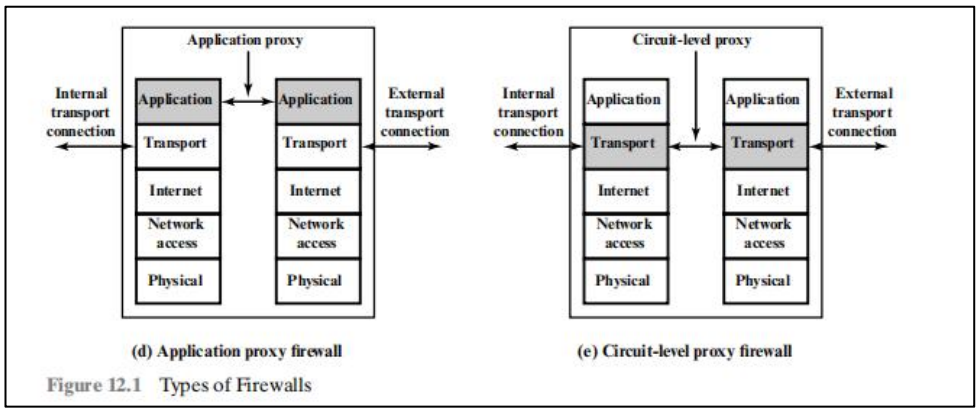


Figure 12.1 Types of Firewalls

3.The principle of packet filtering firewall and stateful inspection filtering firewall.

(1)Packet Filtering Firewall

A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.

(2)Stateful Inspection Filtering Firewall

The firewall maintains the state information for each session, where session states include a combination of communication phase and the endpoint application state.

When a stateful packet filtering gateway receives a data packet, it checks the packet against the known state of the session. If the packet deviates from the expected session state, the gateway blocks the rest packet of the session.

4.What is bastion host?

A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. Typically, the bastion host serves as a platform for an application-level or circuit-level gateway.

5.SummaryU8

(1)The firewall is a kind of network isolation mechanism.

(2)Packet filter, stateful packet filter, application gateway, circuit level gateway are typical technologies used in firewall.

(3)In DMZ networks, DMZ is an isolated network between the private network and the Internet.

(4)The DMZ is used to deploy services for external network.

6.The configuration of firewall

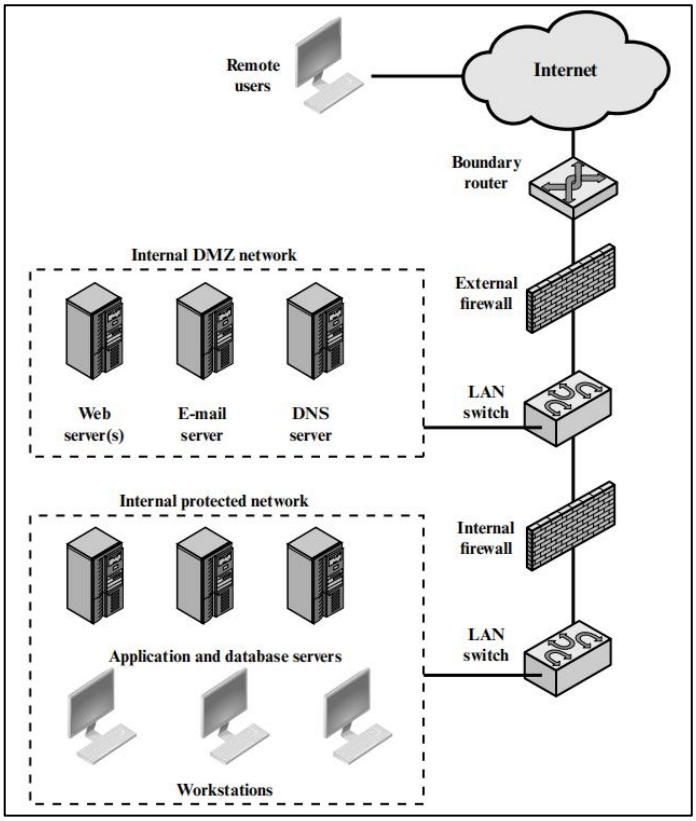
(1)Demilitarized Zone

• The firewall defines a DMZ (Demilitarized Zone) demarcated by the outer router and the internal router.

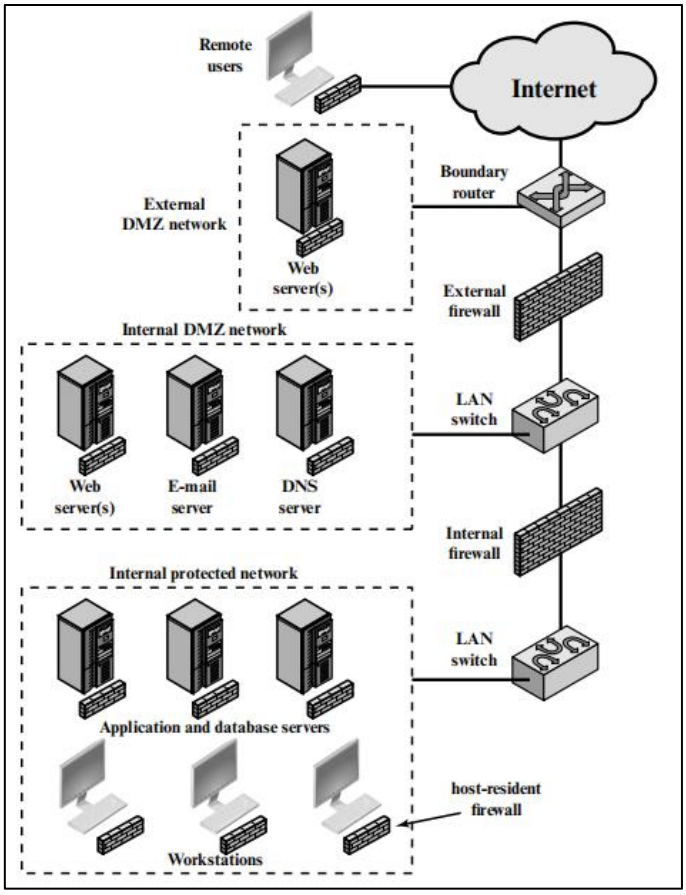
• The bastion host and information server are located within the DMZ.

• The DMZ can be considered an isolated network between the private network and the Internet.

• The architecture reveals only the DMZ network to the outside world.

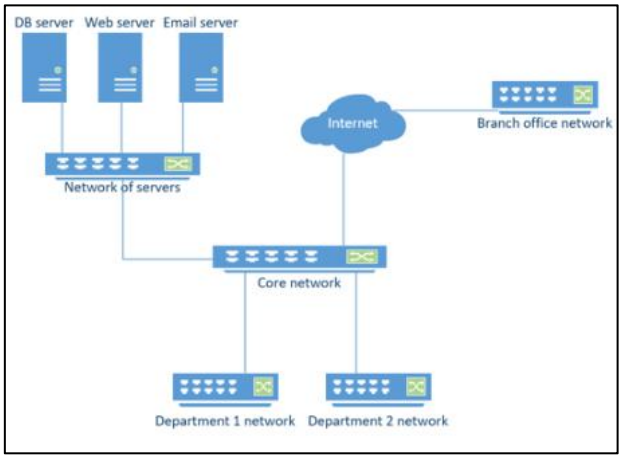


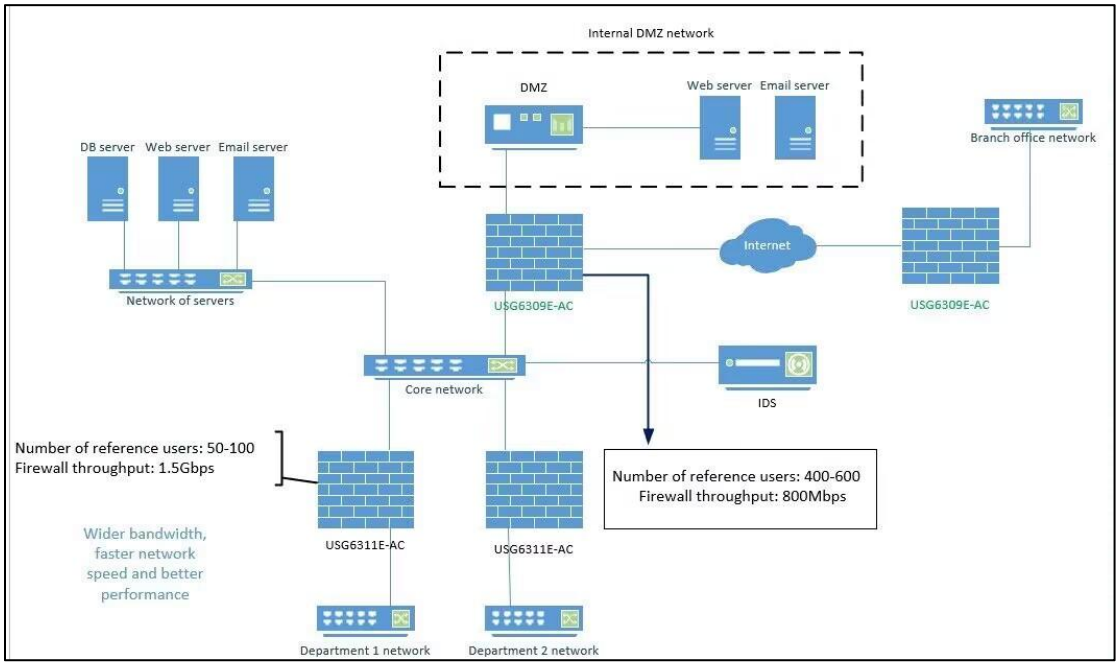
(2)Distributed Firewall



习题&重点 U8

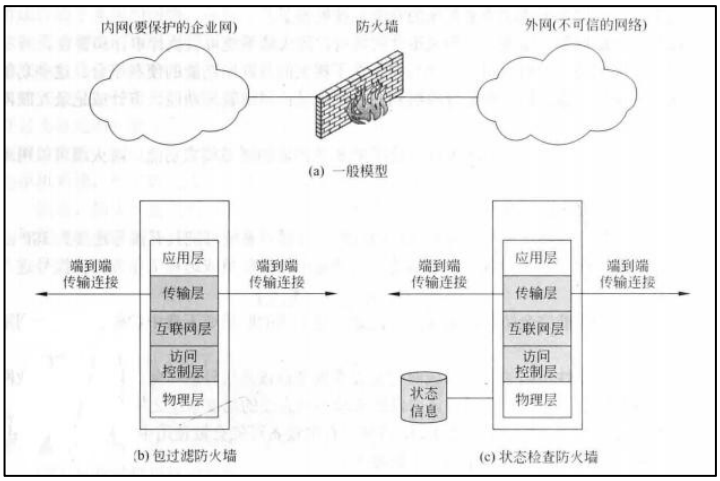
1.通过部署网络安全设备来设计网络的保护解决方案。应给出受保护网络的拓扑结构、安全设备的模型和关键参数。

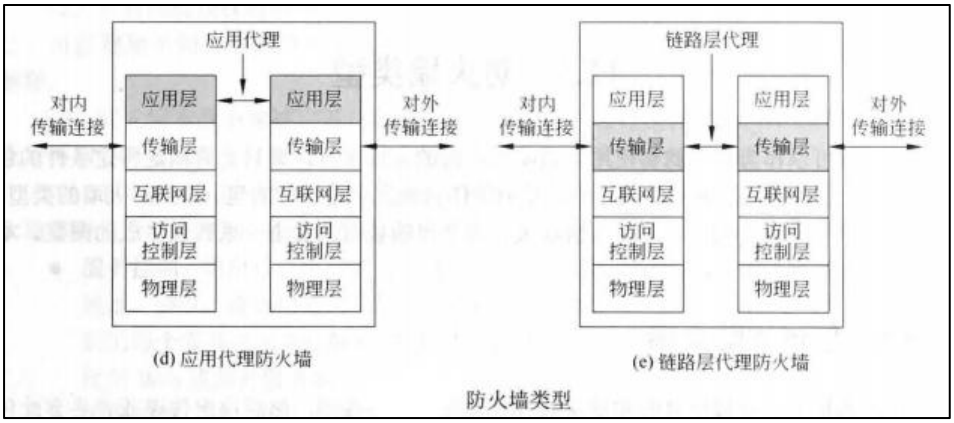




2.防火墙的类型和模型

包过滤防火墙、状态检测防火墙、应用代理防火墙、链路层代理防火墙





3.包过滤防火墙和状态检测防火墙的原理

(1)包过滤防火墙

数据包过滤防火墙对每个传入和传出的 IP 数据包应用一组规则，然后转发或丢弃该数据包。

(2)状态检测防火墙

•防火墙维护每个会话的状态信息，其中会话状态包括通信阶段和端点应用程序状态的组合。

•当有状态数据包过滤网关接收到数据包时，它会根据会话的已知状态检查数据包。如果数据包偏离预期的会话状态，则网关将阻止会话的其余数据包。

4.什么是堡垒主机？

堡垒主机是由防火墙管理员识别为网络安全关键强项的系统。通常，堡垒主机充当应用程序级或电路级网关的平台。

5.总结 U8

(1)防火墙是一种网络隔离机制。

(2)分组过滤器、有状态分组过滤器、应用网关、电路级网关是防火墙中使用的典型技术。

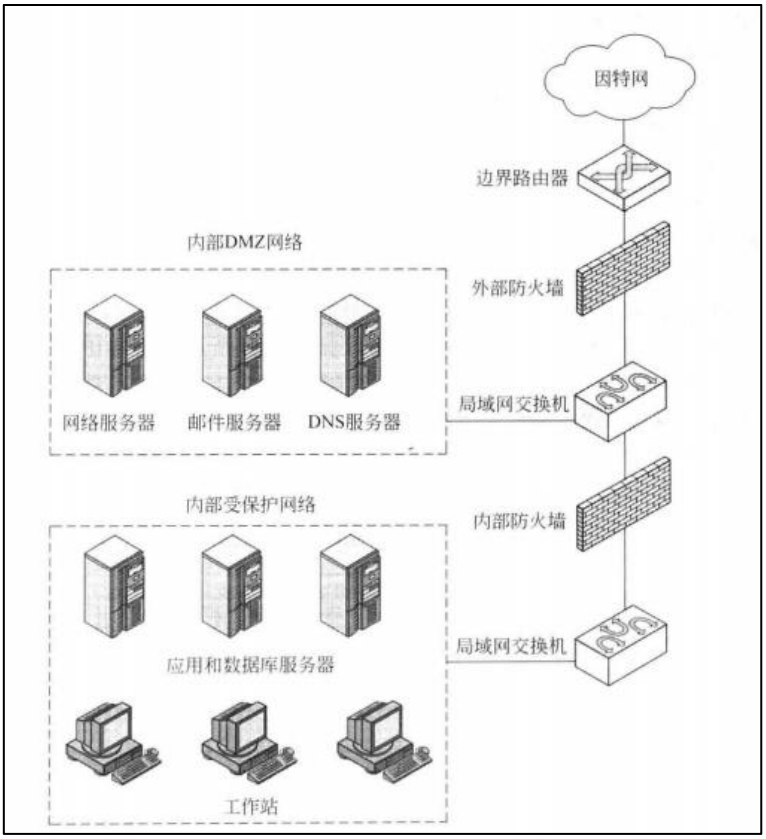
(3)在 DMZ 网络中，DMZ 是专用网络和互联网之间的隔离网络。

(4)DMZ 用于为外部网络部署服务。

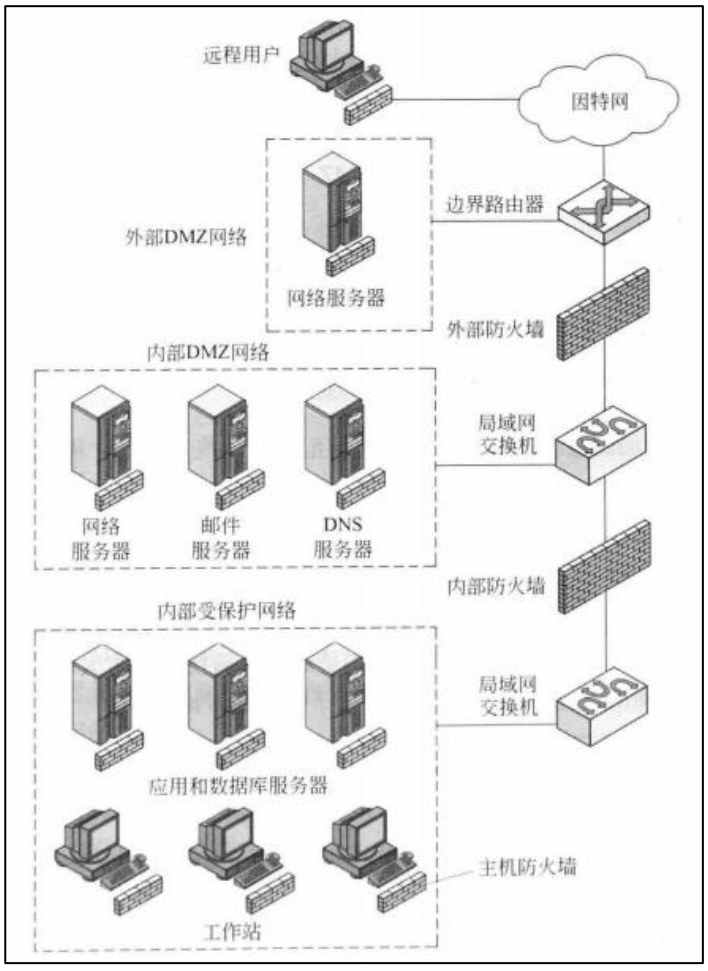
6.防火墙的配置

(1)停火区网段

- 防火墙定义了由外部路由器和内部路由器划分的 DMZ（非军事区）。
- 堡垒主机和信息服务器位于 DMZ 内。
- DMZ 可以被视为专用网络和互联网之间的隔离网络。
- 该架构仅向外部世界显示 DMZ 网络。


因特网
边界路由器
内部DMZ网络
外部防火墙
网络服务器
邮件服务器
DNS服务器
局域网交换机
内部受保护网络
内部防火墙
局域网交换机
应用和数据库服务器
工作站

(2)分布式防火墙


远程用户
因特网
外部DMZ网络
边界路由器
网络服务器
外部防火墙
内部DMZ网络
局域网
交换机
网络
服务器
邮件
服务器
DNS
服务器
内部防火墙
内部受保护网络
局域网
交换机
应用和数据库服务器
主机防火墙
工作站