Lecture NS7 2018

Chapter 16

1. Discuss the principal components of a network access control (NAC) system

Answer: pp. 520-521

2. Name four common NAC enforcement methods.

Answer: pp. 522-523

3. What is the Extensible Authentication protocol

Answer: fig. 16.2, pg. 523

4. EAP can be described in the context of a four-layer model. Indicate the functions of each of the four layers. You may need to refer to RFC 3748.

Answer：

a) Lower layer. The lower layer is responsible for transmitting and receiving EAP frames between the peer and authenticator. EAP has been run over a variety of lower layers including PPP, wired IEEE 802 LANs, IEEE 802.11 wireless LANs, UDP and IKEv2, and TCP.

b) EAP layer. The EAP layer receives and transmits EAP packets via the lower layer, implements duplicate detection and retransmission, and delivers and receives EAP messages to and from the EAP peer and authenticator layers.

c) EAP peer and authenticator layers. Based on the Code field, the EAP layer demultiplexes incoming EAP packets to the EAP peer and authenticator layers.

d) EAP method layers. EAP methods implement the authentication algorithms and receive and transmit EAP messages via the EAP peer and authenticator layers. Since fragmentation support is not provided by EAP itself, this is the responsibility of EAP methods.

Reference: https://tools.ietf.org/html/rfc3748

5. Discuss the main aspects of the **Cloud Security as a Service.**

Answer: pp.541-543

6. List some commonly used cloud-based data services. Explore and compare these services based on their flexibility and security.

	AWS(China)	Azure(China)	AliCloud
flexibility	4.5	4.5	4.5
security	4	2	4.5

As the big brother of cloud computing, AWS has developed its computing service matrix led by EC2 in terms of elastic computing, providing 10 different products using them to meet the user's requirements for computing power. However, the product lacks application scenarios and cannot meet the direct needs of users. Users need to build some computing services themselves. Give 4.5 points.

In terms of security, AWS provides a number of security and compliance services, such as identity authentication system, certificate system, WAF system, key management system, etc., to help users better standardize their own business and achieve better business development. Give 4 points

In the basic ability of cloud computing-elastic computing, Azure seems to be more inclined to implement the scenario by users themselves. The computing services provided are relatively basic, and only six services such as virtual machine, application service and batch processing are available. So give 4.5.

On the security front, Azure only provides key Vault, Active Directory, and multi-factor authentication, with limited usage and can only give 2 points.

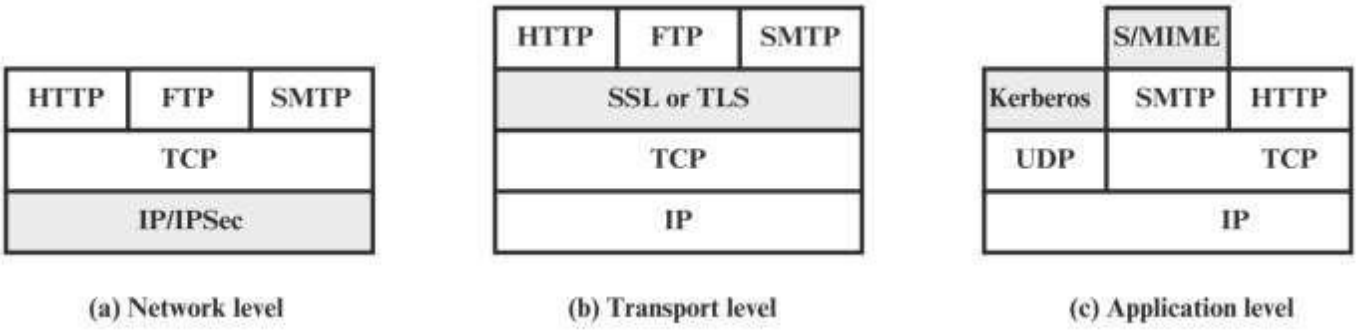
Alibaba Cloud has invested heavily in flexible computing, with many services including cloud servers, proprietary networks, container services, elastic scaling, and load balancing. But in the computing world, it is more focused on the underlying computing power, not on the top-level packaging. Unfortunately, it didn't involve some new technology, so give him 4.5 points.

In terms of security, Alibaba Cloud has developed 14 security products based on Cloud Shield, covering WAF, content filtering, data encryption, ddos protection, data wind control and many other functions to protect users' data security. Give 4.5 points.

As can be seen from the table above, their flexibility is similar. In terms of safety, Alibaba is the winner.

Chapter 17

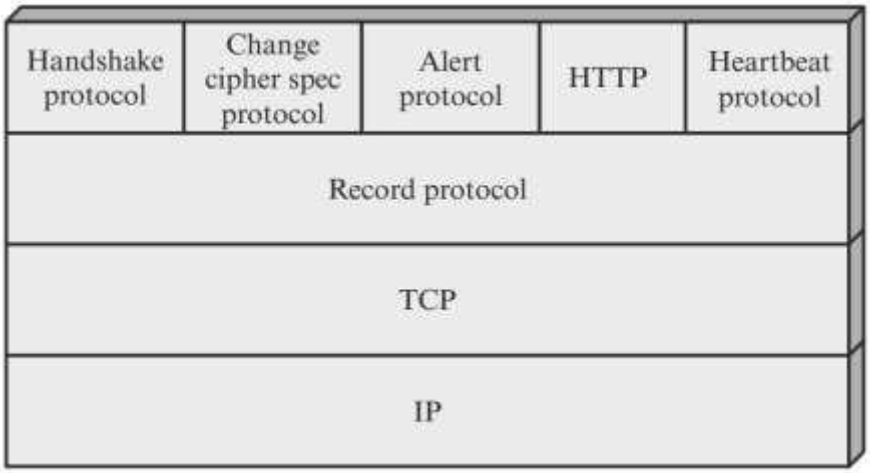
7. What are the advantages of each of the three approaches shown in Figure 17.1?



Answer

a) The advantage of using IPsec is that it is transparent to end users and applications and provides a general-purpose solution.
b) For full generality, SSL (or TLS) could be provided as part of the underlying protocol suite and therefore be transparent to applications. Alternatively, TLS can be embedded in specific packages.
c) The advantage of this approach is that the service can be tailored to the specific needs of a given application.

8. Discuss the TLS protocol stack



Answer: fig. 17.2, pp.549-550

9. Explain the difference between a TLS connection and a TLS session

Answer:
Connection: A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For TLS, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session.
Session: A TLS session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

10. List and briefly discuss the parameters that define a TLS session state

Answer
Session identifier: An arbitrary byte sequence chosen by the server to identify an active or resumable session state. **Peer certificate:** An X509.v3 certificate of the peer. **Compression method:** The algorithm used to compress data prior to encryption. **Cipher spec:** Specifies the bulk data encryption algorithm (such as null, DES, etc.) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as the hash_size. **Master secret:** 48-byte secret shared between the client and server. **Is resumable:** A flag indicating whether the session can be used to initiate new connections.

11. List and briefly discuss the parameters that define a TLS session connections

Answer

Server and client random: Byte sequences that are chosen by the server and client for each connection. **Server write MAC secret:** The secret key used in MAC operations on data sent by the server. **Client write MAC secret:** The secret key used in MAC operations on data sent by the client. **Server write key:** The conventional encryption key for data encrypted by the server and decrypted by the client. **Client write key:** The conventional encryption key for data encrypted by the client and decrypted by the server.

Initialization vectors: When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the TLS Handshake Protocol. Thereafter the final ciphertext block from each record is preserved for use as the IV with the following record.

Sequence numbers: Each party maintains separate sequence numbers for transmitted and received messages for each connection. When a party sends or receives a change cipher spec message, the appropriate sequence number is set to zero. Sequence numbers may not exceed $2^{64} – 1$.

Questions from:

- **NS7_3_TN**
- **NS7_2_TN**