Contents

[1 王铁民 + 李茂川 2](#_Toc417329413)

[2 张楠 + 卜野 5](#_Toc417329414)

[3 胡志愷 + 何双 6](#_Toc417329415)

[4 张淳阳 + 陈怡斐 8](#_Toc417329416)

[5 肖瀚 + 王一如 9](#_Toc417329417)

[6 乔赫良+ 陈晓宇 11](#_Toc417329418)

[7 Clyde + 赵子懿 13](#_Toc417329419)

[8 吴真 + 杨海钰 14](#_Toc417329420)

**Chapter 3, 43 questions**

**------------------------Owner for Q 1-30-------------------**

# 王铁民 + 李茂川

**1.**

**a.** Define cryptography.

Cryptography is the use of mathematical operations to protect message travelling between parties or stored on a computer. <<Book definition, not all right., this definitions looks like for Encryption.

Cryptography is the science concerned with the study of secret communication.

“encryption" basically is some process or algorithm (known as a **cipher**) to make information hidden or secret

**b.** What is confidentiality?

Confidentiality means the people who intercept messages cannot read them.

**c.** Distinguish between plaintext and ciphertext.

Plaintext is original message. Human readable text

Ciphertext is the result of calculation with a cryptographic algorithm on a plaintext

Encryption is a cryptographic process that turns the plaintext into a seemingly random steam of bits called the ciphertext.

**d.** Which is transmitted across the network—the plaintext or the ciphertext?

Both plaintext and ciphertext can be transmitted across the network, For confidentiality, ciphertext should be selected.

**e.** What is a cipher?

A cipher is a specific mathematical process used in encryption and decryption.

**f.** What is a key?

A key is a random string of bits (ones or zeros)

**g.** What must be kept secret in encryption for confidentiality?

Keeping the key secret

**h.** What is a cryptanalyst?

A cryptanalyst is someone who cracks encryption

**2.** Complete the enciphering in Figure 3-2.

|  |  |  |
| --- | --- | --- |
| n | 4 | 14 +4 =r |
| o | 8 | 15 + 8=w |
| w | 15 | 23 + 15 -26 = l |
| i | 16 | 9+16=y |
| s | 23 | 19 + 23 -26=p |
| t | 16 | 20 + 16 -26=j |
| h | 3 | 8 + 3 = k |
| e | 9 | 5 + 9 = n |
| t | 12 | 20 + 12 -26=f |
| i | 20 | 9 + 20 -26 = c |
| m | 6 | 13 + 6 = s |
| e | 25 | 5 + 25 -26 = d |

**3.**

**a.** Which leaves letters unchanged—transposition or substitution ciphers?

Substitution

**b.** Which leaves letters in their original positions—transposition or substitution ciphers?

transposition

**4.** Complete the enciphering in Figure 3-3.

hnitwteos

**5.**

**a.** In codes, what do code symbols represent?

code symbol represent complete words or phrases

**b.** What is the advantage of codes?

People can do encoding or decoding manually without a computer.

**c.** What are the disadvantages?

Codebook must be distributed ahead of time. If one codebook is intercepted, all confidentiality is lost.

**6.** Finish encoding the message in Figure 3-4.

**Message Code**

From 17434

Akagi 63717

To 83971

Truk 11131

STOP **34058**

ETA 53764

6 PM 73104

STOP **26733**

Require 29798

B 72135

N 54678

STOP **61552**

**7.**

**a.** Why is the word *symmetric* used in symmetric key encryption?

Because both parties encrypt and decrypt with same key.

**b.** When two parties communicate with each other using symmetric key encryption, how many keys are used in total?

In two-way communication with symmetric key encryption, two parties use only **one** key for encryption and decryption in both directions.

**c.** What type of encryption cipher is almost always used in encryption for confidentiality?

Symmetric

**8.**

**a.** What is the best way to thwart exhaustive searches by cryptanalysts?

To make the key long

**b.** If a key is 43 bits long, how much longer will it take to crack it by exhaustive search if it is extended to 45 bits?

2^2 (4-1) more times

**c.** If it is extended to 50 bits?

2^7(128-1) more times

**d.** If a key is 40 bits long, how many keys must be tried, on average, to crack it?

2 ^ 39

**e.** How long must a symmetric encryption key be to be considered strong today?

*Today, a symmetric key that is 100 bits long or longer is considered a strong symmetric key*

**9.** Why is cryptography not an automatic protection?

It only works if companies have and enforce organizational processes that don’t compromise the technical strengths of cryptography.

**10.**

**a.** What are the two advantages of RC4?

ONE: Rc4 is extremely fast and use only a small amount of RAM.

TWO: RC4 use a broad range of key length

**b.** Why is an RC4 key length of 40 bits commonly used?

National export restrictions in many countries once limited commercial products to 40-bit encryption.

**c.** Is this a strong key?

**No**

**11.**

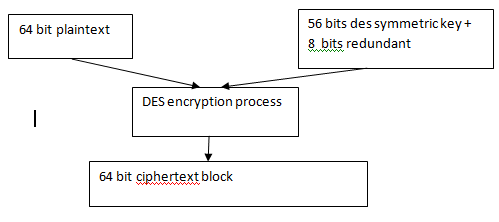
**a.** How long is a DES key?

56

**b.** Is this a strong length?

No

**c.** Describe block encryption with DES.

****

**12.**

**a.** How does 3DES work?

 3DES simply applies DES three times in a row for extra length

**b.** What are the two common effective key lengths in 3DES?

56\*2 = 112, 56\*3 =168

**c.** Are these lengths strong enough for communication in corporations?

Yes

**d.** What is the disadvantage of 3DES?

**Very slow**

**13.**

**a.** What is the big advantage of AES over 3DES?

 AES is efficient enough in terms of processing power and RAM requirement.

**b.** What are the three key lengths offered by AES?

128,192,256

**c.** Which strong symmetric key encryption cipher can be used with small mobile devices?

RC4 ????

**d.** Which symmetric key encryption cipher probably will dominate symmetric key encryption in the near future?

AES

**14.**

**a.** It is claimed that new and proprietary encryption ciphers are good because cryptanalysts will not know them. Comment on this.

Security professionals deride this as security through obscurity because it relies on secrecy, or an attacker’s inability to obtain information about cipher, rather than the robustness of the cipher itself. If the untested cipher’s details become know, it could result in a catastrophic loss of security.

**b.** What is security through obscurity, and why is it bad?

security through obscurity is the principle of relying on secrecy to create security by hiding potential vulnerabilities.

In practice, ciphertext encrypted with proprietary algorithms typically is cracked quickly even if the attacker does not know the detailed cipher

**15.**

**a.** Distinguish between cryptography and cryptographic systems.

Cryptographic system is a package set of cryptographic countermeasure for protecting dialogue.

**b.** Distinguish between cryptographic systems and cryptographic system standards.

The standard specifies both the protections to be applied and the mathematical processes that will be used to provide protection. Popular cryptographic system standards includes SSL/TLS and IPsec

**c.** Why is the first handshaking stage the negotiation of security methods and options?

~~A specific set of options in SSL/TLS is called cipher suite.~~ Before the two parties in an SSL/TLS connection do anything else, they must negotiate a specific cipher suite for the communication session.

**d.** What is an impostor?

A person who pretends to be someone else in order to deceive others.

**e.** What is authentication?

Communication partners prove their identities to each other.

**f.** What is mutual authentication?

When both parties authenticate themselves, this is mutual authentication.

**g.** Why is a secure keying phase necessary?

Confidentiality ciphers require keys, Authentication require secret. Both the keys and secrets are simply long strings of bits that must be kept between the two parties. In most cases, keys and secrets must be sent securely. Sending keys and secret secretly is generally called keying.

**16.**

**a.** What three protections do cryptographic systems provide on a message-by-message basis?

First, the sender adds an electronic signature to each message.

Second, all good electronic signature technologies also provide message integrity.

Third, the sender encrypts the combined message and electronic signature for confidentiality.

**b.** What is an electronic signature?

Electronic signature allows receiver to authenticate each message. ???

**c.** What two protections do electronic signatures usually provide?

Message-by-message authentication and message integrity.

**d.** Distinguish between the handshaking stages and ongoing communication.

P167

**17.**

**a.** In SSL/TLS, what is a cipher suite?

It is a specific set of security methods and options for a particular cryptographic system standard.

**b.** Why do companies want to create policies that define security methods and options for a particular application that is used between corporate partners?

Due to wide variation in the strength of SSL/TLS cipher suites, companies must develop risk-based policies for the selection of cipher suites, only allowing cipher suites with suitable strength for the risks facing the application.

**18.**

**a.** In authentication, distinguish between the supplicant and the verifier.

 In authentication, the party trying to prove its identity is called the supplicant. The other party is verifier who test the credentials accepts or rejects the supplicants.

**b.** What are credentials?

Proofs of identity.

**c.** How many supplicants and verifiers are there in mutual authentication between two parties? Explain.

One  supplicant and one Verifier at the same time. The two parties can take turn being supplicants and verifiers.

**19.**

**a.** In hashing, what is the hash?

 Hash is the hashing result.

**b.** Is encryption reversible?

Yes

**c.** Is hashing reversible?

No

**d.** Is hashing repeatable?

Yes

**20.**

**a.** Is MS-CHAP used for initial authentication or message-by-message authentication?

initial authentication

**b.** How does the supplicant create the response message?

????

**c.** How does the verifier check the response message?

Verifier adds password to the challenge message it sent. Hashes the combination. If the two response messages are equal, the supplicant knows the password and is authenticated. Server logs the client in

**d.** What type of encryption does MS-CHAP use? (This is a trick question but an important one.)

MD5

**e.** In MS-CHAP, does the server authenticate itself to the client?

**No**

**21.**

**a.** When Alice sends a message to Bob, what key will she use to encrypt the message?

Bob’s public key for confidentiality

Alice’s private key for authentication

**b.** Why is “the public key” not a good answer to Question 21?

Each side has public and private key. Every public key is different.

**c.** What key will Bob use to decrypt the message?

Bob’s private key.

**d.** Why is “the private key” not a good answer to Question 21b?

Each side has public and private key. Every private key is different.

**e.** In a classroom with 30 students and a teacher, how many public keys will there be?

At least 31 public keys

**f.** How many private keys?

At least 31 public keys

**22.**

**a.** What is the main drawback to public key encryption?

Slow and expensive to use

**b.** What is the most popular public key encryption cipher?

RSA

**c.** What is the other commonly used public key encryption cipher?

ECC ??

**d.** Which need to be longer—symmetric keys or public keys? Justify your answer.

**e.** How long are strong RSA keys?

1024

**f.** How long are strong ECC keys?

512

**23.** Julia encrypts a message to David using public key encryption for confidentiality. After encrypting the message, can Julia decrypt it?

**No**

**24.** Explain how public key encryption can facilitate symmetric session key exchange.

**25.**

**a.** What is the purpose of Diffie–Hellman key agreement?

**b.** Can an attacker who captures the exchanged keying information compute the symmetric session key?

**26.**

**a.** In public key encryption for authentication, which key does the supplicant use to encrypt?

His own private key, he wants to prove that the message comes from him, not others

**b.** Does the verifier decrypt the ciphertext with the supplicant’s public key? (If not, explain what key it does use.)

the verifier decrypts the ciphertext with the True Party’s public key.

**c.** Who is the true party?

The true party is the one the sender claims to be.

**d.** What does the sender attempt to prove it knows that only the true party should know?

It attempts to prove that only he knows the True Party’s private key, so that it proves that it is the true party.

**27.**

**a. In public key authentication, what must the sender know that an impostor should not be able to learn?**

True party’s private key

**b. For what type of authentication is a digital signature used—initial authentication or message-by-message authentication?**

Message-by-message authentication, sender create a hash for the plaintext, and sign the hash with his own private key and have a digital signature, and then encrypt the plaintext + signature with a symmetric key, at last send the encrypted message body to receiver.

**c.** How does the supplicant create a message digest?

Use a hash function to create the message digest for the plaintext

**d.** How does the supplicant create a digital signature?

To encrypt the hash code with his own private key

**e.** In public key encryption, what is “signing?”

Signing ~~a message digest~~ means encrypting it with the sender’s private key. << Not very good

**f.** What combined message does the supplicant send?

Plaintext + digital signature, in book, depicted as:

| DS | Plaintext|

**g.** How is the combined message encrypted for confidentiality?

They use a shared secret key and an encryption algorithm negotiated before in the handshake phase

**h.** How does the verifier check the digital signature?

1, Verifier decrypts the entire message and get back the: DS | Plaintext, with the shared symmetric key

2, Verifier hashes the plaintext and get a new message digest

3, Verifier retrieve the true party’s public key, and decrypts the DS to retrieve the message digest from supplicant

4, Compare the 2 digests, if identical, then the message is authenticated.

**i.** Does the verifier use the sender’s public key or the true party’s public key to test the digital signature?

true party’s public key, which means the key is obtained from CA – the trusted source, not from the sender

**28.**

**a.** Besides authentication, what security benefit does a digital signature provide?

1, Message integrity,

2, non-repudiation

**b.** Explain what this benefit means.

1, if the message in transmit was altered, the 2 digests will differ, so that the verifier can recognize the change

2, In theory, only the supplicant has the private key which was used to sign the message digest, it could be treated as an Evidence of Origin for the verifier.

**c. Do most message-by-message authentication methods provide message integrity as a by-product?**

YES, All real-world message-by-message authentication methods provide message integrity as a by-product.

**29.**

**a.** Contrast the key the sender uses for encryption in public key encryption for confidentiality and public key encryption for authentication.

For sender to achieve confidentiality, he uses receiver’s public key to encrypt the message

Authentication, he uses sender’s/his own private key to encrypt the message

**b.** Contrast the key the receiver uses for decryption in public key encryption for confidentiality and public key encryption for authentication. (Careful!)

For receiver to achieve confidentiality, he uses his own private key to decrypt, only he knows his private key, nobody can decrypts the message

Authentication, he uses sender’s public key to decrypt, anyone can obtain sender’s public key, in this case, the sender just wants to assure the message is surely coming from the sender.

**30.**

**a. From what kind of organization can a verifier receive digital certificates?**

From a trusted source == CA == Certificate Authority

**b. Are most CAs regulated?**

No, Unfortunately, few countries regulate CAs, so the verifier must only accept digital certificates from certificate authorities it trusts by reputation.

**c. Does a digital certificate indicate that the person or firm named in the certificate is trustworthy? Explain.**

No. When a CA gives a digital certificate to a person or organization, this does not mean that the CA vouches for the honesty of the party named in the certificate. It merely asserts that a certain party has a certain public key.

**------------------------Owner for Q 31-38-------------------**

# 张楠 + 卜野

**31.**

**a.** What are the two most critical fields in the digital certificate?

**b.** What field in a digital certificate allows the receiver of a certificate to determine if the certificate has been altered?

**c.** What three things must the receiver of a digital certificate check to ensure that a digital certificate is valid?

**d.** What are the two ways to check a certificate’s revocation status?

**32.**

**a.** Does a digital signature by itself provide authentication? Explain why or why not.

**b.** Does a digital certificate by itself provide authentication? Explain why or why not.

**33.**

**a.** What two cryptographic protections does an HMAC provide?

**b.** Do HMACs use symmetric key encryption, public key encryption, or hashing?

**c.** What is the benefit of HMACs over digital signatures?

**34.**

**a.** Why can’t HMACs provide nonrepudiation?

**b.** Why is it usually not a problem that HMACs fail to provide nonrepudiation?

**35.**

**a.** What is a replay attack?

**b.** Can the attacker read the contents of the replayed message?

**c.** Why are replay attacks attempted?

**d.** What are the three ways to thwart replay attacks?

**e.** How do time stamps thwart replay attacks?

**f.** How do sequence numbers thwart replay attacks?

**g.** How do nonces thwart replay attacks?

**h.** In what types of applications can nonces be used?

**36.**

**a.** What is quantum key distribution?

**b.** What are the two advantages of quantum key distribution?

**c.** Why is quantum key cracking a major threat to many traditional cryptographic methods?

**37.**

**a.** What is the definition of a VPN?

**b.** Why do companies transmit over the Internet?

**c.** Why do they transmit over untrusted wireless networks?

**d.** Distinguish between the three types of VPNs.

**e.** What does a VPN gateway do for a remote access VPN?

**f.** What does a VPN gateway do for a site-to-site VPN?

**g.** Which types of VPNs use VPN gateways?

**38.**

**a.** Distinguish between SSL and TLS.

**b.** For what type of VPN was SSL/TLS developed?

**c.** For what type of VPN is SSL/TLS increasingly being used?

**------------------------Owner for Q 39 - 46-------------------**

# 胡志愷 + 何双

**39.**

**a.** At what layer does SSL/TLS operate?

**b.** What types of applications can SSL/TLS protect?

**c.** What are the two commonly used SSL/TLS-aware applications?

**d.** Why is SSL/TLS popular?

**40.**

**a.** SSL/TLS was created for host-to-host (browser–webserver) communication. What device can turn SSL/TLS into a remote access VPN?

**b.** In SSL/TLS remote access VPNs, to what device does the client authenticate itself?

**c.** When a remote client transmits in an SSL/TLS VPN, how far does confidential transmission definitely extend?

**d.** What three services do SSL/TLS gateways commonly provide?

**e.** What is webification?

**f.** What software does the client need for basic SSL/TLS VPN operation?

**g.** For what purposes may the client need additional downloaded software?

**h.** Why installing the additional downloaded software on the browser may be problematic?

**i.** Why is SSL/TLS attractive as a remote access VPN technology?

**j.** What problems do companies face if they use it as a remote access VPN technology?

**k.** Which of the three types of VPNs can SSL/TLS support?

**41.**

**a.** At what layer does IPsec operate?

**b.** What layers does IPsec protect?

**c.** Compare the amount of cryptographic security in IPsec with that in SSL/TLS.

**d.** Compare centralized management in IPsec and SSL/TLS.

**e.** Why is IPsec’s transparent protection attractive compared with SSL/TLS’ nontransparent protection?

**f.** Which versions of IP can use IPsec?

**42.**

**a.** Distinguish between transport and tunnel modes in IPsec in terms of packet protection.

**b.** What are the attractions of each?

**c.** What are the problematic issues of each?

**43.**

**a.** What does an SA specify? (Do not just spell SA out.)

**b.** When two parties want to communicate in both directions with security, how many IPsec

SAs are necessary?

**c.** May there be different SAs in the two directions?

**d.** What is the advantage of this?

**e.** Why do companies wish to create policies for SAs?

**f.** Can they do so in SSL/TLS?

**g.** How does IPsec set and enforce policies?

**Chapter 4, 22 questions**

**1.**

**a.** Explain the four general goals for secure networking.

**b.** How can information be gathered from encrypted network traffic?

**c.** Give an example of how new technology has made networks less secure.

**d.** How does the castle model relate to secure networking?

**e.** What is meant by “death of the perimeter?”

**f.** How does the city model relate to secure networking?

**2.**

**a.** What is a denial-of-service attack?

**b.** Other than a DoS attack, what could cause a company’s webserver crash?

**c.** What are the main goals of DoS attacks?

**d.** Is a slow degradation of service worse than a total stoppage? Why?

**3.**

**a.** What is the difference between a direct and indirect DoS attack?

**b.** What is backscatter?

**c.** What types of packets can be sent as part of a DoS attack?

**d.** Describe a SYN flood.

**e.** How does a DDoS attack work?

**f.** What does a handler do?

**------------------------Owner for Q 4-11-------------------**

# 张淳阳 + 陈怡斐

**4.**

**a.** How does a P2P attack work?

**b.** How does a reflected attack work?

**c.** What is a DRDoS attack, and how does it work?

**d.** What is a Smurf flood?

**e.** What type of packet is sent in a Smurf flood? Why?

**f.** How could a malformed packet cause a host to crash?

**5.**

**a.** What is black holing?

**b.** Is black holing an effective defense against DoS attacks? Why?

**c.** How can the effects of SYN floods be mitigated?

**d.** What is a false opening?

**6.**

**a.** Why do hosts use ARP?

**b.** Can ARP poisoning be used outside the LAN? Why not?

**c.** Why do hosts send ARP requests?

**d.** What is ARP spoofing?

**e.** How could an attacker use ARP spoofing to manipulate host ARP tables?

**7.**

**a.** Explain ARP poisoning?

**b.** Why does the attacker have to send a continuous stream of unrequested ARP replies?

**c.** Do switches record IP addresses? Why not?

**d.** Does the attacker have to poison the gateway’s ARP tables too? Why?

**e.** Why does all network traffic go through the attacker after poisoning the network?

**8. a.** How can ARP poisoning be used as a DoS attack?

**b.** How can static IP and ARP tables be used to prevent ARP poisoning?

**c.** Can static IP and ARP tables be effectively used in large networks? Why not?

**d.** Why would limiting local access prevent DoS attacks?

**9.**

**a.** What is a SLAAC attack?

**b.** Why do host automatically prefer IPv6 addressing?

**c.** What has to be introduced to a network for a SLAAC attack to work?

**d.** Would a SLAAC attack work on an existing IPv6 network? Why not?

**e.** Could a rogue router direct internal traffic to an outside rogue DNS server? How?

**10.**

**a.** What is the main access control threat to Ethernet LANs?

**b.** What is the main access control threat to wireless LANs?

**c.** Why is the access control threat to wireless LANs more severe?

**d.** Is eavesdropping usually a concern for wired LANs, wireless LANs, or both?

**11.**

**a.** Why is 802.1X called Port-Based Access Control?

**b.** Where is the heavy authentication work done?

**c.** What are the three benefits of using a central authentication server?

**d.** Which device is the verifier? Explain. (Trick question.)

**e.** Which device is called the authenticator?

**------------------------Owner for Q 12-19-------------------**

# 肖瀚 + 王一如

**12.**

**a.** How does an EAP session start?

**b.** What types of messages carry requests for authentication information and responses to these requests?

**c.** Describe how the central authentication server tells the authenticator that the supplicant is acceptable.

**d.** How does the authenticator pass this information on to the supplicant?

**e.** In what sense is EAP *extensible*?

**f.** When a new authentication method is added, what device software must be changed to use the new method?

**g.** Why is there no need to change the operation of the authenticator when a new EAP authentication method is added or an old EAP authentication mode is dropped?

**h.** Why is this freedom from the need to make changes in the switch beneficial?

**13.**

**a.** What standard do most central authentication servers follow?

**b.** How are EAP and RADIUS related in terms of functionality?

**c.** What authentication method does RADIUS use?

**14.**

**a.** What is the most common attack against wireless networks? Why?

**b.** Which IEEE standard governs WLAN transmission?

**c.** Which device acts as a relay between wired and wireless networks?

**d.** What is the typical range of a WLAN?

**e.** What is the difference between an open network and a private network?

**f.** Who would set up a rogue access point? Why?

**g.** Give examples of both internal and external harm caused by unauthorized wireless access.

**h.** Are you liable if someone else uses your wireless network to commit a crime? Why, or why not?

**15.**

**a.** What man-in-the-middle attack is a danger for 802.11 WLANs?

**b.** Physically, what is an evil twin access point?

**c.** What happens when the legitimate supplicant sends credentials to the legitimate access point?

**d.** In what two types of attacks can the evil twin engage?

**e.** Are evil twin attacks frequent?

**f.** Where are they the most frequently encountered?

**g.** How can the danger of evil twin attacks be addressed?

**16.**

**a.** How would a wireless DoS attack be carried out?

**b.** What type of devices could be used to flood the transmission frequency for a WLAN?

**c.** What device could be used to identify a DoS flood if the entire frequency is being flooded by EMI?

**d.** What type of attack commands could be sent to cause a wireless DoS attack?

**e.** What would happen if a wireless network were flooded with CTS frames?

**17.**

**a.** Why is it impossible to extend 802.1X operation using EAP directly to WLANs?

**b.** What standard did the 802.3 Working Group create to extend 802.1X operation to WLANs with security for EAP?

**c.** For 802.11i, distinguish between outer and inner authentication.

**d.** What authentication method or methods does outer authentication use?

**e.** What two extended EAP protocols are popular today?

**f.** Distinguish between their options for inner authentication.

**g.** Is 802.11i security strong? Explain.

**18.**

**a.** What was the first core wireless security standard?

**b.** What encryption algorithm does it use?

**19.**

**a.** What prompted the Wi-Fi Alliance to create WPA?

**b.** Compare WPA and 802.11i security.

**c.** What does the Wi-Fi Alliance call 802.11i?

**d.** Despite its security weaknesses, why do many companies continue to use WPA instead of 802.11i?

**------------------------Owner for Q 20 – 22 + 1 – 5 in next chapter -------------------**

# 乔赫良+ 陈晓宇

**20.**

**a.** Why is 802.1X mode unsuitable for homes and small offices?

**b.** What mode was created for homes or very small businesses with a single access point?

**c.** How do users in this mode authenticate themselves to the access point?

**d.** Why is using a shared initial key not dangerous?

**e.** How are PSK/personal keys generated?

**f.** How long must passphrases be for adequate security?

**21.**

**a.** What is the purpose of a wireless IDS?

**b.** How do wireless IDSs get their data?

**c.** What is a rogue access point?

**d.** What are the two alternative to using a centralized wireless IDS?

**e.** Why are they not attractive?

**22.**

**a.** Does the use of spread spectrum transmission in 802.11 create security?

**b.** What are SSIDs?

**c.** Does turning off SSID broadcasting offer real security? Explain.

**d.** What are MAC access control lists?

**e.** Do they offer real security? Explain.

**Chapter 5 – 5.5, 21 questions**

**1. a.** List the AAA access controls.

**b.** Explain each in a sentence.

**c.** What are the four bases for authentication credentials?

**d.** What is two-factor authentication’s promise?

**e.** How can a Trojan horse defeat this promise?

**f.** How can a man-in-the-middle attack defeat this promise?

**g.** What is RBAC? (Do not just spell it out).

**h.** Why is RBAC less expensive than access control based on individual accounts?

**i.** Why is it less error-prone? (The answer is not specifically in the text.)

**j.** Why do technologically strong access controls not provide strong access control in real organizations?

**2.**

**a.** Distinguish between mandatory access controls and discretionary access controls.

**b.** What is multilevel security?

**c.** What are SBU documents?

**d.** Do they need to be considered in access controls?

**e.** Why are access control models needed?

**3.**

**a.** Why is having a single point of building entry important?

**b.** Why are emergency exits important?

**c.** What should be done about them?

**d.** List the four elements of entry authorization in CobiT.

**e.** Why is loading dock security important?

**f.** What access control rules should be applied to loading docks?

**g.** What steps should be taken to reduce the danger of environmental damage?

**h.** List rules for working in secure areas.

**4.**

**a.** What is siting?

**b.** Distinguish between UPSs and electrical generators.

**c.** If wiring cannot be run through walls, what should be done to protect the wiring?

**d.** What should be done to protect laptops taken off-premises?

**e.** What controls should be applied to off-site equipment maintenance?

**f.** What controls should be applied to equipment disposal or reuse?

**g.** What controls should be placed over employees taking equipment off-site?

**5.**

**a.** What special controls are required by terrorism threats?

**b.** Why is it necessary to prevent piggybacking?

**c.** What advice would you give a company about CCTV?

**d.** What is Dumpster™ diving?

**e.** How should trash bins be protected?

**f.** What can be done to reduce the dangers of desktop PC theft and unauthorized use?

**------------------------Owner for Q 6 – 13 -------------------**

# Clyde + 赵子懿

**6.**

**a.** What are reusable passwords?

**b.** Why is password cracking over a network difficult to do?

**c.** In what two ways can password-cracking programs be used?

**d.** Which is safer for the cracker? Why?

**7.**

**a.** Why is it a problem to use the same password at multiple sites?

**b.** Why is it difficult to enforce a policy of using a different password at each site?

**c.** Why are password duration policies important?

**d.** What are password resets?

**e.** Why are password resets dangerous?

**f.** How can password resets be automated?

**g.** Why are password reset questions difficult to create?

**h.** How may password resets be handled in high-risk environments?

**8.**

**a.** What is the book’s recommended password policy for length and complexity?

**b.** How can password-cracking programs be used to enforce password strength policy?

**c.** Before you run a password-cracking program on your company’s computers to check for weak passwords, what should you do?

**9.** What is the likely future of passwords?

**10.**

**a.** Distinguish between magnetic stripe cards and smart cards.

**b.** What are one-time-password tokens?

**c.** What are USB tokens?

**d.** What is the advantage of USB tokens compared to cards?

**e.** What is the attraction of proximity tokens?

**11.**

**a.** Why is it important to disable lost or stolen access devices?

**b.** Give an example of two-factor authentication not mentioned in the text.

**c.** What is a PIN?

**d.** Why can PINs be short—only four to six digits—while passwords must be much longer?

**12.**

**a.** What is biometric authentication?

**b.** On what two things about you is biometric authentication based?

**c.** What is the major promise of biometrics?

**13.**

**a.** Describe the three scanner actions in the enrollment process.

**b.** What are key features?

**c.** Why are they necessary?

**d.** What does the server do with the key features created by the enrollment scan?

**e.** What is a template?

**f.** What is user access data?

**g.** What are match indices, and how are they related to decision criteria?

**------------------------Owner for Q 14 – 21 -------------------**

# 吴真 + 杨海钰

**14.**

**a.** In biometrics, what is a match?

**b.** Distinguish between false acceptances and false rejections.

**c.** What are false acceptance rates (FARs) and false rejection rates (FRRs)?

**d.** For computer access, why is a false acceptance bad?

**e.** Why is a false rejection bad?

**f.** Which is worse from a security viewpoint?

**g.** Which is worse from a user acceptance viewpoint?

**15.**

**a.** For watch lists of criminals, what is a false acceptance?

**b.** For watch lists of criminals, which is worse from a security viewpoint, a false acceptance or a false rejection? Explain.

**c.** For watch lists of people who should be allowed to enter a room, which is worse from a security viewpoint, a false acceptance or a false rejection? Explain.

**16.** What is failure to enrol?

**17.**

**a.** Distinguish between verification and identification.

**b.** Which requires more matches against templates?

**c.** Which is more likely to generate a false acceptance? Why?

**d.** Compare identification with watch list matching.

**e.** Which is more likely to generate a false match? Why?

**18.**

**a.** Suppose that the probability of a false acceptance is one in a million, that there are

10,000 identities in the database, and that there is a watch list with 100 people. What will be the FAR for verification?

**b.** For identification?

**c.** For the watch list?

**19.**

**a.** Distinguish between error rates and deception in biometrics.

**b.** Why fingerprint scanning, which is often deceived, can be acceptable for entry into a supplies cabinet?

**c.** When it may not be sufficient?

**20.**

**a.** What is the advantage of fingerprint recognition?

**b.** What are the disadvantages?

**c.** For what type of use is fingerprint recognition sufficient?

**d.** What is the advantage of iris recognition?

**e.** What are the disadvantages?

**f.** Does iris scanning shoot light into your eye?

**21.**

**a.** What is the advantage of face recognition?

**b.** What does *surreptitious* mean?

**c.** Where is hand geometry recognition used?

**d.** What are the disadvantages of voiceprint recognition?

**e.** What are the most widely used forms of biometric authentication?

**f.** What is the most widely used form of biometrics?