Security

Md. Mohsin Uddin

East West University

mmuddin@ewubd.edu

April 21, 2023

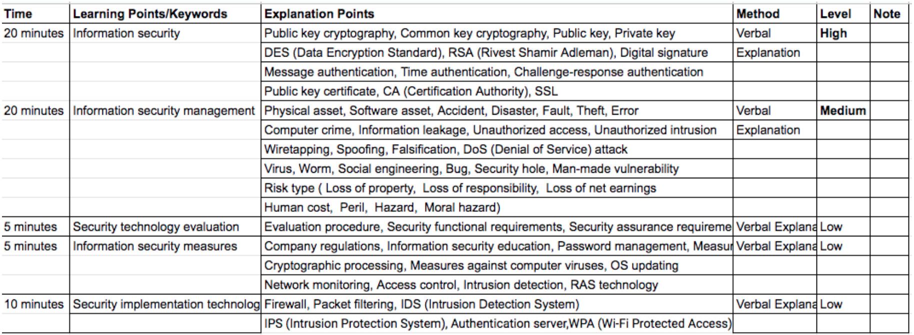
The Course Outline

Course Outline

- **Course Title:** Preparation course for ITEE FE examination
- **Intended Participants:** University Students who are going to take ITEE FE examination
- **Course Duration:** 60 hours

The Lecture Plan

Lecture Plan: Morning Exam, Sec 3-Technology Elements, Chapter 5-Security



Time	Learning Points/Keywords	Explanation Points	Method	Level	Note
20 minutes	Information security	Public key cryptography, Common key cryptography, Public key, Private key	Verbal	**High**	
		DES (Data Encryption Standard), RSA (Rivest Shamir Adleman), Digital signature	Explanation		
		Message authentication, Time authentication, Challenge-response authentication			
		Public key certificate, CA (Certification Authority), SSL			
20 minutes	Information security management	Physical asset, Software asset, Accident, Disaster, Fault, Theft, Error	Verbal	**Medium**	
		Computer crime, Information leakage, Unauthorized access, Unauthorized intrusion	Explanation		
		Wiretapping, Spoofing, Falsification, DoS (Denial of Service) attack			
		Virus, Worm, Social engineering, Bug, Security hole, Man-made vulnerability			
		Risk type (Loss of property, Loss of responsibility, Loss of net earnings			
		Human cost, Peril, Hazard, Moral hazard)			
5 minutes	Security technology evaluation	Evaluation procedure, Security functional requirements, Security assurance requireme	Verbal Explana	Low	
5 minutes	Information security measures	Company regulations, Information security education, Password management, Measur	Verbal Explana	Low	
		Cryptographic processing, Measures against computer viruses, OS updating			
		Network monitoring, Access control, Intrusion detection, RAS technology			
10 minutes	Security implementation technolog	Firewall, Packet filtering, IDS (Intrusion Detection System)	Verbal Explana	Low	
		IPS (Intrusion Protection System), Authentication server,WPA (Wi-Fi Protected Access)			

Objectives

5.1 Information security***

- Understand the concept of information security, and apply them to associated matters.
- Understand the technologies of information security required for information systems development, and apply them to associated matters.

Keywords

5.1 Information security***

- Accountability, Authenticity, OECD “Guideline for the Security of Information Systems and Networks: Towards a Culture of Security” adopted by OECD, Public key cryptography, Common key cryptography, Public key, Private key, DES (Data Encryption Standard), RSA (Rivest Shamir Adleman), Digital signature, Message authentication, Time authentication, Challenge-response authentication, Login (User ID and Password), Callback, IC card, PIN code, One time password, Fingerprint authentication, Vein authentication, Iris authentication, Voice authentication, Face authentication, False rejection rate, false acceptance rate, Public key certificate, CA (Certification Authority), SSL

Objectives

5.2 Information security management**

- Understand the basic concept of information security management.
- Understand the basic concept of threats and vulnerabilities to information assets, as well as methods and procedures for risk analysis and assessment.
- Understand the basic concept of information security policy.
- Understand the purpose of development of security regulations on corporate activities.
- Understand the mechanism of Information Security Management Systems (ISMS) and activities of security institutions.

Keywords

5.2 Information security management**

- Physical asset, Software asset, Accident, Disaster, Fault, Theft, Error, Computer crime, Information leakage, Unauthorized access, Unauthorized intrusion , Wiretapping, Spoofing, Falsification, DoS (Denial of Service) attack, Virus , Worm, Social engineering, Bug, Security hole, Man-made vulnerability Risk type (Loss of property, Loss of responsibility, Loss of net earnings, Human cost, Peril, Hazard, Moral hazard) Risk control, Risk finance, Risk avoidance, Risk transfer, Risk retention, Risk optimization, Risk diversification, Risk concentration, Security policy, Information security measures criteria, Security control regulations, Document control regulations, Information management regulations, Privacy policy, Security education regulations, ISO/IEC 27001, ISMS conformity assessment system, ISMS certification, ISO/IEC 17799 (JIS Q 27002), IPA security center

Objectives

5.3 Security technology evaluation

- Understand the basic concept of information security evaluation.

Keywords

5.3 Security technology evaluation

- Evaluation procedure, Security functional requirements, Security assurance requirements, Assurance level

Objectives

5.4 Information security measures

- Study the information security measures from human, technological, and physical security aspects, and apply them to associated matters.

Keywords

5.4 Information security measures

- Company regulations, Information security education, Password management, Measures against cracking, Cryptographic processing, Measures against computer viruses, OS updating, Network monitoring, Access control, Intrusion detection, RAS technology, Quakeproof and fireproof facilities, Monitoring camera, Locking management, Entrance access control

Objectives

5.5 Security implementation technology

- Understand the outline of security measures implemented in network and database.
- Understand the outline of attacks on applications and security measures.

Keywords

5.5 Security implementation technology

- Firewall, Packet filtering, IDS (Intrusion Detection System), IPS (Intrusion Protection System), Authentication server, WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), Encryption, User authentication, Database access control, Logging, Account management, Password management, Utilization control of external media, Unauthorized access detection, Security measures for Web systems, Secure programming, Buffer overflow attack, Cross-site scripting attack, Web beacon

Analyzation

Analyzation

- Analyzed 42 questions
- Covered most recent years
  - 2021 Q1 Exam
  - 2021 Q2 Exam

Questions

Question 1

Q1. (q3-50) A certain store receives orders from customers through a network using public key cryptography so that a third party cannot know the order details. Which of the following is the appropriate combination of keys used by the store and customers respectively?

	Store	Customers
a)	Public key	Private key
b)	Public key	Public key and private key
c)	Private key	Public key
d)	Private key	Public key and private key

Q1. (q3-50) A certain store receives orders from customers through a network using public key cryptography so that a third party cannot know the order details. Which of the following is the appropriate combination of keys used by the store and customers respectively?

Theme: Security, Category: FE

	Store	Customers
a)	Public key	Private key
b)	Public key	Public key and private key
c)	Private key	Public key
d)	Private key	Public key and private key

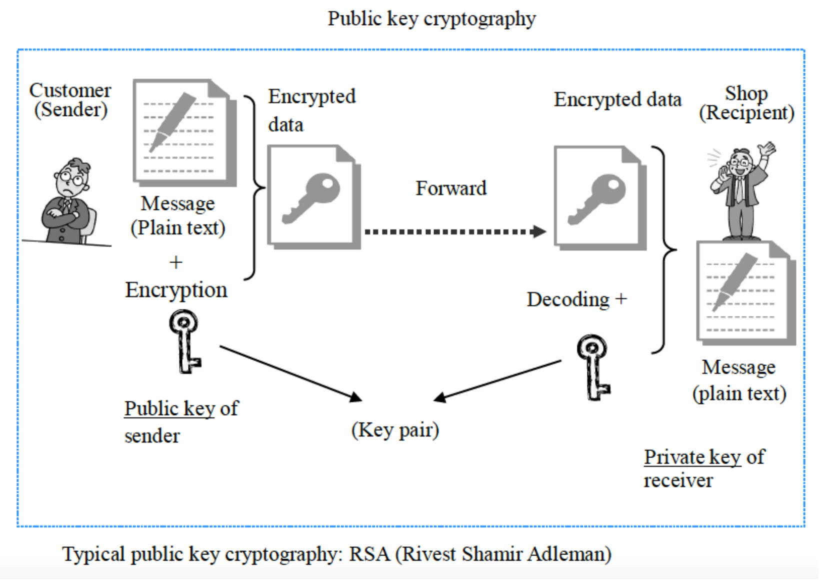
Question 1: Answer Explanation

Public key cryptography forms a pair of keys: a public key and a private key, and shares public keys with multiple senders. The private key is kept confidential by the recipient. While data is encrypted with the public key, the encrypted data is decoded with the private key.

In this question, when the shop receives orders over a network, customers use a public key, and the shop uses the private key. This method is safe because even if wiretapping is performed by a third party, only the party (shop) that has the private key can decode the data.

Therefore, c) is the correct combination.

Question 1: Answer Explanation



Typical public key cryptography: RSA (Rivest Shamir Adleman)

Question 2

Q2. (q3-51) There are two main purposes of using digital signatures for communication. The first purpose is for the recipient to verify the sender of a message. Which of the following is the other purpose?

a. The recipient checks whether any changes are made to the message after it is signed.

b. The recipient checks whether the message is wrongfully decoded during transmission.

c. The recipient checks the sender's ID.

d. The recipient checks whether to return the private key or not.

Q2. (q3-51) There are two main purposes of using digital signatures for communication. The first purpose is for the recipient to verify the sender of a message. Which of the following is the other purpose?

Theme: Security, Category: FE

a. The recipient checks whether any changes are made to the message after it is signed.
b. The recipient checks whether the message is wrongfully decoded during transmission.
c. The recipient checks the sender's ID.
d. The recipient checks whether to return the private key or not.

Question 2: Answer Explanation: Slide I

In a digital signature, the sender attaches a signature created by signing with plain text (refers to unencrypted data), which allows the recipient verify the sender. A signature is an encrypted message digest created from the plain text, and therefore, if the plain text differs, the message digest also differs.

There are two purposes of using a digital signature.

- **Personal authentication function:** The sender encrypts the data with his or her own private key (signing key), and if the recipient can decode it with the public key of the sender, the recipient can verify the sender. Only the sender, who creates the pair of public key and private key, can encrypt so that the encrypted data can be decoded with the public key of the sender.

Question 2: Answer Explanation: Slide II

- **Message authentication function:** If the message is altered, the message digest created from it is different from the signed message digest. Therefore, it can be checked whether the message has been altered or not after the signature is added (for the purpose of preventing the message from falsification). Therefore, a) is the correct answer.

b) From the mechanism of the Internet, neither wiretapping of the message itself can be detected, nor can it be prevented. Therefore, it is not possible to check whether someone else read the message or not.
c) Although a digital signature's objective is user authentication, it is not used for checking the ID of the sender.
d) As the sender is required to confidentially preserve the private key, it is not possible for the recipient to check whether to return it or not.

Question 3

Q3. (q3-52) When a document is sent or received using public key cryptography, which of the following is an appropriate description of how to handle keys so that the content of the document can be kept secret?

a. The encryption and decryption keys may be public, but the encryption algorithm must be kept private.

b. The encryption key may be public, but the encryption algorithm must be kept private.

c. The encryption key must be kept private, but the decryption key may be public.

d. The decryption key must be kept private, but the encryption key may be public

Q3. (q3-52) When a document is sent or received using public key cryptography, which of the following is an appropriate description of how to handle keys so that the content of the document can be kept secret? Theme: Security, Category: FE

a. The encryption and decryption keys may be public, but the encryption algorithm must be kept private.

b. The encryption key may be public, but the encryption algorithm must be kept private.

c. The encryption key must be kept private, but the decryption key may be public.

d. The decryption key must be kept private, but the encryption key may be public

Question 3: Answer Explanation

In public key cryptography, the encryption key and the decryption key are different, and data is kept confidential only with the decryption key. Thus, it is common to publish the encryption algorithm.
Therefore, d) is the appropriate description.
Moreover, as public key cryptography ensures that data is safe from code-breaking, the key is large at about 500 bits, and therefore the encryption and decryption speeds are much slower compared with secret key cryptography. However, it has the advantage that when only one person is required to receive the communication among n number of unspecified users, this can be easily achieved with one decryption key (private key).

Question 4

Q4. (q3-53) Which of the following is a protocol that is used for enhancing the confidentiality of e-mail content?

a. IMAP4
b. POP3
c. SMTP
d. S/MIME

Q4. (q3-53) Which of the following is a protocol that is used for enhancing the confidentiality of e-mail content?

Theme: Security, Category: FE

a. IMAP4

b. POP3

c. SMTP

d. S/MIME

Question 4: Answer Explanation: Slide I

Protocols for enhancing the confidentiality of e-mail content by encrypting the e-mails before they are sent include PGP (Pretty Good Privacy) and S/MIME (Secure Multipurpose Internet Mail Extensions).
Therefore, d) is the correct answer.
However, just like normal e-mails, SMTP and POP are used for sending and receiving e-mails that are encrypted with PGP or S/MIME. The meanings of the other terms are as follows:

- a) IMAP4 (Internet Message Access Protocol version 4) – This is a protocol that is used for receiving e-mails stored in the mailbox of the mail server.

Question 4: Answer Explanation: Slide II

- b) POP3 (Post Office Protocol version 3) – Like IMAP4, it is a protocol for receiving e-mails stored in the mailbox of the mail server. In POP and IMAP, the method of management for the received e-mails is different. In other words, in POP, all e-mails are downloaded to the client, and therefore e-mails are managed by the client. However, in IMAP, e-mails are not downloaded on the client; rather they can be managed by the server.
- c) SMTP (Simple Mail Transfer Protocol) – The protocol for sending e-mails from the mail client to the mail server, and exchanging e-mails between mail servers in the TCP/IP network.

Question 5

Q5. (q3-54) Which of the following is the purpose of using a message digest in a message authentication code?

a. To check that the message has not been falsified

b. To check the encryption method used in the message

c. To check the summary of the message

d. To ensure the confidentiality of the message

Q5. (q3-54) Which of the following is the purpose of using a message digest in a message authentication code?

Theme: Security, Category: FE

a. To check that the message has not been falsified

b. To check the encryption method used in the message

c. To check the summary of the message

d. To ensure the confidentiality of the message

Question 5: Answer Explanation: Slide I

This question concerns a message digest. The concept of a message digest is slightly different from what is generally called a digest. A completely different digest value is generated even if one bit is different, and it is used for checking in the case of falsification.

Therefore, the description of a) is about a message digest.

- MD5 and SHA-1 are two famous algorithms for this, and in MD5, a digest value of 16 octets is generated, while in SHA-1, a digest value of 20 octets is generated. As a message digest is widely used in combination with encryption technology for secured communication, it is often confused as an encryption technology. However, it should be remembered that "encryption is for hiding" and "message digest is for detecting falsification."

Question 5: Answer Explanation: Slide II

- This describes negotiation. Prior to the communication stage, adjusting both ends for encryption technology and encoding method is called negotiation. In SSL (Secure Sockets Layer), negotiation of encryption specifications is performed, while in IP phones, negotiation of the CODEC is performed before actual communication.
- This describes what is commonly known as a digest.
- This describes encryption, and it is not related to the prevention of falsification.

Question 6

Q6. (q3-55) Which of the following is an authentication that exchanges information between two communication entities X and Y as per the procedure described below?

[Procedure]

(1) Y sends a character string (challenge) including random information to X.

(2) Based on the predefined rules between X and Y, X generates a new character string (response) from the string received from Y, and returns it to Y.

(3) Y checks whether the returned character string (response) is correct or not.

a. X authenticates Y.
b. X authenticates Y, and as a result Y authenticates X.
c. Y authenticates X.
d. Y authenticates X, and as a result X authenticates Y.

Q6. (q3-55) Which of the following is an authentication that exchanges information between two communication entities X and Y as per the procedure described below?

[Procedure]

(1) Y sends a character string (challenge) including random information to X.

(2) Based on the predefined rules between X and Y, X generates a new character string (response) from the string received from Y, and returns it to Y.

(3) Y checks whether the returned character string (response) is correct or not.

Theme: Security, Category: FE

a. X authenticates Y.

b. X authenticates Y, and as a result Y authenticates X.

c. Y authenticates X.

d. Y authenticates X, and as a result X authenticates Y.

Question 6: Answer Explanation: Slide I

In Procedure (1), Y does not know whether the receiver is X itself or not. In Procedure (2), X does not know whether the character string sent is from Y or not. However, X generates a new character string based on the rule decided with Y beforehand, and returns it to Y. Y already knows the rules that enable Y to read this newly generated character string. In Procedure (3), Y decodes the returned character string based on the rule decided with X beforehand, and checks that the contents are correct. If the contents are correct, it means that X is the genuine other party with whom the rules were decided beforehand and therefore Y can authenticate X. In this case, it is important that the “rule decided between X and Y” is not known to a third party. Therefore, X usually has a private key available only to X, and Y has a key (public key, or private key) that can decode information that is encrypted by X. In this procedure, X merely receives “character strings including random information” from Y, and

Question 6: Answer Explanation: Slide II

does not receive any other information about Y. In other words, X cannot authenticate Y. Therefore, “c) Y authenticates X” is the correct answer.

Question 7

Q7. (q3-56) When a company's in-house system is remotely accessed from a hotel during a business trip, which of the following is the method for enhancing the authentication process?

a. Initiating a connection by notifying the IP address
b. Initiating a callback connection by using the IP address
c. Initiating a connection by notifying the sender's user ID
d. Initiating a connection by using a one-time password

Q7. (q3-56) When a company's in-house system is remotely accessed from a hotel during a business trip, which of the following is the method for enhancing the authentication process?

Theme: Security, Category: FE

a. Initiating a connection by notifying the IP address
b. Initiating a callback connection by using the IP address
c. Initiating a connection by notifying the sender's user ID
d. Initiating a connection by using a one-time password

Question 7: Answer Explanation: Slide I

Internal systems can be remotely accessed from outside with different methods such as using public lines like analog telephones and ISDN, and accessing over the Internet. In either of these methods, there is a threat of unauthorized access by spoofing. Therefore, authentication is performed to check that genuine user is accessing the system. The most basic authentication method is authentication with user ID and password. User ID and password are registered in an internal system beforehand, and authentication is performed at the time of remote access. In the usual authentication that is based on fixed passwords, leakage or theft of a password may result in unauthorized access by spoofing using this password. Therefore, as a measure for strengthening the password authentication method, a one-time password method where password can be used only once, was designed. As the authentication information circulating on the channel is of the use-and-throw type, it cannot be reused even if it is intercepted. For generating authentication information, there

Question 7: Answer Explanation: Slide II

is the challenge response method that uses a random number, and there is the synchronization method that synchronizes counter data, which creates authentication information. A one-time password can be effectively used on public lines as well as the Internet. Therefore, d) is the correct answer.

- a) Registration of the IP address of permitted PCs in advance, and allowing communication from only registered addresses while denying any communication from other devices is effective for the enhancement of security. However, it does not result in enhanced authentication of PC users if their PCs are fraudulently acquired.
- b) In call back, during remote access over a public line, an internal system disconnects the communication at once, and then reconnects by making a call to the number of the remote device registered in the server. Although it strengthens communication, it is not applicable to remote access over the Internet.

Question 7: Answer Explanation: Slide III

- c) This does not result in enhanced authentication because there is a possibility of obtaining the user ID by illegitimate means that lead to unauthorized access by spoofing.

Question 8

Q8. (q3-57) Which of the following is a characteristic of the security protocol SSL?

a. SSL is a protocol that is used only on a Web server for strengthening security and is located in the network layer.

b. In a Web server using SSL, FQDN is embedded in the digital certificate.

c. A unique digital certificate for personal authentication needs to be prepared for each PC.

d. In Japan, only government agencies can apply for a digital certificate whose common key is 128 bits in length.

Q8. (q3-57) Which of the following is a characteristic of the security protocol SSL?

Theme: Security, Category: FE

a. SSL is a protocol that is used only on a Web server for strengthening security and is located in the network layer.
b. In a Web server using SSL, FQDN is embedded in the digital certificate.
c. A unique digital certificate for personal authentication needs to be prepared for each PC.
d. In Japan, only government agencies can apply for a digital certificate whose common key is 128 bits in length.

Question 8: Answer Explanation I

SSL (Secure Sockets Layer) is a security protocol developed by Netscape Communications Corporation of the United States for ensuring safe HTML communication. Nowadays, it is implemented in major Web browsers and Web servers as a standard function, and SSL is easily available for use. In a Web server using SSL, by embedding the digital certificate in its own FQDN (Fully Qualified Domain Name, complete URL), it can be checked to determine if it matches the URL requested by the Web browser. Therefore, b) is the correct answer.

- a) In TCP/IP, SSL exists in the application layer, while in the OSI basic reference model it exists in the session layer. In addition to Web servers, it is also implemented in FTP and TELNET.

Question 8: Answer Explanation II

- c) The certificate used in SSL can be stored in the file format by exporting it in a Web browser. For example, in Internet Explorer, this can be done by exporting the certificate in the Contents tab under the Internet Options menu. Moreover, by importing this file, it can also be used in other computers.
- d) SSL is an industry-standard security protocol on a global scale, and there is no restriction that 128 bits can be used only by governmental institutions.

Question 9

Q9. (q3-58) Which of the following is an act that refers to social engineering?

a. Attacking an OS by exploiting security holes

b. Creating a computer virus

c. Cracking a password by a dictionary attack in order to intrude into a computer

d. Making a call to ask for a password by feigning the identity of the actual person

Q9. (q3-58) Which of the following is an act that refers to social engineering?

Theme: Security, Category: FE

a. Attacking an OS by exploiting security holes
b. Creating a computer virus
c. Cracking a password by a dictionary attack in order to intrude into a computer
d. Making a call to ask for a password by feigning the identity of the actual person

Question 9: Answer Explanation I

Social engineering refers to the act of using physical means to obtain the required ID and password for unauthorized access to network systems. It also includes the acts of impersonation and obtaining important information about a company or an organization from paper waste. Therefore, d) is the correct answer.

- a) Examples of types of attacks on a security hole in an OS (security flaws and vulnerabilities arising from software design error) include DoS attack (attacking the devices constituting the network, for interrupting the provision of services, and it is also known as denial of service attack and suspension of service attack) for system shutdown and taking control of privileges by command injection (Administrative rights are obtained by entering from the security hole of an OS. All resources can be accessed).
- b) The creation of a virus has nothing to do with social engineering.

Question 9: Answer Explanation II

- c) In a dictionary attack, character strings listed in a dictionary are encrypted with the same method as that used when a password file is created. After the dictionary entry which fully matches with these results is found, the original password is identified by looking for items that match these results.

Question 10

Q10. (q3-59) Which of the following is an example of phishing?

a. Damaging users and servers by embedding a malicious script in a webpage when there are sections on the webpage that display the input contents as is
b. Operating a virus infected computer from outside over a network such as the Internet
c. Secretly collecting personal information of computer users such as their IP addresses and Web behavior, and sending this information to an external location
d. Sending e-mails to people in order to lure them into accessing bogus Web sites that appear to be those of real companies, and stealing their personal information

Q10. (q3-59) Which of the following is an example of phishing?
Theme: Security, Category: FE

a. Damaging users and servers by embedding a malicious script in a webpage when there are sections on the webpage that display the input contents as is
b. Operating a virus infected computer from outside over a network such as the Internet
c. Secretly collecting personal information of computer users such as their IP addresses and Web behavior, and sending this information to an external location
d. Sending e-mails to people in order to lure them into accessing bogus Web sites that appear to be those of real companies, and stealing their personal information

Question 10: Answer Explanation: Slide I

Phishing is a fraudulent act of illegitimately obtaining personal information by using a fake e-mail that appears to be that of a real financial institution or online shopping Web site. With the URL noted in an e-mail sent to multiple unspecified recipients, recipients are tricked into visiting a fake Web site that looks exactly like the Web site of the actual company. If the user does not notice that the Web site is fake and enters his or her personal information such as login ID, password, name, address, and credit card number, this information is sent to the phishing source.
Therefore, d) is the correct answer.

- a) This refers to cross-site scripting. Script not allowed by a user is automatically executed, resulting in the risk of leakage of cookies.
- b) This is unauthorized access through a backdoor. The backdoor itself is a window for unauthorized access, and it may be automatically set up due to virus information, or it may be created through manual operation by a cracker (an intruder).

Question 10: Answer Explanation: Slide II

- c) This refers to spyware. It is software that runs in the background without the user's knowledge, and collects personal information and the computer usage pattern of a user and then sends them to a marketing company or the person who developed the spyware. Generally, it is embedded when some kind of application software is installed. Usually, the user's permission for installation is obtained at that point in time, so it is not necessarily illegal. However, as there are few users who carefully read terms and conditions, this itself is regarded as a problem.

Question 11

Q11. (q3-60) Which of the following is an explanation of the pattern matching method used by antivirus software?

a. Viruses are detected by comparing files before and after infection to check whether any changes are made to the files.
b. Viruses are detected by making a comparison with the signature codes of known viruses.
c. Viruses are detected by monitoring the system for abnormal phenomena caused by viruses.
d. Viruses are detected by performing a matching check with the checksum of a file.

Q11. (q3-60) Which of the following is an explanation of the pattern matching method used by antivirus software?

Theme: Security, Category: FE

a. Viruses are detected by comparing files before and after infection to check whether any changes are made to the files.
b. Viruses are detected by making a comparison with the signature codes of known viruses.
c. Viruses are detected by monitoring the system for abnormal phenomena caused by viruses.
d. Viruses are detected by performing a matching check with the checksum of a file.

Question 11: Answer Explanation: Slide I

Pattern matching methods of antivirus software compare and check the program with known viruses to detect the presence of a virus. A signature code refers to the fingerprint of a computer virus, and it is a unique code that exists in specific computer virus. Therefore, antivirus software can identify and detect viruses from these signature codes.
Therefore, b) is the appropriate answer.

- a) A virus cannot be detected just by a comparison of files before and after infection to check if any changes were made.
- c) A method for the detection of a virus by monitoring abnormal phenomena attributable to the virus is not a pattern matching method. Moreover, antivirus measures fall behind the curve in this method.

Question 11: Answer Explanation: Slide II

- d) Matching with the checksum of a file is one of the methods known as generic detection, and it is used as a means for the detection of suspicious programs and unknown viruses. Therefore, it is different from the pattern matching that can specifically identify known viruses, and it is not generally used as antivirus software like option b).

Question 12

Q12. (q3-61) Which of the following is a result obtained from the risk analysis in the course of understanding the security status, analyzing risks, planning security measures, and implementing the security measures?

a. Identified vulnerabilities
b. Incorporated security controls
c. Security specifications
d. Extent of loss

Q12. (q3-61) Which of the following is a result obtained from the risk analysis in the course of understanding the security status, analyzing risks, planning security measures, and implementing the security measures?

Theme: Security, Category: FE

a. Identified vulnerabilities

b. Incorporated security controls

c. Security specifications

d. Extent of loss

Question 12: Answer Explanation

Risk means “possibility of occurrence of event that interferes with the performance of corporate activities and the results of such interference.” In risk analysis, the possibility of occurrence of a security failure and its impact on information assets is evaluated. In other words, the extent of the loss is obtained as an outcome of risk analysis along with the frequency of occurrence.
Therefore, d) is the correct answer.

- a) Vulnerabilities are obtained as an outcome of the security process.
- b) Implemented security controls are obtained as an outcome during the implementation of security measures.
- c) Security specifications are obtained as an outcome of the formulation of a plan for security measures.

Question 13

Q13. (q3-62) Which of the following is the appropriate sequence of items (1) through (3) that are required for establishing ISMS in JIS Q 27001:2006?

(1) Prepare a Statement of Applicability.
(2) Select control purpose and controls for the treatment of risks.
(3) Analyze and evaluate the risks.

a. (1) → (2) → (3)
b. (1) → (3) → (2)
c. (2) → (3) → (1)
d. (3) → (2) → (1)

Q13. (q3-62) Which of the following is the appropriate sequence of items (1) through (3) that are required for establishing ISMS in JIS Q 27001:2006?
(1) Prepare a Statement of Applicability.
(2) Select control purpose and controls for the treatment of risks.
(3) Analyze and evaluate the risks.
Theme: Security, Category: FE

a. (1) → (2) → (3)
b. (1) → (3) → (2)
c. (2) → (3) → (1)
d. (3) → (2) → (1)

Question 13: Answer Explanation: Slide I

JIS Q 27001:2006 describes the requirements to be satisfied when information security management system (ISMS) is implemented in the organization. In this, it is mentioned that to build the system, an organization should follow the six main steps described below.

- (1) Define the ISMS policy of the organization.
- (2) Define the scope of ISMS. (Note: Scope is a concept that includes applicable range and objectives)
- (3) Risk assessment (evaluation)
- (4) Risk management (Note: Management here refers to the act of identifying potential risks that may arise and their resolutions)
- (5) Select the controls to be incorporated and describe the target of these controls in detail. (Note: Controls indicate methods and means of regulation)
- (6) Prepare a Statement of Applicability (SOA).

Option d) describes this sequence, and therefore d) is the correct answer.

Question 14

Q14. (q3-63) Which of the following is the appropriate description of information security policy that is defined in the ISMS conformity assessment scheme?

a. It is a confidential document that provides important basic policies, and should only be made accessible to relevant personnel within an organization.
b. It is defined in terms of the characteristics of the business, the organization, its location, assets, and technology.
c. It describes the basic security policies which must not be changed even when the business environment or technology changes.
d. It describes the details of security measures and system operations based on a risk analysis of a particular system.

Q14. (q3-63) Which of the following is the appropriate description of information security policy that is defined in the ISMS conformity assessment scheme?

Theme: Security, Category: FE

a. It is a confidential document that provides important basic policies, and should only be made accessible to relevant personnel within an organization.
b. It is defined in terms of the characteristics of the business, the organization, its location, assets, and technology.
c. It describes the basic security policies which must not be changed even when the business environment or technology changes.
d. It describes the details of security measures and system operations based on a risk analysis of a particular system.

Question 14: Answer Explanation: Slide I

In the ISMS certification standards (Ver. 2.0) used in the ISMS conformity assessment scheme, under the basic policy of information security in the annex “Detailed Controls,” the control objective described is “To provide management direction and support for information security.” This basic policy of information security is also called information security policy, and therefore b) is the appropriate description.

- a) Information security measures should be implemented company side, and its basic policy (security policy) should be informed everyone in the organization.
- c) ISMS should be built, implemented, and maintained as a management system, and it should be continuously improved. Basic policy (security policy) should also be periodically reviewed, and it should be continuously improved for optimizing its contents in accordance with changes in business environment and technologies.

Question 14: Answer Explanation: Slide II

- d) Information security policy sets the overall direction and principle concerning information security in the organization, and it is not a detailed description of a particular system.

Question 15

Q15. (q3-64) When the content on a Web server is altered because of unauthorized access to the Web server from an external location, which of the following is the appropriate sequence of measures to be taken after that?

(1)	Analyze each log of the server, IDS (Intrusion Detection System), and firewall to identify the method of unauthorized access, extent of the damage, and intrusion path.
(2)	Reconstruct the system and apply the latest patches and security setting information.
(3)	Disconnect the server from the network.
(4)	Monitor the server for some time after connecting it to the network.

a. (1) → (2) → (3) → (4)

b. (1) → (3) → (2) → (4)

c. (2) → (3) → (1) → (4)

d. (3) → (1) → (2) → (4)

Q15. (q3-64) When the content on a Web server is altered because of unauthorized access to the Web server from an external location, which of the following is the appropriate sequence of measures to be taken after that?

(1)	Analyze each log of the server, IDS (Intrusion Detection System), and firewall to identify the method of unauthorized access, extent of the damage, and intrusion path.
(2)	Reconstruct the system and apply the latest patches and security setting information.
(3)	Disconnect the server from the network.
(4)	Monitor the server for some time after connecting it to the network.

Theme: Security, Category: FE

- a. (1) → (2) → (3) → (4)
- b. (1) → (3) → (2) → (4)
- c. (2) → (3) → (1) → (4)
- d. (3) → (1) → (2) → (4)

Question 15: Answer Explanation: Slide I

In case of detection of unauthorized access to a Web server from an external location, in order to prevent the damage from spreading, it is necessary to promptly disconnect the Web server from the network. A description of this is provided in (3). Next, a survey should be conducted to determine the extent of damage. In concrete terms, each log of the server, IDS (Intrusion Detection System), and firewall should be analyzed, and the intrusion path and method as well as the range of the unauthorized access should be identified. This is noted in (1). Next, the damaged area that was identified should be reinforced, and the network reconstructed. Especially, the intrusion path is the area that does not have adequate security, so it is necessary to take adequate measures henceforth. In concrete terms, the latest patches and security setting information that are revised based on the damage should be applied. With regard to the Web server also, falsified content and the damaged area should be restored. This is mentioned in (2). As per the aforementioned procedure,

Question 15: Answer Explanation: Slide II

the network should be reconstructed, and the Web server that is now safe should be connected to the network. Since the intruder may attempt unauthorized access again if security is not adequate, temporary monitoring should be strengthened and the situation should be closely watched. This is noted in (4).
Therefore, d) is the correct answer.

Question 16

Q16. (q3-65) Which of the following is the act of obtaining a password or other confidential information from a person within an organization by using unauthorized means such as feigning an emergency situation?

a. Social engineering
b. Trojan horse
c. Password crack
d. Stepping-stone attack

Q16. (q3-65) Which of the following is the act of obtaining a password or other confidential information from a person within an organization by using unauthorized means such as feigning an emergency situation?
Theme: Security, Category: FE

a. Social engineering
b. Trojan horse
c. Password crack
d. Stepping-stone attack

Question 16: Answer Explanation: Slide I

Instead of using electronic methods, the act of illegitimately obtaining a password or other confidential information using administrative deficiencies attributable to human behavior, or deficiencies in physical security is called a) social engineering. For example, it includes acts such as, feigning the identity of the user and making the request to the system administrator such as "I forgot my password so please tell me it because I am working on something very urgent" to obtain the password, or pretending to be the system administrator and asking the user to give his or her password. In addition, shoulder surfing, which means covertly looking over someone's should when he or she is entering his or her password with a keyboard, and scavenging, which means obtaining important information by recovering the discarded forms and other material from a dust bin are also social engineering.

Question 16: Answer Explanation: Slide II

- b) A Trojan horse is a form of computer virus. Although it may appear normal from the outside, it is an unauthorized program that executes a malicious code that functions as a backdoor and damages the system or leaks information. Like a worm, it does not self-diffuse, and it exists as an independent program without infecting other programs.
- c) Password crack refers to illegitimately analyzing a password with electronic methods such as a dictionary attack or a brute force attack.
- d) In the stepping-stone attack, instead of directly attacking the target, the attacker indirectly attacks through a network by using another site that has vulnerabilities. It attempts to hide the identity of the attacker.

Question 17

Q17. (q3-66) In a user authentication method that compares the input password with the registered password, which of the following is a measure for preventing theft of a registered password through unauthorized access to the password file?

a. The hash value of the user ID corresponding to the password is registered. At the time of authentication, the input user ID is converted using the hash function, and the registered password and the input password are compared.

b. The file in which the password is registered without modification is compressed. At the time of authentication, the compressed file is decompressed and compared with the input password.

c. A password is registered as is. At the time of authentication, the input password and the registered password are both converted with hash function and then compared.

d. A password is converted into a hash value and registered. At the time of authentication, the input password is converted with the hash function and then compared with the registered password.

Q17. (q3-66) In a user authentication method that compares the input password with the registered password, which of the following is a measure for preventing theft of a registered password through unauthorized access to the password file?

Theme: Security, Category: FE

a. The hash value of the user ID corresponding to the password is registered. At the time of authentication, the input user ID is converted using the hash function, and the registered password and the input password are compared.

b. The file in which the password is registered without modification is compressed. At the time of authentication, the compressed file is decompressed and compared with the input password.

c. A password is registered as is. At the time of authentication, the input password and the registered password are both converted with hash function and then compared.

d. A password is converted into a hash value and registered. At the time of authentication, the input password is converted with the hash function and then compared with the registered password.

Question 17: Answer Explanation

A hash value is a value of fixed length determined from the data assigned by a certain algorithm. The characteristics of the hash values are “If the original data differs, hash value derived from it usually differs, and the hash value is rarely the same,” and “even if the hash value and the hash function are known, the source data cannot be identified.” Therefore, if a password is converted into a hash value, the original password cannot be recovered from the hash value even if the password file is stolen, and hence d) is the correct answer.
a) Covering a user ID with the hash function has nothing to do with password theft prevention.
b), c) If the entire password file is stolen, fraudulent use of stolen passwords cannot be prevented, and unauthorized users cannot be kept out.

Question 18

Q18. (q3-67) Which of the following is the management approach for preventing falsification or destruction of data by unauthorized execution of a program that can be commonly available to users?

a. Collection of a system access log

b. Comparison of the source program and the executed program

c. Storage of source programs in multiple locations

d. Setting of access rights for files

Q18. (q3-67) Which of the following is the management approach for preventing falsification or destruction of data by unauthorized execution of a program that can be commonly available to users?

Theme: Security, Category: FE

a. Collection of a system access log
b. Comparison of the source program and the executed program
c. Storage of source programs in multiple locations
d. Setting of access rights for files

Question 18: Answer Explanation: Slide I

In order to maintain the convenience for users whereby they can continue sharing a program, setting access restrictions for data processed by the program is an effective management approach for preventing falsification and destruction of the data.
Therefore, “d) Setting of access rights for files” is the appropriate preventive measure.

- a) Taking an access log is certainly useful to ascertain whether unauthorized execution of a program occurred based on access records, and also for the recovery of damaged data with the update journal, but it cannot prevent damage to the data.
- b) As the program itself may be altered and it may be executed illegitimately, “Comparison of the source program and the executed program” is helpful in ascertaining the cause of damage, but it cannot prevent damage.

Question 18: Answer Explanation: Slide II

- c) Storing source programs in multiple locations certainly acts as an antitheft measure for the source programs, but it cannot prevent damage.

Question 19

Q19. (q3-68) Which of the following is an explanation of a Web beacon?

a. It is a virus that is downloaded from a Web site and deletes image files from a PC.

b. It is a latent error in an application program used on a website.

c. It is an unfair trick that damages both the PC and Web server itself through a malicious script.

d. It is an image embedded in a Web page to collect information about access patterns of users.

Q19. (q3-68) Which of the following is an explanation of a Web beacon?
Theme: Security, Category: FE

a. It is a virus that is downloaded from a Web site and deletes image files from a PC.
b. It is a latent error in an application program used on a website.
c. It is an unfair trick that damages both the PC and Web server itself through a malicious script.
d. It is an image embedded in a Web page to collect information about access patterns of users.

Question 19: Answer Explanation

Web beacon refers to an image embedded in e-mails of HTML format or webpages to collect the access information of users.
Therefore, d) is the correct answer.
Usually, it is a very small image which is not noticed by users. If users access the Web site or e-mail where a Web beacon is embedded, a server is accessed to fetch that image data. The server records this access information, and secretly collects the access pattern of users. Beacon actually means "indicator". Since it is a very small image, it is also called a Web bug in many cases. This Web beacon is the subject of heavy recent criticism, and some e-mail programs can be set so that image files do not open during e-mail preview.

Question 20

Q20. (q3-69) In a wireless LAN, which of the following is used for restricting a connection with terminals other than those pre-registered at the access point?

a. AES
b. IEEE 802.11b
c. MAC address filtering
d. TKIP

Q20. (q3-69) In a wireless LAN, which of the following is used for restricting a connection with terminals other than those pre-registered at the access point?

Theme: Security, Category: FE

a. AES
b. IEEE 802.11b
c. MAC address filtering
d. TKIP

Question 20: Answer Explanation

In a wireless LAN, MAC address filtering restricts access by terminals not registered at the access point beforehand. A MAC address is a fixed physical address assigned to the NIC (Network Interface Card) of the terminal. Therefore, by registering the MAC address of the permitted terminal at the access point beforehand, the connection of unregistered devices can be restricted.
Therefore, c) is the correct answer.

- a) AES (Advanced Encryption Standard) – This is an encryption algorithm that uses common key cryptography.
- b) IEEE 802.11b – It is a communication standard for a wireless LAN that uses the 2.4GHz band. There is no access restriction for each terminal.
- d) TKIP (Temporal Key Integrity Protocol) – It is a protocol that enables encrypted communication and detects the falsification of frames in a wireless LAN.

Question 22

Q22. (2021 A FE AM-q35) Which of the following is an appropriate description of a Trojan horse?

a. A brute force attack software tool
b. A malicious computer program that presents itself as a legitimate one
c. A malicious user that steals private information from a system
d. A software tool to decrypt an encrypted password

Q22. (2021 A FE AM-q35) Which of the following is an appropriate description of a Trojan horse?

Theme: Security, Category: FE

a. A brute force attack software tool
b. A malicious computer program that presents itself as a legitimate one
c. A malicious user that steals private information from a system
d. A software tool to decrypt an encrypted password

Question 23

Q23. (2021 A FE AM-q36) Which of the following properties for information security defined in ISO/IEC 27000:2018 refers to a guarantee that the message data received is the same as the message data sent?

a. Availability
b. Confidentiality
c. Integrity
d. Non-repudiation

Q23. (2021 A FE AM-q36) Which of the following properties for information security defined in ISO/IEC 27000:2018 refers to a guarantee that the message data received is the same as the message data sent?
Theme: Security, Category: FE

a. Availability
b. Confidentiality
c. Integrity
d. Non-repudiation

Question 24

Q24. (2021 A FE AM-q37) Which of the following is an example of ransomware?

a. A range of different types of software including adware, spyware, and freeware

b. Malicious software blocking access to a victimized computer and demanding money to unblock it

c. Software that assigns randomized MAC addresses to PCs to ensure user privacy on the Internet

d. Software that generates random numbers needed by computer security application software

Q24. (2021 A FE AM-q37) Which of the following is an example of ransomware?

Theme: Security, Category: FE

a. A range of different types of software including adware, spyware, and freeware

b. Malicious software blocking access to a victimized computer and demanding money to unblock it

c. Software that assigns randomized MAC addresses to PCs to ensure user privacy on the Internet

d. Software that generates random numbers needed by computer security application software

Question 25

Q25. (2021 A FE AM-q38) A typical example of security threats is information leakage when a sender sends data containing important information to a receiver. Which of the following is the most appropriate measure to prevent information leakage?

a. The data is encrypted with a private key before being sent to the receiver via email. In a separate email, the private key is sent to the receiver so that the receiver can decrypt the data.

b. The data is password-locked, and it is attached in an email that includes the password in the text part of the email. Before the email is sent, the receiver address is checked to make sure that the email is sent to the correct address.

c. The receiver creates a pair of public/private keys and sends the public key to the sender. The data is encrypted with the public key and sent to the receiver via email. The receiver then decrypts the data with the private key.

d. The sender compresses the data on a USB memory as much as possible before giving the USB memory to the receiver so that the receiver can utilize the rest of the memory space effectively.

Q25. (2021 A FE AM-q38) A typical example of security threats is information leakage when a sender sends data containing important information to a receiver. Which of the following is the most appropriate measure to prevent information leakage?

a. The data is encrypted with a private key before being sent to the receiver via email. In a separate email, the private key is sent to the receiver so that the receiver can decrypt the data.

b. The data is password-locked, and it is attached in an email that includes the password in the text part of the email. Before the email is sent, the receiver address is checked to make sure that the email is sent to the correct address.

c. The receiver creates a pair of public/private keys and sends the public key to the sender. The data is encrypted with the public key and sent to the receiver via email. The receiver then decrypts the data with the private key.

d. The sender compresses the data on a USB memory as much as possible before giving the USB memory to the receiver so that the receiver can utilize the rest of the memory space effectively.

Question 26

Q26. (2021 A FE AM-q39) Which of the following is a type of malware that embeds itself within a program and inserts its copy into other programs?

a. Backdoor
b. Trojan horse
c. Virus
d. Worm

Q26. (2021 A FE AM-q39) Which of the following is a type of malware that embeds itself within a program and inserts its copy into other programs?

Theme: Security, Category: FE

a. Backdoor

b. Trojan horse

c. Virus

d. Worm

Question 27

Q27. (2021 A FE AM-q40) According to ISO/IEC 27000:2018 (Information security management systems Overview and vocabulary), which of the following is the definition of “level of risk”?

a. Magnitude of a risk expressed in terms of the combination of consequences and their likelihood
b. Terms of reference for evaluating the significance of a risk
c. The priority order assigned to the risks to be handled
d. Weakness of an asset or control that can be exploited by threats

Q27. (2021 A FE AM-q40) According to ISO/IEC 27000:2018 (Information security management systems Overview and vocabulary), which of the following is the definition of “level of risk”?

Theme: Security, Category: FE

a. Magnitude of a risk expressed in terms of the combination of consequences and their likelihood
b. Terms of reference for evaluating the significance of a risk
c. The priority order assigned to the risks to be handled
d. Weakness of an asset or control that can be exploited by threats

Question 28

Q28. (2021 A FE AM-q41) Which of the following is dynamic analysis of malware?

a. Malware is identified by calculating the hash value of the subject for analysis and crosschecking it against a list of known malware hash values that are registered in an online database.
b. On the basis of the file extensions and content of file headers on a hard disk, malicious program files with false extensions are detected.
c. The subject for analysis is extracted from communication data on a network and reverse compiled, and the functions of the subject for analysis are investigated from the code obtained.
d. The subject for analysis is run in a sandbox, and its behavior and external communication are observed.

Q28. (2021 A FE AM-q41) Which of the following is dynamic analysis of malware?

Theme: Security, Category: FE

a. Malware is identified by calculating the hash value of the subject for analysis and crosschecking it against a list of known malware hash values that are registered in an online database.

b. On the basis of the file extensions and content of file headers on a hard disk, malicious program files with false extensions are detected.

c. The subject for analysis is extracted from communication data on a network and reverse compiled, and the functions of the subject for analysis are investigated from the code obtained.

d. The subject for analysis is run in a sandbox, and its behavior and external communication are observed.

Question 29

Q29. (2021 A FE AM-q42) Which of the following technologies is the most suitable to divide the whole company network into networks by department?

a. DMZ (DeMilitarized Zone)
b. NAT (Network Address Translation)
c. VLAN (Virtual Local Area Network)
d. VPN (Virtual Private Network)

Q29. (2021 A FE AM-q42) Which of the following technologies is the most suitable to divide the whole company network into networks by department?

Theme: Security, Category: FE

a. DMZ (DeMilitarized Zone)
b. NAT (Network Address Translation)
c. VLAN (Virtual Local Area Network)
d. VPN (Virtual Private Network)

Question 30

Q30. (2021 A FE AM-q43) An SQL injection attack caused the SQL statement below to be executed. Which of the following does the SQL statement do? Here, the accounts table contains account information in each row.

SELECT * FROM accounts WHERE username='1' or '1'='1';
DROP TABLE accounts;

a. It creates a new user '1'.
b. It creates a pop-up box that shows the first username in the "accounts" table.
c. It selects all the records in the "accounts" table and deletes the "accounts" table from the database.
d. It selects one record from the "accounts" table and drops the rest of the records in the table.

Q30. (2021 A FE AM-q43) An SQL injection attack caused the SQL statement below to be executed. Which of the following does the SQL statement do? Here, the accounts table contains account information in each row.

SELECT * FROM accounts WHERE username='1' or '1'='1';
DROP TABLE accounts;

Theme: Security, Category: FE

a. It creates a new user '1'.
b. It creates a pop-up box that shows the first username in the "accounts" table.
c. It selects all the records in the "accounts" table and deletes the "accounts" table from the database.
d. It selects one record from the "accounts" table and drops the rest of the records in the table.

Question 31

Q31. (2021 A FE AM-q44) To provide a guarantee to its online customers that all credit card information is protected when transferred between their PC and the web service over public networks, which of the following technologies should be used?

a. S/MIME

b. SSH

c. TLS

d. VPN

Q31. (2021 A FE AM-q44) To provide a guarantee to its online customers that all credit card information is protected when transferred between their PC and the web service over public networks, which of the following technologies should be used?

Theme: Security, Category: FE

a. S/MIME
b. SSH
c. TLS
d. VPN

Question 32

Q32. (2021 S FE AM-q34) Which of the following is classified as a web beacon?

a. A potential error of an application program used for a website
b. A technique to collect user information, such as access trends, by embedding a small image in a web page
c. A virus that is downloaded from a website that deletes image files on a PC
d. An abusive method of using a malicious script that is harmful to both client PC and web server

Q32. (2021 S FE AM-q34) Which of the following is classified as a web beacon?

Theme: Security, Category: FE

a. A potential error of an application program used for a website
b. A technique to collect user information, such as access trends, by embedding a small image in a web page
c. A virus that is downloaded from a website that deletes image files on a PC
d. An abusive method of using a malicious script that is harmful to both client PC and web server

Question 33

Q33. (2021 S FE AM-q35) When risk treatment is classified as risk avoidance, risk reduction, risk acceptance, and risk sharing, which of the following risk treatments is risk avoidance?

a. Applying appropriate controls to lower a risk

b. Discontinuing some operations that have a risk

c. Knowingly and objectively not taking any action on a risk

d. Transferring a risk to other parties

Q33. (2021 S FE AM-q35) When risk treatment is classified as risk avoidance, risk reduction, risk acceptance, and risk sharing, which of the following risk treatments is risk avoidance?

Theme: Security, Category: FE

a. Applying appropriate controls to lower a risk
b. Discontinuing some operations that have a risk
c. Knowingly and objectively not taking any action on a risk
d. Transferring a risk to other parties

Question 34

Q34. (2021 S FE AM-q36) Which of the following is installed into an in-house network or server by an intruder to enter through an access path other than the normal path?

a. Backdoor

b. Forensic

c. Strict routing

d. Thin client agent

Q34. (2021 S FE AM-q36) Which of the following is installed into an in-house network or server by an intruder to enter through an access path other than the normal path?

Theme: Security, Category: FE

a. Backdoor

b. Forensic

c. Strict routing

d. Thin client agent

Question 35

Q35. (2021 S FE AM-q37) Biometric authentication includes a verification method that extracts physical characteristics and another verification method that extracts behavioral characteristics. Which of the following is the method that uses behavioral characteristics?

a. Performing authentication by extracting characteristics from pen speed and pressure when a signature is provided

b. Performing authentication by extracting characteristics from the bifurcation angle of the bifurcation point of a blood vessel or from the distance between adjacent bifurcation points

c. Performing authentication by extracting the characteristic point called minutia from the pattern formed by ridges

d. Performing authentication by extracting the characteristics of chaotic wrinkles in the eye from the pupil to the outside

Q35. (2021 S FE AM-q37) Biometric authentication includes a verification method that extracts physical characteristics and another verification method that extracts behavioral characteristics. Which of the following is the method that uses behavioral characteristics?

Theme: Security, Category: FE

a. Performing authentication by extracting characteristics from pen speed and pressure when a signature is provided
b. Performing authentication by extracting characteristics from the bifurcation angle of the bifurcation point of a blood vessel or from the distance between adjacent bifurcation points
c. Performing authentication by extracting the characteristic point called minutia from the pattern formed by ridges
d. Performing authentication by extracting the characteristics of chaotic wrinkles in the eye from the pupil to the outside

Question 36

Q36. (2021 S FE AM-q38) Which of the following is an encryption method that can be used for encrypting data managed in a database using the same key for encryption and decryption?

a. AES
b. PKI
c. RSA
d. SHA-256

Q36. (2021 S FE AM-q38) Which of the following is an encryption method that can be used for encrypting data managed in a database using the same key for encryption and decryption?

Theme: Security, Category: FE

a. AES
b. PKI
c. RSA
d. SHA-256

Question 36: Answer Explanation

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information.
AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection.
Public key infrastructure (PKI) governs the issuance of digital certificates to protect sensitive data, provide unique digital identities for users, devices and applications and secure end-to-end communications.

Question 37

Q37. (2021 S FE AM-q39) A given application only has the functions of retrieving and displaying user information from a database that stores such information. Considering information security management, which of the following is the appropriate database access right assigned to an account that the application uses when it accesses the database? The names and scopes of rights are listed below.

[The names and scopes of rights]
Reference right: Permits a record to be selected
Update right: Permits a record to be inserted, updated, and dropped
Administrator right: Permits a table to be displayed, created, altered, and dropped

a. Administrator right

b. Reference right

c. Update right

d. Update right and reference right

Q37. (2021 S FE AM-q39) A given application only has the functions of retrieving and displaying user information from a database that stores such information. Considering information security management, which of the following is the appropriate database access right assigned to an account that the application uses when it accesses the database? The names and scopes of rights are listed below.
[The names and scopes of rights]
Reference right: Permits a record to be selected
Update right: Permits a record to be inserted, updated, and dropped
Administrator right: Permits a table to be displayed, created, altered, and dropped

Theme: Security, Category: FE

a. Administrator right
b. Reference right
c. Update right
d. Update right and reference right

Question 38

Q38. (2021 S FE AM-q40) A cybersecurity incident response plan is defined as a set of instructions to aid the cybersecurity team to detect, respond to, and recover from cybersecurity incidents. The cybersecurity incident response plan resolves issues, such as cybercrime, data loss, and service outages that threaten daily work. Which of the following is part of the cybersecurity incident response plan?

a. Attacking systems with scripts

b. Containment

c. Social engineering activities

d. Stealing user credentials

Q38. (2021 S FE AM-q40) A cybersecurity incident response plan is defined as a set of instructions to aid the cybersecurity team to detect, respond to, and recover from cybersecurity incidents. The cybersecurity incident response plan resolves issues, such as cybercrime, data loss, and service outages that threaten daily work. Which of the following is part of the cybersecurity incident response plan?

Theme: Security, Category: FE

a. Attacking systems with scripts
b. Containment
c. Social engineering activities
d. Stealing user credentials

Question 39

Q39. (2021 S FE AM-q41) Between a client and web server, which of the following is used for inspecting the data that is sent from the client to the web server and blocking attacks, such as SQL injections?

a. Cluster configuration
b. Load balancing function
c. SSL-VPN function
d. WAF

Q39. (2021 S FE AM-q41) Between a client and web server, which of the following is used for inspecting the data that is sent from the client to the web server and blocking attacks, such as SQL injections?

Theme: Security, Category: FE

a. Cluster configuration
b. Load balancing function
c. SSL-VPN function
d. WAF

Question 39: Answer Explanation

A web application firewall (WAF) protects web applications from a variety of application layer attacks such as cross-site scripting (XSS), SQL injection, and cookie poisoning, among others. Attacks to apps are the leading cause of breaches. They are the gateway to your valuable data. It is a firewall that monitors, filters and blocks data packets as they travel to and from a website or web application. A WAF can be either network-based, host-based or cloud-based and is often deployed through a reverse proxy and placed in front of one or more websites or applications.

Question 40

Q40. (2021 S FE AM-q42) Which of the following is an appropriate description of SSH?

a. It cannot use public key pairs, and it uses a password for authentication.

b. It helps in securely loading web site pages over HTTPS.

c. It provides a secure channel for server maintenance over a public network.

d. Its use is required in the Intranet.

Q40. (2021 S FE AM-q42) Which of the following is an appropriate description of SSH?

Theme: Security, Category: FE

a. It cannot use public key pairs, and it uses a password for authentication.
b. It helps in securely loading web site pages over HTTPS.
c. It provides a secure channel for server maintenance over a public network.
d. Its use is required in the Intranet.

Question 41

Q41. (2021 S FE AM-q43) Which of the following is an appropriate description concerning Sender Policy Framework (SPF) for email communication?

a. It is a policy of the public relations department to designate a specific person to send emails.

b. It is an email sent from a spoofed email address without authorization.

c. It matches the sender mail server IP address with the information from the domain server and accepts or rejects email.

d. It sends an email to the address of a specific person instead of sending them to multiple email addresses.

Q41. (2021 S FE AM-q43) Which of the following is an appropriate description concerning Sender Policy Framework (SPF) for email communication?

Theme: Security, Category: FE, Text Book: Page no. 390

a. It is a policy of the public relations department to designate a specific person to send emails.
b. It is an email sent from a spoofed email address without authorization.
c. It matches the sender mail server IP address with the information from the domain server and accepts or rejects email.
d. It sends an email to the address of a specific person instead of sending them to multiple email addresses.

Question 41: Answer Explanation

SPF (Sender Policy Framework): This is a method for sender domain authentication that manages an IP address list of proper mail servers authorized to send e-mail from a given domain. It enables automated rejection of e-mail sent from unrelated mail servers. It is an extended specification of SMTP, and is defined as RFC 4408.

Question 42

Q42. (2021 S FE AM-q44) Which of the following is an appropriate explanation of OP25B for email communication?

a. Blocking communication to port 25 to reduce mass-scale delivery of spam or junk emails
b. Blocking emails that are sent to more than 25 recipients at once due to organizational policy
c. Blocking Simple Mail Transfer Protocol (SMTP) communication except those sent to port 25
d. Blocklisting email addresses that send spams by monitoring email communication to port 25

Q42. (2021 S FE AM-q44) Which of the following is an appropriate explanation of OP25B for email communication?

Theme: Security, Category: FE, Text Book: Page no. 390

a. Blocking communication to port 25 to reduce mass-scale delivery of spam or junk emails
b. Blocking emails that are sent to more than 25 recipients at once due to organizational policy
c. Blocking Simple Mail Transfer Protocol (SMTP) communication except those sent to port 25
d. Blocklisting email addresses that send spams by monitoring email communication to port 25

Question 42: Answer Explanation

Outbound Port 25 Blocking (OP25B) is a measure to prevent any intentional or unintentional sending of bulk unsolicited email through an Internet provider's outbound email server. Many spam emails are directly routed using the port 25 to the servers of recipients. By blocking the port 25, it can limit the use of port 25 which accordingly block the flow of spams.
You can send emails by using using outbound email server of Port 465 (SMTP over SSL/TLS) if port 25 is blocked.

Any Questions?

References

IT Fundamentals (New FE Textbook Vol. 1)