Total Marks : 60

2 Marks

30 x 2 = 60

1) Write about information leakage in E-Commerce

Answer : **Information leakage:** The leakage of trade secrets in E-commerce mainly includes two aspects: (a) the content of the transaction between the vendor and customer is stolen by the third party; (b) the documents provided by the merchant to the customer or vice versa are illegally used by the another. This intercepting and stealing of Online documents is called information leakage.

2) Write a short note on typopiracy.

Answer : Typopiracy is a variant of Cyber Squatting. Some fake websites try to take advantage of users common typographical errors in typing a website address and direct users to a different website. Such people try to take advantage of some popular websites to generate accidental traffic for their websites. e.g. www.goggle.com, www.facebook.com

3) List the different types of security technologies in E-Commerce

Answer : The security technologies in E-Commerce transactions are roughly classified into
(i) Encryption technology
(ii) Authentication technology
(iii) Authentication protocols

4) What is digital signature?

Answer : A digital signature is a mechanism that is used to verify that a particular digital document, message or transaction is authentic.

5) Write about phishing

Answer : Phishing is acquiring critical data like login credentials through telephone, sms, e-mail or any social media by the crackers disguising as authentic.

6) Define non-repudiation.

Answer : Non-repudiation: Repudiation refers to any act of relinquishing responsibility for a message. Non-repudiation ensures that the signer who digitally signed the document cannot deny having signed it. The digitally signed documents strengthen its recipient integrity claims. Therefore, the recipient can strongly insist on the signature of the sender so as not to be easily denied at a later time.

7) When was DES introduced?

Answer : It was introduced in America in the year 1976.

8) What is the use of digital certificates?

Answer : Digital certificates are used to verify the Trust worthiness of the sender.

9) Who is 3D-Secure?

Answer : 3D-Secure was developed by Visa

10) What is the basic concept 3D-Secure?

Answer : To link the financial authorization process with an online authentication system.

11) How TLS and SSL differ?

Answer : TLS differs from SSL in the generation of symmetric keys.

12) How many domains are in authentications model?

Answer : There are 3 domains in authentications model.

13) When SSL renamed?

Answer : Secure Sockets Layers (SSL) was renamed as Transport Layer Security (TLS) in 2001.

14) What is the principle of SSL?

Answer : To establish a secure communication channel between a client and a server.

15) What is the role of security certifications in authentication technology?

Answer : To ensure Authentication, Integrity and Non-repudiation.

16) Who are the participants involve inset purchase?

Answer : 1) The customer
2) The seller
3) The payment gateway

17) What is another name of Asymmetric encryption?

Answer : RSA (Rivest-Shamir-Adleman) algorithm.

18) What is digital certificates?

Answer : (i) A digital certificate (also known as public key certificate) is an electronic document used to prove the ownership of a public key
(ii) This certificate includes the information about the sender's identity, digital signature and a public key

19) What is the review ability?

Answer : Capability of monitoring activities to audit and track the operations.

20) Is it DES safe for many application?

Answer : No, DES is not safe for many application.

21) Name the worldwide format accepted by digital signature

Answer : Digital signatures use a standard worldwide accepted format that is called Public key infrastructure(PKI).

22) How many types of Autheutication protocols are there in E-Commerce?

Answer : There are two kinds of security authentication protocols widely used in E.Commerce.

23) What is the another name for asymmetri assymetric cencryption?

Answer : Asymmetric encryption is also called as Rivest-Shamir - Adleman (RSA)

24) By whom Pretty Good privacy developed?

Answer : Pretty Good Privacy (PGP) was developed by Phil Zimmermann in 1991.

25) What must be used by attacker will extract the credit card information and sell it in black markets?

Answer : Using malware, Cross Site Scripting or SQL Injection, an attacker will extract the credit card information and sell the acquired data on black markets.

26) What is RSA?

Answer : Asymmetric encryption also called as RSA (Rivest-Shamir-Adleman) algorithm. It uses public-key authentication and digital signatures.

27) Name few licensed certifying authority.

Answer : The digital certificate are being issued by a licensed Certifying Authority (CA). NIC, Safescript, TCS, MTNL, e-Mudhra are some of the authorized Certifying Authorities under Government of India

28) What is PKI?

Answer : Digital signatures use a standard, worldwide accepted format, called Public Key Infrastructure (PKI), to provide the highest levels of security and universal acceptance.

29) What is purpose of using digital signatures?

Answer : Digital signatures are widely used for avoiding forging or tampering of important documents such as financial documents or credit card data.

30) How SET was developed?

Answer : SET was developed in 1996 by VISA and MasterCard, with the participation of GTE, IBM, Microsoft and Netscape.