Chapter 10 Review Questions

1. Which technology is NOT a core feature of a mobile device?
2. physical keyboard
3. small form factor
4. local non-removable data storage
5. data synchronization capabilities
6. Agape was asked to make a recommendation regarding short-range wireless technologies to be supported in a new conference room that was being renovated. Which of the following would she NOT consider due to its slow speed and its low deployment levels today?
7. ANT
8. Bluetooth
9. Infrared
10. NFC
11. Calista is designing the specifications for new laptop computers to be purchased by her company. She is comparing the different types and sizes of USB connections found on the devices. Which type USB connection would she NOT find on a laptop?
12. Type D
13. Mini
14. Micro
15. Standard
16. In her job interview, Xiu asks about the company policy regarding smartphones. She is told that employees may choose from a limited list of approved devices but that she must pay for the device herself; however, the company will provide her with a monthly stipend. Which type of enterprise deployment model does this company support?
17. BYOD
18. COPE
19. CYOD
20. Corporate-owned
21. Pakpao has been asked to provide research regarding a new company initiative to add Android smartphones to a list of approved devices. One of the considerations is how frequently the smartphones receive firmware OTA updates. Which of the following reasons would Pakpao NOT list in his report as a factor in the frequency of Android firmware OTA updates?
22. Both OEMs and wireless carriers are hesitant to distribute Google updates because it limits their ability to differentiate themselves from competitors if all versions of Android start to look the same through updates.
23. Because many of the OEMs had modified Android, they are reluctant to distribute updates that could potentially conflict with their changes.
24. Wireless carriers are reluctant to provide firmware OTA updates because of the bandwidth it consumes on their wireless networks.
25. Because OEMs and wireless carriers want to sell as many devices as possible, they have no financial incentive to update mobile devices that users would then continue to use indefinitely.
26. What is the process of identifying the geographical location of a mobile device?
27. geotracking
28. geolocation
29. geoID
30. geomonitoring
31. Which of these is NOT a risk of connecting a mobile device to a public network?
32. Public networks are beyond the control of the employee’s organization.
33. Replay attacks can occur on public networks.
34. Public networks may be susceptible to man-in-the-middle attacks.
35. Public networks are faster than local networks and can spread malware more quickly to mobile devices.
36. Paavo was reviewing a request by an executive for a new subnotebook computer. The executive said that he wanted USB OTG support and asked Paavo’s opinion regarding its security. What would Paavo tell him about USB OTG security?
37. USB OTG uses strong security and the executive should have no concerns.
38. Subnotebooks do not support USB OTG.
39. An unsecured mobile device could infect other tethered mobile devices or the corporate network.
40. Connecting a mobile device as a peripheral to an infected computer could allow malware to be sent to that device.
41. A friend of Ukrit told him that he has just downloaded and installed an app that allows him to circumvent the built-in limitations on his Apple iOS smartphone. What is this called?
42. Rooting
43. Sideloading
44. Jailbreaking
45. Ducking
46. Which of the following technologies provides for pictures, video, or audio to be included in text messages?
47. MMS
48. QR
49. SMS
50. ANT
51. What prevents a mobile device from being used until the user enters the correct passcode?
52. swipe identifier (SW-ID)
53. screen lock
54. screen timeout
55. touch swipe
56. Gaetan has attempted to enter the passcode for his mobile device but keeps entering the wrong code. Now he is asked to enter a special phrase to continue. Which configuration setting is enabled on Gaetan’s mobile device?
57. reset to factory settings
58. extend lockout period
59. enable high security
60. lock device
61. What does containerization do?
62. It splits operating system functions only on specific brands of mobile devices.
63. It places all keys in a special vault.
64. It slows down a mobile device to half speed.
65. It separates personal data from corporate data.
66. What allows a device to be managed remotely?
67. mobile device management (MDM)
68. mobile application management (MAM)
69. mobile resource management (MRM)
70. mobile wrapper management (MWM)
71. Which of these is NOT a security feature for locating a lost or stolen mobile device?
72. remote lockout
73. last known good configuration
74. alarm
75. thief picture
76. What enforces the location in which an app can function by tracking the location of the mobile device?
77. location resource management
78. geofencing
79. GPS tagging
80. Graphical Management Tracking (GMT)
81. Which of these is considered the strongest type of passcode to use on a mobile device?
82. password
83. PIN
84. fingerprint swipe
85. draw connecting dots pattern
86. Jabez needs to alert through an SMS text message those corporate users who have a specific brand and type of mobile device regarding a serious malware incident. What technology will she use?
87. MCM
88. COPE
89. MAM
90. push notification services
91. Which tool manages the distribution and control of apps?
92. MAM
93. MDM
94. MCM
95. MFM
96. Which type of OS is typically found on an embedded system?
97. SoC
98. RTOS
99. OTG
100. COPE