

SULIT



BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENDIDIKAN POLITEKNIK
KEMENTERIAN PENDIDIKAN TINGGI

JABATAN TEKNOLOGI MAKLUMAT & KOMUNIKASI

PEPERIKSAAN AKHIR
SESI DISEMBER 2017

DFP6033 : SECURE MOBILE COMPUTING

TARIKH : 10 APRIL 2018
MASA : 2.30 PETANG - 4.30 PETANG (2 JAM)

Kertas ini mengandungi **DUA PULUH EMPAT (24)** halaman bercetak.

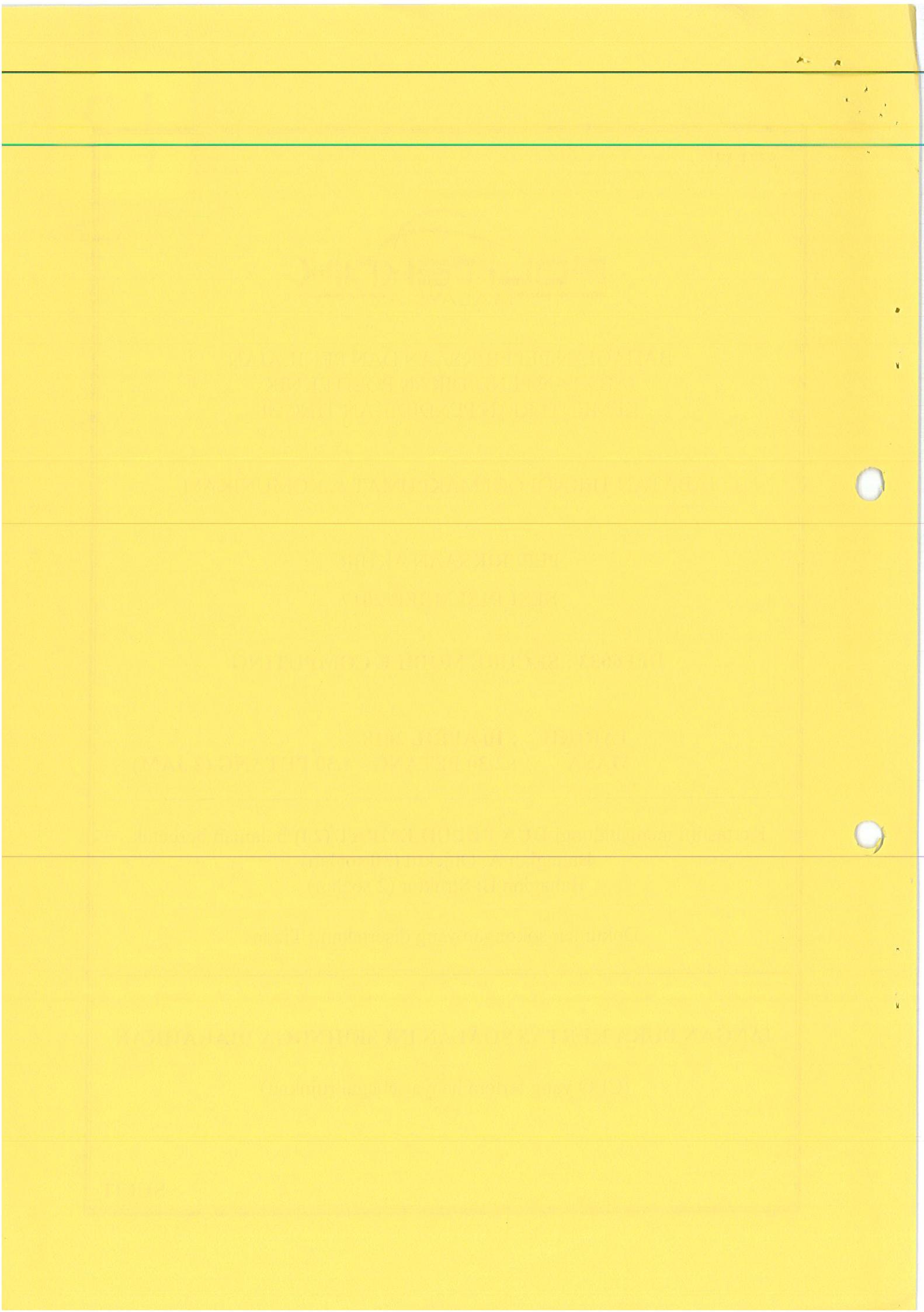
Bahagian A: Objektif (30 soalan)

Bahagian B: Struktur (2 soalan)

Dokumen sokongan yang disertakan : Tiada

JANGAN BUKA KERTAS SOALANINI SEHINGGA DIARAHKAN
(CLO yang tertera hanya sebagai rujukan)

SULIT



SECTION A : 45 MARKS
BAHAGIAN A : 45 MARKAH

INSTRUCTION:

This section consists of **THIRTY (30)** objective questions. Mark your answers in the OMR form provided.

ARAHAN :

*Bahagian ini mengandungi **TIGA PULUH (30)** soalan objektif. Tandakan jawapan anda di dalam borang OMR yang disediakan.*

CLO1
C1

1. Based on the statement below, identify the **CORRECT** mobile computing aspect.
*Berdasarkan pernyataan di bawah, kenalpasti aspek Pengkomputeran Mudah Alih yang **BETUL**.*

"It is the actual program that runs on the mobile hardware. It deals with the characteristics and requirements of mobile applications".

"Ia adalah program sebenar yang beroperasi pada peranti mudah alih. Ia menangani ciri-ciri dan keperluan sesuatu aplikasi mudah alih".

- A. Mobile Software / *Perisian Mudah Alih*
- B. Mobile Hardware / *Perkakasan Mudah Alih*
- C. Mobile Communication / *Komunikasi Mudah Alih*
- D. Mobile Wireless Computing / *Pengkomputeran Mudah Alih*

CLO1
C2

2. Determine the **TRUE** statement about Mobile Computing.

*Tentukan kenyataan yang **BETUL** mengenai Pengkomputeran Mudah Alih.*

- A. A technology that allows transmission of data, voice and video via any wireless enabled device and must having to be connected to a fixed physical link.

Teknologi yang membolehkan penghantaran data, suara dan video melalui mana-mana peranti berkemampuan tanpa wayar dan mestilah disambungkan ke pautan fizikal tetap.

- B. A technology that allows transmission of data, voice and video via any wireless enabled device without having to be connected to a fixed physical link.

Teknologi yang membolehkan penghantaran data, suara dan video melalui mana-mana peranti berkemampuan tanpa wayar tanpa perlu dihubungkan ke pautan fizikal tetap

- C. A technology that allows transmission of data, voice, video and image via any wired enabled device without having to be connected to a fixed physical link.

Teknologi yang membolehkan penghantaran data, suara, video dan imej melalui mana-mana peranti berkemampuan dengan wayar tanpa perlu dihubungkan ke pautan fizikal tetap.

- D. A technology that allows transmission of data, voice, video and image via any wired enabled device and must having to be connected to a fixed physical link.

Teknologi yang membolehkan penghantaran data, suara, video dan imej melalui mana-mana peranti berkemampuan dengan wayar dan mesti disambungkan ke pautan fizikal tetap

Question 3-4 is based on TRUE and FALSE questions.

Soalan 3-4 adalah berdasarkan soalan-soalan BETUL dan SALAH.

CLO1
C1

3. State whether the above statement is TRUE or FALSE.

Nyatakan sama ada pernyataan di atas adalah BETUL atau SALAH.

“The technology of mobile communication allows us to communicate with others in different locations without the usage of cables. One of the type is ANALOG communication. ANALOG communication is 1G Frequency Division Multiple Access (FDMA).”

Teknologi komunikasi mudah alih membenarkan kita berkomunikasi dari pelbagai lokasi tanpa penggunaan wayar. Salah satu bentuk komunikasi ialah komunikasi ANALOG. Komunikasi ANALOG merupakan Frequency Division Multiple Access (FDMA) 1G.”

- A. TRUE / BETUL
B. FALSE / SALAH

CLO1
C1

4. State whether the statement below is TRUE or FALSE.

Nyatakan sama ada pernyataan di bawah adalah BETUL atau SALAH.

“There are 3 Tier architecture for mobile computing; Presentation tier, Application tier and Data tier. Presentation tiers responsible for presenting the information to the end user.”

“Terdapat senibina 3 Tier untuk Pengkomputeran Mudah Alih; Presentation tier, Application tier dan Data tier. Presentation tier bertanggungjawab untuk mempersemprehankan maklumat kepada pengguna akhir.”

- A. TRUE / BETUL
B. FALSE / SALAH

CLO1
C2

5. Figure A1 shows an infrastructure for radio wave-oriented. Choose the **CORRECT** statement for X and Y.

*Rajah A1 menunjukkan infrastruktur berorientasikan gelombang radio. Pilih kenyataan yang **BETUL** untuk X dan Y.*

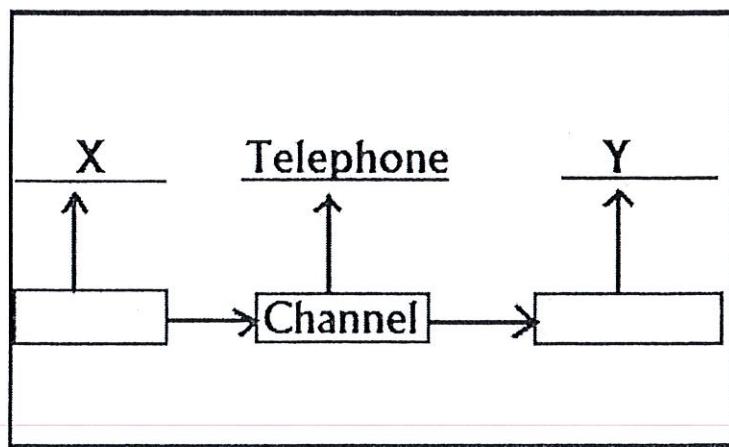


Figure A1 / Rajah A1

- A. X = SENDER; Y= SENDER
- B. X = RECIEVER; Y= SENDER
- C. X = SENDER; Y= RECEIVER
- D. X = RECEIVER; Y= RECEIVER

CLO1
C2

6. Identify the tiers that controls the detailed of business logic of processing user input, obtaining data and making decisions.

Kenalpasti tier yang mengawal logik perniagaan terperinci bagi pemprosesan input pengguna, memperoleh data dan membuat keputusan.

- A. Device tier
- B. Database tier
- C. Application tier
- D. Presentation tier

CLO1
C2

7. State the name of layer X and Y based on Figure A2.

Nyatakan nama lapisan X dan Y berdasarkan Rajah A2.

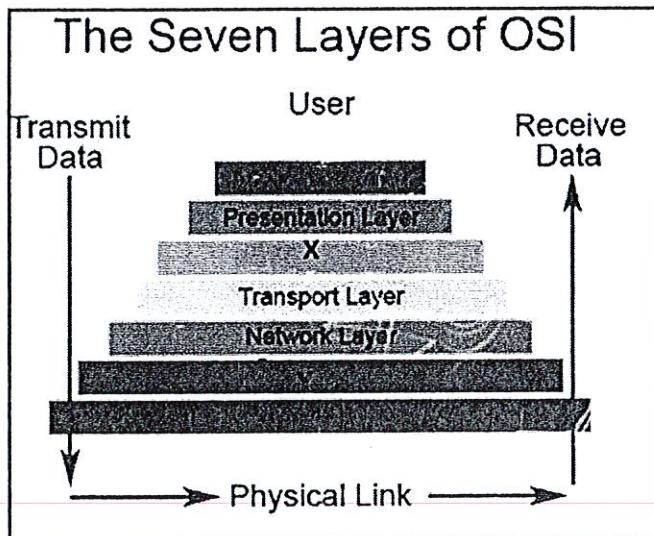


Figure A2 / Rajah A2

- A. X = SESSION ; Y=SIGNAL
- B. X = SESSION ; Y= DATA
- C. X = SIGNAL ; Y=PATH
- D. X = DATA ; Y=SIGNAL

CLO1
C1

8. Which of the following is NOT examples of real security and privacy threats?

Manakah antara berikut BUKAN merupakan contoh ancaman keselamatan dan privasi sebenar?

- A. Hackers
- B. Virus
- C. Spam
- D. Worm

CLO1 C1	9. In computer security, X represents the information in a computer system that can only be accessed for reading by authorized parties. Identify X. <i>Dalam keselamatan komputer, X mewakili maklumat dalam sistem komputer yang hanya boleh diakses untuk dibaca oleh pihak yang dibenarkan. Kenalpasti X.</i> A. Integrity / Integriti B. Authenticity / Keaslian C. Availability / Ketersediaan D. Confidentiality / Kerahsiaan
CLO1 C2	10. Identify the process in which a user is identified via a username and password. <i>Kenalpasti proses dimana pengguna dikenalpasti menerusi katanama pengguna dan katarahsiaan.</i> A. Auditing B. Accounting C. Authorization D. Authentication
CLO1 C2	11. Choose which one of the following does NOT help with mobile data security? <i>Pilih antara berikut yang manakah TIDAK membantu dengan keselamatan data mudah alih?</i> A. MDM software / Perisian MDM B. Website blacklisting / Senarai hitam laman web C. Virtual Private Network(VPN) access / Akses Virtual Private Network(VPN) D. Implementing Bring Your Own Devices(BYOD) / Melaksanakan Bring Your Own Devices(BYOD)

- CLO2
C3 12. Three-tier architecture is used by a large number of applications that work with data. Most of the modern enterprise applications, portal solutions and websites are constructed in this manner. Based on Figure A3, choose the best answer to describe Data - tier architecture model.

Senibina tiga peringkat digunakan oleh sebilangan besar aplikasi yang berfungsi dengan data. Kebanyakan aplikasi perusahaan moden, penyelesaian portal dan laman web dibina dengan cara ini. Berdasarkan Rajah A3, pilih jawapan yang terbaik untuk menerangkan model senibina Data - tier.

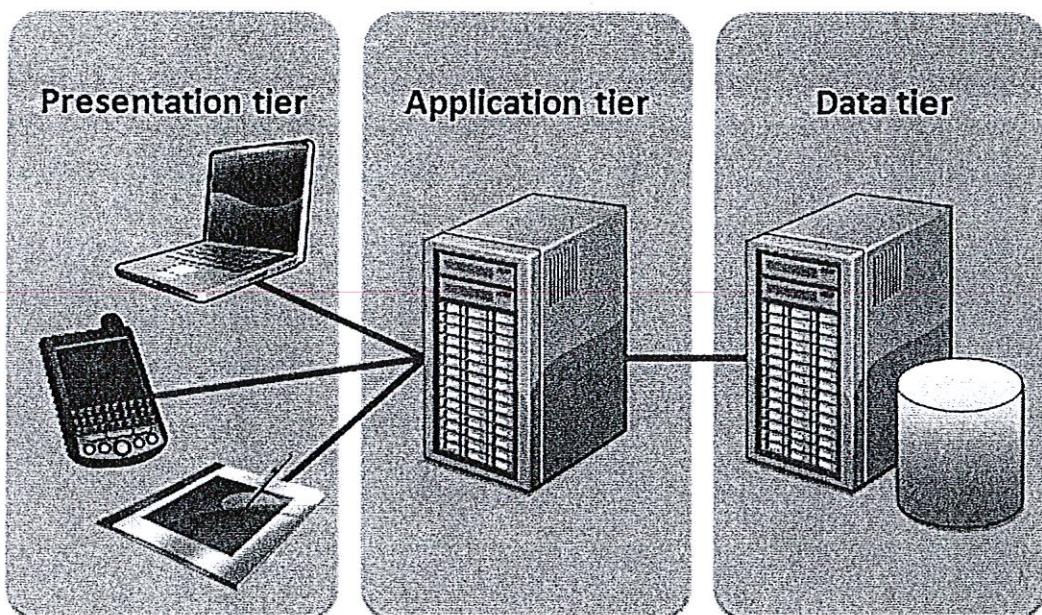


Figure A3 / Rajah A3

- A. Houses database servers where information is stored and retrieved.
Server pangkalan data rumah di mana maklumat disimpan dan diambil.
- B. Data in this tier is kept dependent of application servers or business logic.
Data di peringkat ini bergantung kepada pelayan aplikasi atau logik perniagaan
- C. It assures the calculations and operations performed between input-output requirements and data.
Ia menjamin pengiraan dan operasi yang dilakukan antara keperluan input dan data.
- D. It enables the input of requirements and the presentation of results.
Ia membolehkan input keperluan dan pembentangan keputusan

CLO2
C3

13. Arrange the evolution of wireless generation in sequence based on Table A1 below.

Susun evolusi generasi tanpa wayar mengikut turutan, berdasarkan Jadual A1 di bawah.

Table A1 / Jadual A1

I	Voice , Data & Video Signals Video Telephony Internet Surfing
II	Voice Signals only Analogue Cellular Phones
III	Voice & Data Signals Digital Fidelity Cellular Phones
IV	Interoperability Protocol Mobile IP

- A. II → I → IV → III
- B. IV → II → III → I
- C. II → III → I → IV
- D. I → IV → III → II

CLO2
C3

14. Relate Figure A4 to the most suitable statement that best described the cellular network concept illustrated.

Hubungkan Rajah A4 kepada pernyataan yang sesuai, yang menerangkan dengan tepat konsep rangkaian selular yang digambarkan.

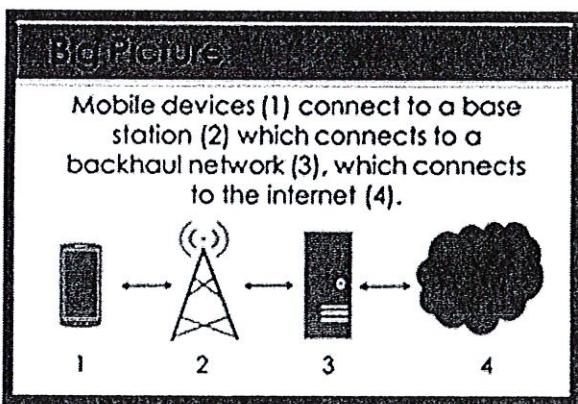


Figure A4 / Rajah A4

- A. A cellular network is a cell network distributed over land through mobile where each mobile includes a fixed location transceiver known as mobile station.

Rangkaian selular adalah rangkaian sel yang diedarkan melalui tanah melalui telefon bimbit di mana setiap mudah alih termasuk lokasi penerima tetap dikenali sebagai stesen bergerak.

- B. Cellular networks give subscribers features over alternative solutions, including decreased capacity.

Rangkaian selular memberikan ciri-ciri pelanggan melalui penyelesaian alternatif, termasuk penurunan kapasiti.

- C. A cellular network is a radio network distributed over land through cells where each cell includes a fixed location transceiver known as base station.

Rangkaian selular adalah rangkaian radio yang diedarkan ke atas tanah melalui sel di mana setiap sel termasuk penerima lokasi tetap dikenali sebagai stesen pangkalan.

- D. Cellular networks give subscribers features over alternative solutions, including increased interference from other signals.

Rangkaian selular memberi pelanggan ciri berbanding penyelesaian alternatif, termasuk gangguan yang meningkat daripada isyarat lain

CLO2
C2

15. Based on GSM architecture in Figure A5, identify the component shown in area I, II, and III.

Berdasarkan arkitektur GSM pada Rajah A5, kenalpasti antaramuka yang ditunjukkan di ruangan I, II, dan III.

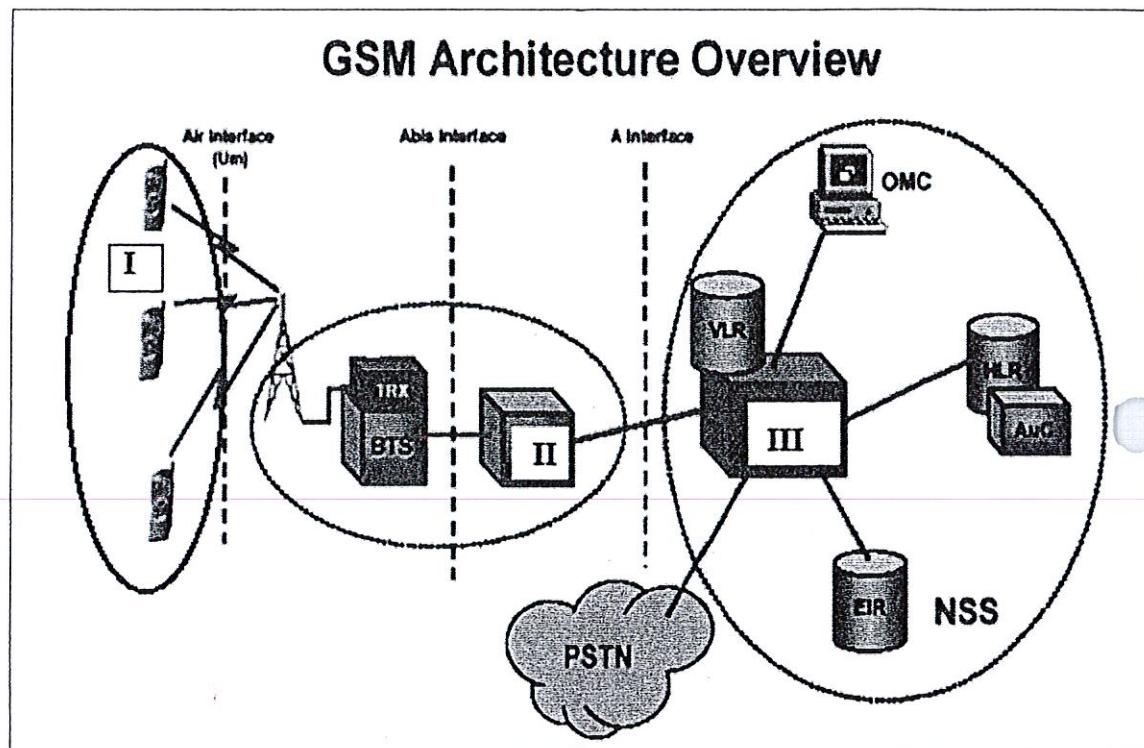


Figure A5 / Rajah A5

- A. I = MS ; II = BSC; III = MSC
- B. I = BSC ; II = MS; III = MSC
- C. I = MSC ; II = MS; III = BSC
- D. I = BSC ; II = MS; III = BTS

CLO2
C3

16. Based on description in Figure A6, relate it with the **CORRECT** type of attack.

Berdasarkan penerangan di Rajah A6, kaitkan ia dengan jenis serangan yang BETUL.

- A cellular phone can simply "join up" with another cellular provider's network.
Telefon selular boleh bergabung dengan pembekal rangkaian selular lain

- Cellular phones are generally promiscuous when it comes to joining networks
Telefon selular akan bergabung secara rambang dengan rangkaian.

- Cellular network are defined by a simple three-digit number and a three-digit country code.
Rengkaian selular definaskan dengan tiga digit mudah dan tiga digit kod negara

Figure A6 / Rajah A6

- A. Voice mail attack / Serangan Mel Suara
- B. Rogue station attack / Serangan stesen penyangak
- C. Rogue Femtocell attack / Serangan penyangak Femtocell
- D. Rogue mobile device attack / Serangan penyangak peralatan mobil

CLO2
C3

17. Based on Figure A7, choose the best answer to describe the given situation.

Berdasarkan Rajah A7, pilih jawapan terbaik yang menggambarkan situasi yang diberi.

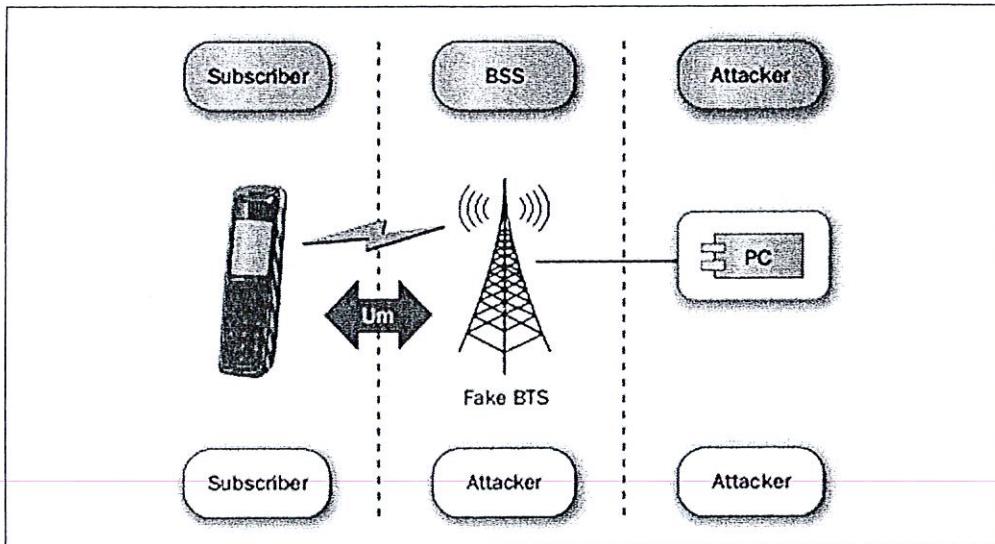


Figure A7 / Rajah A7

- A. GSM Spoofing
- B. Rogue Spoofing
- C. Femtocell Spoofing
- D. Voicemail Spoofing

CLO2
C3

18. Choose two places that permit enforced in Android Security Model.

Pilih dua tempat yang memberi kebenaran penguatkuasaan di dalam Model Keselamatan Android.

- A. Kernel and Application Framework Level
- B. Transport Framework and Kernel Level
- C. Application Component and Data Storage
- D. Permission Based Security and Application Security

CLO2
C1

19. Name a virus in mobile phones that may be hidden in an apparently harmless program or data.

Namakan virus pada telefon mobil, yang boleh berselindung di sebalik pengaturcaraan atau data yang kelihatan tidak membahayakan.

- A. Snort
- B. Honeypot
- C. Blue bomb
- D. Trojan horse

CLO2
C1

20. Identify vulnerabilities that gain complete access to the device and its contents, and starts communicating with and receiving instructions from one or more command and control servers.

Kenalpasti kelemahan yang mendapat capaian lengkap terhadap alatan dan kandungannya, dan mula berkomunikasi dan menerima arahan dari satu atau lebih pelayan kawalan.

- A. Botnet
- B. Worm
- C. Root kit
- D. Trojan horse

CLO2
C2

21. Select which mobile Operating System does not allow users to turn data encryption off.

Pilih Sistem Pengoperasian mudah alih manakah tidak membenarkan pengguna menutup data penyulitan.

- A. iOS
- B. Android
- C. Windows
- D. Symbian

CLO2
C2

22. Identify the term that is used when users download an application from outside the device's native application store.

Kenalpasti istilah yang digunakan apabila pengguna memuat turun aplikasi dari luar stor aplikasi asal peralatan.

- A. Backdoor app installation
- B. Non-app store downloads
- C. Sneaky app additions
- D. Sideload

CLO2
C2

23. Allowing workers to connect to an organization's servers using a wireless network introduces risks for host. Most security experts recommend the use of X, a network configuration in which mobile devices access an intranet securely while moving from one physical location to another. Identify X.

Membenarkan pekerja menghubungkan pelayan organisasi menggunakan rangkaian tanpa wayar boleh mengundang risiko. Kebanyakan pakar rangkaian menyarankan penggunaan X, konfigurasi rangkaian dimana peralatan mobil mencapai intranet dengan lebih selamat sementara memindahkan dari satu lokasi fizikal ke lokasi yang lain. Kenalpasti X.

- A. Modem
- B. Phone / Telefon
- C. Wireless / Tanpa wayar
- D. Virtual Private Network / Rangkaian Peribadi Virtual

- CLO2 24. The scenario below is one of the examples of wireless spoofing attack. Choose the type of spoofing described in the statement.

Senario di atas menggambarkan salah satu contoh dalam serangan ‘wireless spoofing’. Pilih jenis spoofing yang diterangkan dalam pernyataan di bawah.

The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.

‘Hijacker’ memperoleh alamat IP hos yang sah dan mengubah kepala paket supaya kelihatan seperti hos yang sah tersebut merupakan sumbernya

- A. IP Spoofing
- B. PC Spoofing
- C. Frame Spoofing
- D. MAC Address Spoofing

- CLO2 25. Interpret the scenario below.
Tafsirkan senario di bawah.

It is the forging of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source

Ini adalah kepala e-mail yang menyerupai email asal supaya mesej yang muncul daripada seseorang atau sesuatu tetapi berlainan dari punca yang asal.

- A. Spamming
- B. Footprinting
- C. Nonrepudiation
- D. E-Mail Spoofing

CLO2
C3

26. A mobile device can be easily attacked by various threats. Consumers may have downloaded applications that contain malware. As a consumer, choose the best method to secure your mobile devices.

Sebuah alat mudah alih mudah diserang oleh pelbagai ancaman. Pengguna mungkin telah memuat turun aplikasi yang mempunyai malware. Sebagai pengguna, pilih kaedah terbaik untuk memastikan peranti mudah alih anda selamat.

- A. Use sharing app installer.

Menggunakan pemasang aplikasi pengkongsian .

- B. Download apps from trusted App Store.

Memuat turun aplikasi dari kedai app yang dipercayai.

- C. Choose apps with the highest rating.

Memilih aplikasi yang mempunyai rating tertinggi.

- D. Download apps that does not required user permission before installation.

Memuat turun aplikasi yang tidak memerlukan kebenaran pengguna sebelum pemasangan.

CLO2
C3

27. You have received a warning email regarding a latest virus that is spreading in Malaysia. Choose three email characteristics indicating that, this is a hoax warning.

Anda telah menerima e-mel amaran mengenai virus terbaru yang merebak di Malaysia. Pilih tiga ciri-ciri emel yang menunjukkan bahawa ini adalah amaran palsu.

- I. The message is from a trusted source.

- II. The message was forwarded many times.

- III. The message requests that you forward the message to others.

- IV. The message warns of a virus that will infect your computer by simply reading the message.

- A. I, II, III

- C. II, III, IV

- B. I, II, IV

- D. None of the above

CLO2
C3

28. Based on Figure A9, select the best answer that describe the situation given.

Berdasarkan Rajah A9, pilih jawapan terbaik yang menggambarkan situasi diberi.

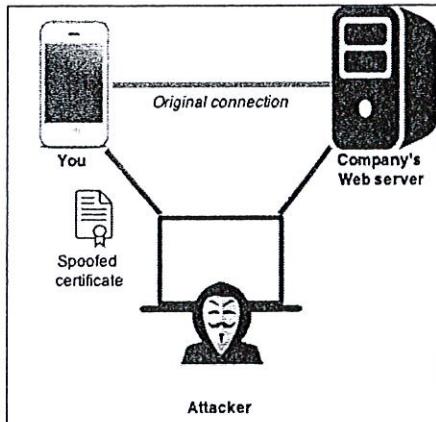


Figure A9 / Rajah A9

- A. Wireless Spoofing
- B. Man In The Middle Attacks
- C. Denial of Service Attacks
- D. Class of Illicit Use Attacks

CLO2
C3

29. Figure A10 is an example of mobile application that is under attack. Choose which type of attack in mobile environments that has been illustrated by the figure.

Rajah A10 adalah contoh aplikasi mudah alih yang telah diserang. Pilih jenis serangan dalam persekitaran mudah alih yang digambarkan oleh gambarajah di bawah

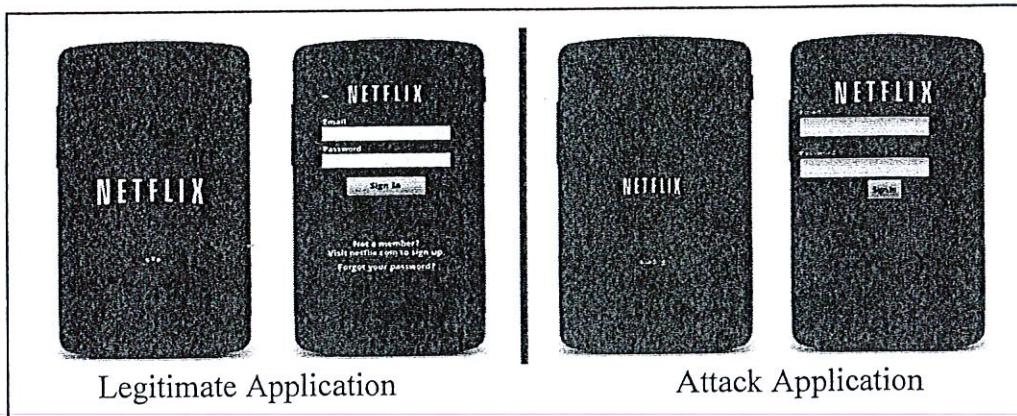


Figure A10 / Rajah A10

- A. Class of Illicit Use Attacks
- B. Wireless Spoofing
- C. Man-In-The-Middle Attacks
- D. Denial of Service Attacks

CLO2
C3

30. Eric is a new hacker and lack of experience. He only uses easily available hacking tools such as shell scripts and password crackers. Relate in which Eric's threat could be classified.

Eric adalah seorang penggodam yang baru dan kurang pengalaman. Dia hanya menggunakan alat penggodam yang mudah didapati seperti shell scripts dan pemecah kata laluan. Kaitkan kemungkinan kelas ancaman Eric.

- A. External / Luaran
- B. Internal / Dalaman
- C. Structured / Berstruktur
- D. Unstructured / Tidak berstruktur

SECTION B : 55 MARKS
BAHAGIAN B : 55 MARKAH

INSTRUCTION:

This section consists of TWO (2) structured questions. Answer ALL questions.

ARAHAN:

Bahagian ini mengandungi DUA (2) soalan berstruktur Jawab SEMUA soalan.

QUESTION 1

SOALAN 1

CLO1
C1

- a) State TWO (2) characteristics of information security.

Nyatakan DUA (2) ciri-ciri keselamatan maklumat.

[2 marks]
[2 markah]

CLO1
C2

- b) Based on Figure B1, identify the type of security model illustrated.

Berdasarkan Rajah B1, kenalpasti jenis model keselamatan tersebut.

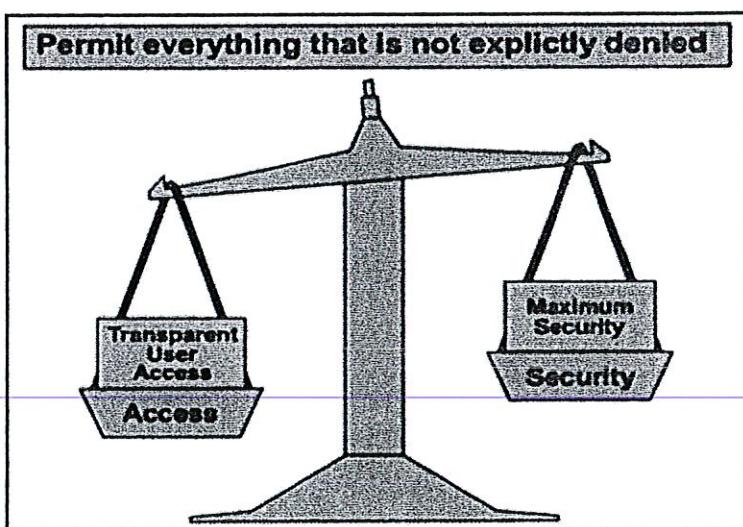


Figure B1/Rajah B1

[2 marks]
[2 markah]

- CLO2
C2 c) Explain the differences between unstructured threats and structured threats, and give **ONE (1)** example.

Jelaskan perbezaan antara ancaman yang tidak berstruktur dan ancaman berstruktur serta berikan SATU (1) contoh.

[3 marks]
[3 markah]

- CLO2
C2 d) Explain the Configuration weakness in security vulnerability
Terangkan kelemahan konfigurasi dalam kerentanan keselamatan

[4 marks]
[4 markah]

- CLO2
C3 e) Draw a diagram to illustrate typical Distributed DoS structure.
Lukiskan rajah untuk menggambarkan struktur 'Distributed DoS'.

[7 marks]
[7 markah]

- CLO2
C3 f) Illustrate and explain Man In The Middle attack in mobile computing.
Lukiskan dan terangkan serangan Man In The Middle didalam pengkomputeran mudah alih.

[7 marks]
[7 markah]

QUESTION 2**SOALAN 2**CLO2
C1

- a) List **TWO (2)** aspects of the mobile computing.

Senaraikan DUA (2) aspek pengkomputeran mudah alih..

[2 marks]
[2 markah]

CLO2
C2

- b) Explain the Three- Tier mobile architecture with the aid of a diagram.

Terangkan senibina Three-Tier dengan bantuan gambarajah.

[3 marks]
[3 markah]

CLO2
C2

- c) *A key part of any mobile phone specification is its operating frequency bands. The supported frequency bands determine whether a certain handset is compatible with a certain network carrier.*

Based on the statement above, explain **TWO (2)** of the wireless generation in Malaysia.

Berdasarkan pernyataan di atas, terangkan DUA (2) generasi tanpa wayar di Malaysia.

[3 marks]
[3 markah]

CLO2
C3

d) Illustrate the following wireless network topologies

Illustrasikan topologi rangkaian tanpa wayar berikut

i. Point to point connection.

[1 marks]
[1 markah]

ii. Star topology

[3 marks]
[3 markah]

iii. Mesh network.

[3 marks]
[3 markah]

CLO1
C1

e) Briefly describe the Global System for Mobile Communication (GSM).

Terangkan secara ringkas Global System for Mobile Communication (GSM).

[2 marks]
[2 markah]

CLO2
C2

f) Explain the meaning of “Jailbreak”.

Terangkan maksud "Jailbreak"

[3 marks]
[3 markah]

- CLO2 g) A new installed app was requesting a permission to access your mobile device's storage and information, describe what are the risks involve by allowing the app access and what are the countermeasure if a security attack happen on your mobile device?

Satu aplikasi yang baru dipasang sedang memohon kebenaran untuk memasuki sistem storan dan maklumat peralatan mudah alih anda, terangkan risiko-risiko yang terlibat dan apakah tindakan yang boleh diambil jika serangan keselamatan berlaku kepada peranti mudah alih anda?

[5 marks]
[5 markah]

- CLO2 h) Illustrate a Risk Model for Mobile ecosystem
Lukiskan Model Risiko untuk ekosistem mudah alih.

[5 marks]
[5 markah]

SOALAN TAMAT

