Second Semester Examination
2016/2017 Academic Session

June 2017

CST431 – Systems Security & Protection
[Keselamatan & Perlindungan Sistem]

Duration : 2 hours
[Masa : 2 jam]

INSTRUCTIONS TO CANDIDATE:
[ARAHAN KEPADA CALON:]

- Please ensure that this examination paper contains **FOUR** questions in **TEN** printed pages before you begin the examination.

  *[Sila pastikan bahawa kertas peperiksaan ini mengandungi **EMPAT** soalan di dalam **SEPULUH** muka surat yang bercetak sebelum anda memulakan peperiksaan ini.]*

- Answer **ALL** questions.

  *[Jawab **SEMUA** soalan.]*

- You may answer the questions either in English or in Bahasa Malaysia.

  [Anda dibenarkan menjawab soalan sama ada dalam bahasa Inggeris atau bahasa Malaysia.]

- In the event of any discrepancies, the English version shall be used.

  [Sekiranya terdapat sebarang percanggahan pada soalan peperiksaan, versi bahasa Inggeris hendaklah diguna pakai.]

1. (a) What are **tiga (3)** key objectives of computer security as specified in NIST handbook? Provide a detailed answer.

*Apakah **tiga** (**3**) objektif sekuriti komputer seperti yang dinyatakan dalam buku panduan NIST? Berikan jawapan terperinci.*

(10/100)

(b) Explain the following computer security terminologies.

Terangkan terminology-terminologi sekuriti komputer berikut.

(i) Attack

Serangan

(ii) Countermeasures

Langkah balas

(iii) Risk

Risiko

(iv) Threat

Ancaman

(v) Vulnerability

Kelemahan

(10/100)

(c) Anti-malware (formerly known as anti-virus) is used to detect and remove malware from your computer. Is anti-malware still relevant and effective in combatting malware? Please support your answer with examples.

Anti-malwer (sebelum ini dikenali sebagai anti-virus) digunakan untuk mengesan dan membuang malwer dari komputer anda. Adakah anti-malwer masih relevan dalam menangani masalah malwer? Sila sokong jawapan anda dengan contoh.

(10/100)

(d) Cryptography is the practice and study of techniques for secure communication in the presence of third parties.

Kriptografi adalah praktik dan kajian teknik-teknik untuk memastikan komunikasi selamat dalam persekitaran yang melibatkan pihak ketiga.

(i) What is the difference between symmetric and asymmetric (public) encryption?

Apakah perbezaan di antara penyulitan simetri dan tak-simetri?

(ii) How can these encryption method be attacked?

Bagaimanakah kaedah penyulitan ini diserang?

(20/100)

(e) Encryption protects against passive attack (eavesdropping). A different requirement is to protect against active attack (falsification of data and transactions), i.e. to verify if the message has been tampered with.

Penyulitan memberi perlindungan terhadap serangan (pasang telinga). Keperluan yang lain adalah memberi perlindungan terhadap serangan aktif (pemalsuan data dan transaksi), iaitu untuk menentusahkan bahawa mesej tersebut telah diusik.

(i) Diagrammatically show how message authentication using Message Authentication Code (MAC) is done.

Dengan menggunakan gambar rajah, tunjukkan bagaimana pengesahan mesej menggunakan "Message Authentication Code" (MAC) dilakukan.

(ii) Discuss a situation where MAC is required.

Bincangkan suatu situasi di mana MAC perlu digunakan.

(20/100)

(f) Consider the simple substitution cipher as shown below:

Pertimbangkan substitusi sifer mudah seperti berikut:

```
plain:   a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher:  c a k s y i b l t z p d m u h f n v e g o w r j q x
```

(i) Encrypt the text "**security is an important computer science domain**".

*Sulitkan teks "**security is an important computer science domain**".*

(ii) What is the resulting cipher text if the encryption is executed twice on the text specified in (f)(i)?

Apakah teks sifer yang terhasil sekiranya penyulitan tersebut dilakukan dua kali ke atas teks biasa yang dinyatakan dalam (f)(i)?

(iii) In your opinion, is this a good encryption method?

Dalam pandangan anda, adakah kaedah penyulitan ini baik?

(30/100)

2. (a) Explain the differences between block ciphers and stream ciphers.

Terangkan perbezaan-perbezaan di antara sifer blok dan sifer strim.

(10/100)

(b) List **three (3)** types of attacks that can be carried out on encrypted messages using cryptanalysis.

*Senaraikan **tiga (3)** jenis serangan yang boleh dilakukan ke atas mesej tersulit dengan menggunakan kripanalisis.*

(15/100)

(c) What is a one-way function?

Apa yang dimaksudkan dengan fungsi sehala?

(5/100)

(d) RSA Public-key Encryption was invented by Rivest, Shamir & Adleman of MIT in 1977 and is widely used public-key algorithm.

Penyulitan kekunci-awam RSA dicipta oleh Rivest, Shamir & Adleman dari MIT dalam tahun 1977 dan ianya merupakan algoritma kekunci-awam yang paling ketara digunakan.

(i) Write the RSA algorithm for encryption and decryption process.

Tuliskan algoritma RSA untuk proses penyulitan dan nyah-penyulitan.

(10/100)

(ii) The following are steps to generate public and private keys. Given the value p=17, q=11 and e=7, find out the private key, KR and public key, KU.

Key Generation

Select p,q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\Phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\Phi(n), e) = 1; 1 < e < \Phi(n)$
Calculate d	$de \bmod \Phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Berikut adalah langkah-langkah untuk menjana kekunci awam dan persendirian. Sekiranya diberikan bahawa nilai p=17, q=11 dan e=7, carikan kekunci persendirian, KR dan kekunci awam, KU.

Penjanaan kekunci

Pilih p,q	*p dan q adalah perdana, $p \neq q$*
Kirakan $n = p \times q$	
Kirakan $\Phi(n) = (p - 1)(q - 1)$	
Pilih integer e	*$\gcd(\Phi(n), e) = 1; 1 < e < \Phi(n)$*
Kirakan d	*$de \bmod \Phi(n) = 1$*
Kekunci awam	*$KU = \{e, n\}$*
Kekunci persendirian	*$KR = \{d, n\}$*

(30/100)

(e) Briefly describe DomainKeys identified Mail (DKIM).

Perihalkan secara ringkas DomainKeys identified Mail (DKIM).

(10/100)

(f) Secure Socket Layer is a general-purpose set of protocols; relies on TCP and is transparent to applications.

Secure Socket Layer merupakan set protokol untuk tujuan awam yang bergantung kepada TCP dan adalah telus kepada aplikasi.

(i) Draw the SSL protocol stack for HTTP.

Lukiskan tindanan protokol SSL untuk HTTP.

(ii) What is the role of heartbeat protocol in SSL?

Apakah peranan protokol "heartbeat" dalam SSL?

(15/100)

(g) What is the advantage of IPSec over SSL?

Apakah kelebihan IPSec berbanding dengan SSL?

(5/100)

3. (a) Services mentioned in X.800 are: confidentiality, integrity, availability, non-repudiation, authentication, access controls and accountability. Describe each services by using Healthcare domain as a senario.

Perkhidmatan-perkhidmatan yang disebut dalam X.800 adalah: kerahsiaan, integriti, ketersediaan, bukan penolakan, pengesahan, kawalan-kawalan capaian dan kebertanggungjawaban. Bagi setiap satu, terangkan fungsi piawaian tersebut untuk domain Penjagaan Kesihatan.

(35/100)

(b) Assume that Unsalted password scheme record had two fields in it: [user_email, Hash(password)]. A user login would be verified by looking up the appropriate record based on user_email, and then checking if the corresponding hashed password field matched the hash of the password input by the user trying to log in. By contrast, a salted scheme would have three fields: [user_email, salt, Hash(password+salt)] and login verification would similarly require looking up the salt and using it when matching hashes.

Bayangkan bahawa kata laluan Unsalted skim rekod mempunyai dua bidang di dalamnya: [user_email, Hash(password)]. Suatu login pengguna dapat disahkan dengan melihat sehingga rekod yang sesuai berdasarkan user_email, dan kemudian memeriksa jika cincangan sepadan medan kata laluan dipadankan dengan kata laluan dimasukkan oleh pengguna yang cuba untuk log masuk. Sebaliknya, satu skim yang menggunakan Salt mempunyai tiga bidang: [user_email, garam, Hash(kata laluan Salt)] dan pengesahan log masuk memerlukan Salt dipadankan dengan nilai cincangan.

(i) If the attacker's goal is to break *your* password via a dictionary attack, does the lack of salting in Unsalted scheme make this goal substantially easier?

Jika matlamat penyerang ialah memecahkan kata laluan anda melalui serangan kamus, adakah kekurangan "salting" dalam skim "Unsalted" menjadikan matlamat penyerang ini mudah dicapai?

(ii) If the attacker's goal is to break at least half of the passwords via a dictionary attack, does the lack of salting in Unsalted scheme make this goal substantially easier?

Jika matlamat penyerang ialah memecahkan sekurang-kurangnya separuh daripada kata laluan melalui serangan kamus, adakah kekurangan "salting" dalam skim "Unsalted" menjadikan matlamat penyerang ini mudah dicapai?

(iii) You are contacted by the attacker and given a set of password hashes (that's it, no user_name, no salt). By assuming the hash function is known, is there a measurement you could make in order to infer either the hashes are likely salted or not?

Anda dihubungi oleh seorang penyerang dan diberikan satu set kata laluan cincangan (yang ada, tiada user_name, tiada Salt). Dengan mengandaikan fungsi cincangan dikenali, apakah suatu ukuran yang anda boleh buat untuk membuat kesimpulan sama ada cincangan tersebut adalah nilai "Salt" atau bukan "Salt"?

(25/100)

(c) Key management is an important part of any cryptosystem. Key management may be achieved by using a trusted third party (TTP). Name and describe a method of key management that involves TTP.

Pengurusan kekunci boleh dilaksanakan dengan menggunakan khidmat pihak ketiga yang dipercayai (TTP). Nama dan terangkan suatu kaedah pengurusan kekunci yang melibatkan TTP.

(20/100)

(d) List **one** (**1**) soft biometrics and explain the process of enrollment, verification and identification of this biometrics.

*Senaraikan **satu** (**1**) biometrik lembut dan terangkan proses pendaftaran, pengesahan dan pengecaman biometrik ini.*

(20/100)

4. (a) In a University department, there is an administrator (Mr Alex), three lecturers (Dr Bob, Dr Clark and Dr Douglas) and a Head of Department (Prof Hendrik). Three documents concerning the department are **salary.doc**, **timetable.doc** and **marks.doc**. The Head of Department has permission to read all of the documents and has write access to **salary.doc**. The administrator has read and writes access to **timetable.doc** and read access to **salary.doc**. The lecturers each has read access to **timetable.doc** and write and read access to **marks.doc**. Information regarding the permissions each staff member has regarding the documents will be stored in an access control table indexed by subjects and objects.

*Di dalam sebuah jabatan Universiti, terdapat seorang pentadbir (Encik Alex), tiga orang pensyarah (Dr.Bob, Dr.Clark dan Dr.Douglas) dan seorang ketua Jabatan (Prof Hendrik). Terdapat tiga dokumen berkaitan dengan jabatan iaitu **gaji.doc**, **jadualwaktu.doc** dan **markah.doc**. Ketua jabatan mempunyai kebenaran untuk membaca semua dokumen dan akses menulis pada **gaji.doc**. Pentadbir mempunyai akses untuk membaca dan menulis **jadualwaktu.doc** dan membaca **gaji.doc**. Setiap pensyarah pula mempunyai akses baca pada **jadualwaktu.doc** dan tulis dan baca pada **markah.doc**. Maklumat mengenai kebenaran setiap ahli kakitangan mengenai dokumen-dokumen tersebut disimpan dalam satu jadual kawalan akses yang diindeks oleh subjek dan objek.*

(i) Represent the information given as a capability table.

Wakilkan maklumat yang diberi sebagai jadual keupayaan.

(ii) By employing Role Based Access Control(RBAC), illustrates the RBAC model.

Dengan menggunakan Capaian Berdasarkan Kawalan Peranan (RBAC), gambarkan model RBAC itu.

(20/100)

(b) Consider the following polices: Bell-LaPadula, Biba's low-water-mark policy, Clark-Wilson, Chinese Wall. Which of the listed policies would an organization be most likely to use if

Pertimbangkan polisi-polisi berikut: Bell-LaPadula, Biba's low-water-mark, Clark-Wilson dan Chinese Wall polisi. Yang manakah polisi-polisi disenaraikan mungkin akan diguna oleh sesebuah organisasi jika

(i) they maintain a source code repository, and want to make sure any source code that is modified by untrusted subjects is itself marked as untrusted.

mereka mengekalkan repositori kod sumber, dan mahu pastikan mana-mana kod sumber yang diubahsuai mengikut subjek yang tidak dipercayai itu sendiri ditanda sebagai tidak dipercayai.

(ii) they are a company that performs security audits of major corporations, and are worried about conflicts of interest when individual auditors they employ audit multiple corporations.

mereka adalah sebuah syarikat yang menjalankan audit keselamatan syarikat utama, dan bimbang mengenai konflik kepentingan apabila Juruaudit individu yang mereka ambil juga mengaudit berbilang syarikat.

(iii) they are a major retailer that wants to ensure the integrity of their data regarding stock, payments, customer credit, etc., and are particularly concerned about separation of duty and maintaining specific integrity properties such as “Customer account balance at the close of the business day is equal to the balance at the beginning of the day minus any payments and plus any interest”.

mereka adalah suatu peruncit utama yang ingin memastikan integriti data mereka mengenai saham, bayaran, kredit pelanggan, dan sebagainya, dan terutamanya bimbang tentang pembahagian tugas dan mengekalkan sifat-sifat integriti yang tertentu seperti "baki akaun pelanggan pada penutup hari perniagaan adalah sama dengan baki pada awal hari tolak sebarang bayaran dan sebarang faedah.

(30/100)

(c) Consider a system that used the Bell-LaPadula model to enforce confidentiality and the Biba model to enforce integrity.

Pertimbangkan satu sistem yang menggunakan model Bell-LaPadula bagi mengawal kerahsiaan dan model Biba untuk menguatkuasakan integriti.

(i) If the security classes were the same as integrity classes, what objects could a given process access (if some security class that also served as its integrity class)?

Jika kelas-kelas keselamatan adalah sama seperti kelas integriti, objek-objek apakah yang dapat dicapai (jika sebahagian kelas keselamatan berfungsi seperti kelas integriti)?

(ii) Why is this scheme not used in practice?

Mengapa skim ini tidak digunakan?

(20/100)

(d) (i) Explain how a replay attack may be performed on a Wi-Fi network and the mitigation of such attack using Trusted Third Party (TTP) server.

Terangkan bagaimana satu serangan ulang tayang dapat dilakukan di rangkaian Wi-Fi dan langkah mitigasi serangan tersebut dengan Pelayan Pihak Ketiga yang boleh dipercayai (TTP).

(ii) Read this excerpt from the news:

The program, Runescape Gold Hack, promised to give the gamer free virtual currency to use in the game - but it in fact was being used to steal log-in details from unsuspecting users. "When the researchers looked at the source code we found interesting information," explained Mr Ben-Itzhak to the BBC. "We found that the malware was trying to steal the data from people and send it to a specific email address."

Baca petikan ini dari berita:

Sebuah program, Runescape Gold Hack menjanjikan pemberian mata wang maya percuma kepada peminat permainan video untuk digunakan dalam permainan - tetapi ia sebenarnya digunakan untuk mencuri maklumat log masuk daripada pengguna yang tidak menyedarinya.' Apabila penyelidik melihat kod sumber tersebut kami mendapati maklumat yang menarik,' jelas Encik Ben-Itzhak kepada BBC. "Kami dapati bahawa malwer tersebut telah cuba mencuri data dari orang ramai dan menghantarnya ke alamat e-mel tertentu."

Describe the types of malware involved. Recommend effective measures to protect the user against this malware.

Jelaskan jenis malware terlibat. Cadangkan langkah-langkah yang berkesan untuk melindungi pengguna terhadap malware ini.

(20/100)

(e) (i) What is the aim of System Hardening?

Apakah matlamat Pengerasan Sistem?

(ii) Complexity of mobile operating system leads to security threats such as malware attack. List **three** (**3**) approaches to reduce operating system complexity in mobile architecture.

*Kerumitan sistem pengoperasian mudah alih membawa kepada ancaman keselamatan seperti serangan malwer. Senaraikan **tiga** (**3**) pendekatan untuk mengurangkan kerumitan sistem pengoperasian dalam seni bina mudah alih.*

(10/100)

- oooOooo -