UNIVERSITI SAINS MALAYSIA

Second Semester Examination
2015/2016 Academic Session

June 2016

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 **NINE** printed pages before you begin the examination.

  *[Sila pastikan bahawa kertas peperiksaan ini mengandungi **EMPAT** soalan di dalam **SEMBILAN** 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) (i) Feistel cipher is used in the DES algorithm. Describe the operation of a Feistel cipher.

Cifer Feistel digunakan untuk algoritma DES. Terangkan fungsi operasi cifer Feistel.

(10/100)

(ii) Briefly describe **two** (**2**) modes of operation of DES.

*Secara ringkas, terangkan **dua** (**2**) mod operasi bagi DES.*

(10/100)

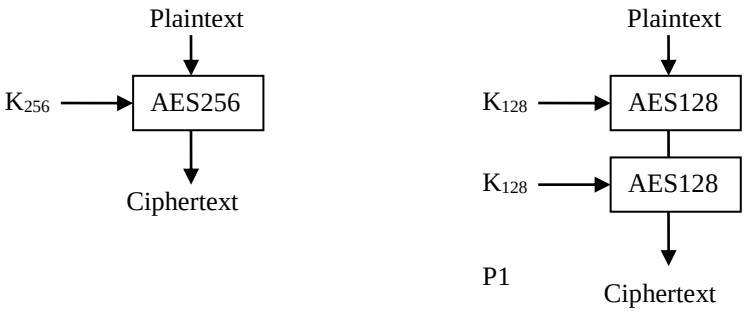
(iii) Explain why a stream cipher fails to protect message integrity.

Terangkan kenapa cifer strim gagal untuk memelihara integriti mesej.

(10/100)

(b) In the following diagram, K_{256} is the key with 256 bits length and K_{128} is a key with 128 bits length.

Berdasarkan diagram, K_{256} adalah kekunci 256 panjang bits dan K_{128} adalah kekunci 128 panjang bits.



(i) Which implementation of these two AES modes is more secure (or are they equally secure)? Justify your answer.

Di antara kedua-dua model AES ini; model manakah yang lebih selamat (atau mempunyai keselamatan yang setara)? Berikan justifikasi anda.

(20/100)

(ii) Explain the relationship between block size and key size in AES?

Jelaskan hubungan di antara saiz blok dan saiz kekunci pada AES?

(20/100)

(c) Describe how one can

Terangkan bagaimana seseorang boleh

(i) use a hash function to design a block cipher.

menggunakan fungsi cincang untuk mereka bentuk blok cifer.

(15/100)

(ii) use a block cipher to design a hash function.

menggunakan blok cifer untuk mereka bentuk fungsi cincang.

(15/100)

2. (a) In Diffie-Hellman protocol, what happens if Alice and Bob have accidentally chosen the same value for their private keys?

Untuk protokol Diffie-Hellman, apa akan terjadi jika Alice dan Bob secara tidak sengaja memiliki nilai kunci persendirian yang sama?

(20/100)

(b) Explain why asymmetric key system cannot be used in creating a MAC?

Jelaskan mengapa sistem kekunci tak asimetri tidak boleh digunakan untuk menjanakan MAC?

(20/100)

(c) In a public-key system using RSA, you intercept the ciphertext *C = 10* sent to a user whose public key is *e=5, n=35*. (**Hint:** Brute force attack)

*Di dalam sistem kunci-awam yang menggunakan RSA, anda memintas teks-sulit C = 10 yang dihantar kepada pengguna yang mempunyai kunci awam e=5, n=35. (**Petua:** serangan secara Brute force)*

(i) What is the user's private key?

Apakah kunci peribadi pengguna?

(10/100)

(ii) What is the plaintext?

Apakah teks nyata yang dihantar?

(10/100)

(d) Consider the following threats to Web security and describe how each is countered by a particular feature of SSL.

Pertimbangkan ancaman-ancaman berikut untuk keselamatan Sesawang dan terangkan bagaimana setiap ancaman dikendalikan dengan menggunakan ciri-ciri SSL.

(i) Man-in-the-middle attack: An attacker intervenes during key exchange, acting as the client to the server and as the server to the client.

Serangan orang di tengah: Penyerang menyerang semasa pertukaran kunci dilakukan, yang mana penyerang bertindak sebagai pelanggan untuk pelayan dan sebagai pelayan kepada pelanggan.

(10/100)

(ii) IP spoofing: Use forged IP addresses to fool a host into accepting bogus data.

Pemendayaan IP: Menggunakan alamat IP yang dipalsukan untuk menipu sesebuah hos agar menerima data palsu.

(10/100)

(iii) IP hijacking: An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts.

Perampasan IP: Sambungan aktif dan disahkan di antara dua hos terganggu dan penyerang mengambil tempat salah satu daripada hos tersebut.

(10/100)

(iv) SYN flooding: An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacked TCP module typically leaves the “half-open connection” around for a few minutes. Repeated SYN messages can clog the CP module.

Kebanjiran SYN: Penyerang menghantar mesej TCP SYN untuk meminta sambungan tetapi tidak bertindak balas kepada mesej terakhir untuk mewujudkan sambungan sepenuhnya. Modul TCP yang diserang biasanya meninggalkan bahagian "Sambungan setengah terbuka" sekitar untuk beberapa minit. Pengulangan mesej SYN boleh menyumbat modul TCP.

(10/100)

3. (a) There are three types of system security breaches – loss of integrity, loss of confidentiality, and loss of availability. Assume you have an internet banking account with a major local bank. For each of the following scenarios, identify the most accurate type of security breach encountered.

Terdapat tiga jenis pelanggaran keselamatan sistem – kehilangan integriti, kehilangan kerahsiaan, dan kehilangan ketersediaan. Anggap anda memiliki akaun bank internet dengan suatu bank tempatan yang terkemuka. Untuk setiap daripada scenario yang berikut, kenal pasti jenis pelanggaran keselamatan yang paling tepat untuk mensifatkan keadaan tersebut.

(i) You cannot login despite providing the correct username and password.

Anda tidak dapat log masuk sungguhpun memberikan nama pengguna dan kata laluan yang betul.

(4/100)

(ii) Another bank sends you a personal loan offer when your savings account balance reaches below RM5,000.00.

Suatu bank lain menghantar kepada anda tawaran pinjaman peribadi apabila baki akaun simpanan anda mencecah kurang daripada RM5,000.00.

(4/100)

(iii) You notice RM350.00 is missing from your account, with no trace of that amount in all the transactions.

Anda menyedari kehilangan RM300.00 daripada akaun anda, tanpa sebarang kesan yang mana jumlah itu dalam semua urus niaga.

(4/100)

(iv) You receive a call from a share market trader, urging you to buy shares in certain companies. When you ask him how he got your phone number, he says he got it from a bank employee.

Anda menerima panggilan dari seorang peniaga pasaran saham, mendesak anda membeli saham syarikat-syarikat tertentu. Apabila anda menanya beliau bagaimana dia memperoleh nombor telefon anda, dia kata dia mendapatkannya daripada seorang pekerja bank.

(4/100)

(v) Your home address in your account profile shows an address that you are not familiar with.

Alamat rumah anda di dalam profil akaun menunjukkan alamat yang anda tidak kenal.

(4/100)

(b) Both a Certificate Authority(CA) and a Key Distribution Centre such as in PKI and Kerberos respectively, are trusted entities that are needed for secure key exchange. Briefly explain the differences between the two in terms of scalability and trust.

Pihak Berkuasa Akuan dan Pusat Agihan Kekunci seperti mana yang terdapat pada implementasi PKI dan Kerberos, adalah entiti yang dipercayai untuk penukaran kekunci secara selamat. Jelaskan secara ringkas perbezaan di antara keduanya dari segi tahap skala dan kepercayaan.

(20/100)

(c) (i) Describe how a man-in-the-middle attack may be performed on a Wi-Fi network and the consequences of such an attack.

Huraikan bagaimana serangan orang-ditengah dapat dilancarkan di rangkaian Wi-Fi dan akibat dari serangan tersebut.

(20/100)

(ii) Explain how a man-in-the-middle attack on a Wi-Fi network can be defeated.

Terangkan bagaimana serangan orang-ditengah pada rangkaian Wi-Fi dapat ditewaskan.

(20/100)

(d) The inclusion of the salt value into the UNIX password scheme increases the difficulty of guessing by a factor equal to 2b, where b is the length of the salt in bits. But the salt is stored in plaintext in the same password file item as the corresponding cypher text password. Hence the salt string is known to the attacker and need not be guessed.

So why is it asserted that the salt increases system security?

Penggunaan nilai garam ke dalam skim kata laluan UNIX meningkatkan kerumitan untuk meneka sebanyak faktor 2b, di mana b adalah panjang garam dalam bit. Tetapi nilai salt ini disimpan secara teks biasa bersama item fail kata laluan bersama kata laluan teks capaian yang sepadan. Justeru itu nilai garam tidak perlu diteka dan boleh diketahui penyerang.

Jadi mengapa masih ditegaskan bahawa garam dapat meningkatkan keselamatan sistem?

(20/100)

4. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED (ordered from highest to lowest) and two categories: Nuclear and Army.

We consider four subjects:

- President has a TOP SECRET clearance for Nuclear and Army,
- Colonel has SECRET clearance for Army and Nuclear,
- Major has only CONFIDENTIAL clearance for Army, and
- Soldier has only UNCLASSIFIED clearance for Nuclear.

We also have some objects (documents):

- The army position at security level SECRET,
- The number of army units at security level CONFIDENTIAL,
- The number of nuclear units at security level CONFIDENTIAL,
- The costs of the nuclear program at security level UNCLASSIFIED,
- The costs of the army at security level UNCLASSIFIED, and
- The nuclear code at security level TOP SECRET.

Diberikan peringkat keselamatan iaitu RAHSIA PUNCAK, RAHSIA, SULIT dan UNCLASSIFIED (dikelas dari tertinggi ke terendah) dan terdapat dua kategori: Nuklear dan Tentera.

Kita akan mempertimbangkan empat subjek:

- *Presiden mempunyai pelepasan RAHSIA BESAR untuk Nuklear dan Tentera,*
- *Kolonel mempunyai pelepasan RAHSIA untuk Nuklear dan Tentera,*
- *Major mempunyai pelepasan SULIT untuk Tentera,*
- *Askar hanya mempunyai pelepasan TIDAK DIKELASKAN untuk Nuklear.*

Kita juga mempunyai objek (dokumen) seperti berikut:

- *Jawatan askar adalah pada peringkat keselamatan RAHSIA,*
- *Bilangan unit askar pada peringkat keselamatan SULIT,*
- *Bilangan unit nuclear pada peringkat keselamatan SULIT,*
- *Kos program nuclear pada peringkat keselamatan TIDAK DIKELASKAN,*
- *Kos askar pada peringkat keselamatan TIDAK DIKELASKAN dan*
- *Kod nuclear adalah pada peringkat keselamatan RAHSIA BESAR.*

(a) Based on the Bell-LaPadula and Biba security models; explain the difference between the two models.

Berdasarkan model keselamatan Bell-LaPadula dan BIBA; jelaskan perbezaan kedua-dua model tersebut.

(10/100)

(b) Answer the following questions based on the Bell-LaPadula model. Justify your answers.

Jawab soalan-soalan berikut berdasarkan model Bell-LaPadula. Justifikasikan jawapan anda.

(i) Can the President compute the overall defence costs (army + nuclear)?

Bolehkah Presiden mengira kos pertahanan keseluruhan (askar + nuklear)?

(ii) Can the Major compute the total number of nuclear and army units?

Bolehkah Major mengira number keseluruhan unit nuklear dan askar?

(iii) Can the Colonel compute the total number of nuclear and army units?

Bolehkah Kolonel mengira number keseluruhan unit nuklear dan askar?

(iv) Can the Colonel change the army position?

Bolehkah Kolonel mengubah jawatan askar?

(v) Can the Major change the nuclear code?

Bolehkah Major menukar kod nuklear?

(vi) Can the Soldier change the nuclear code?

Bolehkah Askar menukar kod nuklear?

(30/100)

(c) Does the answer obtained in 4(b)(vi) demonstrate the preservation of Integrity. Justify your answer.

Adakah jawapan yang diperoleh dari 4(b)(vi) menunjukkan pemeliharaan Integriti. Justifikasikan jawapan anda.

(10/100)

(d) In the NIST RBAC model, what is the difference between Static Separation of Duty (SSD) and Dynamic Separation of Duty (DSD)? Explain by using examples.

Dalam model NIST RBAC, berikan perbezaan di antara Pengagihan Tugas Statik (SSD) dan Pengagihan Tugas Dinamik (DSD)? Terangkan jawapan anda menggunakan contoh.

(20/100)

(e) (i) A system administrator needs to harden a server. List down **two** (**2**) steps in hardening the server.

*Seorang pentadbir sistem perlu memperkukuhkan sebuah pelayan. Senaraikan **dua** (**2**) langkah perkukuhan pelayan.*

(10/100)

(ii) Among the categories of viruses; boot sector and macro are two different types of viruses which infect the system boot files and applications that are embedded with macro functionality. Encrypting the executable files can protect software systems. When a program is invoked, the executable files are decrypted and executed. Consider an administrator has two possibilities to store the necessary cryptographic keys:

- The key is stored on a smart card held by an authorised employee with appropriate administrative rights.
- The key is stored in a tamper-resistant device that decrypts and executes commands.

Compare the security of these alternatives. How could an attacker bypass these controls?

Di antara kategori virus; dua jenis virus adalah boot sector dan makro yang masing-masing menyerang fail sistem boot dan aplikasi yang mempunyai fungsi makro. Penyulitan fail pelaksanaan dapat memelihara sistem perisian. Apabila sebuah program dimulai; fail pelaksana akan dinyahsulit dan dilaksana. Andaikan seorang pentadbir mempunyai dua kaedah menyimpan kekunci kriptografi berkenaan:

- *Kekunci disimpan pada kad pintar yang dipunyai oleh seorang pekerja yang mempunyai hak dan kuasa tertentu.*
- *Kekunci disimpan pada alat kalis-ubah yang boleh menyahsulit dan melaksanakan arahan.*

Bandingkan ciri keselamatan bagi kaedah ini. Bagaimana seorang penyerang melangkaui ciri keselamatan ini?

(20/100)