UNIVERSITI SAINS MALAYSIA

Second Semester Examination
2010/2011 Academic Session

April/May 2011

CST431/CST335 – 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) Assume you have just opened an account with a local bank. The bank issues you an ATM (automated teller machine) card with a secret pin number, so that you can deposit and withdraw cash from any of the bank's teller machines.

(i) Explain **one** (**1**) possible vulnerability of this system.

(ii) Explain **one** (**1**) possible threat to this system.

(iii) Explain **one** (**1**) potential risk using this system.

(iv) What possible counter measure you can take to safeguard your assets? Explain your answer.

(v) What possible counter measure the bank can take to safeguard your assets? Explain your answer.

(10/100)

(b) The following table, *Students*, shows details about students taking various programs, number of units completed and their average marks. Statistical queries (i.e. COUNT, SUM, AVG, MAX, MIN) are allowed on all attributes, but individual entries in Units Completed and Average Marks columns cannot be read directly.

Name	Sex	Program	Units Completed	Average Marks
Alice	F	MBA	8	63
Bill	M	CS	15	58
Cindy	F	CS	16	70
David	M	MIS	22	75
Eric	M	CS	8	66
Fiona	F	MIS	16	81
Gloria	F	MBA	23	68
Henry	M	CS	7	50
Isaac	M	MIS	21	70

(i) Using statistical queries, write SQL statement(s) to obtain Cindy's average marks. Assume there is no query restriction.

(ii) If query restriction is set at k=3, what does it mean?

(iii) With query restriction set at k=3, can Cindy's average marks be obtained? If yes, write SQL statements how this can be done. If not, explain why.

(10/100)

(c) If a worm has already infected a few computers in an organization, what steps can be taken to reduce its spread to other computers in the organization's intranet as well as the internet?

(5/100)

2. (a) Briefly describe how the following techniques can be used to protect programs against buffer overflow attacks.

(i) Random canary.

(ii) Guard pages.

(10/100)

(b) Validating input is one of the essentials of writing a secure program.

(i) What aspects of input should be checked by the programmer? Briefly describe.

(ii) Besides buffer overflow, what else can bad input do to a program? Use an example to explain your answer.

(10/100)

(c) Assume you want to permanently and securely delete a file on your hard disk, so that its contents are no longer recoverable. A friend has given you the following pseudocode for a secure file delete application. Will the application code work as intended? Briefly explain your reasons.

```
Patterns = [ 10101010, 01010101, 11001100, 00110011, 00000000, 11111111 ]
Open file for update
For each pattern
    Go to start of file
    Overwrite file contents with pattern
Close file
Remove file
```

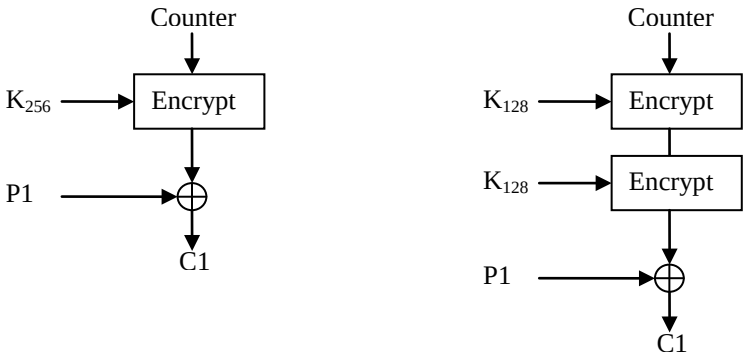
(5/100)

3. (a) Based on the given diagram:

(i) Which implementations of the counter modes are more secure?

(ii) Justify your answer.

(**Note**: K_{256} is the key with 256 bit length and K_{128} is a key with 128 bit length).



(7/100)

(b) A crypto-system based on RC4 has been using the same key, *k*, for some time. Assume you intercept C_1, which you know the corresponding plaintext is P_1. Describe how you can use this information to masquerade as the sender when communicating to the recipient.

(4/100)

(c) In RSA public-key encryption/decryption scheme, each user has a public-key, *e*, and private-key, *d*. Suppose Bob leaks his public-key. Rather than generating a new *n*, he decides to generate a new *e'* and *d'* based on his old *n*. Is this safe? Justify your answer.

(7/100)

(d) In Secure Socket Layer (SSL) protocol:

(i) Is the session key chosen by a client or server?

(ii) How is it communicated to the other party?

Use diagram in your explanation.

(7/100)

4. (a) Trusted entities such as CA in PKI and Kerberos in KDC require secure key exchange protocol. Briefly explain the differences between the two in terms of scalability and trust.

(5/100)

(b) Answer the following questions on IDS:

(i) List and briefly define three classes of intruders.

(ii) What are the three benefits that can be provided by IDS?

(iii) Describe the differences between a host-based IDS and a network-based IDS.

(iv) Describe the types of sensors that can be used in a NIDS.

(v) What is a honeypot?

(5/100)

(c) Firewalls protect the internal network from attacks that are coming from the outside network.

(i) Can firewalls protect against virus infections (consider the different types of firewalls in your answer)?

(ii) How does cryptographic protection at the TCP/IP layer or at the application layer affect a firewall's ability to protect against viruses?

(10/100)

(d) USM allows its students to use laptops at schools as well as when they are not within the wireless parameter of the university. Based on the above scenario, propose a security architecture to protect the university's intranet.

(5/100)

1. (a) Anggap anda baru membuka akaun dengan suatu bank tempatan. Bank itu mengeluarkan suatu kad ATM dengan nombor pin rahsia, supaya anda boleh menyimpan dan mengeluarkan wang daripada mana-mana mesin ATM bank itu.

(i) Jelaskan **satu** (**1**) kelemahan yang mungkin bagi sistem ini.

(ii) Jelaskan **satu** (**1**) ancaman yang mungkin bagi sistem ini.

(iii) Jelaskan **satu** (**1**) risiko yang mungkin menggunakan sistem ini.

(iv) Apa langkah balas yang anda boleh ambil untuk melindungi aset anda? Jelaskan jawapan anda.

(v) Apa langkah balas yang boleh diambil oleh bank untuk melindungi aset anda? Jelaskan jawapan anda.

(10/100)

(b) Jadual berikut, *Pelajar*, menunjukkan maklumat mengenai pelajar yang mengikuti pelbagai program, bilangan unit terkumpul dan purata markah mereka. Pertanyaan statistik (contoh: BILANGAN, JUMLAH, PURATA, MAKS, MIN) dibenarkan ke atas semua atribut, tetapi kemasukan inidividu untuk lajur Unit Terkumpul dan Purata Markah tidak boleh dibaca secara terus.

Nama	Jantina	Program	Unit Terkumpul	Purata Markah
Alice	P	MBA	8	63
Bill	L	CS	15	58
Cindy	P	CS	16	70
David	L	MIS	22	75
Eric	L	CS	8	66
Fiona	P	MIS	16	81
Gloria	P	MBA	23	68
Henry	L	CS	7	50
Isaac	L	MIS	21	70

(i) Dengan menggunakan pertanyaan statistik, tulis pernyataan SQL untuk memperolehi purata markah Cindy. Anggap tiada sekatan pertanyaan.

(ii) Jika sekatan pertanyaan ditetapkan pada k=3, apakah maknanya?

(iii) Dengan sekatan pertanyaan ditetapkan pada k=3, bolehkah purata markah Cindy diperolehi? Jika ya, tulis pernyataan SQL yang menunjukkan cara ia boleh dilakukan. Jika tidak, terangkan kenapa.

(10/100)

(c) Jika suatu cecacing telah menjangkiti beberapa komputer dalam suatu organisasi, apakah langkah-langkah yang boleh diambil untuk mengurangkan penyebarannya ke komputer lain dalam intranet organisasi itu serta internet?

(5/100)

2. (a) Terangkan secara ringkas cara teknik-teknik berikut boleh digunakan untuk melindungi atur cara daripada serangan limpahan penimbal.

(ii) Kenari rawak.

(ii) Halaman pengawal.

(10/100)

(b) Mengesahkan input merupakan salah satu keperluan penting untuk menulis atur cara terjamin.

(i) Dari segi apakah input harus diperiksa oleh juru atur cara? Jelaskan secara ringkas.

(ii) Di samping limpahan penimbal, apa lagikah yang boleh dilakukan oleh input buruk terhadap sesuatu atur cara? Gunakan contoh untuk menerangkan jawapan anda.

(10/100)

(c) Anggap anda ingin menghapuskan secara kekal dan terjamin suatu fail daripada cakera keras, supaya kandungannya tidak boleh didapatkan kembali. Seorang rakan telah memberikan anda pseudokod berikut bagi atur cara penghapusan fail terjamin. Boleh kod atur cara ini berfungsi seperti dikehendaki? Terangkan secara ringkas alasan anda.

```
Corak = [ 10101010, 01010101, 11001100, 00110011, 00000000, 11111111 ]
Buka fail untuk kemaskini
Bagi setiap corak
    Pergi ke pangkal fail
    Tulis semula kandungan fail dengan corak
Tutup fail
Hapus fail
```

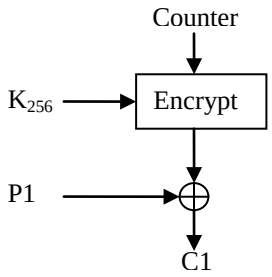
(5/100)

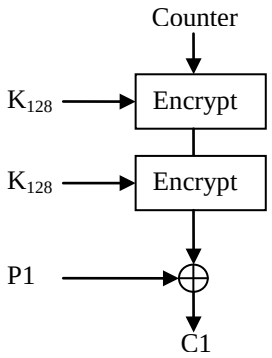
3. (a) Berdasarkan gambar rajah yang diberi:

(i) Implimentasi ‘counter mode’ yang manakah lebih selamat?

(ii) Jelaskan jawapan anda.

(**Nota**: K_{256} adalah kekunci 256 bit dan K_{128} adalah kekunci 128 bit).





(7/100)

(b) Satu sistem kripto berasaskan RC4 telah mengunakan kekunci yang sama, *k*, untuk beberapa ketika. Anggapkan anda telah dapat C_1 yang mana anda tahu P_1 adalah teks aslinya. Terangkan bagaimana anda boleh mengunakan maklumat ini untuk menyamar sebagai penghantar bila berkomunikasi dengan penerima.

(4/100)

(c) Pada skema enkripsi/dekripsi kekunci-awam RSA, setiap pengguna mempunyai kekunci awam, *e*, dan kekunci persendirian, *d*. Katakan kekunci persendirian Bob telah diketahui umum. Oleh kerana tidak mahu menjana *n* yang baru, dia mengambil kepututsan untuk menjana *e'* dan *d'* yang baru berdasarkan nilai *n* yang lama. Adakah proses ini selamat? Jelaskan jawapan anda.

(7/100)

(d) Untuk protokol *Secure Socket Layer* (SSL):

(i) Adakah kunci sesi dipilih oleh pengguna atau pelayan?

(ii) Bagaimana kunci ini dihantar kepada parti yang satu lagi?

Gunakan gambar rajah dalam penjelasan anda.

(7/100)

4. (a) Entiti-boleh-percaya seperti CA dalam PKI dan KDC dalam Kerbero memerlukan protokol penukaran kunci selamat. Jelaskan secara ringkas perbezaan di antara keduanya dari segi tahap kepercayaan dan skala.

(5/100)

(b) Jawab soalan-soalan *IDS* yang berikut:

(i) Senarai dan beri pengertian ringkas tiga kelas penceroboh.

(ii) Apakah tiga faedah yang dapat diberikan oleh *IDS*?

(iii) Jelaskan perbezaan di antara *host-based IDS* dan *network-based IDS*.

(iv) Terangkan jenis alat-deria (*sensors*) yang boleh digunakan oleh *NIDS*.

(v) Apa itu *honeypot*?

(5/100)

(c) Aplikasi keselamatan tembok-api melindungi rangkaian dalaman daripada serangan yang datang daripada rangkaian luar.

(i) Bolehkah aplikasi keselamatan pintu-api melindungi rangkaian dalaman daripada jangkitan virus? (fikirkan kepelbagaian jenis aplikasi keselamatan pintu-api dalam jawapan anda)?

(ii) Bagaimana perlindungan kriptografi pada lapisan TCP/IP atau lapisan aplikasi mempengaruhi kecekapan aplikasi keselamantan pintu-api melindungi serangan virus?

(10/100)

(d) USM membenarkan pelajar-pelajarnya menggunakan komputer riba di pusat pengajian dan juga apabila mereka tidak berada di dalam lingkaran tanpa wayar universiti. Berasaskan daripada senario di atas, cadangkan satu senibina keselamatan untuk mengawal intranet universiti.

(5/100)