Maharishi University of Management
Computer Science Graduate Examination
Course: CS

Dear Sandy Lonnqvist*:

Re: Rabindra Shrestha, Student ID No. 000-98-2971
Enclosed: Midterm exam materials (2 pages of exam materials and 10 pages of blank paper)

Exam administered on June 2, 2012, from **12:00PM - 2:00PM. Student may not begin earlier and may not end at a later time!**

Begin promptly **Start Time:** 12:00 pm
Collect promptly **End Time:** 2:00 pm

Please observe the following protocols:

1. Confirm the photo ID matches the student Rabindra Shrestha and initial upper right-hand corner of this page.
2. Monitor each student for the duration of the exam.
3. Collect cell phones, all other electronics, and personal items.
4. Prohibit all blank paper other than that provided in the exam packet.
5. Prohibit all books and notes (all exams are closed-book unless otherwise indicated).
6. No student may not leave the test area during the specified exam times for any reason (no bathroom or other personal breaks).
7. All exams are copyrighted and may not be further copied, viewed, or distributed.
8. Document any suspicious behavior and report to the MUM DE office.
9. Total test time is 2 hours, no exceptions.
10. Return the attendance verification today, by fax or email.

Proctor Comments (optional): _____

Proctor's Name (printed): Sandy Lönngvist
Proctor's Signature: Sandy Lönngvist
Date: 06/02/12

Return the entire exam including this sheet in the enclosed self-addressed, stamped envelope or Federal Express envelope. The envelope must be mailed by your institution; **students may not mail their own exams**. Please return all exams including those not taken.

Contact information for Rabindra is 515-999-0195. Please direct proctoring fees to the student.

Thank you for making this test possible for Rabindra. Contact me with questions regarding exam instructions.

Biran Saine
Distance Education Coordinator
Phone: (641) 472-7000 Ext. 5120
Fax: (641) 472-1182
csde@mum.edu

Maharishi University of Management
Engaging the Managing Intelligence of Nature
Computer Science Department

CS 466 DE: Introduction to Computer Security

Mid Term Exam: 02-June-2012

Instructor Name : Mrudula Mukadam

Answer all the 14 questions and clearly assign correct question number to your answers. I have assigned a score to every question in square brackets at the beginning of each question.
Please write down your name and student ID on each paper of the answer sheet.
No personal items are permitted in the exam room including electronic devices, computers, calculators, cell phones, and PDAs.

Total test time: 2 hrs **Total Points: 105** **Closed book/ Closed Notes**

(1) [12] Answer the following questions about digital signatures.

- **a.** [5] What is a digital signature?
- **b.** [7] Let m be a message. Suppose Alice and Bob share a secret key k. Alice sends bob m||{m}k (i.e. the message and it's encipherment under k). Is this a digital signature? Why or why not? Explain your answer.

(2) [11] Answer the following questions about Kereberos protocol.

- **a.** [6] Describe briefly the roles of the 3 different servers used in Kereberos.
- **b.** [5] What is a potential problem of the Kereberos protocol?

(3) [9] Policy restricts the use of e-mail on a particular system to faculty and staff. Students cannot send or receive e-mail on that host. Classify the following mechanisms as secure, precise, or broad and briefly justify your answer.

- **a.** [3] The e-mail sending and receiving programs are disabled.
- **b.** [3] As each letter is sent or received, the system looks up the sender (or recipient) in a database. If that party is listed as faculty or staff, the mail is processed. Otherwise, it is rejected. (Assume that the database entries are correct.)
- **c.** [3] The e-mail sending programs ask the user if he or she is a student. If so, the mail is refused. The e-mail receiving programs are disabled.

(4) [9] In Bell-LaPadula model, the security levels are TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories are A, B, and C. Specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Also briefly explain your answer. Assume that discretionary access controls allow anyone access unless otherwise specified.

- **a.** [3] Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, {B}).
- **b.** [3] Paul, cleared for (TOP SECRET, {A, C}), wants to access a document classified (SECRET, {B, C}).
- **c.** [3] Sammi, cleared for (TOP SECRET, {A, C}), wants to access a document classified (CONFIDENTIAL, {A}).

(5) [9] Briefly explain any 3 advantages of CAs (Certification Authorities) over KDCs (Key Distribution Center).

(6) [8] Let's say that I can control some process by sending a "stop" or "start" message to a server. The fact that I am starting or stopping the process is not a secret, so I don't have to encrypt the "start" or "stop" message. But it is important that I am the only person who can stop or start the process. Therefore, I digitally sign the "stop" or "start" message with my private key. The server then decrypts the hash with my public key to make sure that I was the one who sent the message. Briefly describe what is wrong with this protocol.

(7) [8] Considering role of trust, sometimes a "back-door" is purposefully used through which the security mechanism can be bypassed. The trust resides in the belief that this back door will not be used except as specified by the policy.
Based on your experience as an IT professional, briefly describe a situation in which planting a back door would be needed & explain how it could be used and misused.

(8) [6] Please give an example of a trade-off between the principle of psychological acceptibility and the principle of least privilege.

(9) [6] Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file Alicerc, and Bob and Cyndy can read it. Cyndy can read and write the file Bobrc, which Bob owns, but Alice can only read it. Only Cyndy can read and write the file Cyndyrc, which she owns. Assume that the owner of each of these files can execute it.
Create the corresponding access control matrix.

(10) [6] Briefly explain how Clark-Wilson integrity model supports the principle of separation of duty.

(11) [6] Differenciate between a known plaintext attack and a chosen plaintext attack.

(12) [6] We've learnt 12 design principles in this course till now. Please relate 2 of them to the SCI principles that we've studied.
[Hint: Principle of complete mediation – Infinity at a point]

(13) [5] Bob's password is "flower", but one day by accident he discovers that the password "blowfish" also works. This is a complete mystery to him because he has never used "blowfish" as a password. Please give an explanation for this behavior. The following answers are not acceptable.

A. "there is a bug in the program"
B. " 'blowfish' was a backdoor planted by the vendor"
C. "Bob added 'blowfish' but forgot about it"

(14) [4] What is the cipher text for word "SECURITY" using a rail-fence cipher with a key of 3?

Dear Student:

Reminder of procedures governing this exam: You must read and sign this letter. Submit to your proctor with the completed exam.

Each student is required to comply with the following protocols:

1. You must present a photo ID with your name.
2. You must leave all personal items outside of the test room, including cell phones, laptop computers, and books and notes. The only personal items you may bring are writing implements and erasers.
3. You may not bring any paper, blank or otherwise or books.
4. You may not leave the exam room during the exam for bathroom or personal breaks.
5. All exams are copyrighted. Any attempt to view, copy, or distribute the exam beyond the scope of your exam laws is a violation of copyright law and subject to legal penalty.
6. You must begin and end the exam at the predetermined times and you may not exceed the total test time of 2 hours.

Any violation of the above procedures will result in a grade of No Credit for the exam.

Student's Name (printed): Rabindra Shrestha

Student's Signature: Rabindra

Date: 05-06-2012

Midterm Exam CS (April 2012 Term) June 2, 2012

Student Name_____

Student ID_____

Ans to (a) Digital signature :- (Private key encryption and broadcast)

In Asymmetric encryption technique subject encrypts plaintext with public key of object and send to object. The object decrypt cipher text using own private key. To protect possibility of decryption from intruder, sender encrypts the message with his private key for reciever to match validity of encryption. This technique of associating subject's private key in message is known as digital signature

Alice → Bob : $m \| \{m\}_K$

$m \| \{m\}_{K_{Alice}}^{-} \| K_{Bob}^{+} \Rightarrow$ Digital signature

(b) Alice → Bob : $m \| \{m\}_K$

→ Above message is not associated with Digital signature

— for it, Alice should put his private key with message or cipher text to Bob. So that Bob used his Private key to decypher and matched Alice Public associated with message for validity & Reliability of received message.

So, Digital signature message should like

Alice → Bob : $m \| \{m, K_{Alice}^{-}\}_{K_{Bob}^{+}}$

Ans to Q^n 2

Kereberos Prototocal :-

- It is improvement "Denning - .... " protocol of integrity [illegible].
- improved over Authorization process with third party Key Distribution ~~server~~ center (KDC).
- 3 Servers are used in authorization communication betn 2 parties. Say Alice and Bob.
- 3 Servers
  - (a) Authorization server
  - (b) Ticket granting server
  - (c) Key distribution server

(a) Authorization server :- it authorized the client say Alice
$T_A = \{ [illegible] \, T \, R_1 \}_K$

(b) Ticket granting server :- once authorized, they issue Ticket which is used in second party to get public key of [illegible] [illegible] as
$T_{A,B} = \{ [illegible], T_A \}_{K_1}$

(c) Key distribution server :-

once decrypted [illegible] from Alice, Bob's connects with key distribution server with that Ticket to get public key of Alice in decrypting the original message.

Midterm Exam CS (April 2012 Term) June 2, 2012

Student Name_____

Student ID_____

(2) (b) potential problem :-

- the server need to online to provide service all time
- Introducer can harm the message communication if pattern of Third party key ~~Part~~ generation ~~can be~~, ticket authentication comes to know.

Ans to qn (3)

(a) It is kind of Broad. As the system is disabled for student, then it is not kind of security implementation For precise, the system should check if the operation is allowed

(b) Secure :- operation checks whether it is valid (~~Service~~ Policy defined) operation or not.

(c) Freeze :- As from origin of operation checks the validity of operation

Ans to qn 4 :-

Bell - LaPadula model deals with confidentiality of data. So it checks clearance of security with security level of object.

(a) None of access granted for Robin.

To read access,
iff $l(o) <= l(s)$ and s has discretionary access [illegible].

Here, it doesn't matched the condition

(b) Read access for Paul here.

as Paul clearance >= required clearance level and ~~Secure~~ for A and C. But Document clearance level is [illegible] with B and C. So, due to integrity issue with B, only read access for [illegible] [illegible] here.

(c) [illegible] [illegible] [illegible] [illegible] to Sam.

As Top Secret clearance with A, C and ~~want~~ can have write access with confidential / with A here

Midterm Exam CS (April 2012 Term) June 2, 2012

Student Name_____

Student ID_____

Ans to qn 5

(1) no need to online. CA issues certificate to client and they use that certificate to receiver. But in KDC, client would request key then receiver need to get sender's public key. So all of time need to online

(2) Out of failure operation; it no need to be online. No failure of system due to unavailability of KDC.

(3) As CA uses identity of user. It is portable. Can be placed in floppy device to validate authentication. But key for KDC only applicable with two interacting parties.

Ans to qn (6):-

With digital signature, message can be make secure. But in this scenario, to protect unauthorized access, there should be implement authentication control over system with access control. For this, System have to maintain access control level with role per user with secure login system. For secure login system digital signature can be used to transfer message as secured. Then only it will be applicable to make secure with Stop and Start message to command system.

Ans to. no 7

Yes, implementing back-door ~~in~~ with application ~~to~~ purposefully violates trust worthy with vendor. ~~to~~ Some code ~~of~~ may required also. If there is less security ~~but~~ vulnerability. Such as for configuring ~~init~~ initial setup of application which need to configure from its own internal system. So at initial, to create user credential also. It may needed.

2nd ly, to make recover / access of hacked modified or ~~lost~~ login and ~~to~~ locked the system. Or that code is may provided. But if a IT professional, ~~he~~ never ~~is~~ ~~pursued~~ to create back door ~~in~~ system due to following reason.

— it ~~may~~ lose Trust with vendor

— Risk of attacks from back door as well

— Who develops the system ~~or~~ they ~~started~~ ~~to load~~ may misuse it ~~for~~ for personal benefit or may bargain with vendor or own employee.

— Finally, it violates overall security of the system. Which can be achieved from proper implementation not using back door.

Midterm Exam CS (April 2012 Term) June 2, 2012

Student Name_____

Student ID_____

Ans qn 9

Subject = { Alice, Bob, Cyndy }

Object = { Alicerc, Bobrc, Cyndyrc }

R = { own, read, write, execute }

	Alicerc	Bobrc	Cyndyrc
Alice	own, execute	read	
Bob	read	own, execute	
Cyndy	read	read, write	read, write, execute

Ans for qn (5)

Clark - wilson integrity model that supports the principle of seperation of duty.

In Clark - wilson integrity model deals of integrity of data. And Subject can write to file of and only if i(O) <= i(S). So, Subject can write to object with higher premilage. In principle of seperate duty, the operation is carried out one subject and its object which make possible of seperation of duty. For example,

- Developer develope application in development environment that Developer has 4 privilage
- Deployer deploys application from development env to Production environment. i.e. Suppose in clark - wilson I write

Ans to qn (11)

- Known plaintext attacks is where access to the confidential information which is in form of plain text. For example; Sql injection. ~~Send~~ based on basis of username say 'Bob', try to attack with infected password like ['' or 1 = 1]. Similarly, hit and trial of common credential information.

- Chosen plaintext attacks is where access over confidential information by means of plain text. ~~with~~ and it's some standard encryption format. for example; Dictionary attack. Using set of possible combination of credential, it tries to encrypt in similar encryption and try to match of ~~with~~ actual encrypting and one match ~~it~~ then that credential ~~is~~ will be known.

Midterm Exam CS (April 2012 Term) June 2, 2012

Student Name____

Student ID____

Ans to qn 12

1. Certificate Authority (CA) implementation for secure communication can be relation with SCI's Rishi, Chandas, Devata i.e Knower, Known and Knowing.

SSL uses CA as third party to verify authorized user who knows the information (Devta) and client is knower as Chandas who will get information and vendor who is as Known who had information.

2. Principle of separation of duty -

At the level of consciousness everyone can feel own potentiality and perform as he/she has best caliber to higher [illegible] field which will create best outcome for every individual and recognized as his/her caliber and trust by society. Similarly, principle of separation of duty provides clear security clearance on integrity of information that provides trustworthy to clients.

Midterm Exam CS (April 2012 Term) June 2, 2012

Student Name_____

Student ID_____

Ans to. qn 13

(1) In this case, the system may be lack of implementation with unique user name. So, there might be another user with same user name but password is 'blowfish'. And system just checks is password is available with user name is bob or not. And there is not any implementation of permutation of system after successful login.

(2) Next issue may be the password encryption is not properly implemented.

Suppose

e("flower") = e("blowfish").

i.e. wrong proper implementation logic in e() => exception missed

Ans to. qn 14

rail-fence cipher :- k=3

C("SECURITY") -

↑

k=3

= C R

= "CURITYSE

Midterm Exam CS (April 2012 Term) June 2, 2012

Student Name_____

Student ID_____

Ans to qn 8

Trade-off betn the principle of psychological acceptability and principle of least privilege.

- If the privilege is less than acceptable, then someone cannot operate that kind of operation. for example, if only read permission than cannot write. But principle of psychological acceptability, if someone can write privilege, then he/she can read also.

But principle of psychological acceptability is not always valid with respect to Least Privilege

for example,

Top secrete may not allow to read some one read secret information (confidentiality) But not write or modify information.

— Jaji Guru Das