Maharishi University of Management
Computer Science Graduate Examination
Course: CS

Dear Ashley Crisp:

Re: Abdulghani Alshberi, Student ID No. 000-98-3129
Enclosed: Final exam materials (2 pages of exam materials and 10 pages of blank paper)

Exam administered on July 21, 2012, from **11:00AM - 1:00PM. Student may not begin earlier and may not end at a later time!**

Begin promptly **Start Time:** 11am
Collect promptly **End Time:** 1pm

Please observe the following protocols:

1. Confirm the photo ID matches the student Abdulghani Alshberi 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): Ashley Crisp
Proctor's Signature: Ashley Crisp
Date: 7/21/12

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 Abdulghani is . Please direct proctoring fees to the student.

Thank you for making this test possible for Abdulghani. 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

11am
1pm

Patient Care
Medical Unit
7125 Ps

Maharishi University of Management

Engaging the Managing Intelligence of Nature

Computer Science Department

CS 466 DE: Introduction to Computer Security

Final Exam - July 21, 2012

Instructor Name : Mrudula Mukadam

Please answer all the 11 questions. 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. Clearly assign the question number to your answer.
No personal items are permitted in the exam room including electronic devices, computers, calculators, cell phones, and PDAs. No additional papers are allowed, blank sheets are included in the exam packet. The complete exam including the questions and the scratch papers must be returned to the proctor.

Total test time: 2 hrs **Total Points: 120** **Closed book/ Closed Notes**

(1) [22] Answer the following questions in regards to malicious logic.

(A) [8] What is the difference between Logic bombs and Bacteria? Explain with an example.

(B) [10] One of the ways to defend against a computer virus is to distinguish between data & instructions. Explain how this protection mechanism helps to prevent a virus spread.

(C) [4] Which of these types of malicious logic are designed to avoid detection by a virus detection program?

a) TSR viruses
b) encrypted viruses
c) trojan horses
d) boot sector infectors
e) polymorphic viruses

(2) [20] Answer the following questions related to Intrusion Detection Systems (IDS).

(A) [4] What are the 2 desirable characteristics of an IDS?

(B) [12] One view of IDSs is that they should be of value to an analyst trying to disprove that an intrusion has taken place. Consider the following scenario.
A system has classified and unclassified documents in it. An employee is accused of using a word processing program during the last month to secretly save copies of classified documents. Discuss, if and how, each of the three forms of intrusion detection mechanisms (Anomaly, Misuse, and Specification) could be used to argue against this accusation.

(C) [4] Security guards at a professional soccer match notice that two men are climbing over the fence; the security guards detain these men. Which intrusion detection model is being used here? Support your answer with brief explanation.

(3) [20] Answer the following questions related to vulnerability analysis.

(A) [12] Briefly explain the 4 steps in the flaw hypothesis methodology.

(B) [8] What are the goals of penetration testing and how does this compare with the goals of formal verification?

(4) [10] Consider the following scenarios in the Drib corporation. You need to write down the design principle that is the most applicable one for that scenario.

(A) [2] Users are classified into four classes. Moving information from one class to another requires approval of more than one user.

(B) [2] Each server has the minimum knowledge of the network necessary to perform its task.

(C) [2] In the Drib corporation, the four servers in the DMZ zone are all on separate computers.

(D) [2] The use of write-once media in the log server. (Deny all modifications to write-once media)

(E) [2] Configuration of firewalls should be simple so that administrators will feel comfortable doing it.

(5) [9] Briefly explain any 3 of your favorite SCI points that you've learned in this course so far.

(6) [6] What do you mean by a distinguished name? How will it look like for a person named Jack Davis who works at IBM in a Quality Assurance dept?

(7) [5] Is cryptography used in the Drib system for integrity, confidentiality, or both? Briefly justify your answer.

(8) [4] Explain in short the difference between authentication and authorization.

(9) [2] In the Dribble corporation, the IP address of outer firewall is x, that of the DMZ web server is y and that of the DMZ DNS server is z. Which of these IP addresses are known to the external Internet users?

(10) [2] Which statistical model is likely to be used to detect someone guessing passwords?

(11) [20] State true or false for the following questions. Also briefly justify your answer. No points for simply guessing the answer without any justification.

(A) [4] A manipulation detection code is based on timestamps.

(B) [4] The access control policy that is implemented in the internal Drib network is originator controlled.

(C) [4] Vulnerability of a system increases when threats are high.

(D) [4] Security logging is the analysis of log records to present information about the system in a clear and understandable manner.

(E) [4] A programming language has no affect on whether or not a program is vulnerable to a buffer overflow attack.

Jai Guru Dev

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): ABDULGHANI ALSHBERI

Student's Signature: _____

Date: July 21, 2012

Final Exam CS (April 2012 Term) July 21, 2012

Student Name Abdulghani Alshberi

Student ID 983129

1)

a) Logic bombs: They are ~~usually~~ usually an insider job and caused unexpected events to happened in the system, like if an employee set the system in a way that when his payroll record is deleted, the entire payroll records are deleted.

Bacterid: They are programs that consume system resources, like a program that just keeps creating folders infinitly.

B) ~~Because~~ Viruses are program codes that ment to do something, so all the viruses have ~~considered~~ instructions. Even if they try to inter a file as data, they soon reveal there bad behavior. so distinguishing between data and instrutions helps to determine which files have the possibility to ~~had~~ hold viruses.

c) encrypted viruses and polymorphic viruses.

2)

a) Intrusion detection system ~~should~~ is better not to be very complicated ~~or error~~ or takes lots of time.

b) Anamoly: what is usaul is known

what is unusal is bad.

- It is ~~not very usual~~ not unusal for anybody to use Microsoft Word (MW) to save files as long as those files are not moved outside the company.

Misuse: what is bad is known

what is not bad is good.

- nothing says that it's bad to save copies of classified files using (MW).

specification: what is good is known

what is not good is bad

There are no specifications or requirements ~~that~~ saying that no employee can ~~ca~~ save copies of classified files using (MW)

Final Exam CS (April 2012 Term) July 21, 2012

Student Name Abdulghani Alshberi

Student ID 983129

~~c) misuse model because simply~~

c) specification model because there is a very specific rule that if anyone is seen climbing the fence he should be arrested.

3) a) information gathering: simply get all possible documents and resources about the system.

- Flaw hypothesics: draw a plan and have a set of procedures to try.
- Flaw test: test all the procedures specified in the hypothesies.
- Generalization: get general conclusion about the flaw to help detect similar ones.

b) penetration testing sets a bunch of hypothesies and runs them on a system to try to move the system to a compromised state.

Formal verification use mathematics to prove that the flaw exists and has a preconditions that after running through the system should match a bunch of post conditions.

The tester has a bad day if he didn't find a flaw using penetration testing and he has a bad day whe he finds a flaw using formal verification.

4) a) seperation of privilage principle.

b) least privilage principle.

c) least common ~~mechanisme~~ mechanisme principle.

d) fail-safe principle.

e) economy of ~~mechanisme~~ mechanisme principle.

5) - Even though ~~applying~~ applying some security principles might look like waste of time but the systems that has a good security foundations last longer and function better. Meditation might look like wasting time but rested people proved to be more functional and effective.

- A system might ~~have~~ have very good security techniques but the ignorense of a user can still cause damage. Meditation is a very powerfull technique but if it was not taught by a teacher it can be applied wrong causing a headache and a bad experience.

- Never give your password to anybody. It is only for you to used it to log on the system. The Mantra is only yours. Don't give it to anybody. It is your own password to awarness.

Final Exam CS (April 2012 Term) July 21, 2012

Student Name Abdulghani Alshberi

Student ID 983129

6) A distinguished a name is a unique name that seperate a person from anothe and it's used in the certificates.

let's say Var = Jack-Davis-IBM-Quality Assurance dept

{Hash[var]-var}
certificate company Privatekey

7) cryptography is used when the administrators move the customer data from the web-clone server to the customer service group server. the web-clone server should always manitain high integrity and make sure that nobody overwrites the information in it and the administrators have no need to know the customers data (confidentiality).

So, cryptography is used for both.

~~8) Authorization comes before~~

8) Authentication comes first to make sure that this person is allowed to log into the systemthen comes Authorization to specify what this person is authorized to do.

9) the IP address of the outer firewall (X).

10) threshold metric.

11) a) true: because manipulation code for the current files is compared with the latest manipulation code to make sure they are the same and the way to know when was the manipulation code created is by having a time stamp.

b) true: because nobody can change the privilages of the Groups.

c) false: because vulnerability is related to the design and flaws of the system while threats are outsider risks.
~~but if you reverse the question the answer will be true.~~

d) false: Auditing is the analyses of log records to present information about the system in a clear and understandable manner.

e) false: C++ is more vulnerable to a buffer overflow attack than Java because C++ gives the programmer the ability to manipulate pointers and have control on the memory.

Final Exam CS (April 2012 Term) July 21, 2012

Student Name_____

Student ID_____

Final Exam CS (April 2012 Term) July 21, 2012

Student Name_____

Student ID_____

Final Exam CS (April 2012 Term) July 21, 2012

Student Name_____

Student ID_____

Final Exam CS (April 2012 Term) July 21, 2012

Student Name_____

Student ID_____

Final Exam CS (April 2012 Term) July 21, 2012

Student Name_____

Student ID_____

Final Exam CS (April 2012 Term) July 21, 2012

Student Name_____

Student ID_____

Final Exam CS (April 2012 Term) July 21, 2012

Student Name_____

Student ID_____