...es of blank papers)
...ent may not begin

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

CS 466 DE: Introduction to Computer Security
Mid Term Exam: 12-Sept-2015
Instructor Name : Murzal Arsya

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] 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. *[4] Anna, cleared for (CONFIDENTIAL, {C}), wants to access a document classified (CONFIDENTIAL, {B}).* – neither

B. *[4] Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, {B}).* – write

C. *[4] Jesse, cleared for (SECRET, {C}), wants to access a document classified (CONFIDENTIAL, {C}).* – read

(2) *[12] Policy restricts the use of electronic mail on a particular system to faculty and staff. Students cannot send or receive electronic mail on that host. Classify the following mechanisms as secure, precise, or broad and briefly justify your answer.*

A. *[4] The electronic mail sending and receiving programs are disabled.* – SECURE

B. *[4] 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.)* – PRECISE

C. *[4] The electronic mail sending programs ask the user if he or she is a student. If so, the mail is refused. The electronic mail receiving programs are disabled.* – BROAD

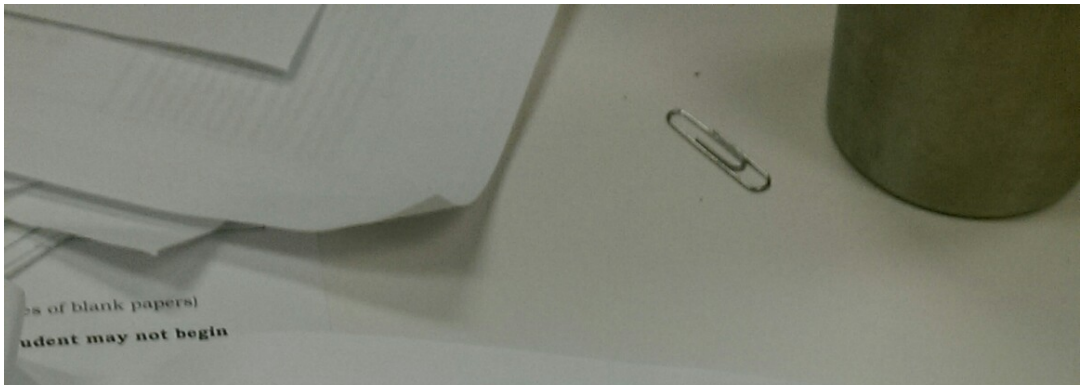
(3) *[10] Alice wants to send a large message M to Bob by maintaining the integrity of the messa... She also wants to assure Bob that the message indeed came from her. How would she do that? (Hint: Think about digital signatures)*

4) *[9] What are the 3 different servers used in Kerberos. Briefly explain their roles in this prot...*

) *[9] Briefly explain any 3 ways by which a Trudy can compromise the verification of a certifi...*

[6] Suppose that you are given a task to design an Authentication system based on Passw... What suggestions would you give the user to choose strong passwords? In other words, write down any 3 characteristics of strong passwords.

6] Give an example of a situation in which a compromise of confidentiality leads to a ompromise in integrity.



...s of blank papers)

...udent may not begin

(8) *[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.*

(9) *[5] 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) *[5] A cryptographer once stated that cryptography could provide complete security and that any other computer security controls were unnecessary. Why is he wrong? (Hint: Think of an implementation of a cryptosystem, and ask yourself what aspect(s) of the implementation can cryptography not protect.)*

11) *[5] The Clark Wilson integrity model supports which one of the following principles? Briefly justify your answer.*

a) principle of least privilege
b) principle of fail-safe defaults
c) principle of economy of mechanism
d) principle of complete mediation
e) principle of open design
f) principle of separation of privilege
g) principle of least common mechanism
h) principle of psychological acceptability

2) *[5] Relate any SCI principle to what you've learnt in the course so far.*

) *[5] Let e_{CA} be the public key of a CA, d_{CA} be the private key of that CA and e_{Jack} be the public key of Jack. How would a certificate issued by CA for Jack look like?*

[8] Fill in the blanks.

a. *[2]* vulnerabilities *are weaknesses in the systems that allow an attacker to carry out a threat.*

b. *[2]* Chinese Wall Model *is a model of a security policy that refers equally to confidentiality and integrity, and deals with conflict of interest.*

c. *[2] Maharishi's Vedic Science is based on* knower (Rishi) *, process of knowing (Devata) and the known (Chandas) and the wholeness from which they arise.*

[2] In an ACM, only allowed permissions are shown. A blank square in the ACM means that the associated process has no permissions on the associated object. This follows the principle of fail-safe defaults

Jai Guru Dev

Midterm Exam (3 Hour 2015 Term) September 12, 2015

Student Name: Yelisiy Kolemyk

Student ID: 983801

1. (A) Anna has neither access.

(B) confidential is greater than UNCLASSIFIED and the empty set is a subset of {BY} so the ~~object~~ subject, so the Robin can write.

(C) SECRET is greater than CONFIDENTIAL, so Jesse can read

2. (A) SECURE - the electronic mail being ~~disabled~~ is definitely SECURE, because it restricts students from sending and receiving ~~email~~ programs and it is secure, as specified in security policy. Since the state is only a subset of the states specified in a security policy, this mechanism is definitely secure.

(B) PRECISE - when the system looks up the sender in the database, when the letter is sent or received it is best described as precise.

Because precise mechanism will restrict the system to set of states which is exactly the same set of states which is specified by security policy.
so if the party in database is listed as faculty or stuff the letter will be processed, otherwise- rejected.

Broad → (C.)
The system only asks the user if he or she is the student and only based on this criteria, if answer is ~~"No"~~ "Yes" the mail is refused.
So if the student answers "No" he/she may be able to actually send an email successfully, which is causing the system to enter non-secure state.
that's why this is a broad mechanism.

of blank papers)

Midterm Exam CS (July 2015 Term) September 12, 2015

Student Name Yuliya Kolesnyk

Student ID 983801

(3.) In order to maintain the integrity of the message and to be assured of the origin integrity (that the message came really from Alice) Alice has to use digital signature.

1. Alice should encrypt the message (M) with her private key to get M1.
2. Alice should encrypt the M1 with Bob's public key to get M2
3. Alice then sends M2 to Bob.
4. Bob decrypts M2 with his private key to get M1.
5. Bob uses Alice's public key to decrypt M1 to get M.

If M is the same then Bob could be assured of origin integrity - that Alice indeed sent the message, because only Alice knows the sec key to create M1 (she encry if on the first place using private key).

(4.) Kerberos is using Needham-Schroeder protocol as modified by Denning and Sacco.
Kerberos pays attention - emphasizes the difference between authentication (determining who user is) and authorization (determining what the user, that is already authenticated, allowed to do).

Kerberos as a name refers to the three headed dog from Greek mythology that guarded the gates of hell.
The three heads → the three servers are:

1. Authentication server (AS) - it authenticates the user and issues him a ticket that allows him to use the authorization server.

Ticket-granting server (TGS) - which is authorization server and the role of it is to check if the user is authorized to use the requested server and if Yes then issue a ticket to use this server

Midterm Exam (5 July 2015 Term) September 12, 2015

Student Name: Yuliya Kolesnyk

Student ID: 983801

3. Target server (Prin) makes sure that the ticket, issued by authorization (TGS) server is valid and if yes then gives user access to the server.

Question 5

3 ways that Trudy can compromize verification of certificate:

1. Trudy can steal somebody's identity and get certificate using this stolen identity.

2. Trudy can add the public key of a bogus (fake) CA to the list of Trusted Root certification Authorities in a browser to send a certificate which is signed by the bogus (fake) CA to the browser.

3. Trudy can steal the private key of the certification authority (CA) and then use it to sign any certificate totally certificate. If a CA's private key gets stolen (known by some intruder), then every certificate that is signed using this key should be declined - revoked. This is a very big problem (disadvantage) of Certification Authorities (CA.

Question 6

Characteristics of strong passwords:

- The password should be about 16 bits of randomness → 16 characters.
- The password should be complex enough - include special characters (like: &@#) and upper case (ABC) and lower case (abc) letters in

of blank papers)

Midterm Exam CS (July 2015 Term) September 12, 2015

Student Name Yuliya Kolesnyk

Student ID 983801

In order to be secure from dictionary attacks.

- use password phrase acronym like (I am an MUM Student) so that the password is IaaMS which is the first letter of each word).
- the password should be changed regularly.
- different passwords should be used on different accounts.

Question 4.

Compromize between confidentiality and integrity.

The following example compromizes confident and integrity, such as keeping certain data confidential to eliminate integrity concerns:

- James and Ann work in the same big com

James can read RoomCOI.Proctor a

Ann can read RoomCOI.University.

Both of them can read MUMCOI.

If James can write as well to MLLMCOI. Professor then he will be able to read information from RoomCOI. Proctor and write it to MLLMCOI. Professor, and that will be Ann able to read this information.
This is not confidential and if James writes then MLLMCOI. Professor is altered, which compromizes integrity.
So this example is a compromize between confidentiality and integrity.

Question 8

This scenario is wrong because this is not how the digital signature works.
In order to digitally sign it the following should be done: This is the correct:

- digitally sign "stop" and "start" message with my private key to get M1.
encrypt M1 with server's public key to get M2.
Then send M2 to the server.

blank papers)
may not begin

Midterm Exam CS (July 2015 Term) September 12, 2015

Student Name Yuliya Kolesnyk

Student ID 983801

- Server decrypts M2 with his private key to get M1.
- Server uses my public key to decrypt M1 to get M.

In the scenario described "stop" and "start" is not encrypted with server's public key after being digitally signed by my private key.

And server does not firstly use his private key to decrypt the message before using my public key.

This is the wrong thing in the given scenario.

Question9

Access Control Matrix

	alicerc	bobrc	cyndyrc
Alice	OX	R	
Bob	R	OX	
Cyndy	R	RW	ORWX

Question10

Midterm Exam CS (July 2015 Term) September 12, 2015

Student Name Yuliya Kolesnyk

Student ID 983801

Question 11

Clark-Wilson model requires separation of duty (principle of separation of privilege) for maintaining of the allowed and certified relations.

Here are some enforcement and certification rules that support this idea:

- Enforcement rule 1 (ER1) - system has to maintain the certified relation and also has to ensure that only Transformation Procedures (TPs) certified to run on a CDI manipulate that CDI.
- Enforcement rule 2 (ER2) - system must associate a user with ea TP and set of CDIs. If the user is not associated with a particular TP and CDI, then the TP cannot access that CD as a user (ou

Certification Rule 3.

relation must meet the allowed relations ments imposed by the requirements of separation of duty principle (that should

why the allowed relation be certified).

that's why Clark-Wilson model supports - relates to principle of separation of privilege.

Question 12.

⊖ A threat is a potential violation of security. SCI's approach to mitigating threats is to disallow the birth of the enemy (attacker).

there are many ways to implement access control matrix (ACM) like ACL, CL, PACL. All of relative creation is a manifestation of the field of pure consciousness.

Midterm Exam CS (July 2015 Term) September 12, 2015

Student Name Yuliya Kolesnyk

Student ID 983801

⊖ Bell-LaPadula model is based on subjects, objects and security classifications, and rules (no read-up and no write down). Maharishi's Vedic Science is based on knower (Rishi), process of knowing (Devak) and the known (Chandas) and the wholeness from which they arise.

Question 13

The certificate looks like this:

Jack, Jack's address, e_{jack}, issuer, serial#, expiration date || Σ Hash(Jack, Jack's addr e_{jack}, issuer, serial#, expiration date) Σ

rsity of Managen
Graduate Exam.

Question 19

Answers:

- Vulnerabilities
- Chinese wall model
- Knower (Rishi)
- principle of fail-safe defaults

Iterm Exa
lent Name_
lent ID____

Q (1)[12] Answer the following question about digital Signature.

A)What is digital Signature?

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash

•The document is first run through a one-way hashing algorithm that is very difficult to invert (e.g., MD5 or SHA)

• The hash typically produces a fixed-length result independent of the original document size

• The document owner applies his private key to the hashed document – this encrypted result is called the signature block

• The signature block is appended to the document and both are sent to the receiver

• When the document arrives, the receiver first computes the hash of the document as agreed upon

• Then the receiver applies the sender's public key to the signature block, getting the hash computed by the sender

• This hash must match the hash of the document computed by the receiver

• A digital signature also makes it possible to sign e-mail messages and other digital documents such that they cannot be repudiated by the sender late

B) Let m be a message. Suppose Alice and Bob share a secret key k. Alice sends Bob m || { m }k (that is, the message and its encipherment under k). Is this a digital signature?

First, Alice has authenticated the contents of the message, because Bob deciphers { m }k and can check that the message matches the deciphered one. Because

only Bob and Alice know k, and Bob knows that he did not send the message, he concludes that it has come from Alice. He has authenticated the message origin and integrity. However, based on the mathematics alone, Bob cannot prove that he did not create the message, because he knows the key used to create it. Hence, this is not a digital signature

Q[2][11] Answer the following questions about kereboeros Protocol.

A)Describe briefly the roles of the 3 different servers used in kerboeros

Kerberos uses the Needham-Schroeder protocol as modified by Denning and Sacco. Kerberos is used to control access to servers (file server, print server, etc). It emphasizes the difference between authentication (determining who the user is) and authorization (determining what the authenticated user is allowed to do).

The name Kerberos refers to the three headed dog from Greek mythology that guarded the gates of hell. The three heads are

1. The authentication server which authenticates a user and issues him a ticket that allows him to use the authorization server

2. The authorization (ticket-granting) server checks whether the user is authorized to use

the requested server and if so issues him a ticket to use the server.

3. The server checks to make sure that the authorization server's ticket is valid and

if so grants the user access to the server.

B) what is potential problem of kerboeros?

Kerberos relies on clock synchronization and also dictionary attack is possible which can break this protocol.

Q.3 [9] Policy restricts the use of electronic mail on a particular system to faculty and staff. Students cannot send or receive electronic mail on that host. Classify the following mechanisms as secure, precise, or broad.

a. The electronic mail sending and receiving programs are disabled.[secure]

b. 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.)

[precise]

c. The electronic mail sending programs ask the user if he or she is a student. If so, the

mail is refused. The electronic mail receiving programs are disabled. [broad]

Solution:

The electronic mail sending and receiving programs are disabled.

Secure
The security mechanism restricts students from sending and receiving programs causing the system to be in secure states as specified in the security policy. However, since this state is only a subset of the states specified in the security policy (state where faculty and staff can send and receive email cannot be reached) this mechanism can be described as secure at best.

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 the database entries are correct.)

Precise.
The stated security mechanism will restrict the system to set of states which is the same set of states as specified by the security policy. Hence the security mechanism is precise.

The electronic mail sending programs ask the user if he or she is a student. If so, the mail is refused. The electronic mail receiving programs are disabled.

Broad.
Students could answer 'No' when they are asked if he or she is a student. Thus, they may be able to successfully send an email causing the system to be in a state which is non-secure. Hence, this is a broad mechanism.

Q[4][9]

The security levels are TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest)The categories are A, B and C. Discretionary access controls allow anyone access unless otherwise specified

[3] Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, {B}). What types of access does she have?

CONFIDENTIAL is greater than UNCLASSIFIED and the empty set (the categories of Robin) is a subset of {B} so the object dominates the subject and hence Robin can write.

[3] Paul, cleared for (TOP SECRET, {A, C}), wants to access a document classified (SECRET, {B, C}). What type of access does he have?

neither

[3] Sammi, cleared for (TOP SECRET, {A, C}), wants to access a document classified (CONFIDENTIAL, {A}). What types of access does he have?

read

Homework 4 solutions

Due: 9th February(Monday), in class

1. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that the discretionary access controls allow anyone access unless otherwise specified.

a. Paul, cleared for (TOP SECRET, {A,C}}, wants to access a document classified (SECRET, {B,C}}.

b. Anna, cleared for {CONFIDENTIAL,{C}}, wants to access a document classified (CONFIDENTIAL, {B}}.

c. Jesse, cleared for {SECRET, {C}}, wants to access a document classified {CONFIDENTIAL, {C}}.

d. Sammi, cleared for {TOP SECRET, {A,C}}, wants to access a document classified {CONFIDENTIAL, {A}}.

e. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access the document classified (CONFIDENTIAL, {B}).

Answers:

Let A's compartment be (L_A, C_A) and B's be (L_B, C_B). The simple security condiion says that A can read B if and only if $L_A \geq L_B$ and $C_B \prod C_A$. The *-property says that A can write B if and only if $L_B \geq L_A$ and $C_A \prod C_B$. Remember that TOPSECRET ≥ SECRET ≥ CONFIDENTIAL ≥ UNCLASSIFIED.

a. L_{Paul} = TOPSECRET ≥ SECRET = L_{doc}, so Paul cannot write the document. Paul cannot read the document either, because C_{doc} = { B, C } א { A, C } = C_{Paul}.

b. L_{Anna} = CONFIDENTIAL ≥ CONFIDENTIAL = L_{doc}, but C_{doc} = { B } א { C } = C_{Anna} so Anna cannot read the document, and C_{Anna} = { C } א { B } = C_{doc}, so Anna cannot write the document.

c. L_{Jesse} = SECRET ≥ CONFIDENTIAL = L_{doc}, and C_{doc} = { C } ∏ { C } = C_{Jesse}, so Jesse can read the document. As $L_{Jesse} > L_{doc}$, however, Jesse cannot write the document.

d. As L_{Sammi} = TOPSECRET ≥ CONFIDENTIAL = L_{doc} andC_{doc} = { A} ∏ { A, C } = C_{Sammi}, Sammi can read the document. But the first inequality means Sammi cannot write the document.

e. As C_{Robin} = ∅ ∏ { B } = C_{doc} and L_{doc} = CONFIDENTIAL ≥ UNCLASSIFIED = L_{Robin}, Robin can write the document. However, because $L_{doc} \geq L_{Robin}$, she cannot read the document

Q5[9] Advantages of CAs over KDCs

The CA doesn't have to be online. It can be in a locked room, create a certificate and put it on a floppy disk. A user has to communicate with a KDC online (as described in lecture 8) to get a session key.

• Since a CA is not online, it can be simpler (economy of mechanism)

• There is no single point of failure for a CA. But if the KDC (Cathy) goes down, Alice and Bob cannot create a session key.

• Certificates are not security sensitive. All an attacker can do is delete certificates, he can't create bogus certificates because he doesn't have the private key of the CA.

• Since a compromised CA doesn't have a private key, it can't decipher conversations but a compromised KDC can (it has the keys that it shares with the users that trust it). That is, you have to trust a KDC more than a CA. All you give the CA is your public key.

Q 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 obrc, 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.

a. Create the correspond ing access matrix

	alicerc	*bobrc*	*cyndyrc*
Alice	ox	r	
Bob	r	ox	
Cyndy	r	rw	orwx

Q. 10[6] Briefly explain how clark-wilson integrity model support the separation of duty .

The system must associate a user with each TP and set of CDIs. The TP may access those CDIs on behalf of the associated user. The TP cannot access that CDI on behalf of a user if she/he is not associated with that TP and CDI.

- System must maintain, enforce certified relation
- System must also restrict access based on user ID (*allowed* relation)
- Now we have human, and we have to enforce separation of duty and authentication

Q 11[6] Differentiate between a known plaintext attack and chosen plaintext attack.

- Known plaintext
  Adversary has the ciphertext for a known plaintext, wants to find the key
- Chosen plaintext
  Adversary can generate ciphertext for any plaintext, wants to find the key

The **known**-**plaintext attack** (KPA) is an **attack** model for cryptanalysis where the attacker has access to both the **plaintext** (called a crib), and its encrypted version (ciphertext). These can be used to reveal further secret information such as secret keys and code books.

A **chosen**-**plaintext attack** (CPA) is an **attack** model for cryptanalysis which presumes that the attacker can obtain the ciphertexts for arbitrary **plaintexts**. The goal of the **attack** is to gain information which reduces the security of the encryption scheme

1a Logic Bombs:

A programs that performs an action that violates the site security policy when some external event occurs. Example: program that deletes company's payroll records when one particular record is deleted. The "particular record" is usually that of the person writing the logic bombs.

Bacteria: A program that absorbs all of some class of resources. Example: Shell commands of Unix system, while true do mkdir x chdir x done

1b Virus - data: written to program, Instructions: then executes

Treating data and instructions as separate types, and requires certifying authority to approve conversion. Certifying authority will not make mistakes and assumption that tools, supporting infrastructure used in certifying process are not corrupt. All the virus have data and instructions, so distinguishing between data and instructions helps to determine which resources have the possibility to hold the viruses.

1c encrypted virus and polymorphic virus

Extra: Malicious Logic: Malicious Logic is a set of instructions that causes site security policy to be violated. In SCI terms this is analogous to a violation of natural laws.

Extra: Diff formal verification and Penetration Testing

Formal Verification: Preconditions – Program - Post Condition

Penetration Testing: System characteristics, environment & state – program / system – system state

Mock 4: Formal Verification: Mathematically verifying that a system satisfies certain constraint. Penetration Testing: Testing to verify that a system satisfies the certain constraint. Penetration testing is a testing technique, not a verification technique. It can prove the presence of vulnerabilities but absence of vulnerabilities.

2a. Minimize false positive and minimize false negative.

2b.

Principle of Intrusion Detection

No anomalies: No Misuse: **Specs satisfied:**

Anomaly Detection looks for unexpected events

Misuse detection looks for what is known to be bad

Specification-based detection looks for what is known not to be good.

Consider the following situation at Annapurna (the cafeteria at M.U.M.)
A diner must show a badge or purchase a meal before eating at Annapurna.
Each diner uses a tray. If the number of trays washed in a day does not equal the number of diners counted by the door checker, then somebody has cheated
Annapurna and eaten for free.
By analogy, this is an example of which of the following:

Misuse modeling

Consider the following policy implemented by Annapurna (the cafeteria at M.U.M.)
A student usually accesses only the dining room and the dish room. If a student is found in the kitchen this is reported (he/she may be trying to put some chicken in the soup).
By analogy, this is an example of which of the following:

The student here is a process. The places he/she can visit are like files and programs. Entering kitchen is like a process attempting to access file that its specification says that it shouldn't. This is specification based modeling.

Consider the following information about Annapurna, the cafeteria at MUM.
From past experience Annapurna has determined that each student on the average drinks one pint of milk per day. Based on this information they budget for X gallons of milk per day. If on some day, all X gallons have been used before the midday meal, there is reason to suspect that someone is stealing milk.
By analogy, Annapurna is doing what kind of modelling here?

Anomaly modeling is statistical in nature. The phrase "each student on the average drinks one pint of the milk per day" indicates the statistical nature of this.

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 3 forms of intrusion detection (Anomaly, Misuse and Specification) could be used to argue against this accusation.

2 c. A security guards at a professional soccer match notice that two men are climbing over the fence; the security guards detain these men. Which ID models used here justify your answer.

3 a. Briefly explain the 4 steps in the flaw hypothesis methodology

Information gathering: Become familiar with system's functioning. Ideally acquire the knowledge of the system that a potential hacker has. Read manuals & specification (open design), Look how system manages privileged users.

Flaw hypothesis: Draw on knowledge to hypothesize vulnerabilities, e.g. If manual indicates a maximum length of some field, try a longer length.

Flaw Testing (do not harm): Assign priorities & test out hypothesis (e.g. focus on external attack rather than inside job). Avoid exploiting the flaw unless management does not believe the flaw exists. As with any test, it must be as simple as possible and must be repeatable.

Flaw Generalization: Generalize vulnerability to find others like it. E.g. If an account with default password found generalized two things: 1) users poorly educated in password management 2), There may be other account with default passwords.

3 b. What are the goals of penetration testing and how does this compare with the goals of formal verification.

Goals: Attempt to violate specific constraints in security and / or integrity policy .implies metric for determining success, Must be well-defined. Ex. Subsystem designed to allow owner to require others to give password before accessing file.

Formal Verification:

A tester had a bad day when he finds a bug

Mathematically verifying that a system satisfies certain constraints

Required: post conditions satisfy constraint

Penetration technique:

Penetration tester had a bad day if he does not find a bug

Testing to verify that a system satisfies certain constraints

Hypothesis stating system characteristics, environment, and state relevant to vulnerability

Result is compromised system state.

Apply tests to try to move system from state in hypothesis to compromised system state.

Formal Verification	**Penetration Testing**
Mathematically verifying that a system satisfies certain constraints	**Testing to verify that a system satisfies certain constraints.**
Precondition: states assumptions about the system	**Hypothesis stating system characteristics, environment and state relevant to vulnerability**
Postconditions: result of applying system operations of preconditions input. Postcondition satisfies constraint.	**Result is compromised system state. Apply tests to try to move system from state in hypothesis to compromised system state.**
Program	**Program / system**

4

a) Users are classified into four classes. Moving information from one class to another requires approval of more than user.

Principle of separation of privilege

b) Each Server has the minimum amount of knowledge of the network necessary to perform its task

Principle of least privilege

c) In the Drib Corporation, the four servers in the DMZ zone are all on separate computers.

Least Common Mechanism

d) The use of write-once media in the log server. (Deny all modifications to write-once media)

Principle of Fail-Safe defaults

e) Configuration of firewalls should be simple so that administrators will feel comfortable doing it.

Principle of Psychological Acceptability

The use of write-once media in the log server. (Can't alter it and can only destroy it if they have access to the room containing the log server).

Principle of least privilege

5 Briefly explain any 3 of your favorite SCI points that you have learned in this course so far.

There are two main forms of malicious logic, viruses and worms. There is only one form of “delicious” logic: deep rest and then perform dynamic activity.

A buffer overflow attack causes data to flow outside the boundaries of the memory reserved for it. Here breaking boundaries is bad. However breaking boundaries to our thinking is good because it allow us to have access to the field of all possibilities. TM gives us access to this field.

In Security system lecture we learned the contrast that how a machine used by developer is configured with how the DMZ web server is configured. Knowledge is different in different state of consciousness.

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 QA dept?

A distinguished name identifies a principal. It consists of a series of fields, each with a key and a value.

/O=IBM/OU=Quality Assurance/CN=Jack Davis/

7 Is cryptography used in the Drib system for integrity, confidentiality, or both? Justify

Both. Here Integrity is main concern and confidentiality is secondary with regard to updating the web server since most of the data is public and displaying on public web page (open design). Only the commercial transaction data is considered private. So cryptography is primarily used to ensure used to ensure data integrity(I,e Turdy makes no changes during transfer) and secondarily for confidentiality.

8. Explain in short the difference between authentication and authorization.

Authentication: Binding of a principal to a representation of identity internal to the system.

Authorization: Access control checks for resource allocation based on the assumptions that binding.

9. 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.

Since DMZ purely separating internal network from external network, external internet user will get IP address x.

10. Which statistical model is likely to be used to detect someone guessing passwords.

Threshold metric

11a. A manipulation detection code is based on timestamps

False: It is based on permission bits which included in the signature and a keyless cryptographic checksum. But not Timestamp which is used to prevent replay attacks.

11b. The access control policy that is implemented in the internal drib network is originator controlled.

Assignment 11 Wk 13

11c. Vulnerability of a system increases when threats high.

True: Since threat is a possible danger that might exploit a vulnerability to breach security

11d. Security logging is the analysis of records to present information about the system in a clear and understandable manner.

False. Security logging is the recording of events or statistics to provide system use and performance.

11e. A Programming language has no effect on whether or not a program is vulnerable to a buffer overflow attack.

False. Since it modifies the data beyond its buffer, the program behaves abnormally.

Buffer Overflow: A buffer overflow occurs when a program or process tries to store more data in a buffer than it was intended to hold.

Formal Verification	**Penetration Testing**
Mathematically verifying that a system satisfies certain constraints	**Testing to verify that a system satisfies certain constraints.**
Precondition: states assumptions about the system	**Hypothesis stating system characteristics, environment and state relevant to vulnerability**
Postconditions: result of applying system operations of preconditions input. Postcondition satisfies constraint.	**Result is compromised system state. Apply tests to try to move system from state in hypothesis to compromised system state.**

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 Qn 2

Kereberos Protocol :-

- It is improvement "Denning - ...." protocol of integrity [illegible].
- improved over Authorization process with third party Key Distribution ~~Server~~ Centre (KDC).
- 3 Servers are used to authorize 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

$T_A = \{ \text{[illegible]} T ! R_1 \}_K$

(b) Ticket Granting Server :- Once authorized, they issue Ticket which is used in second part to get public key of [illegible]

$T_{A,B} = \{ \text{[illegible]}, T_A \}_{K_1}$

(c) Key distribution Server :-

Once decrypted [illegible] from Alice, Bob's connect 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 for 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 ~~[illegible]~~ 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, Chandos, Devela i.e Know, Known and Knower.

SSL uses CA as third party to verify authorized user who knows the information (Devla) and client is Knower as Chandos who will get information and vendor who is as Known who had information

(2). Principle of Separation of duty -

At the [illegible] of [illegible] everyone can feel own potentiality and perform at his/her best caliber to higher [illegible] field which will create [illegible] 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