Take Home Assessment II

Started: Dec 7 at 8:24am

Quiz Instructions

Rules

- This exam is worth a total of 85 points.
- You will have 150 minutes to complete the exam once started.
- You are allowed to access your class notes, and lecture slides during the exam
- **It is a good idea to take a snapshot of the exam before submitting as some students have experienced loss of essay answers upon submission in previous years**
- If you are uncertain about the details of a particular problem, make any **reasonable** assumptions that you feel are necessary to solve it. Be sure to write down your assumptions in Q1 essay space organized by question #.
- **You are to neither give nor receive aid on this exam. You may not show or discuss this exam or your answers with anyone at least till after the term ends.**

Question 1	0 pts

This is space for including any assumptions you have made while solving/answering the problems above. Organize them by Question #/description. You may also use this space to show work on any of the questions so you have the opportunity for partial credit. Don't forget to organize this by Question #/Name

Edit   View   Insert   Format   Tools   Table

12pt ∨   Paragraph ∨   ⋮

Question 10: Assume executable code held elsewhere

p   ⌨ ⓣ | 7 words | </> ↗ ⋮

Question 2   3 pts

Consider the following two security labels:

Label 1: (Restricted: {p1})

Label 2: (Secret: {p1, p3})

Here Restricted and Secret are security levels with Restricted < Secret. p1, p2 and p3 are categories. Which of the following statements is true (**pick one**)?

○ Neither label dominates the other

○ Label 1 dominates Label 2

○ None of the above

◉ Label 2 dominates Label 1

Question 3   4 pts

Which of the following is an example of typo squatting (pick all that apply)?

☐ ww1.google.com

☑ www.microsoft.z.com

☑ www.nettlix.com

☑ www.dictionery.com

Question 4   3 pts

Consider a Role-Based Access Control (RBAC) system where a role **R1** and role **R2** are mutually exclusive. **R1** has permissions to perform operations **Review** and **Approve** on resource **Report**, and **R2** has permissions to perform operation **Edit** on resource **Report**. No other role in the system has permissions to perform any operation on resource **Report**. Which of the following statements **CANNOT be true** in this setting (**pick one**)?

○ Users Alice and Bob can both be assigned to R1

○ Users Eve and Mallory can both be assigned to R2.

○ User Alice can be assigned to R1 and user Bob can be assigned to R2.

● User Candice can Edit resource Report and Review her edits to Report.

Question 5   5 pts

A company has 10 job functions. On average there are 20 employees in each job function. Similarly, on average an employee in each job function needs 1000 permissions to properly execute their task. The number of assignments (i.e., permission and/or role assignments) that need to be managed when using a DAC model (X) and when using RBAC (Y) model are as follows (**pick one**):

○ X = 100, 000; Y = 20, 200

● X = 20, 000; Y = 10, 200

○ X = 20, 000; Y = 10, 000

○ X = 200, 000; Y = 10, 200

Question 6   4 pts

Which of the following are desirable for a good biometric (pick all that apply)?

- ☑ Permanence

- ☑ Universality

- ☑ Uniqueness

- ☐ Plasticity

Question 7   4 pts

Consider Discretionary Access Control (DAC) and Mandatory Access Control (MAC). For each statement below select True from the drop-down if the statement is **ALWAYS** true, and select False if it can **EVER** be false.

DAC is so named because access is granted at the discretion of users owning resources in the system

| True   ⌄ |

In MAC, resource access is mediated by a system wide policy managed my a few privileged users and not by regular users

| True   ⌄ |

DAC is the default access control model in Linux

| True   ⌄ |

MAC requires two-factor authentication

| False   ⌄ |

Question 8   4 pts

Which of the following is an input handling vulnerability (pick one or more)?

☑ Buffer Overflow

☑ SQL Injection

☐ TOCTOU Error

☐ Race Condition

Question 9   4 pts

Which of the following is a runtime defense against buffer overflows (pick one or more)?

☐ Stack Guard

☑ Guard Pages

☐ Stack Shield

☑ No-execute Bit

Question 10   2 pts

One defense against buffer overflow attacks is to associate "don't execute" bits with portions of computer memory where executable code should not be located. Which portions of the memory ought to be so protected. Explicitly state in the margin any assumptions you think you must make to defend your answer. (select all that apply below)

☐ text segment

☑ heap

☑ stack

☐ data segment

Question 11   4 pts

Mandatory Access Control Models (part a)

BIBA: The table below lists subjects, objects, and their associated integrity levels. The relationship between the levels is as follows: **Purple > Green** > **Orange**

Subject	Subject Integrity Level	Object	Object Integrity Level
Alice	Purple	Yoyo	Green
Bob	Green	XRay	Purple
Carol	Green	Zebra	Orange

Compute whether the specified subject has "Read" or "Append" (i.e., write only) or "Both" accesses to the specified object (see table below) using the BIBA model.

Subject	Object	Rights
Alice	XRay	both
Bob	Zebra	write
Carol	Yoyo	both
Carol	Zebra	write

Question 12   6 pts

Mandatory Access Control Models (part b)

BIBA: The integrity labels are updated to include project categories, p1, p2, and the updated labels are shown in the table below. Re-evaluate the rights (read or append/write-only or both) associated with each subject and object pair using the BIBA model.

Subject	Subject Integrity Level	Object	Object Integrity Level
Alice	Purple: {p1, p2}	Yoyo	Green: {p1}

| Bob | Green: {p2} | XRay | Purple: {p1, p2} |
| Carol | Green: {p1, p3} | Zebra | Orange: {p3} |

Compute whether the specified subject has read or append (i.e., write only) or both accesses to the specified object (see table below) following the BIBA model.

Subject	Object	Rights
Alice	XRay	
Bob	Zebra	
Carol	Yoyo	

Question 13   5 pts

Mandatory Access Control Models (part c): **Chinese Wall**
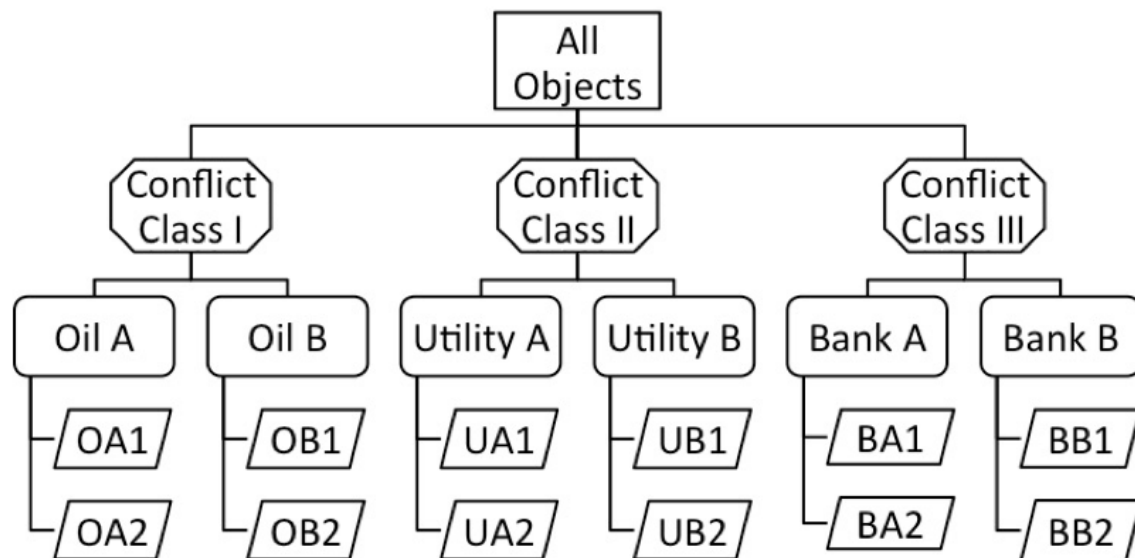

Figure above depicts organization of objects into datasets (e.g., Bank A) and conflict of interest classes (e.g., Conflict Class I) at consulting firm ConFirm X that uses Chinese Wall access model. Jane, Bob, Emily, Marcus, and Alice are consultants with the firm.

Which of the following statements describing access rights can be TRUE (i.e., access allowed) or have to be FALSE (i.e., access not allowed) with respect to the above figure in a Chinese Wall model. Assume that the consultants have no other accesses than those explicitly stated in each statement.

Bob can read OA1, OA2 and UB2

> True ˅

Emily can read BA1 and write BA2

> True ˅

Marcus has read access to UA1 and UB2

> False ˅

Alice is given read and write access to UB1 and read access to UB2

> True ˅

Jane is given read access to UB1 and write access to BB2

> True ˅

Question 14

4 pts

What is the difference between a 'role' in RBAC and a 'group' commonly used in UNIX?

Edit   View   Insert   Format   Tools   Table

12pt ˅   Paragraph ˅ | ⋮

p
0 words

Question 15
4 pts

What is *-property in BLP confidentiality model and why is it needed?

Edit   View   Insert   Format   Tools   Table

12pt ∨   Paragraph ∨   ⋮

p
0 words

Question 16
4 pts

What is StackGuard and how does is protect against stack smashing attacks?

Edit   View   Insert   Format   Tools   Table

12pt ⌄   Paragraph ⌄   ⋮

p   ⌨ ⓘ │ 0 words   </> ↗ ⋮

Question 17   3 pts

How are "Linux Capabilities" different from the concept of "Capabilities" ?

Edit   View   Insert   Format   Tools   Table

12pt ⌄   Paragraph ⌄   ⋮

p   ⌨ ⓣ   0 words   </> ↗ ⋮

Question 18   2 pts

When biometrics are used for surveillance which of the following is a more critical concern?

○ False Positive

○ False negative

Question 19   4 pts

Which of the following statements are true in the context of Incident Response? (pick all that apply)

☑ Training response personnel is key part of "Preparation" phase

☑ Defining roles and responsibilities for handling an incident is part of "Preparation" phase

☑ Identifying the scope of the incident is critical to proper Containment

☐ Removing artifacts of the incident from affected systems is part of "Detection and Analysis" phase

Question 20   3 pts

What is the essential difference between origin integrity/authenticity (provided by a keyed MAC) and non-repudiation (provided by a digital signature)?

Edit   View   Insert   Format   Tools   Table

12pt ∨   Paragraph ∨   ⋮

p   ⌨ ⓣ | 0 words | </> ↗ ⋮

Question 21   5 pts

One-Time Password Protocols

Suppose we modified the S/KEY protocol as follows:

i. during setup phase the user securely shares a **"seed"** value with the server maintains a user-side local counter **UCTR** initialized to 1 (this is incremented by the user after each successful login)

ii. the server stores the **seed** value and sets up a server-side local counter **SCTR** initialized to 1 (this is incremented by the server after each successful user login)

iii. to login the user hashes the **seed** value **UCTR** number of times (i.e., 3 times if current UCTR is 3) and sends the resulting hash value (i.e., h^3(seed)) as the login password

iv. when the server receives a password, it hashes the **seed** value **SCTR** number of times (i.e., 3 times if current SCTR is 3) and checks whether user sent password matches this computed value; if the password matches it accepts the login and increments the counter **SCTR**

v. when a user successfully logs in he increments his counter **UCTR**

a) If this is the only factor of authentication, is this a good one-time password protocol? State YES or NO (2 pt)

b) Justify your answer (3 pts)

Edit   View   Insert   Format   Tools   Table

12pt ⌄   Paragraph ⌄   ⋮

p   ⌨   ⓣ | 0 words | </>   ↗   ⋮

Question 22   **2 pts**

Which of the following is a better programming language to use if one wants to avoid buffer overflows altogether? (pick all that apply)

☑ Java

☐ C

☐ C++

☑ Rust

Crypto Primitives and Security Properties

Alice and Bob share symmetric keys $K1_{AB}$ and $K2_{AB}$. Each have an asymmetric key pair (SK_A, PK_A) and (SK_B, PK_B) respectively. Here SK_A denotes secret-key (also called private key) of Alice and PK_A denotes public-key of Alice. Assume that they both have have **access to authentic copies of each others' public-keys.** Recall the notation that $x \parallel y$ means the concatenation of x with with y, $\{x\}_K$ denotes the the encipherment of of x using key K, $h(x)$ denotes a hash of x, and $MAC_K(x)$ denotes MAC of x with key K.

Question 23   4 pts

For the message from Alice to Bob shown below identify what security properties are provided. Select **one or more properties** among those provided.

$$A \rightarrow B : \{m\}_{K2_{AB}} \parallel MAC_{K1_{AB}}(\{m\}_{K2_{AB}})$$

- ☑ origin authenticity

- ☑ confidentiality

- ☐ non-repudiation

- ☑ message integrity

Question 24   2 pts

Justify your answer above.

Edit   View   Insert   Format   Tools   Table

12pt ∨   Paragraph ∨   ⋮

p

0 words

Quiz saved at 10:01am

Submit Quiz