CIS 4360 – Introduction to Computer Security – Fall 2010 – with answers

Name: ..... Number: .....

Second Midterm

Instructions

This is a closed-book examination. Maximum score **100 pts**.
There are 5 questions, each is weighted 20pts.
You have 60 minutes.

Q.1 .....

Q.2 .....

Q.3 .....

Q.4 .....

Q.5 .....

Total .....

1. This question concerns Cryptography and Access Control. **(2+2)+3+2+2+3+(3+3)=20 pts**

(a) Compare the advantages of Public key Cryptography over Symmetric Key Cryptography and conversely.

- *Advantages of PKC over SKC*: **Answer:** The application keys are public; Many more applications, e.g., digital signtures, key exchange; threshold applications.
- *Disadvantages of PKC over SKC*: **Answer:** We need a trusted third party to manage certificate (that certify the public keys of users); PKC applications are several orders slower than SKC (mainly because modular exponentiations take longer to compute than symmetric key operations).

(b) What is an Access Control matrix? **Answer:** A matrix whose rows are indexed by the subjects $s \in S$ and columns by the objects $o \in O$, for which the entry in the (s, o) cell contains a list of operations that s can perform on o.

(c) If the access rights are kept with the subjects then every subject is given **capability** .

(d) If the access rights are kept with the objects then every object has **Access Control List**.

(e) Define a lattice $(L, \leq)$. **Answer:** A (non-empty) set L with an ordering $\leq$ such that: for any $a, b \in L$ there is a $lub(a, b)$ and a $glb(a, b)$.

(f) Let $H = \{0, 1, 2, 3\}$, with the natural order "$\leq$". Let $\mathcal{C}$ be the set of subsets of $C = \{a, b, c\}$. Consider the set of L of all pairs (h, X) where X is a subset of C.

i. How many elements does L have?
Answer: $2^3 \cdot 4 = 32$.

ii. Define an ordering $\leq$ on L which makes it into a lattice.
$(h, X) \leq (h', X')$ if: $h \leq h'$ **and** $X \subseteq X'$

2. This question concerns the Bell-LaPadula model.

(2+2+2+3+2)+2+3+2+2=20 pts

(a) Fill in the gaps (choose words from, or similar to: classified, yellow, lattice, secert, mandatory, unclassified, a linear structure, information flows, unclassified, discretionary, object, subject, access mode, stream, top secret).

i. The Bell-LaPadula model employs access control matrices to model **mandatory** access policies of the **Orange** Book.

ii. In the context of Computer Security what does:

A. MAC stand for? **Mandatory Access Control**

B. DAC stand for? **Discretionary Access Control**

iii. The security levels set L can be linear. What are the 4 security levels in the Orange Book called?

Top Secret, **Secret**, **Classified**, **Unclassified**.

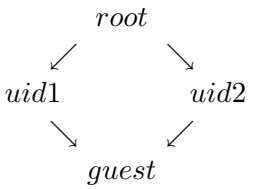
iv. The security levels set L can also have a partially ordered structure. Illustrate below one such structure. —**see Slide 29, Computer Security**. What is it called? **Answer: A Lattice**

v. In class our diagrams for security level sets involved vectors "↑" (usually pointing upwards). What do these stand for? **Answer:** Information flows.

(b) The BLP model is based on, (TRUE or FALSE)

- an Information flow model: TRUE
- an integrity model: FALSE
- a privacy model: TRUE
- some other model: FALSE

(c) You are given a security policy stating that a subject has access to an object if and only if the security level of the subject dominates the security level of the object. What is the effect of using the following lattice with this policy?



Answer. The *root* has access to all files; users *uid*1, *uid*2 have access to their individual files and guest files; guests have no access to user files and can only access their own files.

(d) Describe the ss-property in terms of the basic access mode observe

Answer. The ss-property requires that for observe access the level of the subject has to dominate the level of the object.

(e) Describe the *-property in terms of the basic access modes alter.

Answer. The *-property requires that for alter access, the level of the subject is dominated by the level of the object.

3. This question concerns the Bell-LaPadula (BLP) model. **2+2+2+3+2+3+3+3=20 pts**

(a) The BLP model is based on, (TRUE or FALSE, more than one may apply)

- an Information flow model: TRUE
- an integrity model: FALSE
- a privacy model: TRUE
- some other model: FALSE

(b) The BLP model states policies for changing access rights or the creation/deletion of subjects or objects. **FALSE**

(c) In BLP there must be no information flow from **high** security level objects to **low** security level objects.

(d) The BLP model has three security properties. State them: **Answer:**

i. ss property
ii. *-property
iii. DAC property

(e) **The BellLaPadula (BL) model** (choose from: the security, management, dynamic, integrity, secure, covert, private, confidentiality, the soundness)

- only deals with confidentiality, not integrity,
- does not address management of access control,
- contains covert channels.
- is not dynamic

(f) State the *-property for BLP: **Answer:**
"*No write-down policy*"
$\forall(s, o, a) \in b$ with $a =$ *append* or *write* we must have: $f_C(s) \leq f_O(o)$.
($f_S(s) \leq f_O(o)$ is also acceptable).

(g) Justify the *-property for BLP: **Answer:**
If write-down were allowed then information would flow "upwards", in the wrong direction, violating the security level direction in the Information flow model.
Alternatively: write-down establishes covert channels, etc.

(h) What does "*tranquility*" mean in the BLP model. **Answer.**
The tranquility principle limits the applicability of BLP to systems where security levels do not change dynamically. It allows controlled copying from high security levels to low security levels via trusted subjects.
More specifically, the tranquility principle of the BLP model states that the classification of a subject or object does not change while it is being referenced. There are two forms to the tranquility principle: "strong tranquility" for which the security levels do not change during the normal operation of the system; "weak tranquility" for which the security levels may never change in such a way as to violate a defined security policy (of BLP). Weak tranquility is desirable as it allows systems to observe the principle of least privilege. That is, processes start with a low clearance level regardless of their owners clearance, and progressively accumulate higher clearance levels as actions require it.

4. This question concerns the HRU model, Biba and the Clark-Wilson model.

2+4+4+6+4=20 pts

(a) The HRU model states policies for changing access rights or the creation/deletion of subjects or objects. **TRUE**

(b) **The HRU model.** Complete the sentences: (choose from: secure, leaks, creation, removal, access rights, generation, integrity, undecidable, adds, removes, authorization, deletion, did, did not)

- The HRU model defines authorization systems that allow for the creation or deletion of subjects and objects and for changing access rights.
- An access matrix M leaks the right r if there is a command that adds the right r in a position of M that did not previously contain r.
- An access matrix M is safe with respect to the right r if no sequence of commands can transform M into a state that leaks r.
- Given an access matrix M and a right r, verifying the safety of M with respect to the right r is an undecidable problem.

(c) **The Biba model**

- In the diagram below put labels: one above the line, the other below, and up to two labels on the line. Choose from: *alter, read, write.*

- State the "*Subject low watermark property*": Subject s can read (observe) and object o at any integrity level. The new integrity level of s is $\inf\{f_S(o), f_O(o)\}$ where $4f_S(o), f_O(o)$ are the integrity levels before the operation of s, o respectively.

(d) **The Clark Wilson model.** Complete the sentences: (choose from: can, cannot, secure, responsibilities, Unconstrained Data Items (UDIs), well formed, append-only log, Constrained Data Items (CDI), duties, Transformation Procedures (TPs))

- Integrity is enforced by well formed transactions.
- Integrity is enforced by separation of duties.
- Data items governed by the security policy are called Constrained Data Items (CDI)
- Conversion of UDIs to CDIs is a critical part of the system which cannot be controlled solely by the security mechanisms in the system.
- CDIs can be manipulated by Transformation Procedures (TPs)
- All Transformation Procedures (TPs) must write to an append-only log.

(e) **The Clark-Wilson model.** Complete the sentences: (choose from: can, cannot, Unconstrained Data Items (UDIs), append-only log, Constrained Data Items (CDI), Transformation Procedures (TPs))

- Data items governed by the security policy are called *Constrained Data Items (CDI)*
- Conversion of UDIs to CDIs is a critical part of the system which *cannot* be controlled solely by the security mechanisms in the system.
- CDIs can be manipulated by *Transformation Procedures (TPs)*
- All Transformation Procedures (TPs) must write to an *append-only log.*

5. This question concerns the Chinese Wall model and Information flows model.

4+4+6+6=20 pts

(a) In the Chinese Wall model there must be no information flow **accross** objects which have datasets with **a conflict-of-interest.**

(b) The *-property for the Chinese Wall model.**Answer:**
A subject s is granted write access to an object o only if,
s **has no** *read* **access to an object** o' **with:** $y(o) \neq y(o')$ and $x(o')$ is not empty.

(c) **The Chinese Wall model.** Complete the sentences: (choose from: Company Dataset (CD), integrity, content, Conflict of Interest class (COI)) **Answer:**

- An object o is sanitized if its COI class is empty.
- *ss-property.* Subject s is granted access to an objet o only if, for all objects o' that s has had access to: either $y(o) = y(o')$ AND $y(o) \notin x(o')$.
- what does "$y(o) = y(o')$" mean: **Answer:** Objects o, o' belong to the same CD.
- what does "$y(o) \notin x(o')$" mean: **Answer:** Object o does not belong to the COI class of object o'.

(d) **Information Flow models.** Complete the sentences: (choose from: Information Flow (IF), equivocation, confidential, BellLaPadula, secure)

- In the *BelLaPadula* model, information can flow from a low security level to a high security level through access operations without any loss of *confidential* information.
- An *Information Flow (IF)* system is secure if there is no illegal information flow.
- The information flow from x to y is measured by the *equivocation* (conditional entropy) $H(x|y)$ of x, given y.

Mike Burmester