1. Partial orders.

(a) What is the smallest partial order?

(b) What is the second smallest partial order?

(c) Let $S_n$ be the \{e_1, \ldots , e_n\}. Are the following partial orders, if not explain what is necessary to make it into a partial order or why it cannot be made into a partial order?

i. the set $S_2$ and the relationship $e_1 \leq e_2, e_2 \leq e_1$.

ii. the set $S_2$ and relations $e_1 \leq e_1, e_2 \leq e_2$.

iii. the set $S_3$ and relations $e_1 \leq e_1, e_2 \leq e_2 e_3 \leq e_3 e_2 \leq e_3 e_1 \leq e_2$.

iv. the set $S_3$ and relations $e_1 \leq e_1, e_2 \leq e_2 e_3 \leq e_3 e_2 \leq e_3 e_1 \leq e_3$.

2. Lattices.

(a) Draw a hasse diagram of each of the lattices containing 2, 3, and 4 nodes respectively.

(b) Given that $e_1 \leq e_2$, under what conditions is there an edge going from $e_1$ to $e_2$ in the hasse diagram.

(c) Is an upside hasse diagram also a hasse diagram? Explain.

(d) If an inverted and non-inverted hasse diagram are both lattices, must they be the same lattice? Explain?

(e) Can a partial order always be extended into a lattice? If so, explain how. If not, explain under what conditions it can.

(f) Complete the lattice in which $a \leq b, b \leq c, a \leq d, c \leq d$ and draw its hasse diagram.

(a) If a process has read secret and unclassified, what is the minimum label it can write?
(b) If a user has a secret clearance, what labels can she read.
(c) Can a user have an unclassified clearance? What does it mean?

4. MilSec Lattices.
(a) Draw a MilSec lattice with the categories $A$, $B$, $C$ and compartments \{A\}, \{B\}, \{C\}, \{A, B\}, \{A, B, C\}.
(b) If a user reads $A$ at secret and $B$ at top secret, what level and compartment results?
(c) If a user reads $A$ at confidential and $C$ at secret, what level and compartment results?

5. Biba Low-water mark.
(a) Given the MilSec lattice in the previous problem, what is the low water mark after reads of $A$ at secret and $B$ at top secret.
(b) Given the MilSec lattice in the previous problem, what is the low water mark after reads of $a$ at secret and unclassified.

6. Chinese wall. Given two conflict of interest classes,
- one containing Ford, GM, and Toyota and
- the other containing Citibank and Chase.
(a) Could information flow from Chase to Toyota?
(b) Could information flow in the same system Toyota to Citibank?
(c) If so, describe a mechanism to prevent such a flow? If not, what prevents a flow?

(a) Give an example of what you’d want to use a Transformation Procedure for and explain why.
(b) Give an example of what you’d want to use a Integrity Verification Procedure for and explain why.
(c) Give an example of what might need careful administrative controls and describe what the controls protect.
(d) Are audit logs and authentication needed just with clark-wilson or are they needed in other security models? Explain.

8. Lipner.

(a) Can ordinary users use compile tools?
(b) Who may modify logs and why?
(c) What can system programmers do?
(d) How is separation of duty enforced?

9. Denial of Service.

(a) Consider a computer system which is available on the internet and provides 10 seconds of CPU time to access a proprietary database. If there is one CPU for this service, what would it take to jam the service?

(b) Assume that to prevent Denial of Service, the provider institutes a limit of 10 users per source IP number per day. Does this prevent denial of service?

(c) Is there something that can be done in terms of non-physical protection to prevent a physical denial of service?