1. a) Explain the operation of the Unix set-uid (suid) permission. *(6 marks)*

   b) Outline how password-based login authentication works in Unix. *(6 marks)*

   c) Sketch how a Domain and Type Enforcement mechanism, such as that used by SELinux can help safeguard against a buffer overflow vulnerability in application software. *(6 marks)*

   d) What is a Botnet? Would a virus scanner prevent the operation of a botnet? Explain your answer. *(6 marks)*

   e) The access matrix model was originally developed to help understand the meaning of access control. Explain this statement. *(6 marks)*

2. a) A simple multilevel secure database management system is to be designed. Each row in a database table is assigned a separate security-level, and subjects at any security-level may access the table (but not necessarily every record in the table). For example, consider the following Customer-information table (*custid* is primary key).

custid	*level*	Name	Company
0031	topsecret	Monty	Springfield Nuclear
1002	secret	Wolfcastle	Planet Springfield
1022	unclassified	Moe	Moe's Tavern

   Given the usual ordering between the specified security levels, a secret process may read the Moe and Wolfcastle entries but not the Monty entry, and so forth. You should assume that when a new tuple is inserted into the table it is assigned the security-level of the subject inserting it.

   i. Propose suitable multilevel security rules that govern how database operations `UPDATE` and `SELECT` should behave. *(8 marks)*

   ii. Given that primary key values are unique in a table, explain how a Trojan-Horse running at top-secret could establish a covert-channel and signal two bits of information to a subject operating at secret. Suggest how the covert channel might be closed. *(7 marks)*

   b) Describe how the MLS DBMS mechanism in Part b) of this question could form part of a Chinese-Wall policy mechanism that ensured that a user cannot access customers records from competing companies. In answering the question be sure to explain *why* the Chinese Wall is enforced. *(10 marks)*

3. Bob provides a tax-return calculation service on his website `www.bob.com`.

a) Suppose that Bob implements the tax-calculation in an Java applet `tax` that a visitor Alice to Bob's website runs (in her browser).

Write a Java security policy entry for Alice that grants Bob's applet read and write access to files in directory `file:/usr/home/alice/tax`. *(5 marks)*

Explain why Bob's applet should be signed and by whom. *(5 marks)*

b) Suppose that Alice is authorized to run a tax application `taxConsult.jar` hosted on Bob's server. Bob uses JAAS to control access. Develop a Java security policy entry for Bob that permits the application access Alice's tax files in directory `file:/usr/home/tax/alice` (on Bob's file system) when executed by Alice. *(5 marks)*

c) There is a concern about SYN-flood based denial of service attacks on `www.bob.com`. Bob uses a (flawed) implementation of SYN-cache whereby the state associated with a half-open connection is stored in the hashtable bucket indexed as $h(i.p)$, where $h()$ is a one-way hash function, i is the IP address of `www.bob.com` and p is the requested port on `www.bob.com`. Describe how an attacker can still carry out a SYN flood on this host and outline how the SYN-cache scheme should have been implemented. *(10 marks)*