1.(a)

m[p[0]][1] = p[1]

(b) In words, the backward pointer of the heap that p[0] point to ( m[p[0][1] ) should point to p[1] which is the backward pointer of the newly freed heap. As a result, the backward pointer m[p[0]][1] will point to the m[p[1]]

2.(a) access can be granted to BigOil documents as Jill has just started work, he has no access to the BigOil competitor. In other words:

s (Jill) can access y(c) (BigOil) as the following condition is satisfied: for all c’ that s can read, y(c) is not x(c’)

(b) access cannot be granted to PeakOil documents as Jill now has access to BigOld document. The rule “subjects cannot work for their clients’ competitor” applies.

(c) As the \*-Property stated, Jill can write to WarBucksBank only if Jill cannot read any WarBucksBank competitors. Since WarBucksBank has no competitor, Jill can write to WarBuckBank

3.(a) Since every administrator has a smartcard, the password is only issued for people in charged so the system can log all activities of the administrator. Only the administrator should know the password

(b) Smart card can be hack easily, especially for such an important system like voting system. People who belongs to class 3 attackers can invest to hack the smartcard. Smart card is slow, it cannot implement many more secured protocol

(c) It is not mentioned that the sequence will be terminated after a certain failed attempt, brute force attack can be applied but the efficiency depends on the length and complexity of the password (how many bits are set to 1). Generally, such brute force attack can be applied for smart card.

4.(a) Overwriting the code requires attacks like buffer overflow. However, GNU+Linux has security protocol that randomly moves starting address to different location for processes and have a canary to check the return address. Therefore, in the worst case, buffer overflow only overwrite a lot of variables (since buffer overflow may still occur in such system). It is likely that it will overwrite the canary as well but it wont be directed to execute malicious code.

(b) A smart card contains a very small program and has no protection for memory. When it is booted up, only a string “vsn 0.97” appears. Windows are much more complex and use segments and paging. Segments are protected from each other so basically the glitch which increase the buf[i] will not be allowed to access data outside of its own segment. Besides, a processing speed on a window machine is much faster, make it more difficult to create a pulse/glitch when the while loop is checked.