CS4440/7440 Malware Analysis & Defense Take-home Quiz, 4/21/2016 Name:

Directions. Answer each question in the space provided. Turn in this exam by class time (3:00pm CST) on Monday, 24th, 2017.

Question 1. A common code transformation employed by polymorphic and metamorphic viruses is to take a chunk of code that involves a branch condition and to rewrite the code by reversing the branch condition. The resulting code is semantically equivalent, but looks very different. Consider the following code sequence:

```
L1:   inst1
      inst2
      cmp %eax,%ecx
      blt L2      ; branch less than
      inst3
      inst4
      inst5
      br L3
L2:   inst6
      inst7
      inst8
L3:   inst9
```

Rewrite the above code by reversing the branch condition. The appropriate opcode is **bge** (branch greater than or equal). The resulting code sshould be semantically equivalent to the sequence above.

CS4440/7440 Malware Analysis & Defense Take-home Quiz, 4/21/2016 Name:

Directions. Answer each question in the space provided. Turn in this exam by class time (3:00pm CST) on Monday, 24th, 2017.

Question 2. Give two examples of evolutionary heuristics used by metamorphic engines (other than any mentioned in this quiz).

Question 3. Why don't viruses use strong encryption techniques (AES or DES)?

CS4440/7440 Malware Analysis & Defense Take-home Quiz, 4/21/2016 Name:

Directions. Answer each question in the space provided. Turn in this exam by class time (3:00pm CST) on Monday, 24th, 2017.

Question 4. The Zmist polymorphic virus, discussed by Ször and Ferrie in "Hunting for Metamorphic", does not alter the entry point of the virus. It uses an entry-point obscuring (EPO) technique. However, Ször and Ferrie point out that this technique can cause a problem for the virus. What is the problem?

Question 5. Both polymorphic and metamorphic viruses involve the mutation of the virus code. Still, there is a one principal difference between the two forms of viruses. What is it?