I (30)	
II (40)	
III (30)	
Bonus (5)	
Total	

Test 2
2015 – CSCE 201

Note: All materials that were covered during the Fall 2015 semester may be in the final exam. This test is just a sample wrt. type of questions and difficulties.

Answer the following questions. Be brief and precise!

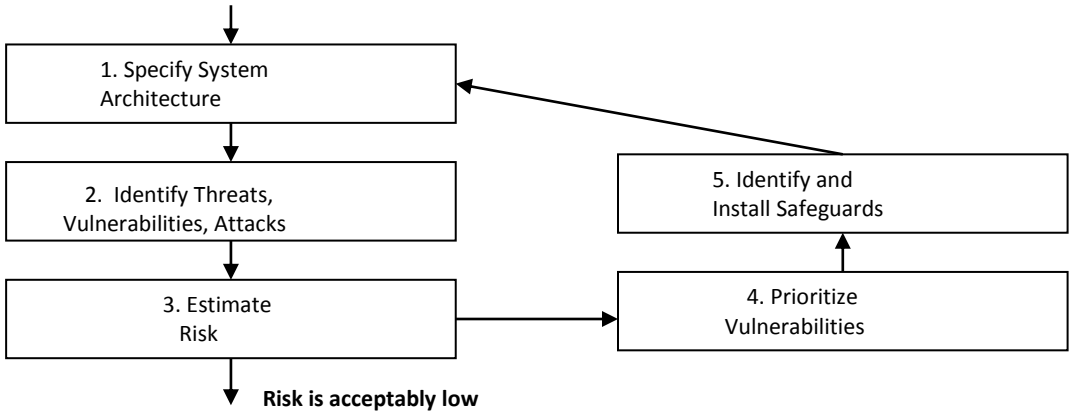
I. 30 points

1. (10) Strong security often comes at the cost of reduced functionality and ease of use. Describe how password-based authentication may reduce ease of use and functionality.

- Ease of use:

- Functionality:

2. (20)



Consider the risk assessment chart above. Discuss each step in the chart in the context of cyber security risk for your personal computer.

1.

2.

3.

4.

5.

What does it mean that the risk is "acceptably low?"

II. 40 points *Short answers*

1. (20) Asymmetric (public) key encryption supports strong confidentiality and authentication. However, none of the current public key encrypotion methods are unbreakable.
    - Explain what does it mean that an encryption method is computationally secure.

    - Consider the case when a malicious attacker gains access to an authorized user's private key. How will it effect the strength of the authentication provided by public key encryption?

2. (20) Your best friend, knowing that you are taking a cyber security course, asks your help. Lately, it takes a longer to boot his system than previously, and occasionally his system becomes unresponsive. Most of his activities are via web browser.
    - Describe three main steps you would perform to identify and solve the problem of your friend's computer.

    - Describe three recommendations that your friend should follow to reduce the risk of future compromises.

III. 30 points *Exercises*

1. (20) As a newly appointed system security officer, you have decided to implement intrusion detection (IDS) capabilities You have decided to go with an anomaly-based IDS, that looks for deviation from normal usage.
    - Explain the advantages and disadvantages of your choice with respect to false positives and false negatives.

    - Assume that you manage to set up your anomaly-based IDS that has acceptable level of accuracy. What are concerns with respect to your IDS that you need to address as your organization grows?

2. *(10)* You are purchasing a new laptop. You identified two models that provide similar capabilities. However, one of the two models support biometrics-based authentication, while the other one permits password-based authentication only. The model with biometrics is $500.00 more expensive than the other. Which laptop would you purchase (you have the necessary funds to purchase either of them but you want to use your money smartly)? Why?

Bonus question (5 points)
Describe the privacy risk of social networks.