

Name: _____

USC ID: _____

CSci 530 Midterm Exam

Fall 2013

Instructions:

Show all work. No electronic devices are allowed. This exam is open book, open notes. You have **100 minutes** to complete the exam.

Please prepare your answers on separate sheets of paper. You may write your answers on the sheet of paper with the question (front and back). If you need more space, please attach a separate sheet of paper to the page with the particular question. **Do NOT extend your answer on the back of the sheet for a different question, and do NOT use the same extra sheet of paper to answer more than one question.** The exam will be split apart for grading by different people, and if part of your answer for one question appears on a page given to a different grade because the sheet contains parts of the answer to more than one question, then you will NOT receive credit for that part of the answer not seen by the grader. In particular, **each numbered questions must appear on separate pieces of paper so that the exam can be split for grading.**

Be sure to include your **name** and **USC ID** number **on each page**.

There are **100 points** in all and **3 questions**.

	Q1	Q2	Q3		Total Score
Score					

Name: _____

USC ID: _____

1. **(20 points) Policy Management** – For each of the following methods of representing policy, match the method with the **major** characteristics or relevant terms discussed in class. This is **not** a one-to-one mapping. So more than one approach may match a characteristic or term, and a single characteristic or term may also match more than one approach. We are looking for specific characteristics and terms, for which you will receive credit. If you list what is a minor characteristic, while you will not lose credit, you will not get credit either. You will lose a point if you associated a term with a characteristic that does not apply to the method. There are more blanks in the page below than actual correct answers, so you do not need to fill in all the blanks.

1. Bell La Padula
2. Biba
3. Role-Based Access Control
4. Access Control List
5. Capability List
6. Access Matrix

a) Associated with object

b) Separation of roles

c) Identity based

d) Star Property

e) Integrity

f) Mandatory Access Control

g) Associated with user

h) Often Sparsely Filled

Name: _____

USC ID: _____

2. (40 points) Cryptography and Key Management

Answer the following questions regarding cryptography and key management:

- [illegible]

USC ID: _____

You have been hired by a smartphone maker to add biometric authentication to their smartphone, in answer to customer demand caused by the fingerprint reader on the new iPhone. Your new employer is insisting that this integration be done right, not simply as a gimmick that can be readily defeated. Because you have taken a security course at USC, you understand some of the issues surrounding policy and multi-factor-authentication, and you are ready to design a solution. In answering the questions that follow, put yourself in the shoes of an adversary, and think about how they get access to a phone, and what kinds of things they might be capable of doing, then design your approach to mitigate the impact of such attacks.

- 4

Name: _____

USC ID: _____

- c. How will you support authentication by the user to basic services on the internet, and will the user need to authenticate each time. Your answer to this described your solution to single-sign-on. (5 points)

- d. For internet services requiring stronger authentication, describe some approaches that support multi-factor authentication. In your design, which factors are used, and at what point in the users experience are each factor checked? (15 points - answer on back of page)