Name: _______________________ **USC ID:** _______________________

CSci 530 Midterm Exam

Fall 2018

Instructions:

Show all work. This exam is open book, open notes. You may use electronic devices if your references materials are stored on the device, and as long as communication is disabled (e.g. Airplane mode). You may not use your device for communications and you may not use it to retrieve information from the web or files stored elsewhere. 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) Identity and Authentication -** For each of the following methods of identification or authentication, 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 method may match a characteristic or term, and a single characteristic or term may also match more than one method. 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. Kerberos Authentication
   2. Needham and Schroeder
   3. Passwords
   4. Smartcard or chip card or EMV card
   5. Digital Signature (annotate your answer with your assumption)
   6. Shibboleth
   7. The fingerprint sensor on a smartphone
   8. Facebook Connect

   a) Something you know
   _____ _____ _____ _____ _____ Annotation if necessary: _____________

   b) Something you have
   _____ _____ _____ _____ _____ Annotation if necessary: _____________

   c) Something about you
   _____ _____ _____ _____ _____ Annotation if necessary: _____________

   d) Uses a trusted third party
   _____ _____ _____ _____ _____ Annotation if necessary: _____________

   e) Requires specialized hardware to implement
   _____ _____ _____ _____ _____ Annotation if necessary: _____________

   f) Supports single sign on
   _____ _____ _____ _____ _____ Annotation if necessary: _____________

   g) Implements federated identity management
   _____ _____ _____ _____ _____ Annotation if necessary: _____________

For digital signatures, these may be implemented using private keys stored in various ways. Annotate any answer(5) with your comment about where the private key is stored.

Name: ______________________ **USC ID:** ______________________

2. (40 points) Short and medium length answers

a. Explain why low privileged users are allowed to write to highly classified documents in the Bell-Lapdula access control model. (10 points)

b. Describe the advantages of using the Cipher-block chaining (CBC) mode of operation for AES (Advanced Encryption Standard) as compared with using AES as a block cipher (also known as Electronic code book mode - ECB). In answering, be sure to mention the situations in which an adversary might be able to obtain information from or create or modify messages without knowledge of the encryption key.
(30 points answer on back of page)

Name: ______________________ **USC ID:** ______________________

3. (40 points) Design problem – The Most Recent Facebook Data Breach

Last week Facebook announced yet another serious data breach in their system that was caused by the introduction of new features that allow and individual to see how their own profile would appear when viewed by another Facebook user. At first glance, this would seem to be a useful feature that would enable greater awareness of privacy by letting users readily determine what information in their accounts is visible to others. Unfortunately, the implementation of this feature created a significant security vulnerability in itself, one that Facebook claims to have since fixed.

A) The faulty implementation: The easiest way to implement this feature, called "view as", was to allow the processes attempting to view the profile as another user to assume the identity of that user – and then to execute the code to view the requesting users profile. What could go wrong? (this is a rhetorical question, while you can answer if you like, I don't require an answer at this time). The question that I am posing to you is how this assumption of identity relates to the concept of delegation of authority that we discussed in class, whether as a proxy, or as providing credentials or using roles from the digital distributed system security architecture? So that you don't go off in the wrong direction here I will give you a hint that this is NOT really delegation, but I want you to tell me why it is not. (15 points)

B) The data breach occurred because users viewing the profile as another user were able to capture the credentials used by the process, and reuse those credentials to view anything viewable by the "viewed as" user, not just the viewing user's profile. Can you suggest some changes that might be needed to prevent mis-use of the credentials? (15 points answer on back of page).

C) Discuss your thoughts regarding how “credentials” might have been captured, and some of the problems in how such credentials are stored and communicated that could have enabled this breach. I don’ t expect or require you to know precisely what occurred, but consider how credentials are stored in various web-based federated identity management systems (e.g. our coverage of Passport) and discuss how that kinds of credential management could lead to the problems exposed in this breach. (10 points)