Assignment 1 – Due Tuesday, September 11

1. Find a news story of a recent security incident that involved a malicious attacker (that shouldn't be hard!), and describe what happened. Your description should include a statement about each of the "big three" security goals, indicating whether it was violated (and if it was, *how* it was violated). Also speculate on what type of attacker was involved and what the attacker's motive may have been.

2. Consider the following scenario: You're sitting in a coffee shop, using their WiFi, and want to buy something from Amazon. The following "conversation" shows a direct use of public-key cryptography in an attempt to have a secure conversation (the second and third messages contain the actual data that is described).

   ```
   Send: Hi amazon.com, I'd like to send my credit card number to you
   Received: Hi - I'm amazon.com, and here's my RSA public key
   Send: Here's my credit card number, encrypted with your public key
   ```

   What is wrong with this? Be very specific about the vulnerability, and describe how an attacker can exploit the vulnerability. How can this vulnerability be removed (a very specific technology from our cryptography overview can fix this)?

3. When Dropbox stores files, it first breaks the file up into 4 MB blocks, and stores the blocks in what's called a content-addressable file system: the block is hashed using the SHA-256 cryptographic hash function, and the resulting hash value is used as the "name" of that block in the storage system. The file itself is then the list of hash values for each block of the file. The advantage of this is that if many users store the same block (or the same file) then there is only *one* copy stored on the servers for all users — duplicated data is naturally located and not stored multiple times! What is the danger of storing files/blocks this way? Is this a realistic danger? Include a basic mathematical analysis to justify your answer, and use proper terminology.

4. Consider the following set of subjects and objects in the Bell-LaPadula model, with clearances and classifications as shown (C, S, and TS stand for "Classified", "Secret" and "Top Secret"):

Subject	Clearance
Andy	(C, {TOYS})
Woody	(S, {SNAKES, TOYS})
Buzz	(TS, {SPACE, TOYS})

Object	MAC Label
ToyInventory	(C, {TOYS})
SnakeTypes	(S, {SNAKES})
SpaceMissions	(TS, {SPACE,SNAKES,TOYS})

(a) Write out an access-control matrix that includes all three subjects and all three objects, indicating read and write permissions using letters "R" and "W". Assume that all subjects are operating at their maximum clearance.

(b) Which objects can Woody read?

(c) Is there a file classification/label that would allow Buzz to write to it, and Woody to read from it? Why? Is there a way around this?

5. This is an expanded version of the in-class example of the Chinese Wall model:

Conflict of Interest Classes
CoIClass_1 = {Enron, Exxon, Mobil}
CoIClass_2 = {Amazon, Barnes and Noble}
CoIClass_3 = {Target, WalMart}
CoIClass_4 = {American, Delta, Southwest}

Objects
Object_1 Label: $\langle$Enron,$\text{ColClass}_1\rangle$
Object_2 Label: $\langle$Mobil,$\text{ColClass}_1\rangle$
Object_3 Label: $\langle$Amazon,$\text{ColClass}_2\rangle$
Object_4 Label: $\langle$Target,$\text{ColClass}_3\rangle$
Object_5 Label: $\langle$WalMart,$\text{ColClass}_3\rangle$
Object_6 Label: $\langle$Target,$\text{ColClass}_3\rangle$
Object_7 Label: $\langle$American,$\text{ColClass}_4\rangle$
Object_8 Label: $\langle$Delta,$\text{ColClass}_4\rangle$

(a) If I have accessed Object_2 and Object_4, what objects would I be allowed to access now? Explain your reasoning.

(b) Is there an object that I can now access which changes the objects that I will have access to in the future (assume no new objects are created)? Explain your answer.

6. The "Bandit" wargame on `overthewire.org` consists of a sequence of challenges to test your skill with basic Linux command-line usage. For this question, solve up through Level 5 of the Bandit wargame (getting to Level 6), which will require you to demonstrate skills that are vital for future hands-on exercises in this class (logging in with SSH, examining files, working with directories, working with unusual file names and hidden files, etc.). Document how you solved the challenges by providing a one or two sentence description saying what you did for each level. [*Reminder: Figure these challenges out yourself. Do* ***not*** *search for solutions online, or ask others for solutions.*] Note: If you solve the first *20 levels*, you will receive 5 points extra credit.

7. Log in to `csc581.uncg.edu` using the login credentials you are given in class. Use the "secret directory" trick to create a directory that contains a text file that only someone who knows the name of the directory can access. In your homework submission, write down the name of the secret directory so I can find the file. The text file can contain anything — a favorite movie quote, fun fact, whatever — amuse me, but keep it inoffensive.