**Assignment 3**

**Due: March 31st**

1. **( 10 points) For the given Access matrix below:**
2. **Draw access control lists for s1, s2 and s3**

f1 => [ (s2: o,r,w) ]

f2 => [ (s1: o,r,w), (s2: r), (s3: r) ]

f3 => [ (s1: o,r,w), (s3: r) ]

f4 => [ (s3: o,r,w) ]

f5 => [ (s1: w), (s2: o,r,w), (s3: r) ]

f6 => [ (s3: o,r,w) ]

**b. Draw capability lists for s1, s2 and s3**

s1 => [ (f2: o,r,w), (f3: o,r,w), (f5: w) ]

s2 => [ (f1: o,r,w), (f2: r), (f5: o,r,w) ]  
 s3 => [ (f2: r), (f3: r), (f4: o,r,w), (f5: r), (f6: o,r,w) ]

1. **(12 points) Which of these is an example capability system, and which is an ACL-based approach?**
2. **A wedding ceremony has a list of invited guests.**

This is an ACL based approach, only invited guests are allowed to enter.

1. **Your office has card-swipe access, where the magnetic code on the card is matched against a list of employees.**

This is an ACL based approach, only employees in the system are allowed entry.

1. **You give your car keys to your roommate.**

This is a capability approach. There is no list, the authorized person is whoever holds the key.

1. **Your car has a parking permit specifying where you're allowed to park.**

This is a capability approach. There is no list, anyone with access can park anywhere.

1. **(10 points) Capabilities could be described as an authorization mechanism that is based on “something you have”. How might we analogously describe the following mechanisms for controlling access to confidential information?**
2. **Access control lists.**

Access control lists can be described as a mechanism for controlling access to confidential information based on “need to know” approach. If something is deemed necessary for someone to know, that person gets put on a list of people who can access the information.

**b. Encryption.**

Similarly to capability, encryption can be described as a mechanism for controlling access to confidential information based on “something you have” as having a key or algorithm can allow the user to decipher the encrypted message.

1. **(10 Points)** 
   1. **Suggest a way of implementing protection domains using access control lists.**

Once a certain condition by a user is met they can be automatically added to the ACL for that particular subject. One example is a study system similar to dualingo where a user is given access to further levels after completing certain challenges.

* 1. **Suggest a way of implementing protection domains using capability tickets.**

Using capability tickets a user can be granted singular access by the system. An example of something like this is a coupon for a free haircut, a user is given one time access to a service. Furthermore the user can give away this access to someone else.

1. **(14 points) Discuss the strengths and weaknesses of implementing an access matrix using capabilities that are associated with domains.** The main strengths of implementing such a system is a. the easy of authenticating the capability and b. the fact that these capabilities can be moved from domain to domain without much hassle. The main drawback of such a system however is the fact that it is rather difficult to remove the capability. This downside gets solved by implementing the system with access matrix, but this has its own downside of heightened strain on the system while checking authenticity of a request.
2. **(14 Points) A secure biometrics system authenticates the user based on his/her physiological (e.g., fingerprint, face, voice) or behavioral (e.g., gait, hand gesture, keystroke) traits. Typically, a binary classification model will be developed to generate predicted probabilities based on the input information. Please explain:**
3. **How do you convert the predicted probabilities into class predictions?**

To create a prediction a computer model must be trained to properly recognize the biometric parameters of whoever it needs to give access to. This could include gait, typing pattern, retina or fingerprint. With some it can take a longer time, with others it could be as simple as a one-time scan. Afterwards this program will be able to recognize the one utilizing the scan with hopefully satisfactory accuracy.

**b. How do you generate the ROC curve when you want to evaluate your system performance?**

To generate a Receiver Operating Characteristic curve all we have to do is plot the true positive against he false positive rate of the system. Here it would show the range of sensitivity the system can achieve on different settings.

\

1. **(10 Points) A security company proposes the following authentication scheme using a hash function: the client and the server both maintain a secret string, which is initialized to some 16-word random value. Whenever the client wants to authenticate itself, the server will generate a random challenge 𝑟𝑟, of length 16 words, and send it to the client. The client replies ℎ(𝑠𝑠 ‖ 𝑟𝑟) and the server will verify its value. If it is a match, both sides will update 𝑠𝑠 by appending 𝑟𝑟 to it (i.e., 𝑠𝑠 ← 𝑠𝑠 ‖ 𝑟𝑟). Otherwise, the server rejects the client and leaves 𝑠𝑠 unchanged. After a cursory look, an experienced attacker says:” They’d better not to use MD family. Its only good if ℎ is a random oracle.”** 
   1. **(8 points) Explain why an MD family like MD4 or MD5 is not a good candidate. You may ignore the padding.**

Both MD4 and MD5 have been found to be prone to collisions, making them susceptible to hash length attacks. Due to these finding the Message Digest family algorithms are now seen as rather weak and ineffective methods of encrypting information.

* 1. **(2 points) Explain why a RO is secure.**

Random Oracle is as it says in the name, random. It has a desirable property that all possible values have an equal chance to be the correct value, not only that but all of its parts are completely independent, thus making it more resistant to cracking attempts.