Homework#1 [25/100 points]

Assigned: January 31, 2018
Due: February 16, 2018

Task 1 - Cybersecurity Breaches [13 points]

1) [5 points] The story filling headlines for years surrounds high-profile cyber-attacks and the resulting data breaches against private and public sectors. Just last year (2017), we have seen several industry-leading companies that have been victimized. The followings are some of the incidents that make news headlines.

   - Equifax Breach 2017
   - Uber Data Breach
   - NHS Cyber attack

   For each incident listed above, summarize what happened by identifying the threats, vulnerabilities and the attacks. What were the major consequences/impact of the event? Then, classify each of the acts as violation of confidentiality, of integrity, or availability, or some combination thereof. Also, what have we learned from each incident? What types of security controls can help the company prevent/mitigate such an attack? (Please do not limit your readings only to the links provided.)

2) [4 points] The principle of psychological acceptability aims to minimize the burden of security mechanisms enforcement on humans. Find one real-world attack that exploit the vulnerability that is associated to this principle (i.e. when human create end-runs around the mechanisms). Proper citations to sources must be provided. Also, for the case that you refer to, can the principle be applied in the design or the operation of such system, why or why not?

3) [4 points] We hear of new attacks and have seen so many repeated story on security breaches, even to the industry-leading companies. In your opinion, what do you think are the leading causes for continuing security breaches, especially for the ones that can be prevented? And do you agree or disagree with the argument made by Ross Anderson in his article titled 'Why Cryptosystems Fail?'? Give reasons for your answer.

Task 2 – Password Cracking Program [12 points]

Note: *After completing this part of the assignment you should 1) understand how to securely store passwords, 2) how to derive hashed passwords in a secure manner and 3) know how to generate a moderately strong password.*

4) [8 points] Write a password cracking program

You will play a role of an adversary who have obtained the stolen hashed password of an e-commerce website's customers. The stolen password file is pswd.txt provided. The format of each line of the file is:

username : salt : iterations : hashed password.

Refer to https://www.owasp.org/index.php/Hashing_Java on how to derive hashed passwords in pswd.txt. The hashed password and the salt (32-byte array) that you obtained were encoded with Base64 (https://docs.oracle.com/javase/8/docs/api/java/util/Base64.html). You would need to decode the salt first before using.

Write a **Java program** to determine the plaintext password of the given hashed password. Your task is to crack as many passwords as possible. Your program should print on the screen the username and the plaintext password, in the format:

username::plaintext password

A point will be given for each password cracked. You need to submit the java program and a readme.txt file explaining how to run the code. You may run a dictionary attack and hybrid attack on the passwords, but the link to the dictionary or the file itself needs to also be submitted. If you can crack more than the points assigned for this question, the points will be added to your assignment as a bonus.

You need to submit all your source code in one zip file. Your Java program should be just the Java source code (not your .class files or Eclipse workspaces). You should include the following comment section in all your files.

```
/*
 * Name: [Your name]
 * Description: [Description of the program]
*/
```

5) [4 points] Document your approach. Explain the algorithm that you use in your password cracking program.

This homework is to be done individually. You must write your answer *independently*.

To submit an assignment, log into home.nyu.edu, go to Academic -> NYU Classes -> Special Topic: Practical Computer Security -> Assignments, and upload your answer in PDF format/zip file. Make sure that you 'submit' the assignment before the deadline.

Late homework will be marked down by 20% for every day of lateness.