School of Computing & Information Technology

CSCI262/CSCI862 System Security
Spring 2018

Assignment 2 (15 marks, worth 10%)

Due 11:55pm Monday 24^{th} September 2018.

Make sure you include referencing for answers where it would obviously be needed.

1. You have two puzzles with parameters as follows:

   `Puzzle A:` One sub–puzzles. $k = 6$.

   `Puzzle B:` Eight sub-puzzles. $k = 3$.

   You should provide, for both cases other than part (b), the following:

   (a) The distribution of the number of cases that require each number of hashes. **1 Mark**

   (b) Explain the method you used to obtain your distributions. Don't go into too many details or show working, it's more "I wrote a C++ program to ... and then using ... I ...". **0.5 Mark**

   (c) A graph of the distribution of the data above. **0.5 Mark**

   (d) The average number of hashes needed. **0.5 Mark**

   (e) The standard deviation for the distribution of the number of hashes needed. **0.5 Mark**

   You should assume that if there are N possible solutions you check the N^{th} by hashing even if all others have failed and there has to be a solution.

   It's okay to submit an Excel or similar file with the distributions and graphs in them.

2. Which general security principle is violated in the following pseudo-code? Modify the pseudo-code to fix the potential security problem. **1 Mark**

```
permit = CheckAccess()
IF (permit  ==  Access_Denied)
     Print "Access Denied"
ELSE
     Print "Access Granted"
     Run Function()
```

3. Consider that the incidence of viral attachments in email messages in 1 in 800. Your malware checker will correctly identify a message as viral 95% of the time. Your malware checker will correctly identify a message as non–viral 95% of the time. Your malware checker has just flagged a message as being malware. What is the probability that the message is actually okay? Justify your answer using Bayes theorem. **1 Mark**

4. Describe, in your own words, a specific instance of an insider placing malware within a system. You should describe the type of malware placed, the expected likely impact, and some details regarding the outcome. This is not meaning a hypothetical scenario you have made up, find an actual real world example. **2 Marks**

5. In the context of phishing, list 8 points that can be used in checking the legitimacy of an email. Justify why each is appropriate as an indicator. Note that some points could relate to characteristics of legitimate messages, and others could be indicators of a phishing message. **2 Marks**

6. Every hour the worm **X** spreads from each infected computer to one previously uninfected computers. In answering these questions you should explain how you determined your answers.

   (a) Give a table showing the number of infected computers at each hour across a 24 hour period. At time $t = 0$ the number of **X** infected computers is $N = 1$. **0.5 Mark**

   (b) By time $t = 6.5$ a counter worm **W** has been developed and it is deployed on one infected computer. **W** removes malware **X** from any host **W** is on. The counter worm **W** spreads slightly more quickly than **X**, with each **W** spreading to two **X** infected hosts each hour, provided such hosts are available.

   Provide another table showing the spread of **W** and the impact on **X** across an appropriate time frame, starting from $t = 0$ again.

   Note the offset in time means that at $t = 6.5$ the number of **X** infected computers reduces by 1, so the spread of $t = 7$ will be slightly smaller than before. Overall the number of **X** infected computers will go up on the hour, and down on the half hour. **1.5 Marks**

   (c) Graph the two cases against each other, clearly indicating on it where $N = 0$. **0.5 Mark**

   (d) Assume that at time $t = 9$, **X** evolves to spread to three uninfected computers each hour. What subsequently happens? **0.5 Mark**

7. Briefly describe, in your own words, each of the following. Be sure to specify the domain and nature of each.

   (a) An XML bomb. **0.5 Mark**

   (b) BlueSmack. **0.5 Mark**

   (c) Mydoom. **0.5 Mark**

   (d) Torpig. **0.5 Mark**

8. Explain what BHO's are and how they have been used maliciously. **1 Mark**

Notes on submission

Please submit a single zip file with all your assignment files in it. Do not include subdirectories, that slows down marking!

1. The deadline is 11:55pm Monday 24^{th} September 2018.
2. Submission is via Moodle.
3. Late submissions will be marked with a 25% deduction for each day, including days over the weekend.
4. Submissions more than three days late will not be marked, unless an extension has been granted.
5. If you need an extension apply through SOLS, if possible **before** the assignment deadline.
6. Plagiarism is treated seriously. Students involved will likely receive zero.