Final Review Sheet
ENEE 457
Fall 2021

Static Analysis:

Consider the following code snippet on which we would like to perform a taint analysis. Type qualifiers are represented by capital letters: A, B, C, D.

```
1   int printf(A char *fmt, ..);
2
3   int main(B int argc, C char *argv[]) {
4           if (argc < 2 || argc > 2){
5                   printf("enter 1 string only");
6                   return 0; }
7           D char *mystring;
8           if (!strcmp(argv[1], "Hello")){
9                   mystring = argv[1];
10          }else{
11                  mystring = "Goodbye";
12                  printf(mystring);
13          }
14          return 0;
15  }
```

1. Identify all the sources and sinks in the code snippet and determine the corresponding settings for the type qualifiers.

2. List all of the constraints on the type qualifiers.

3. Is there a vulnerability in the above code? Is there a solution for the undetermined type qualifiers that satisfies all the constraints? If there is no vulnerability and no solution, it means that our taint analysis has produced a false positive. How can the taint analysis be modified so that the false positive is removed?

Malware:

1. What is the difference between a virus and a worm?

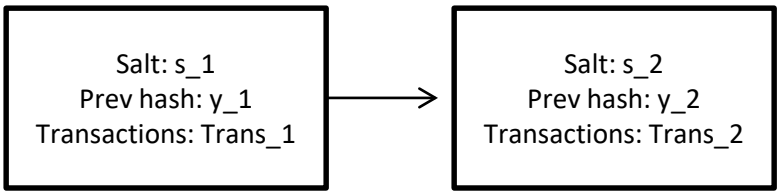
2. What is the difference between a polymorphic and metamorphic virus?

3. What is a virus signature?

4. What is a crypting service?

Bitcoin

Assume the current Blockchain looks like the following and that the current difficulty level is n.



In order to successfully mine the next block (Block 2), a miner needs to find a salt s_3 such that h(s_3, x) = y_3, for x,y_3 of a specific form. What is x in the above example? What is the form of y_3?

Differential Privacy

Show that mechanism M defined below is not differentially private, using the definition of differential privacy and the databases D and D' defined below.

M chooses a value z uniformly at random from $\{-1, 0, 1\}$ and returns the number of UMD students in the database plus z.

Name	UMD Student
Alice	0
Bob	0
Charlie	0
Daniel	1
Edgar	0

Name	UMD Student
Alice	0
Bob	0
Charlie	0
Edgar	0

Dining Cryptographers/MixNets

Using pseudocode, specify how the Dining Cryptographers protocol would work for 4 parties. What happens if two parties collude? Can they combine forces to learn which of the other two parties is broadcasting in a given round? Why or why not?

Password Hashing

Consider using Hellman's table to invert the function $f(x) := x^3 \ mod\ 11$ where $x \in \{1, \dots, 10\}$

Let $m = 4, t = 3$.

What would be the end points for the following start points:

$$SP_1 = 3, SP_2 = 6, SP_3 = 2, SP_4 = 5$$

Which values of $y = f(x)$ could you invert using the table?

Explain the procedure for using the table to invert $y = 4$?

Network Security

Describe an attack that requires both packet sniffing and spoofing

Describe two tools used for packet sniffing and spoofing.

Describe two attacks on the TCP protocol

What is the significance of the sequence number and acknowledgement number in a TCP header?

What is a DNS server and how is it used?

What is meant by the term DNS cache poisoning?

What would the following iptables command do:

iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

Name three chains that are used in iptables. What is each one used for?

Adversarial machine learning

Recall that the machine learning process has two phases: Training and Inference (Testing). What type of adversarial attack can occur during each of these phases? Explain the differences between the two types of attacks and their goals.