Fall 2022 Final Review Sheet
ENEE 457

The final exam will be held in our regular classroom EGR 0108 on Friday, Dec. 16, 2022 from 8-10am. It will cover the material from Lectures 11-17, as well as the material from In Class Labs 1-4 (see lecture notes and in-class labs here: `https://user.eng.umd.edu/~danadach/Security_Fall_22/lectures.html`).

1. **Public Key Cryptography**

   (a) Choose one of the following two problems:

   - Let (N, e) be the public key for textbook RSA, where $N = 3 \cdot 13 = 39$ and $e = 5$. Find the corresponding secret key (N, d). Then encrypt the message $m = 32 \mod 39$, obtaining some ciphertext c. Decrypt c to recover m. Do the computations by hand and show your work.

     Hint: To speed up your computations, use the following facts: $32 = 2^5$, $(2)^5 \equiv -7 \mod 39$ and $(2)^{15} \equiv 8 \mod 39$.

   - Consider the subgroup of Z_{23}^* consisting of quadratic residues modulo 23. This group consists of the following elements: $\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$. We choose $g = 3$ to be the generator of the subgroup. Let $x = 7$ and $y = 6$. Show the messages exchanged in Diffie-Hellman key exchange, as well as the obtained shared key. Do the computations by hand and show your work.

     Hint: To speed up your computations, use the fact that $3^3 = 4 \mod 23$, $2^6 = -5 \mod 23$, $(-5)^2 \equiv 2 \mod 23$ and $-45 \equiv 1 \mod 23$.

   (b) Assume a client and server run the Diffie-Hellman key exchange protocol to obtain a shared key k. Future messages from both server and client will be encrypted using an authenticated symmetric key encryption scheme with key k.
   Explain why the above method of communication is insecure, and how this issue is addressed in the TLS protocol.

2. **Static Analysis**

(a) Briefly explain why static analysis that achieves perfect completeness and soundness is impossible.

(b) 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, E.

```
1   int printf(A char *fmt, ..);
2   B char *fgets(..);
3
4
5   int main () {
6           C char *mystring = fgets(.., network_fd);
7           D char *mystring2 = mystring;
8           E char *mystring3 = ‘‘Hello World’’;
9           mystring2 = mystring3;
10          printf(mystring2);
11          return 0;
12  }
```

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

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

iii. 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?

3. **Malware**

(a) What is the difference between a virus and a worm?

(b) What is the difference between a polymorphic and metamorphic virus?

(c) What is a virus signature?

(d) What is a crypting service?

4. **Password Hashing**

Consider using Hellman's table to invert the function $f(x) := x^3 \mod 11$ where $x \in \{1, \ldots, 10\}$. 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? Justify your answer. Explain the procedure for using the table to invert $y = 4$.

5. **Network Security**

(a) Describe an attack that requires both packet sniffing and spoofing

(b) Describe two tools used for packet sniffing and spoofing.

(c) Describe two attacks on the TCP protocol

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

(e) What is a DNS server and how is it used?

(f) What is meant by the term DNS cache poisoning?

(g) What would the following iptables command do:

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

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

6. **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?

7. **Adversarial Machine Learning**

Assume we have the following machine learning model: Classify input $(x_1, x_2, x_3, x_4) \in \mathbb{R}^4$ as a "yes" instance if $w_1 \cdot x_1 + w_2 \cdot x_2 + w_3 \cdot x_3 + w_4 \cdot x_4 \geq 1$, where $(w_1, w_2, w_3, w_4) \in \mathbb{R}^4$ is a fixed vector of weights. Otherwise classify input (x_1, x_2, x_3, x_4) as a "no" instance.

Given a "yes" instance (x_1, x_2, x_3, x_4) such that $w_1 \cdot x_1 + w_2 \cdot x_2 + w_3 \cdot x_3 + w_4 \cdot x_4 = 1.5$, how could one perturb (x_1, x_2, x_3, x_4) by adding the smallest magnitude error so that the resulting input (x'_1, x'_2, x'_3, x'_4) is classified as a "no" instance by the model?

Hint: To answer the question, you will need to find the gradient of the function $f(x_1, x_2, x_3, x_4) = w_1 \cdot x_1 + w_2 \cdot x_2 + w_3 \cdot x_3 + w_4 \cdot x_4$.