CSCI 345 – Computer and Network Security

Final review, Spring 2018

General information:

1. Final exam: Tuesday, May 1, 8-11 am
2. Cumulative final
3. You may bring a cheat sheet

What to study (chapters are from your textbook “Security in Computing”):

1. Ch. 1:
   a. CIA
   b. Vulnerabilities
   c. Controls
2. Ch. 2:
   a. Authentication
   b. True / False positives / negatives
   c. Access control
   d. Crypto: DES, AES, public key, signatures, certificates, error codes
3. Ch. 3:
   a. Buffer overflow
   b. Other unintentional programming oversights!
   c. Malicious code
   d. Countermeasures
4. IN ADDITION TO Ch. 3
   a. Smashing the stack for fun and profit pdf posted on website
   b. OWASP checklist for secure programming
5. Ch. 4:
   a. Browser attacks
   b. Web attacks: injection, cookie interception & manipulation
   c. Email attacks
6. Ch. 6:
   a. Threats
   b. DoS and DDoS
   c. Wireless
   d. Defense: firewalls, AVs, IDS/IPS (do not forget false/true positives/negatives), SSL/TLS, VPN, Onion routing
7. ADDITIONAL Networking material:
   a. Slides on TCP/IP stack (7_ComputerNetworks)
   b. SANS video tutorials
   c. Krack attack
   d. TCP Sequence number attack
   e. Source routing attack
f. ARP/MAC spoofing

g. DNS poisoning

8. Ch. 12:
   a. Symmetric crypto
   b. Asymmetric crypto
   c. Digital signatures

9. ADDITIONAL Crypto material:
   a. Slides
   b. Information theory – Entropy

10. Questions at the end of each chapter

Sample questions:

1. You are told to design an intrusion detection algorithm that identifies vulnerabilities by solely looking at transaction length, i.e., the algorithm uses a packet length threshold $T$ that determines when a packet is marked as an attack. More formally, the algorithm is defined:

   $$D(k, T) \rightarrow [0,1]$$

   where $k$ is the packet length of a suspect packet in bytes, $T$ is the length threshold, and $(0,1)$ indicate that packet should or should not be marked as an attack, respectively. You are given the following data to use to design the algorithm.

   - attack packet lengths: 1, 1, 2, 3, 5, 8
   - non-attack packet lengths: 2, 2, 4, 6, 6, 7, 8, 9

   Find the true positive rate and the false positive rate for thresholds: 0-9. Draw the ROC curve (true positive rate on y axis, false positive rate on x axis)

2. Does open source coding and design help an attacker or does it help developers defend better? Justify your answer.

3. Describe a programming situation where least privilege strategy should be used to improve security.
4. Think how you can break this program and which OWASP secure coding techniques would make it better:

```java
import java.util.Scanner;
public class InputValidationExample {
    public static void main(String[] args) {
        int[] vals = new int[10];

        for (int i = 0; i < 10; i++) {
            vals[i] = (i+1)*(i+1);
        }

        System.out.print("Please type a number: ");
        Scanner sc = new Scanner(System.in);
        int which = sc.nextInt();

        int square = vals[which-1];
        System.out.println("The square of "+which+" is "+square);
    }
}
```

5. Suggest a technique with which a browser can detect and block clickjacking attacks.

6. What attack is a financial institution seeking to counter by asking its customers to confirm that their expected security picture before entering sensitive data?

7. Suggest how to avoid cookie hijacking.

8. How does the Krack attack work? How can it be avoided?

9. Given a network address and mask find the host number and network IP. Practice here: [https://subnettingpractice.com/](https://subnettingpractice.com/)

10. Write a firewall or IDS rule for a specific attack signature. The syntax for Snort IDS will be given.