CS412 Final (2019 Spring)

May 28, 2019

Last name, first name: _____

SCIPE Number: _____

GENERAL GUIDELINES AND INFORMATION

1. This is a *closed* book exam. No extra material is allowed. If you have a question, raise your hand and wait for the proctor.
2. You have 120 minutes, and there are 120 points. Use the number of points as *guidance* on how much time to spend on each question.
3. Write your answers directly on the test. Use the space provided. If you need more space your answer is probably too long.
4. Be sure to provide (print) your name. **Do this first so you don't forget! Please write or print legibly.** State all assumptions that you make above those stated as part of a question.
5. Leave your CAMIPRO card on the table so it can be checked.
6. With your signature below you certify that you solved these problems on your own, that you turn in your solution, and that there were no environmental or other factors that disturbed you during this exam or that diminished your performance.

Signature: _____

Question	Points
1	
2	
3	
4	
5	
6	
Total	

1 Operating System Security (10p)

(a) Explain how qmail achieves strong security guarantees. (4p)

(b) Name (and explain in one to two sentences) three mechanisms that enforce isolation. (6p)

2 Mitigations: Control-Flow Hijacking (20p)

(a) Give an example each of what types of control-flow transfers are protected under CFI for C/C++ (5p)

(b) Name two mechanisms that protect the backward edge. Discuss trade-offs between them. (5p)

(c) How can CFI be bypassed? Build a concrete example for C using prototypes. (10p)

3 Program Testing: Coverage (30p)

(a) How are sanitizers useful during testing? What policy does ASan enforce? (8p)

(b) Describe limitations of dynamic testing techniques in general and fuzzing in particular (7p).

(c) What is state explosion for symbolic execution and how can it be constrained? (5p)

(d) Give a set of inputs that gives i) full statement coverage, ii) full branch coverage, iii) full path coverage. If you can't define full coverage, state why this is not achievable. (10p)

```
void func(int a, int b, int c) {
  int x = 12, y = 5, z = 0;
  while (a != 0) {
    if (b == 12) break;
    switch (c) {
      case 0: x++;
      case 1: z++;
      default: a--;
    }
  }
}
```

4 Low level attacks (30p)

(a) What is a control-flow hijack attack? Give code for a simple vulnerable function. (10p)

(b) What is a data-only attack? Give code for a simple vulnerable function. (10p)

(c) What is a TOCTTOU attack (give a vulnerable code example)? (10p)

5 Cross-Site Scripting (XSS) (15p)

(a) What is XSS and why is it dangerous? (5p)

(b) Give an example of a reflected XSS attack (write at least about the requirements on the server side, the client side, and how the attack is sent to a client). Why is reflected XSS harder to control for an attacker? (10p)

6 Android (15p)

(a) How does Android isolate applications from other applications on the same device? (4p)

(b) How does Google protect the user from installing malicious programs? (4p)

(c) How are applications restricted from requesting services like camera, location, or internet? (2p)

(d) Android applications are written in Java. How are low-level memory safety vulnerabilities still a problem? (5p)