CS 3710: ICS Exam 2, fall 2019

Name

You MUST write your e-mail ID on **EACH** page and bubble in your userid at the bottom of this first page. And put your name on the top of this page, too.

If you are still writing when "pens down" is called, your exam will be ripped up and not graded – even if you are still writing to fill in the bubble form. So please do that first. Sorry to have to be strict on this!

Other than bubbling in your userid at the bottom of this page, please do not write in the footer section of this page.

There are 6 pages to this exam. Once the exam starts, please make sure you have all the pages. Questions are worth different amounts of points.

If you do not bubble in this first page properly, you will not receive credit for the exam!

Answers for the short-answer questions should not exceed about 20 words; if your answer is too long (say, more than 30 words), you will get a zero for that question!

This exam is CLOSED text book, closed-notes, closed-calculator, closed-cell phone, closed-computer, closed-neighbor, etc. Questions are worth different amounts, so be sure to look over all the questions and plan your time accordingly. Please sign the honor pledge below.

The Tao that is seen
Is not the true Tao,
until You bring fresh toner.

(the bubble footer is automatically inserted into this space)

Page 2: Networks, SQL, CSRF

1. [3 points] List the layers of the ISO (not TCP/IP) model, and give a *brief* description of what each does.

2. [3 points] Of the various types of DoS attacks, which is the most effective? *Briefly*, why?

3. [3 points] *Briefly* describe three different ways to protect against SQL injection attacks.

4. [3 points] *Briefly* describe a realistic exploit against a web form (of your choice) that has a CSRF vulnerability.

Page 3: HTTPS

5. [3 points] *Briefly* explain why the TLS protocol is secure against a "mallory" – a malicious user who can both observe and modify data sent between the two parties.

6. [3 points] *Briefly*, what is the difference between a certificate and a public key?

7. [3 points] *Briefly* describe two attacks against HTTPS and how they worked.

8. [3 points] In the Diffe-Hellman key exchange protocol, the example we discussed used colors. *Briefly*, what are the actual values – and operations – used for the real implementation?

Page 4: Bitcoin and Tor

9. [3 points] *Briefly* describe the two primary reasons why bitcoin mining is hard.

10. [3 points] Various governmental agencies have apprehended people who use Tor, so the anonymity that it provides is not absolute. *Briefly* describe two different vulnerabilities that exist even when Tor is being used.

11. [3 points] *Briefly*, how does a hidden service in Tor work? *Briefly*, how does the Tor browser contact that service?

12. [3 points] Should you mine bitcoin?

Page 5: Modern topics

13. [3 points] *Briefly* explain the differences between the two major types of rootkits.

14. [3 points] *Briefly* describe the four types of virtual machines.

15. [3 points] Imagine that you had a malicious entity (hostile government, etc.) that could monitor ALL of your communications. *Briefly*, how could you *send* information and stay anonymous (including anonymity from it being known that you send encrypted data)?

16. [3 points] Of the various ways that your privacy is violated online, *briefly* describe the one that is hardest to circumvent.

Page 6: No questions here

This page unintentionally left blank.

xkcd #135