CS 3501: ICS Final, fall 2018

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.

_____

_____

_____

_____

Serious error.
All shortcuts have disappeared.
Screen. Mind. Both are blank.

(the bubble footer is automatically inserted into this space)

Page 2: Exam 1 material

1. [3 points] Briefly, what are the goals of public key encryption?

2. [3 points] Briefly explain how RSA can sign a message.

3. [6 points] Name and *briefly* describe each of the four ethical frameworks discussed in class.

Page 3: Exam 2 material

4. [6 points] Write a simple x86 encryptor for a virus. Full credit will require x86 assembly (pick any bit size you want). If you can't write the assembly, write pseudo-code, which will get you partial credit. We are not looking for any advanced encryption here. If your code is more than 10 assembly opcodes, it won't be graded.

5. [3 points] Name the protocol(s) used for TLS key exchange. Also name the protocol(s) for the encrypted session itself.

6. [3 points] Briefly, what aspect of `printf()` allows it to be exploited? Briefly, how does one prevent this?

Page 4: SQL, XSS, CSRF, and Stuxnet

7. [3 points] Briefly, give two ways to prevent against SQL injection attacks.

8. [3 points] Briefly, give a real-world example of an cross-site scripting attack.

9. [3 points] Briefly, why do we care about CSRF?

10. [3 points] Briefly, what were the two most impressive aspects of Stuxnet?

Page 5: Anonymity and Cryptocurrency

11. [3 points] Imagine that you are a "rebel" in a given country, and the government is watching you. They are analyzing all of your communication, and – given any amount of evidence – they would arrest you. Assume that you can install any software that exists – it's only networking communications that are monitored. Briefly, how would you communicate with another "rebel" without getting caught? State any *reasonable* assumptions that you make.

12. [3 points] Briefly, how does one contact a hidden service in Tor?

13. [3 points] Briefly, what is blockchain? Briefly, how does it work?

14. [3 points] Briefly, what is the *difficulty* metric of Bitcoin?

Page 6: Forensics, Rootkits, and VMs

15. [3 points] Briefly, what was the FBI-Apple encryption dispute about?

16. [3 points] Briefly, when is the government allowed to extract the password from you for your encrypted hard drive?

17. [3 points] Briefly, give one advantage and one disadvantage for each of the two types of rootkits.

18. [3 points] Briefly describe each of the four levels of virtual machines.