CS 3710: ICS Final Exam, 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 8 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.

_____

_____

_____

_____

A crash reduces
Your expensive computer
To a simple stone.

(the bubble footer is automatically inserted into this space)

Page 2: Ethics and Networks

1. [3 points] Name and *briefly* describe the four ethical frameworks discussed in class.

2. [3 points] Name and *briefly* describe four ways to abuse each of the ethical frameworks discussed in class.

3. [3 points] *Briefly,* what does *forward secrecy* mean?

4. [3 points] *Briefly,* why is the Diffe-Hellman key exchange secure from an eavesdropper determining the final shared key? We are not asking you to describe the algorithm, but instead to explain why it's secure.

Page 3: Encryption

5. [3 points] Give the formula for finding the next random number in sequence using the linear congruential generator (LCG) method.

6. [3 points] *Briefly*, describe the purpose and use of a random seed.

7. [3 points] Decrypt the following ciphertext using a Caesar cipher with the standard key: `qhyhudvndvwduilvkiprugluhfwlrqv`.

8. [3 points] *Briefly*, what problems would occur if p and q were composite numbers instead of primes? While we realize your answer may exceed the 30 word limit, you still have to be brief here.

Page 4: Viruses

9. [3 points] *Briefly* describe the difference between oligomorphic, polymorphic, and metamorphic viruses.

10. [3 points] Other than the `.data` and `.text` sections, name three sections of a PE64 and/or Elf binary file format. If the purpose is not obvious from the name of the section, then *briefly* describe the purpose.

11. [3 points] *Briefly,* why do binary files (PE64, Elf, etc.) expand when they are loaded into memory?

12. [3 points] Name one anti-debugging technique used by viruses, and *briefly* describe how it works.

Page 5: Modern Topics

13. [3 points] *Briefly*, how does bitcoin determine how much the difficulty should increase or decrease?

14. [3 points] *Briefly*, how would the SOPA and PIPA bills have broken the Internet?

15. [3 points] *Briefly* describe how a kernel level rootkit works.

16. [3 points] What was the most innovative aspect of Stuxnet? *Briefly,* why?

Page 6: Miscellaneous

17. [3 points] *Briefly*, what does a CSRF token guard against?

18. [3 points] Other that biological and digital, name two forensic sciences, and *briefly* describe a type of problem they might help solve.

19. [3 points] *Briefly*, when can the authorities, with the appropriate legal permissions (search warrants, what-not), force you to reveal the password for your encrypted hard drive?

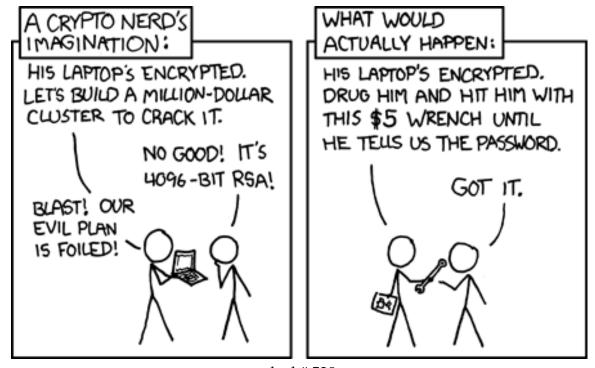20. [3 points] *Briefly* describe what the "security mindset" means.

Page 7: True / False questions

This should go without saying, but you can only pick ONE of the answers. If it's not clear to us which answer you picked, you will not get points for that question. Each question below is worth 2 points.

SQL injection attacks can be solved by properly escaping the input	True	False
One-time pads can use multiple methods of encrypting the plaintext using the random pad	True	False
You should invest in Bitcoin	True	False
A compromised Tor internal node can be used to track some details about the information sent through it	True	False
Format string attacks against `printf()` are prevented by stack canaries	True	False
Properly implemented ALSR (Address space layout randomization) completely prevents buffer overflow attacks	True	False
The SYN flood type of denial of service attack uses very little bandwidth	True	False
Routing happens at the Transport level in the TCP/IP (or the OSI) model of networks	True	False
Sender anonymity has been proven to be possible with email remailers	True	False

Page 8: No questions here

This page unintentionally left blank.

xkcd # 538