CS 3501: ICS Exam 2, 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.

> You step in the stream, But the water has moved on. This page is not here.

(the bubble footer is automatically inserted into this space)

Page 2: Exam 1 Material

1. [3 points] What are the goals of public key encryption?

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

3. [3 points] What two "things" is the security of RSA based on? In other words, what two things make it "hard" to crack RSA?

4. [3 points] When would it be ethical to use a virus creation kit? What would you think must be done to ensure ethical usage of the kit?

Page 3: Viruses

5. [6 points] Write a simple 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.

6. [3 points] Briefly, what is the difference between oligomorphic, polymorphic, and metamorphic viruses?

7. [3 points] Briefly describe the parts of a Windows PE (Portable Executable) file. You need not name everything for full credit – we want to see that you have an idea of how executable files work. And if you mix up a name from PE files and Linux ELF files, that's fine.

Page 4: Binary Exploits and Networking

8. [3 points] Name and *briefly* describe the three primary defenses, as discussed in lecture, that are deployed against allowing buffer overflow attacks to work.

9. [3 points] *Briefly* describe how a viable *heap* buffer overflow attack might work.

10. [6 points] Name and *briefly* describe the layers in the TCP/IP networking model (in other words, skip the presentation and session layers in the OSI model that are not in the TCP/IP model).

Page 5: Web Security

11. [6 points] *Briefly* describe the Diffie–Hellman key exchange protocol. Your answer must have enough detail to explain how it works, but please keep the verbosity down. Full credit will require the formulas used in the protocol; you can get most of the credit with all the details but the formulas. Describing the colors example will get some partial credit, but not as much.

12. [3 points] *Briefly*, what is a *certificate*, as it relates to web site security? What information does it contain?

13. [3 points] Of the various threats to privacy that we discussed in class, which is the largest threat of the set and (briefly) why?

Page 6: TLS

14. [6 points] *Briefly* describe the TLS "handshake" protocol (that sets up the encrypted session). You can use a diagram, as long as it specifies all the relevant points *AND IT IS LEGIBLE*.

15. [3 points] Name the protocol(s) used for TLS key exchange. Also for the encrypted session itself.

16. [3 points] Name *one* of the attacks on TLS that we went over in class, and *briefly* describe how it worked.