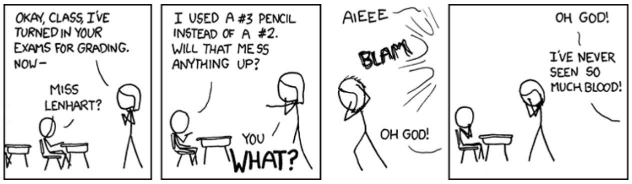
Name: ______________________________ UNI: _____________

Midterm Exam: March 2022
COMS W4182: Computer Security II

Rules

- Remember to write your name and UNI on the exam paper
- If you can, *please* copy the cover sheet to the front of your exam and put your name there
- Books and notes are allowed during this examination. Computer use is permitted for word processing only. (You may hand-write it if you choose and submit a scanned version (as a PDF, *not* as JPGs), but typed material is easier to read…)
- Consultation or collaboration with anyone, in the class or not, is **strictly prohibited**. Email any clarification questions to me.
- This is an untimed, take-home exam. Your answers *must* be uploaded by the indicated time. I strongly urge you to try the upload at least 30 minutes ahead of time—and if you can't make it work, email it to me. Again, that must be done before the deadline.
- Most questions can be answered in just a paragraph or two; if you think you need to write several pages, you're writing too much and may be on the wrong track entirely. If a question is worth only a very few points, that's a pretty good clue that the answer is pretty simple.
- The total points add up to 50.
- Good luck, and may the Force be with you.

Question	Points	Score
1	15	
2	15	
3	10	
4	10	
5	0	
Total:	50	


OKAY, CLASS, I'VE TURNED IN YOUR EXAMS FOR GRADING. NOW–
MISS LENHART?
I USED A #3 PENCIL INSTEAD OF A #2. WILL THAT MESS ANYTHING UP?
YOU WHAT?
AIEEE
BLAM
OH GOD!
OH GOD!
I'VE NEVER SEEN SO MUCH BLOOD!

https://xkcd.com/499/

1. (15 points) A certain web site uses client-side certificates. That is, every user has a certificate, with the private key stored in the browser. To log in, the browser uses that private key in some sort of cryptographic protocol with the web site.

   Should two-factor authentication be used? That is, should some other form of authentication be used as well as this key and protocol? Explain. (Assume that the cryptographic protocol and its implementation are correct.)

   Answer:

   Although the question doesn't say so explicitly, it is reasonable to assume that a "correct" cryptographic protocol verifies the identity of the remote site. The private key cannot, therefore, be used in a phishing attack.

   The question, then, is whether the private key can be stolen or otherwise abused. They key is specified as being stored in the browser, and browsers are not secure—but that wasn't stated in class until after the cut-off date for the midterm. There is also the question of whether the user knows that the browser is visiting—and authenticating to—some site. Finally, there is the chance of physical theft of the device.

   So: the best answer is that it's not secure, but your analysis is crucial.

2. (15 points) In class, I talked about the difficulty of first establishing who owns an IoT device. Some start-up proposes a solution: use NFC (near-field communication, with a range of about 4 cm) to claim or reclaim ownership of the devices. Is this a secure thing to do? Is it usable by average individuals?

   Assume that the NFC reprogrammer is a general-purpose app on your phone. As always, explain your answer.

   Answer:

   It depends, and in particular depends on your threat model. If the items in question are likely to be targeted by thieves and burglars, it's not secure; they can simply claim ownership of the items. Of course, today most items have some form of hardware factory reset buttons, so there's no difference. One can hypothesize someone who sneaks into your house and surreptitiously takes control of your thermostats, but that's not a realistic threat model.

   For it to be insecure, then, we need a situation where the object in question is valuable, portable, and not equipped with a hardware reset. There aren't many things that fit that model. One is phones themselves, but all major vendors have implemented a stronger protection mechanism to prevent resale of stolen phones. The other would be automobiles—for them, this would be a very insecure thing to do.

   Would this be usable? Probably, though from a usability perspective the hard part would be making folks aware of the existence of this app.

3. (10 points) As mentioned in class, password reuse is a serious problem. To combat this, many Internet sites agree to share hashed passwords. Each such entry is tagged with the site and username of who got that password first. Sites use this to reject password changes to something in the list. Explain the *privacy* implications of doing this. (There are implementation difficulties here but they're solvable. Again, the question is about privacy.)

Answer:

There are very serious privacy implications. There has to exist some list of every site's users, which tells anyone with that list who goes where.

There may be a way around this issue, e.g., by using Bloom filters in some fashion, but to argue this you have to explain a solution and how it prevents the problem of password reuse while protecting privacy. Furthermore, coincidental password reuse—Alice and Bob using the same password—is a separate issue and not what the question is about.

4. (10 points) Assume that you are a major public figure and that a foreign intelligence agency wants your phone. However, they won't have custody of you, i.e., they won't grab the phone while you were trying to enter their country. Is it safe for you to use biometric unlock? Explain.

Answer:

As noted, the question is about biometric unlock, which implies that the attackers have your phone. But it's not a custodial situation, where they can overtly demand it from you and demand cooperation on pain of detention or worse. In other words, it's about a theft of some sort, either a nigtht-time burglary, a fake mugging, etc. The question, then, is can they unlock the phone. Since you're a major public figure, there are likely high-resolution photos of you available. The answer, then, depends on whether a biometric can be spoofed. The answer to that is "probably".

5. (0 points) **Bonus question, worth 0 points!**

   What is the answer to the ultimate question of life, the universe, and everything?

Answer:

My answer: 42.

Best answer submitted: It depends.