Name: _____ UNI: _____

Midterm Exam: March 2020
COMS W4182: Computer Security II

Rules

- Remember to write your name and UNI on the blue exam book.
- **Important: also write your name on this paper**.
- You must turn in *both* the exam sheet and the blue book
- Books and notes are allowed during this examination; computers are not permitted.
- This is a time-limited test. All papers must be turned in 75 minutes after the beginning of the test.
- 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 60.
- Good luck, and may the Force be with you.

Question	Points	Score
1	15	
2	10	
3	15	
4	20	
5	0	
Total:	60	

https://xkcd.com/329/

1. (15 points) One of the very difficult problems for web server operators is how to store the private key for certificates—you want them protected but available. Furthermore, these servers are generally located in what are known as "lights out" datacenters—giant rooms or buildings full of computers, but without any people there.

   One suggestion on the table: have someone at central headquarters who is alerted when a server reboots; this person uses biometrics to do a remote decrypt of that server's private key.

   Is this a good idea? Why or why not?

   Answer:

   This is a bad idea.

   Biometrics are not good as cryptographic keys. Thus, a more likely implementation is to authenticate to the remote system and tell it to decrypt the server key—but that's not what the question was about.

   More subtly, how does this person know which remote machine is being connected to? Authenticating the far end requires that it have a cryptographic secret—a private key—to verify its authenticity. In other words, to unlock a private key you have to rely on already-unlocked private key. This is only acceptable if you can show that the unlocked key is less sensitive *and* that knowledge of it by an adversary does not lead to knowledge of the more sensitive key.

2. (10 points) One of the scary threats from IoT is a worm, where a hacked Thing tries to infect other Things of the same type. How would you prevent this? Assume that Things can only communicate directly to their Hubs.

   For convenience, I've attached the network diagram for Things, Hubs, etc., at the end of the exam.

   Answer:

   First, the Hubs can prevent any Thing-to-Thing conversations. That is, they act as packet- or circuit-layer firewalls, and will only all communications directly to the Vendor or (in some setups) the Manager. Second, to prevent indirect infection, the Hub, the Vendor, and the Manager should all implement input validation and sanitization.

   Antivirus code might work, but it's hard, and you'd need a database of patterns.

3. (a) (10 points) Two-factor authentication is more secure than just passwords but is often perceived as inconvenient. Someone suggests that since phones have good location capabilities, that location be used as one factor under certain circumstances. That is, when an employee logs on, their phone is queried for its location. If they're at their desks or in their homes, only a password is needed; if they're elsewhere, some other sort of second factor is required.

   Is this a good idea or a bad idea? Explain.

   Answer:

   Location isn't bad for authentication, but here it probably doesn't work. Suppose that an employee's password has been phished. While the employee is at work, the attacker can try to log in—and the location will be shown, correctly, as "office". Similarly, even using IP address doesn't help for home access, since many consumer ISPs change their users' IP addreses frequently; all you can really register is a block.

Can this be made to work? Possibly, if you (somehow) tie the phone and user volition to the login attempt. But there's not a lot to separate that from two-factor solutions, so it's a bit challenging.

(b) (5 points) Location is obviously very sensitive from a privacy perspective. What should this firm do *if* they adopt this suggestion? (Answer this part regardless of your answer to the first part.)

Answer:

Certainly, any data collected for authentication should be discarded quickly—possibly immediately, possibly as soon as there is no audit need for it. For longer retention, especially for data points not corresponding to home or office, truncate low-order bits to point to a box at least 200 meters square. (Exercise: why not add random noise?)

Depending on the precise threat model, even the stored data for home or office could be made imprecise, but that's often inadvisable. Besides, employers generally know employees' home addresses.

4. (20 points) A government agency uses modern, state-of-the art smartphones to collect various sorts of environmental data, using the phones' cameras, microphones, and accelerometers, plus custom devices coupled to the phones via Bluetooth. Data is collected both by volunteers and by employees. The employee data is considered much more sensitive, since these government employees have the right to go to various places that most people cannot.

   Design a security architecture for this situation. You should make the following assumptions:

   i. It is reasonable to demand more of employees than of volunteers
   ii. The data being collected is sensitive. Knowing the data in the aggregate has commercial value; so does knowing indvidual readings from employee devices (but not volunteer devices).
   iii. The integrity of the data is important
   iv. Because this is sensitive data that may be used in setting environmental policy, some unscrupulous but wealthy organizations may wish to hack the collection sites
   v. Since privacy is part of the answer to the previous question, ignore it here.
   vi. *If you feel the need to make other assumptions, state them explicitly and clearly.*

   Include in your answer any necessary components. You will probably find it helpful to draw a diagram. Make sure you discuss authentication issues.

   N.B.: *Nothing* in this question depends in any way on what was said in class about Bluetooth or wireless in general. *DO NOT* use any part of that in your answer.

Answer:

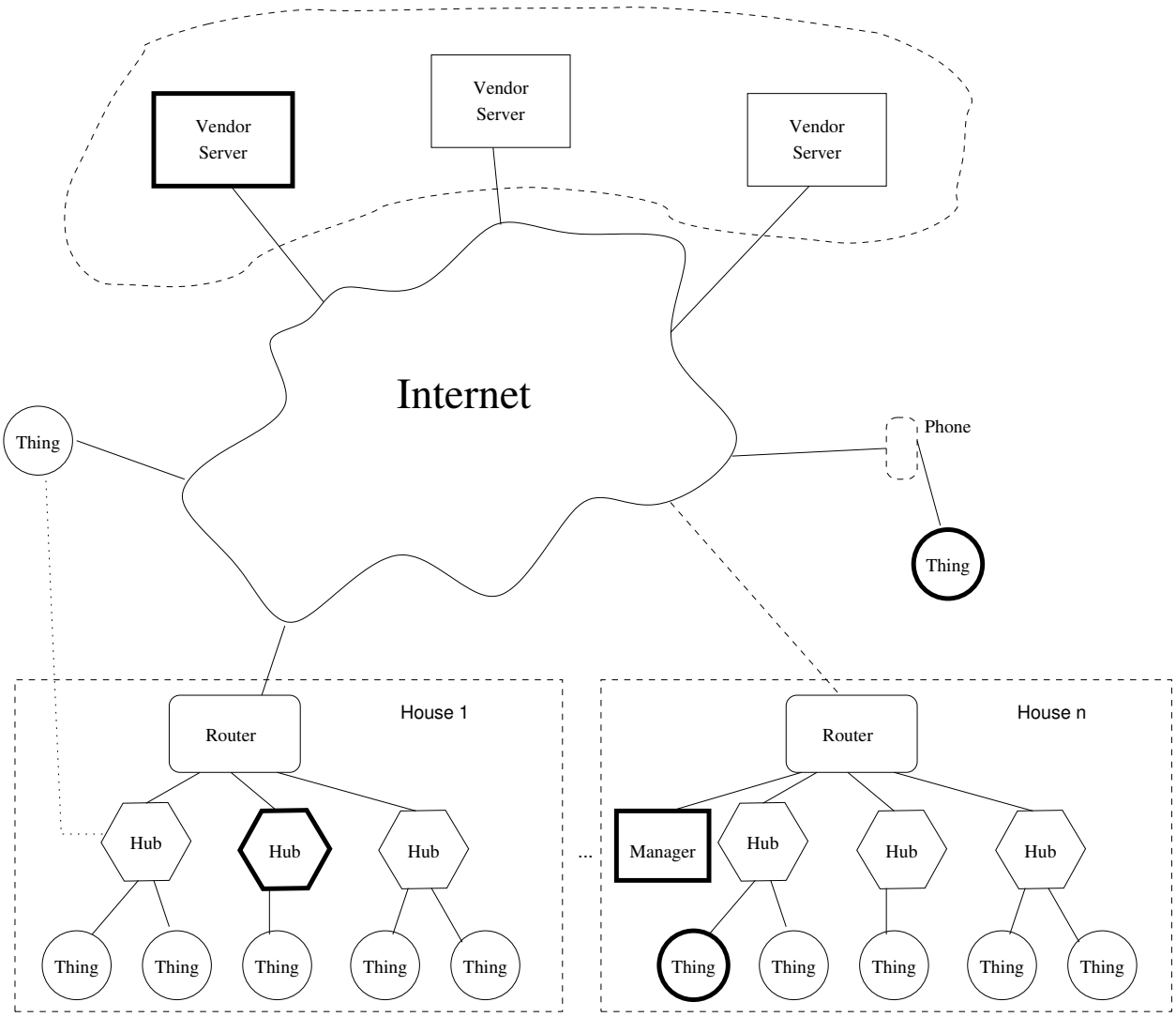
There were many ways to get full credit here. Specifying mandator MFA for employees was necessary; many people also specified optional MFA (via TOTP) for volunteers. Encrypting at least transmissions is necessary; encrypting the data is better. Discussion of security for the server complex is also important.

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

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

Answer:

42.


Vendor
Server
Vendor
Server
Vendor
Server
Internet
Thing
Phone
Thing
House 1
Router
Hub
Hub
Hub
Thing
Thing
Thing
Thing
Thing
...
House n
Router
Manager
Hub
Hub
Hub
Thing
Thing
Thing
Thing
Thing