CSC630

Practice Midterm

May 24, 2019

1 Cybersecurity and Friends

In 3-4 sentences, please formulate your own definitions for "cybersecurity," "hacking," and "cybercrime." How do the terms differ from one another? If you think there are any ambiguities in your definition, please use the word in a sentence.

2 Ethical Hacking

In this question, you are not meant to try and understand how the following situation took place on a technical level. This is an ethics and law question.

Imagine that Sarah, a computer expert, is signing up for a bank account. She notices that the bank requires that passwords be between 8 and 32 characters long, but she was able to sign up with a 64 character password by copying and pasting the password into the field.

She realizes that the password field is *weakly validated*that is, some JavaScript runs in the user's browser that makes sure the password is valid when the user types (which copying and pasting, of course, can circumvent), but nothing validates the password length on the server side.

She tries signing up again, this time using a similar technique to enter an empty password (that is, her password is an empty string). She is successful. For this account, *any password* will let her log in. She suspects that the bank's password authentication system is sloppy.

This question has two parts.

1. Did Sarah do anything "wrong" so far? Do you think she could potentially be charged with cybercrime? How would you have handled the situation differently? Which law would she likely be charged under, if the government or bank were to pursue prosecution?

2. What are Sarah's next steps? In as much detail as possible (but no more than 6-8 sentences), describe what you think she should do next. (Should she report the vulnerability to the bank? If so, how?)

3 Can You Crack It?

The following texts are 'encrypted' using a symmetric encryption technique. The letter frequency distributions for the first fifteen letters of the alphabet for the cleartext is provided below.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**
5	3	5	2	9	2	3	4	5	2	3	2	3	4	10

Now, try to decipher the following ciphertext:

```
Zit jxoea wkgvf ygb pxdhl gctk zit sqmn rgu.
O qd zqaofu q egxklt gf enwtkltexkozn.
```

Document your process along the way!

4 PGP Or Bust

1. What does PGP stand for? What is GPG? What's the difference?
2. How does a PGP private key differ from a public key?
3. What is an X.509 certificate, and how does it differ from a PGP signature?
4. Imagine you are starting a new organization, and you need to ensure that your internal communication is secure. Would you choose to use PGP? Why or why not? If not, what alternative secure communication tools could you use?

5 BYOOS

Imagine that you have decided to build your own operating system kernel that emphasizes *security* as one of its primary differentiating features.

1. What are the primary tasks of the kernel? In other words, what does a kernel do? How is it different from an operating system?
2. What is the threat model of your "secure kernel"? Who (or *what*) are you defending the system against? (Keep in mind that some phones, like iPhones, are designed in some ways to keep their own users out!)
3. Describe two security features that your kernel would feature that other kernels might not.

6 Telephone Troubles

You're talking on the phone with your friend from Montana (you live in Massachusetts), and your seven-year-old cousin asks how the telephone works. After you finish the call, you have plenty of time to spare, so you do your best to explain the American telephone system to him.

In language that the seven-year-old would understand, answer the following questions:

1. Where does the cable that connects the landline telephone to the wall go?
2. Why does the telephone make a tone when I pick it up?

3. How does the telephone connect to people outside of my own town?

4. What does a telephone number mean? Why are there so many numbers? What do they all mean?