Assignment 2: Personnel and Physical Security, Basic Cryptography
Due 6 February 11:59pm in Gradescope.
If using late days, enter "Using late days 2-4", or as appropriate.

1 Personnel and Physical Security Identification and Mitigation: ShopRite Data Security Incident

Please read the article:
`https://www.databreaches.net/millville-shoprite-experiences-data-security-incident/`

1. Identify one personnel or physical security vulnerability that was exploited as part of this incident (a few words, use terminology from the lectures.)
   Solution: The vulnerability that was exploited during this incident was an inadvertent disposing of a device that is used to keep track of personal information. This was a personnel vulnerability incident of operator error.

2. Give a brief (1-2 paragraph) explanation as to how you could mitigate the security vulnerability you identified.
   The first thing that should be done is to train the workers who have access to that device in the importance of keeping it safe due to the personal information it holds. They need to understand that they must make sure the devices stays on the grounds of the business. Next, they should make a system for checking the devices at the end of the work day. It's possible the device was thrown away on accident in this article, so a method of ensuring that did not happen is important.

2 Personnel and Physical Security Identification and Mitigation: Credit Card Attacks

Please read the article
`https://www.theregister.co.uk/2010/10/27/credit_card_flash_attacks/`

1. Identify one personnel or physical security vulnerability that was exploited as part of this incident (a few words, use terminology from the lectures.)
   This is physical security of confidentiality, they are able to steal credit card numbers with devices that mimic what standard scanners look like, which then gives the attackers access to the victim's credit card information.

2. Give a brief (1-2 paragraph) explanation as to how you could mitigate the security vulnerability you identified.
   The main idea would be to improve the fraud detection systems. You can have the fraud detection systems also have an upper limit of how much you are able to spend in any given day. This prevents attackers from stealing an outrageous amount of money. The other solution is to analyze where the

purchases are coming from, and if they are all very far apart then possibly flag the transactions as fraudulent.

3 Personnel Security

In Questions 1 and 2, the URLs are not "hyperlinks", but just text (although some browsers recognize the text as a URL and allow you to click them - under Adobe Reader it is not clickable.) This is inconvenient - you have to cut/paste or retype rather than just clicking on the link.

From a personnel security point of view, why might we have chosen not to make this a hyperlink?

Solution: Operator error is common with hyperlinks in documents and emails. The hyperlink can redirect students to another malicious website instead of the original site. By copy/paste the user can make sure that he will arrive at the location indicated in the text document.

4 Training

When you originally signed up for a CS account, and likely at several other points in your Purdue career, some security awareness training was provided. Name or briefly describe a security awareness training activity you have experienced at Purdue. If you can't think of one, briefly explain why you can't, even though some have occurred.

The university warns against phishing emails as the university is already targeted by scam. Another example can be related to being TA. Some security training regarding the usage of the Purdue employee self-service portal was given as the portal contains a social security number, address, tax information

5 Physical/Personnel Security Issues

For this question, you are asked to identify personnel and physical security vulnerabilities that arise in computer science labs, specifically LWSN B158. Complete the following table by identifying and briefly describing vulnerabilities to fill each of the six slots in the following table:

	Personnel	Physical
Confidentiality		
Integrity		
Availability		

While we do not ask you to describe how to mitigate the vulnerability, you should consider 1) would exploiting the vulnerability likely violate the security expectations of an educational lab, and 2) is it possible to mitigate this in a way that doesn't significantly reduce confidentiality, integrity, or availability (i.e., make the lab unusable.)

Confidentiality-personnel: Someone steals data of the legitimate user. Confidentiality-Physical: Installing external keyboards that log keystrokes. integrity-personnel: TA can raise/lower the grades of students. Integrity-physical: Users can use the logged in account, and change the information. Availability-personnel: Someone from itab may shut down the servers and disable the computers in LWSN B158. Availability-Physical: damage the hardware like the monitor, computer.

6 Crypto: Sample RSA Encryption

Consider a toy RSA example where: $p = 53$, $q = 79$, and $e = 5$
Find the ciphertext using RSA encryption for plaintext $P = 42$. Show all the steps you took to get to the final ciphertext.
(Reminder: Python makes an excellent calculator for large numbers!)

Solution: Given $P = 42, p = 53, q = 79, e = 5$, where P is the plaintext and p,q are large primes...
$N = p \cdot q = 53 \cdot 79 = 4187$
$C = P^e (mod N) = 42^5 (mod 4187) = 2401$

7 Crypto: Sample RSA 2

Using the same p, q, and e values from above, try to encrypt the plaintext $P = 0$.
Why is this an issue, and how is it typically dealt with in practice?

Solution: P = 0 = C is the problem. In practice this is dealt with by restricting the message space to include anything 0 (mod N). This can be done by salting/padding inputs to avoid 0 and ensuring messages are of sufficient length to not outstrip size of N.

8 Crypto: Bad encryption mode

Assume some encryption scheme always encrypts the same plaintext into the exact same ciphertext when using the same key.

1. How does this leak information?
   Solution: The attacker can learn if the same message was sent twice under such a scheme, which can result in information about those plaintexts being leaked through frequency analysis, replay attacks happening, or repeated strings in the ciphertext.

2. What could you do to solve this?
   Solution: Using a better encryption mode such as CBC (Cipher-Block-Chaining) is the most secure fix, however adding a random salt or some extra information that changes will sufficiently change the ciphertext if the diffusion is high enough in the scheme.

9 Crypto: Diffusion

Diffusion states that if we change a single bit of the plaintext, then every bit of the ciphertext should change with probability 0.5. Assume we are using a cipher that has poor diffusion: changing a bit in the plaintext only changes a few neighboring bits in the ciphertext. Explain how this could leak information under a chosen plaintext attack.

Solution: 9. Such a scheme is much more vulnerable to a brute force chosen plaintext attack. An attacker only needs to brute force enough of a block to get a few bits to match up, and can thus discover the original plaintext with much greater probability. Patterns are also visible in the ciphertext, allowing an attacker to more easily use a frequency analysis attack.

It is important to note that such a scheme does not necessarily leak information relating to the key. Simply being able to analyze these patterns and discover the plaintext is enough information leak as it is. Discovering the key could be much more difficult or impossible depending on the specific scheme used.