Assignment 1

Question 1

The policy being imposed is that everyone using the transit must pay for the service. This policy is to protect the public metro, more specifically the metro's service quality. Since we are restricting people using metro's is just because we do not want the people who actually pay for the ticket to suffer, since they are paying for the train's service as well as for its maintenance.

An adversary in this case would be someone who wants to use the service without paying for it. These could be done in many ways. Some of the most common ones would be- jumping over turnstiles, avoid inspection officers while traveling without ticket, using expired tickets or even bribing the officer. These attacks depends on the feasibility, that is, jumping over turnstile depends if it is guarded or not, or how tall it is, and also attackers physical ability to jump over it. If attacker avoids the officer successfully, they might be able to use it for free but if they get caught they pay a fine or if the officer is corrupt, could bribe them and would be able to dodge the huge fine. This would depend on how much money the attacker has. They may even get away with an expired ticket which depends how carefully the gatekeeper/officer inspects the ticket before letting passengers go. A busy time would be ideal and would be able to get past with this. All the above attacks if successful, will violate the policy since they would use the transit without paying.

There are various defense mechanisms in place to avoid such violations. A human gatekeeper is one of them. This will avoid people to attack since they would not be allowed to enter and anyone jumping could be thrown out again. This is the way a human gatekeeper prevents the attacks. Since a human is employed the cost is high and since there could be multiple people employed to ensure proper inspection, the cost could be very high. Other way is by infrequent inspection. This mechanism discourages people to attack or else they have to pay a heavy fine instead of a significantly low price for the ticket. The attacks are still possible since people can be lucky and avoid these inspections. So since humans are deployed, the cost is high. I both the above cases, the risk of deploying a human here could be their integrity. A gatekeeper/officer could be corrupt and for example could allow someone to use the service every time by giving a relatively a small amount instead of buying the ticket or paying the fine. In busy times these mechanisms would be inefficient. Turnstiles is another mechanism that tries to prevent the attacks by having the users to scan their ticket before entering the platform. An attack could be simply jumping over the turnstiles or by two people going through the turnstile with a single ticket scan. The cost of this mechanism is low. To avoid some of the possible attacks a hybrid solution could be implemented. A combination of turnstile and a human gatekeeper could do the work. The inefficiency is lowered as a turnstile could perform it. Since the way to pass a turnstile is only by jumping or two people going through one ticket, a gatekeeper can watch for those and also the number of humans required are less so the cost is reasonable and is efficient (less risk). But again the gatekeeper's integrity may be an issue.

Question 2.

- **Foreign intelligence**: Knowing that Russia and US do not share a good bond, so it might be the case that the stolen laptops could be done by some Russian spy. We are assuming the laptop stolen by the spy belonged to an important person. Since the spy has the laptop, they could try to dig in and get all the details they want. The goal of the spy could just bring some valuable information (or some top secret mission or evidence) and send it back to the Russian intelligence. Then the Russian intelligence could do whatever they want with that information, that could be exposing US bad deeds, or intercepting their missions, etc. Since they did get the laptop easily, the spy's got some valuable information by doing significantly less work. Since the Russian intelligence works with the spy, the funding level is great and also the whole intelligence could be working on getting the information out. So now they have the opportunity, working force and resources. This would be an active attack where they could erase, modify data or could be passive attack based on their agenda.
- **Organized criminals**: It could be a case where an attacker could install malware into some of the laptops in the capitol with an aim of collecting the confidential information (that could overthrow the ruling party) and using that to blackmail them into helping them/or avoiding any investigations related to their work. Assuming this malware was planted by an organization that smuggles in illegal drugs. So in this case they could easily smuggle as they are supported by higher authority that are compromised. Since drug cartels are could have ample resources the work/risk has been significantly reduced. The attack would be an active attack where the data would be gathered and the user could be blocked from deleting (or modifying).
- **Terrorist**: If a terrorist group gets access to the laptop, they could crack into it based on their skills or resources. Assuming they are able to get information from the laptop, they could possibly use itinerary (of a confidential meeting held by the higher authorities) and plan the attack to create instability in the country and further be able to use the resources for other attacks. Or it could be a case where an attacker could install malware into some of the laptops in the capitol with an aim of collecting the confidential information. This may allow them to smuggle arms for a planned terrorist attack. So in this case they may be able to get access to the information (or at least some information) to get an overview of the defense in the area and find vulnerabilities like for example knowing when and where the forces would be less concentrated. Knowing this information, they could smuggle when the opportunity is good. Depending on the size of the terrorist group and the skills, they may or may not have enough time to get access to the information since the malware could be detected at any time and could be neutralized. This way the time they have to get the information could be less. The attack would be a passive attack where the data would be only be collected and the smuggler would plan accordingly.
- **Politically motivated adversaries**: Hacktivists could be the one that could have gotten access to one of the laptops. They have an objective of exposing the political party wrong doings and notifying the public about them. Hacktivists could be a bunch of hackers with the same agenda and could work together. Assuming they have a good amount of knowledge and the skills and since they have resources to achieve their goal (could be posting on the internet, informing a media outlet, or the opposition party). So this could be a perfect opportunity to get information from the laptop device

of a member of the running political party. The attack would be an active attack where the data could be erased, modified or shared to achieve the goal.

Question 3.

So when we use AES in CBC mode, we need an IV to decrypt the first block. So if we fill first block with some random stuff then to decrypt and recover the original message, we do not need the IV since first block is not a part of the message. And without the IV, we can anyways calculate all the blocks except the first one using the ciphertexts. So the message is fully recovered by only knowing the key.

```
AES_CBC_NO_IV(){
      //sender side
      if (sender){
          uint8_t key[32] = get_key();
          std::string message= getMessage();//gets the message to encrypt
          uint8_t sender_iv[32] = get_IV();
          std::string modMessage="";
         //generate a string of the block size = 32 bytes
          for (int i=0; i<32; i++){
            modMessage+="x"
          }
          //prepend the randomString to the original message
          modMessage+=message;
          std::string ciphertext =
                AES_CBC_256_encrypt(modMessage, key, sender_iv);
          send(ciphertext);
      }

      //receiver side
      if (receiver){
          uint8_t key[32] = get_key();
          std::string cipher=receive_ciphertext();
          //generate a random IV
          uint8_t rand_iv[32] = get_IV()
          std::string plaintext =
                AES_CBC_256_dencrypt(cipher, key, rand_iv);
          plaintext = plaintext.substr(32,plaintext.size()-1);
          //first block is excluded from the plaintext decrypted
      }
}
```

Question 4.

It takes on average 3 minutes and 32.502 seconds to get 10 random characters to generate without input. When moving the mouse rigorously, it takes on average 1.71 seconds. For getting the timings for network traffic, I downloaded Kali-Linux vmware file (2.3 gb) from offensive-security's site. I started the download before-hand and ran the command multiple times before the entropy pool was clear and the once it was clear, it started taking some time to generate. So that I what I repeatedly performed to get the timings from internet traffic and it took on average 3.646 sec. While typing, it took on average 4.65 seconds to generate 10 characters. The most effective method was clearly moving the mouse. It was very quick to generate relative to others. Then network traffic was the second most effective way and then typing. So if we combine all of them together it may lead to a more efficient way of generating the random characters. But in the above case the most efficient was moving the mouse.

The following is the raw data of timings it took to generate 10 characters for a specific interaction (or no interaction):

No interaction:

- 3m 20.13s
- 4m 02.68s
- 3m 23.54s
- 3m 23.02s
- 3m 33.14s

Mouse movement:

- 1.71s
- 1.77s
- 1.60s
- 1.93s
- 1.54s

Network traffic-downloading Kali-Linux VMware file of size 2.3gb from offensive-security.com

- 3.65s
- 3.57s
- 3.04s
- 4.34s
- 3.63s

Typing

- 4.48s
- 4.50s
- 4.32s
- 4.98s
- 4.97s