**MIS 6330: IT Security**

**Individual Homework 1**

1. The main difference between passive and active security threats is that passive security threats is that data about the victim or their vulnerabilities may be gathered but no changes are made in data.

Also, passive attacks are generally difficult to detect than active attacks.

Eavesdropping – Passive

Replay – Active

Intrusion – Active

Inference – Passive

1. Confidentiality – High

Integrity – High

Availability – Medium

ATM Machine should have latest and correct information about money available in any account as well as in cash present in ATM machine. Hence, Integrity should be one of the “must have” requirement.

All account details of all customers are confidential and should be   
kept away from any unauthorized person to safe-guard the users and their money.

So, confidentiality should be also a “must have” requirement.

However, if one ATM machine is down on rare occasions, the users can go to do a different bank and still withdraw money with some inconvenience.

Consequently, Availability is a medium requirement.

1. The main difference between feature and assurance is that feature may/may not help in mitigating all risks while assurance means every risk is considered and mitigated.

It is easier to get a feature developed as to develop a feature, test/use cases about a single risk needs to be considered.

Assurance is harder to acquire as all types of risks and their test cases are to be considered.

Therefore, it is important to emphasize on assurance than a feature.

1. The answer to questions asked in assignment are as follows:
   1. The main target were the three power distribution companies (oblenergos) providing power to 2,25,000 customers.
   2. Attack exploited vulnerabilities like
      1. Poor phishing filter (which didn’t screen the mail which had attachment containing BlackEnergy3 malware)
      2. Insufficient protection from malware on machines within network (which didn’t stop BlackEnergy3 from running and providing the attackers with credentials of the employees)
      3. Insufficient network security monitoring (which would have helped in detection of any suspicious reconnaissance activities by the attackers)
      4. Remote access for ICS network was not using 2-factor authentication.
      5. UPS were using online command interface which allowed remote access to UPS system.
      6. Attackers were able to install their custom firmware which made serial-to-Ethernet gateways inoperable (which blocked attempts of communication between telephone systems of these power companies)
   3. Counter measures that should have been taken are as follows:
      1. Employees could be educated to not open email attachments from untrusted sources.
      2. Better firewall could be created which blocks network traffic from untrusted sources.
      3. Better phishing and spam filters could be created for all mails with attachments.
      4. Machines should be regularly updated with virus definitions to make sure they detect and alert the authorities on detecting malware like BlackEnergy3.
      5. Network security monitoring can be done using different types of tools available to make sure any kind of reconnaissance activities can be detected in early stages and attackers could be thwarted before they could do real damage.
      6. Remote access should be given on need-to-know basis and should have 2-factor authentication for better verification.
      7. UPS systems should be kept offline and should have separate power source than the ICS network and other machines.
      8. Updates and patches should be installed on a regular basis to avoid any vulnerabilities to be abused.
      9. Monitoring and auditing the hardware and software system regularly will make sure that only trusted assets are present in the system.
   4. General lessons that can be learnt from this incident are as follows:
      1. Educating employees about cyber security can help in preventing such attacks. If the employees understood the difference between trusted and untrusted sources, BlackEnergy3 malware could not have entered the system.
      2. With proper counter measures, such attack could be detected before attackers could do real damage, even if they get access to the system.
      3. Backup systems or redundancies should be in place for any system that is vital for the working of a system and should work independent from the system for which it is a backup.
      4. Multi-factor authentication helps in weeding out attackers who may get hands on credentials of victims.
      5. All systems connected to the internet should regularly be audited for updates and patches and on finding any vulnerabilities, they should be fixed as soon as possible.
      6. Network security monitoring is imperative to keep in check all suspicious activities and a lot of tools are available for different requirements which should be analyzed by the IT security team.
2. The importance of need to distinguish between vulnerability and threat when assessing security risk will be explained through following example.

During recent WannaCry attacks on Window-based computers worldwide, computer users could be divided in 3 categories

1. People who used Windows based OS with system not updated with latest security releases
2. People who used Windows based OS with system updated with latest security releases
3. People who used OS which are not Windows

People of 1st and 2nd categories both were under same threat. However,   
only people of 1st category were vulnerable to this attack.

So, even under threat, 2nd category was safe from this attack and weren’t   
required to take any steps to prevent the attacks.

Also, people of 3rd category were completely safe as they were not under any threat at all and hence not vulnerable too.

Subsequently, they were not required to take any steps to prevent the attacks just like the 2nd category but even without assessing vulnerabilities.