Alexander Cannell

1. Provide a short comparison between the CIA Triad and the Parkerian hexad.

Parkerian Hexad:

Parkerian Hexad is the CIA Triad but with three more concepts added Possession, Authenticity, and Utility. Possession is the way something is transferred and stored. Authenticity is how true is the data from the owner or creator. Anish talked kindof about Authenticity in his Ted talk, where people will make duplicate apps that look like the real app from a legit company, but these apps will have malware on them. Which people download and cause all sort of problems. Utility is the concept that addresses how useful something is. Or in other words the ability to determine the motivation behind someone obtaining the secure data/item. I think utility is vital in the social engineering world, when trying to get someone to give up information that doesn't seem very useful to the one getting the information which might be vital to the social engineerist. These three kindof reminds me of the law enforcement process of Chain of Custody. Which is the documentation of evidence showing who handled evidence, to prevent tampering, destroying, or loss of evidence. Chain of Custody keeps a paper trail so evidence can be used as evidence and have the ability to be admissible in court.

CIA Triad:

The CIA Triad is a combination of three essential aspects of information security. CIA stands for Confidentiality, Availability, And Integrity. Confidentiality is the ability to keep sensitive information being viewed by unauthorized individuals. In other words Confidentiality is how private something is. Availability is the ability to access the secure item later. In other words Availability is the how accessible is my data? Example: It gives an example in the book quotes a well know saying, “The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts”. That may be a secure system, but your accessability to that Item that is casted in a block of concrete isn't very accessible. We have to be able to use our data to some extent or what is the point of having said data. Integrity is the ability to to protect data from being altered without permission, including stolen or destroyed. In the talk by Anish he talks about boot sector malware, that is specifically designed to destroy the boot sector of a hard drive and to do damages. This is what Integrity means how protected from unauthorized change is our protected item? Again going back to Chain of Custody is a great example.

1. After reviewing the above, what potential attacks are networks vulnerable to, and are there other types of attacks that networks are exposed to that were not mentioned in the book?

The book mentions some different types of potential attacks but the one I didnt seem to catch seeing in the book was a POS Malware, Phishing and Denial of Service Attacks. We have been seeing alot resently about POS Attacks on major company the most recent being the clothing store Eddie Bauer. We just read about Eddie Bauer’s POS Breach in our CSIA 6010 class. Eddie Bauer finding out about the hack in July of 2016 which appeared to stretch back to January of 2016. Malware was found on Eddie Bauer Point Of Sale Machines(POS), which captured credit card and debit card Information. Purchases made online were not affected by the malware. Eddie Bauer is working with the FBI and other Forensics firms to determine what happened and to prevent further incidents from occurring in the future. Denial of Service (DDoS) is "The prevention of authorized access to a system resource or the delaying of system operations and functions." We get DoS/DDoS Attacks annually being a popular company I work for. Most of the time a DoS Attack will slow down request times, and cause major customer impact. Even in some causes bringing down the site. We now have an DoS/DDoS mitigation service that filters out the undesired traffic. Phishing is "The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the e-mail and the web site looks like they are part of a bank the user is doing business with." We have had several incidences of phishing. Our customer support team is trained in dealing with phishing incidents, each are reported to our IT Security Team. Our team also deals with each phishing cases, we help determine if an immediate response from the IT Security team, and we contact as needed. Anish talks about the ability to not only look at one aspect of a node and defend only that and leave the rest unprotected. But the invaluable ability to look at a node in as the book says different layers and depths and testing security that way.

<https://www.youtube.com/watch?v=Jov0LADiX_Q>

<https://www.youtube.com/watch?v=OhA9PAfkJ10>

<https://www.youtube.com/watch?v=9TRR6lHviQc>

<http://www.sans.org/security-resources/glossary-of-terms/>

<http://krebsonsecurity.com/2016/08/malware-infected-all-eddie-bauer-stores-in-u-s-canada/>

<http://bgr.com/2014/03/13/target-data-hack-how-it-happened/>

* 1. Be sure to cite your answer(s) from the readings. You may also use other resources (scholarly or otherwise) to support your answers.

1. Anish mentions "half-full and half-empty" perspectives in terms of security, and how we (corporate, security professionals, individuals, etc.) perceive the fight against intrusions, breaches, etc. Provide your view on his discussion, including any citations that might support your argument for or against success in securing networks.

After Listening to Anish talk about how the world looks at the Security Industry being a half empty perspective sort of people. Anish talks about how this half empty perspective persona is well deserved because as Anish says, “we are conditioned to look at everything that could go wrong.” I believe that both have its merits when it comes to Information Security. On one hand security professionals need to have a sense of paranoia when it comes to how secure is your system. That Paranoia is useful in the regard of being always on your guard, looking for new ways to protect yourself, keeping uptodate with all the current “hacks”, and in frightening your fellow co workers to be always on guard. :) But on the other hand you have this glass is half empty where you arent ignorant of the things I just listed but as the book says “confidently secure.” Where you take every attempted hack as an accomplishment, and have a reinsured demeanor. Plus it is always good to have a good half full glass when crap hits the fan. So I believe as Anish that we need to have a better glass than just an empty or full glass but a bigger one that handles both good qualities.

**Notes:**

Anish Bhimani: Information security professionals have a reputation of being glass half empty. What are the threats that are coming after us distruction of commerce(people who hate), thieves, nation state sponsored hackerism(China; korea). Anish talked about two instances, an increase of DDoS Attacks in 2012, the sophistication was unlike anyone has ever seen. Second instance the development of shunoo virus which is a virus that destroyed the boot sector of a computer. These were both generated by Nation States. He continues on to make the point that we are moving from disruption to destruction. We are seeing a change in the motivation, an increase in sophistication, and better/more use of social engineering attacks. Social Engineering attacks: “Click here to get hacked, ooo that sounds cool. \*Click\*” Typical Cyber Attack: Target Victims, Infects System, Privileged Access, Collect Data, Monitor Details, and Exfiltration of information. He continues in saying that we have moved from protecting an aspect to protecting everything in the chain. We come to the issue of balance in privacy vs security. He poses two questions asking are the defenders or hackers winning is this world of information security? Also how do we determine that like between privacy and security?

Book: Information Security is defined as “protecting information and information systems from unauthorized access use, disclosure, disruption, modification, or destruction”, according to US law. In our efforts to secure our assets, we must also consider the consequences of the security we choose to implement. There is a well-known quote that says, “The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts” The goal of a Security plan is to find the balance between protection, usability, and cost. we must also consider how the level of Security relates to the value of the item being Secured. How do we determine at what point something is reasonably secure? It is far easier to define when something is insecure then completely secure. The book discusses three key aspects of security Confidentiality(Privacy), Integrity(ability to prevent), and Availability(Usable).