Udipto Chowdhury

Prof. Kennedy

FCM 761

04/30/2023

Homework #10

1. Watch the Chelsea Komlo video. What is Chelsea's role in her organization? How does her role make her perspective on security unique from the type of perspectives we covered in previous classes? What metaphor does she give about security in an organization and why is it relevant? What viewpoints does she reference when thinking about defense in depth and why is each viewpoint relevant?
    a. Based on the video presentation with interactive slides, Chelsea Komlo is a Software Engineer at HashiCorp. Her role makes her perspective on security unique from the perspectives we covered in previous classes by advising on how to think outside the box when it comes to fortifying your laptop/desktop/smartphone's security (online or offline). Additionally, she wants us to believe thanks to her visual representations to the point that there are 4 different viewpoints regarding defense in depth: low-level (lines of code), mid-level (collaborative teamwork), high-level (architecture), and highest-level (product strategy; marketing). For metaphor, Komlo presented a picture of a gate without a fence. This makes sense because of the fact that people need to think outside of the box when it comes to ensuring the security of the organization's

infrastructure as well as maintaining security for all. In fact, she stated that one vulnerable third-party library can lead to hundreds of millions of sensitive PII (Personal Identifiable Information) can be stolen with ease only if the company does not bring in their A-game when it comes to security implementation. Since Komlo believed that defense in depth is necessary for a security system with appropriate countermeasures. Every line of code, automated tooling, test case, collaboration, planning/building technological infrastructure, strategizing your product, and analyzing user threat model all play a crucial role when it comes to ensuring peace of mind for security infrastructure. All in all, if people know what they are supposed to be doing, then there is nothing to be worried about.

2. Summarize the Game Theoretic Approach to Model Cyber Attack and Defense Strategies. What are some of the key takeaways of the paper? What is your reflection on it? Is it valid? Too academic? Could you think about how you could apply these strategies to anything we have discussed in class?

    a. The key takeaways for *A Game Theoretic Approach to Model Cyber Attack and Defense Strategies* are to understand the importance of designing a dynamic defense system that can adjust its strategies to achieve the best defensive performance against intelligent attackers and under various attack situations, the emphasis on a research of the dynamic interactions and evolution among cybersecurity attackers and defenders, presenting a non-cooperative zero-sum game in modeling the cyber warfare between attackers and defenders based on the generalized three-level attack/defense strategies game in addition to presenting the case study of three different types of network attacks to demonstrate how the

proposed game theory can be applied in a broad range of cybersecurity problems. If this were to be summarized, cyber attack and defense strategies are like a game of chess: you plan to win. According to Sanjay Goel's *National Cyber Security Strategy and the Emergence of Strong Digital Borders*, since countries are harvesting the social and economic benefits of the Internet, people around the world are concerned about the threats that deal with national security. In other words, there are hackers out there that will try to ruin everyone's day by stealing their personal information. Honestly, the first article is a bit more academic even though the article was not as straightforward as it should be (it is straightforward but not fully straightforward). With that said, they have used a three-level attack/defense strategy model to provide generalized modeling of the strategy choices by attackers and defenders. All in all, the research article talks about how game modules can be implemented when it comes to modeling cyber attacks and defense strategies.