CS2309 Homework 3

Tan Yee Jian (A0190190L)

November 11, 2021

My favourite presentation in CS2309 (2020/21 Semester 1) is **Arms Race in Memory Error Exploit and Defense** by Dr. Liang Zhenkai. His presentation is, in my opinion, one of the most unique because he has a deeper meaning to convey behind his presentation, other than the technical details.

1 What

1.1 What was covered

The presentation was aimed at students with a simple background in operating systems and computer organization, which is lower than many of the machine-learning related talks. He started by explaning what is an activation record (stack frame) in program execution, and how it can be attacked or exploited. He then explained that most of the exploits come from the Von Neumann architecture in computers - instructions as data. Finally, he spends only 6 out of 45 slides on introducing his research on Data Oriented Programming and how exploits are constructed in that model, ending with a one-slide case study.

1.2 What is unique

Most presenters will go on to explain how cool or interesting their projects are, Dr. Liang has a different aim - he wanted to discuss about his philosophy towards research, learning and knowledge generation. In the last 9 slides (20% of the slides), he talked about *Tao*, and how he views learning and researching on cybersecurity - is about being calm and in deep reflection with the knowledge that is at hand. He then added a few martial art references and raises the point of "counter changes with a constant principle", asking the students to "practice, and most importantly reflect" with a picture of Jet Li in the movie *Crouching Tiger, Hidden Dragon* (*2000*) (Figure 1). Finally, he raised the question of (what is) "the mission of university education?" As an ending to his presentation.

2 Why

2.1 Why is this interesting?

The uniqueness of this presentation lies in this last 20%: he prompts us to reflect about our own learning. Indeed, good research is not only about hardwork; novel

Figure 1: Tao over Technique. Taken from Prof. Liang Zhenkai's slides page 40.

research needs deep reflections about the current situation to come up with something novel and/or impactful. In a world where an improvement of 0.1% in testing loss or brute-force parameter tuning are papers of their own, truly impactful research needs more careful thought.

The field of security is best summarized by Figure 2. More secure systems need better defense systems, while new defense systems originate from novel attacks. This require the attacks to be well thought out and be unique.

Similar to the theoretical research which I am interested in, it is required that we ask the **correct** questions to be able to deduce the future research directions. In this regard, these advice are immensely useful and I will keep them with me, more than the technical knowledge presented in all the presentations.

3 How

3.1 How can we learn from this presentation?

In the current situation, it is difficult to cope with the CS2309 assessments without an ongoing UROPS project. This is because students who still have no idea what to research on and is purely interested in the area will only have a semester of self-study before coming up with a research proposal, including a survey paper and a presentation in between, which is too challenging. Furthermore, research is about studying the open problems in respective fields, and by having most of the talk about machine learning is difficult for those who don't have the required background or not interested in the field.

In contrast, Prof. Liang Zhenkai's talk is very beginner friendly and at most requires only CS2100 and CS2106 to understand fully. Furthermore, he imparts his wisdom in research and his own personal thoughts which are very useful to our growth as both students and potential researchers.

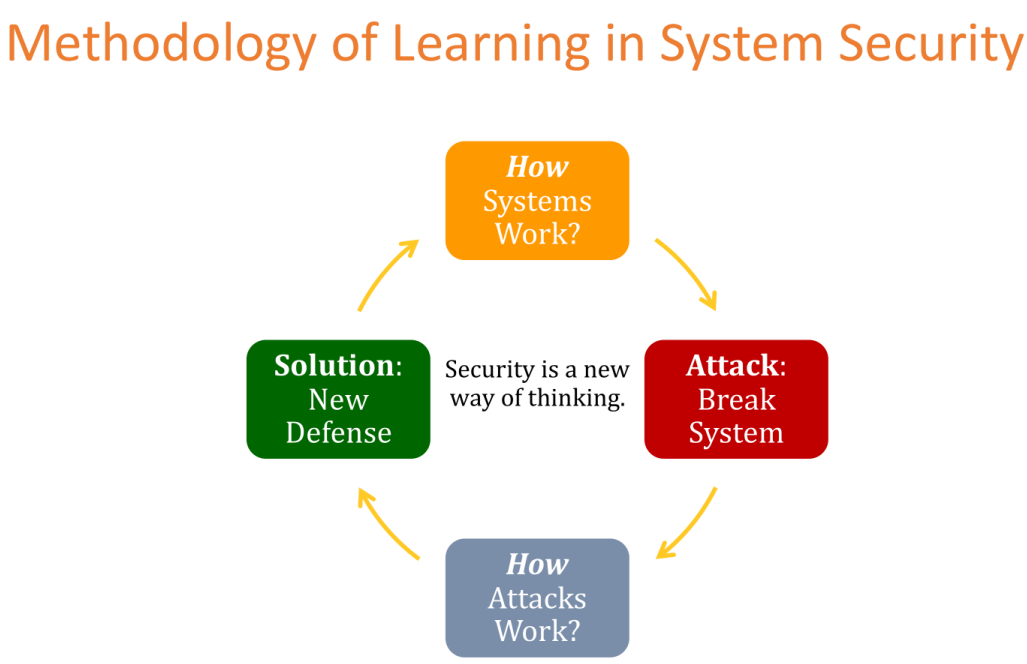

Figure 2: Security. Taken from Prof. Liang Zhenkai's slides page 41.

Therefore, in my future presentations, I will take note of not only student's background knowledge, but also their interests. When the interest is low, some personal advice and wisdom might be the shining gem in the ashes of nonchalance.