Connecting the dots: Foundamental Skillsets and Mindsets for building up surviving skills for a (system security) PhD

Changming Liu

I. Plan for this log

Out of the a few advices that I found helpful from my advisor, "write more, even if it's not your paper, write something everyday." is the one that I've always wanted to try, but stuck with the emptyness in my head. Now since I've came to a milestone where I've finished my first project, it's a good opportunity to connect the dots that I've found for the past year(and 3 months).

I inteded this to be something to update from time to time.

II. Why these exist?

An enormous part of a PhD's life is undoubtedly to learn different techniques dedicated for an ultimate problem. For most, especially for beginners, a puzzling thing is the huge amount of existing practices that you might need to get familiar with. If you just glimpse through them, you might be frustrated by the subtle differences among them. However, if you decided to figure them out, the progress of your own project(dedicated to get something publised) can be severely impacted.

If you talked to some senior members who should have been through all this, a typical answer you can get is that, "" Different tools and techniques are countless, it is easy to be overwhelmed by the huge number of tools that aimed at the same goal. This problem is worsen in acedemia where there are many prototypes projects whose contribution is unknown until you read certain lines of its paper.

As a PhD students, it's your duty to at least get familiar with these different technologies but sometimes, you find yourself burried by some technical details, or you find something too easy to grasp while overlooking its importance.

III. What's magic and what's not

For most, even for the CS-backgrouned students, a balance between being ama(u)zed by the "magic" of computers and figuring out everything behind the magic has accompanied the learning process especially in the beginning period. We always love the "magic", the magic can be "download CodeBlocks, create a C file as instructed, and write Hello world, and press "compile and run"", and boom, you make it! There is no denying the fact that, the magic is why computers are so facinating to the public, the pioneers tried very hard to abstract things to make computers comprehensible for laymans. What make matters worse(better), the magic are all around the learning process, the existance of magic seems norm for many fields mainly because it freed us to do more high level staff with much shorter time.

I'm not sure for other computer fields, for a research field as messy as system security, I struggled a lot to figure out what should I take as magic, and what should not.

A. ELF formats and linkers

IV. Time management

During the process of trying out different time management strategies, although I still think I'm in the middle of the tunnel, I definitely see some lights ahead. More specifically, I tried 2 completely different strategies in the past year, and at least I think conclusion can be drawn for comparing these two.

The first one is quite simple which is just to "devote anytime you can have to a project". I see this as an extention from my past experience which is "I always succeed when I've decided to achieve something". For example, when I'm determined to have good grades, I can achieve high self-discipline and work tirelessly for weeks for the final week, and it worked everytime. Even for the first research project I was assigned to during my master's degree, I work closely with my mentor and implemented a prototype which my senior peer has spent more than a year on but could not deliver.

So, although not completely conciously aware of this, I always attribute the futility of my peers to their inactivity or lazyness.

But as I was trying to implement the same strategy to my first "serious" research project for my PhD, I struggled a lot especially in the beginning perioud. The magic seems gone.

A. Learning to relax

Now looking back at those times, I figured, one major reason for the disappearance of that power is that, relaxing was tiring. Mainly due to the complete change of environment, I have to construct a whole chain of life i.e., use what trick to concentrate and use what to relax myself. And since my focus has been on the research for the whole time, I didn't pay much attention to these trivia and just picked whatever comes handy. The main tool I used to relax myself during that time ws anime and youtube, for one I didn't really enjoy those anime and videos (I just thought now I should relax, so these come handy), plus my English was not good enough to digest the content effortlessly like my Chinese(my native language), and I tried to really exercise my English with that.

As a consequence, those "relaxing" activities turned out wearing me out. A good example is, everytime after I spent my "leisure time", I could never get enough and felt tired. This severely damaged my motives and energy for the serious work i.e., research.

https://mp.weixin.qq.com/s/t1otw17tCwgvvx4lWoQiLA 1. Relaxing is important 2. Doesn't have to sth fancy(e.g. going out for movie, vacation), as long as sth makes you feel relaxed(for me it's sometimes hard to find).

B. Plan your schedule like a pro

How to balance your work and life no doubt comes first to your time management skill. If finding the activity that can relax yourself the most is the ultimate goal for the "life" part, some strategies are also needed for the "work" part.

Unlike "life" part whose quality largely depends on your subjective feelings i.e., if you feel truely relaxed or not, the quality of the "work" part is usually meassured by some relatively objective metrics like productivity, the amout of tasks you get finished in the given amout of time etc,. Despite the fact that the concept of "productivity" is rather objective, how to be productive can be really mythical. As a consequence, in the past year, I usually just mess around waiting for moment of concentration to come, and the result is usually undesirable.

So, just like you can find certain activities to make yourself relaxed(if you're lucky enough), you can also bridge the time from the moment when you should work to the moment you turn productive.

Idea-wise, I choose to kick off with some light-hearted learning of some classic well-studied fields that you feel interested, for example, I found "ELF format and linker" is sth that always comes into sight when I'm reading papers but I never truly know how it works i.e., those things that look "magic" III. These things are well-studied i.e., no stone is left unturned, so you can just admire its beaty and learn from how it's designed. (I cannot remember exactly, but it's said that there are 4 phrases for the development of a research field: to make it possible, to make it work fast,..., to make it invisible), the thing that I choose here is those "invisible" things, or the "magic" like I describe above.

V. Reading Papers

Reading is another gigantic(I intend to use these kind of "scary/exaggerated" words) part of PhD's life.

A. Amount

B. Why this sentence is written.

Instead of passively(often unwillingly) scanning through the content of each paper (whose output for me is usually just the sense of minor achievement of being able to put the paper from "to-read" list to "have read" list without substantial knowledge gain(both technically and literarily)), I found it beneficial to ask why the author wrote this sentence(paragraph)? Often times, this question can be answered even uncontiously(I think this is an ideal state of paper reading).

Many people said, "read paper like you're the reviewer". Undoubtedly there is some truth to it, as reviewing the paper forces you to grind the sentences and evetually get the most out of it. But I often found this burdensome, mainly because reviewership means huge responsibilities(locating the logical errors, justifying the fulfillment of the evaluation e.t.c.). It takes me huge amout of attention and energy to fully understand the writing and technical chain behind one paper. Maybe for senior members, this can be done easily, but for a newbie paper reader as me, this is more challenging than what I can handle just with the energy I can generate for say, a single day.

So, I see the approach mentioned above a less-demanding version of this reviewership approach. This doesn't need you to be an expert as you're required to be if you were to review this paper, it's just based on the writing flow and technical facts present in the paper.