Future Research Directions towards Science of Cyber Security

Bo Liu, Feng Liu, Gene Tsudik, Jia Xu, Jingguo Wang, Moti Yung, Shouhuai Xu

2019-9-20

Scisec2019 has been successfully held in Nanjing on August 9-11. During the conference, a wonderful panel discussion on the topic of Future Research Directions towards Science of Cyber Security was successfully held. Professor Shouhuai Xu, Professor Moti Yung, Professor Gene Tsudik, Dr. Bo Liu and Professor Jingguo Wang participated in this panel discussion, discussing several issues concerning cyber security， which deepen our understanding of the science of cybersecurity profoundly.

Unlike physics and chemistry, atoms and chemical reactions exist whether we like or not, computer security didn't exist before computers, it can be concluded that there was no computer science. But from another perspective, science is a way to organize our knowledge based on the predictable and record ideas in experiments that are repeatable, there is no need for us to be overly obsessed with defining exactly signs of security. We only need to pay attention on doing things that will be useful for the information security aspects. In addition, it would be a great effort to define what systemization of knowledge in securities.

Clearly, knowledge graph is needed to have a systematic view from the top to down to organize cyber security. And there indeed has many different frameworks about security, but it seems like that knowledge of security frameworks is a matter of minutes, most are temporary things. Nevertheless, people moving in understanding very often, even theoretical physics has some unverified, same thing with chemistry, there is no much different with theoretical computer science. Therefore, whatever we do in computer science eventually lead to something that is useful in computation, it can be useful in other sciences. And eventually all these useful things theoretically has to be also useful in the practice of redesign as well as advance information technology. It's good that everyone has their own understanding of computer security, and frameworks are great for they give a lot of thoughts. Just as the graph shows that we should be a blind and work as a blind, always be surprised and try to systemize knowledge.

Since everyone is limited by his own experiences, it's necessary to have interdisciplinary communication to help understand or translate the problem itself to different domains on cyber security. Like macroscopic and microscopic economics, both micro and macro perspectives are important on cyber security, they only differ in the way that level of analysis. When thinking about system security, it's good to focus on one aspect and consider how this aspect can make a link here with different components of the system, and it's important for leaders to discuss cyber security as a strategic issue with the chief information officer, so that they can better manage the risks. Human evolution may be another way to define cyber security, the change of the environment just like the evolution of IT, cyber security may also have an evolutionary law similar to natural selection. And psychology in social science can help understand the motivation of cyber security attack for our adversary is a human. A lot of things that was done in social science, psychology, economics, or even in management science can be applied to understand the issue related with cyber security. But the problem is how to frame the research of the problem unique enough, so it also can contribute back to the management science or social science or psychology. An ideal security expert should be the well trained computer scientists, on that foundation with the knowledge of other disciplines.

Even though metrics are important that can help understand phenomenon and find solutions, there is no such metrics in cyber security. And it may be very difficult to find a law like physics to carry what cyber security should be or how to evolve for its special nature. But we should go into the core of the software language to verify the way we build software. In addition, paying more attention to the assumption, the boundary conditions of the models that we developed, the observation that we try to carry prize, so that it at least can be used to the collection of others research.

As we know that cyber security from the application perspective is about attack and defend. One distinctive feature of security is that there is no single portrait of adversary, which is a moving target. And there's no static situation, the world is going to evolve, so it has to be a dynamic, updatable method by which we characterize trust, the residual thing we tried to characterizes risk, maybe like financial areas, and then try to mitigate it one way or another. There's always security failure, no matter how much formal we make, no matter how good our model is. And most of us do not foresee attacks which will happen. After all discussion of these panelists, we can conclude the key of the conversation is trying to make sure the relevance of the critical research, and making sure what your sooner way in your abstraction is not essential to what you're trying to accomplish.

At the end of the panel discussion, the panelists gave some advices to graduate students. Firstly, it’s highly important for students that their work is not out of date, and should be practically relevant and practically important. Secondly, finding interesting work and concentrating their strength on, no matter which cycle community actually they are doing the work. Thirdly, attending influential conferences if you have any opportunity, it’s pretty good to have a community on cyber security. Last but not least, students should do more hands on events in cyber security.

Disclaimer: This summary is neither reviewed nor edited by the panelists or participants. It is made available on the conference website purely for the purpose of academic knowledge sharing.