# Enlightening Ph.D. Students with the Elegance of Logic

## — My personal memory about Prof. José Meseguer

Shuo Chen
One Microsoft Way
Redmond, Washington, 98052, U.S.A.
shuochen@microsoft.com

**Abstract**

This article provides my recollection about how Prof. José Meseguer enlightened me to study security problems from the logic perspective. His lectures and advices are having a long term influence on my research career.

## Preface

For many of us in the academia, the years in the Ph.D. program are the period when our minds started to open up to the wonder of science and waited to be inspired by some great pioneers in the field. It is one of the most memorable periods in one's life.

The Ph.D. program of computer science in the University of Illinois at Urbana-Champaign (UIUC) consists of three milestones – the qualifying exam, the thesis proposal and the final defense. The first stage, the qualifying exam, has a nice property of "fail-fast". Students are required to pass the exam in the second or the third semester, or they will be asked to quit. The final stage is also short (typically about one year) and often predictable (since the advisor understands the time frame of the student's new job). What I would describe as a long and dark tunnel is the second stage – the baffling period before the thesis proposal. Unlike the first stage, which is mainly to know the field, the second stage is all about knowing yourself – finding out something deep about your true passion. Very fortunately, I got to know Prof. José Meseguer, an enlightening professor who brought the elegance of logic into my mind.

## My research direction before knowing José

My advisor is Prof. Ravi Iyer. He is a renowned expert in the field of fault tolerance and dependable computing. Ravi always encouraged students to study real-world systems to get first-hand experience. He also put great emphasis on empirical measurements of operational data on these systems. A really unique advantage of our

group is that Ravi has a strong background in statistics and probability, because his own Ph.D. degree was in statistics. Our group didn't have much difficulty publishing papers in the most prestigious conference in the field, IEEE DSN.

Ravi envisioned that the fault tolerance expertise in our group could be extended to cover security topics. Under his guidance, a more senior Ph.D. student and I decided to devote our effort to security. Looking back, I see this as a very important growth period in my career. It helped me step into the security area and gave me the confidence to work on real-world systems. I enjoyed so much the real-world systems work, such as modifying network server programs, or even hacking into the OS kernel, to change program behaviors and observe many interesting security consequences caused by these changes. We built automation technologies to conduct large-scale experiments, and systematized the findings by classification and statistics. These studies continued to be published in the fault tolerance community.

Despite the progress, it was difficult to go deeper in my research because there is a fundamental difference between fault tolerance and security: in fault tolerance research, it is often valid to consider faults as a natural phenomenon, and model their arrivals as a stochastic process. Theories of probability and statistics can be nicely applied under this problem setting. Security research, however, usually needs to consider the threat as the action of a deliberate and malicious adversary. It is hard to apply probabilistic approaches to measure the "likelihood of security". In fact, it is even questionable whether such a likelihood can be objectively defined while still being useful. How to formulate a scientific problem then?

This situation baffled me for a few years. On one hand, I was passionate about studying real-world systems to build up my knowledge and collect many empirical insights. On the other hand, these didn't turn into deeper scientific research ideas.

## José's course on formal methods

Although I had fulfilled all the course requirements of the Ph.D. program, Ravi strongly suggested that I should take a few more courses to broaden my scope. He believed that this might help me walk out of the fog. I don't remember why I decided to take José's course on formal methods. It was surely a wise decision, because it opened up a whole new horizon for me.

The lectures in the first few weeks were about natural numbers, arithmetic operations and basic algebras. It amazed me that these elementary-school concepts are so interesting when they are viewed from the perspective of logic. Even more impressively, they were all concretely expressed in rewriting logic, of which the primitive is nothing but matching-and-replacing substrings. The elegance of logic resonated with something hidden in my heart: I like validating claims that can be resolved in a binary

manner, rather than discussing the less exact arguments that are common in other computer science courses.

The course went on. José started to teach how to model an algorithm using rewriting logic and prove its correctness using the Maude theorem prover. At this point, I realized that formal methods are directly relevant to security research. Many important security problems can be defined as program correctness problems, as long as researchers concretely understand the program semantics and the security goals to achieve. In other words, if I was able to define semantics for some insights that I obtained over the years, I would able to bring scientific rigor to my research.

## Face-to-face discussions with José

The most beneficial part of taking José's course was not the lectures, but the invaluable opportunity to discuss ideas with him face-to-face.

It wasn't easy for me to set up the first meeting with José. I was concerned that my ideas were too rudimentary in terms of formal reasoning, and my logic background was quit lacking, so how could José be interested? Eventually, I settled down to one idea and wrote a few pages about it. One day, outside the lecture room, I tried to briefly explain the idea to him. To my surprise, it ended up being a long discussion! José easily understood what I was trying to do, and offered many valuable comments. More importantly, he encouraged me to move forward. This discussion meant a lot for me, because I really needed the encouragement from an expert in the field.

José and I continued the discussion throughout the rest of the semester. We not only discussed specific ideas, but also our thoughts about research in general, such as how theoretical research and empirical research are related, how to show success of a research idea, etc. Through these discussions, it became clear that formal analysis should be a component in my dissertation.

Under the guidance of Ravi and José, I spent one more semester successfully developing the framework for my thesis proposal. I am very grateful for José's enlightenment and encouragement that helped me find my passion and go through the baffling period.

## Our collaborations after my graduation

I joined Microsoft Research Redmond as a security researcher after graduation, and continued to discuss extensively with José. Our project was to use rewriting logic to model the logic of Internet Explorer's graphic user interface, in order to find logic flaws that allow a malicious webpage to spoof the contents in the address bar and the status bar. José brought one of his best students, Ralf Sasse, into this project.

The three of us collaborated tightly, and spent a tremendous amount of effort undererstanding and modeling the source code of Internet Explorer. We flew between Urbana and Redmond several times to expedite the progress. I still remember the night when José waited in the Urbana-Champaign Willard Airport for my flight, which was delayed due to a snowstorm. José brought me to his home and prepared a meal for me. I viewed this as a very special honor that only a close collaborator could have. Yes, José Meseguer, the inventor of rewriting logic, cooked for me!

Our effort was paid off, as we discovered 13 security bugs before Internet Explorer 7 was shipped. Because of the severity, Microsoft asked us to withhold the paper submission. Withholding good new results from publication is a difficult situation for scientists, but José was very supportive, because he understood the societal aspect of security research. Eventually, the project had a happy ending: 11 out of the 13 vulnerabilities were fixed when Internet Explorer 7 was shipped, and our paper was accepted to the top security conference, IEEE Symposium on Security and Privacy.

José and I continued to discuss research ideas because of our shared interest. He invited me to serve on the thesis committee of Ralf Sasse. I know that Ralf and José developed a number of innovative technologies to prove security for a real browser and many cryptographic protocols.

## Long-term influence

I have been working on many security research projects across different areas, including memory safety, browser security, web/mobile application security, and security protocols. Interestingly, program semantics always come into the picture from one angle or another. I continue to be curious about what a program tries to do and what it actually does. Many of my papers demonstrate that logic flaws are causing realistic security and privacy breaches in today's cloud and mobile systems, so formal methods are a valuable solution.

It is clear that the inspiration I got from José many years ago is having a long term influence on my research focus and methodology. I feel very honored to know José as a teacher, a collaborator and a friend. Of course, in his career, José must have inspired many other scholars in different ways. That's why he receives so much respect from the research community. I believe that the respect comes not only from his intellectual contributions, but are a result of his nature of being open, caring, friendly and enlightening. It is really joyful that we are celebrating his achievements. Happy 65$^{th}$ Birthday, José!

## Acknowledgement

The author thanks Cormac Herley for proofreading this article.