Ty Marking 949-274-0522

Mr. Gula

September 30,2017 Mi Casa

12:00pm-2:00pm

Social Mtg. #3

Of the Woes of the Next Generation

Noon lunch on 17th street, if only there was a RPG style quest marker indicator for open parking spaces. A good 15 minutes after first seeing each other engaged in the epic task of finding a spot to halt a few tones of metal, we finally got to Mi Casa, on of Jim Gula’s favorite places to go to dinner with his wife. Thankfully, getting a table was the polar opposite of finding a parking spot. Is there a patron saint of restaurant waits yet? If so I owe them some thanks.

Onto the wonderful conversation I had with Jim. Warning, it was entirely about nerdy and computer science topics. If one were to assign a general theme that most of what we discussed fell under, it would likely be the growing issues in computer science fundamentals and security that will have to be dealt with by my generation. The most defining example of this theme is probably the vast number of places that a program developed by an individual or a small group can be compromised at.

Everyone, individual or company, who publishes or produces code designed to be used by the public or that will contain private information, has a duty to protect that program and data as much as they possibly can. Now, for large companies, it is a delicate balance between paying for the development and testing of security and the potential backlash and fines if a vulnerability is exploited. Some hacks come from companies, cough cough Equifax, playing this game far to greedily, get hacked, and are fined for their negligence. But the topic Jim brought up is what about the individual developer? They cannot possibly have the same level of security as a large company but their products can still be targets. And this is where the problem is, even if the developer devoted every single second of their life to testing the security of the product, a vulnerability could still easily exist arising somewhere in the chain of development leading to the user. Since he is working on an accounting software which is intrinsically a valuable target, Jim was worried about a vulnerability existing that he could do nothing about. It wouldn’t even have to be in his code. If his compiler was compromised, or the compiler that compiled the compiler, or the servers his download is hosted in, or his own private computer, or any of a million other places was compromised, his product could carry malware and vulnerabilities all the way to the end user. There is no easy way to prevent this, only a complete redesign of how software development works could solve this problem. As the value of targets and the skill of hackers increases, something will need to be done eventually. This was just one example of some of the problems we talked about, there is a lot of work to be done but if history has taught us anything its that technology will keep evolving faster than we think.