Questions 02-12-2018

Unleashing MAYHEM on Binary Code:

This article talks about using MAYHEM to find exploitable bugs in binary code. It uses several techniques to find bugs and exploits for specifically binary code, such as hybrid symbolic execution which allows for improved efficiency over similar systems. With all of these techniques considered, do we think that some of the ideas and methods proposed and used in this article can be used to find exploitable bugs and vulnerabilities in a system before the system is deployed to a production environment? On top of this, are there other useful ways to use the information in this article to improve security of a wide variety of applications?

Ransomware: Evolution, Mitigation and Prevention:

Ransomware is a growing issue with attacks being very shadowy figures from an array of global locations using various techniques. With these varying techniques, how might businesses and persons mitigate the effects of ransomware? The attacks usually do not ask for an overly large amount of ransom with the consideration that if it is a low amount, law enforcement cannot afford to expend large amounts of resources on combating it. It seems that it would be easier to mitigate the issue as to avoid it completely. What are some ways that we might can do this?

ShieldFS: A Self-healing, Ransomware-aware Filesystem:

This article discusses a method of detecting and recovering from ransomware using a proposed solution called ShieldFS. I like that the authors discuss some drawback and areas of possible future research to this approach. What if, as addressed in this vulnerability section, attackers somehow can detect ShieldFS and mitigate its detection techniques, or even worse embed the malicious code into ShieldFS or disable ShieldFS? Are these attacks feasible? As mentioned, to do so may compromise the effectiveness of the ransomware. Do we think this is a viable solution to ransomware?