Questions – 03/19/2018

Autonomic Security for Zero Trust Networks:

This article discusses security aspects of a zero-trust network and implementation of these aspects using autonomic loops. We can see from the results of this article that the autonomic response generated by the security loop is much quicker than a manual method. If this security system proves worthy of further research, how might anomaly-based attacks be addressed by this system. It involves monitoring of traffic, so do we think that anomaly attack detection can be integrated? Also, how would the signature-based attacks that are on watched for be updated? There are several methods to do this, so how would this be implemented into the security loop?

Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey:

This article concludes that much improvement can be had by employing updated and accurate training data as well as using an ensemble or multi-part approach to classifiers. With this being the case, what methods of updating the training can we think of? Are there methods of updating the training data accurately and autonomously that we can contemplate? On top of this, can we think of efficient manners of ensemble classification as changes and developments in the field arise?