Adaptive Containerised Honeypots for Cyber-Incident Monitoring

By Amber Higgins

Integrated Masters in Computer Engineering (M.A.I.)
Supervisor: Dr. Stefan Weber

May 2018

The Internet is becoming an increasingly hostile environment, and though the deployment of security technologies is steadily improving over time, there is a huge and increasing gap between current technological threats and the measures in place to mitigate them.

This research has focused on providing enhanced security through incident-monitoring, devising a highly-deployable cyber-incident monitoring system to consolidate threat intelligence collected from a network of honeypots: An approach which promotes reactivity in the face of increased uncertainty about the nature of attacks, emphasising an active rather than passive approach to securing modern infrastructures which have seen an unprecedented growth in connectivity in critical services including health, transport and energy.

In particular, much attention in this research has focused on how such a system can feasibly provide active network defence for organisations in a way that is both practical and usable to operate and maintain. The use of containers and Platform-as-a-Service solutions in the deployment of security applications is an area where there is huge potential in this regard.

While research and industry projects have explored these uses of honeypots before including in the context of cyber-incident monitoring, this research distinguishes itself on the basis of providing a fully-networked system of honeypots packaged as a single deployable unit which can be hosted in Linux-based environments to provide active network defence in modern IT infrastructures.

Attention has also been given to the adaptation of honeypot design to more effectively entice attacks and hence provide improved threat detection, something for which limited conclusive research exists. The exponential increase in connectivity of systems which were traditionally isolated motivates the targeting of such designs at Internet-of-Things botnets, automated attackers whose activities are a growing threat to critical service infrastructures.