Informatics Institute of Technology

In collaboration with

University of Westminster, UK

Quicksand – Reactive Defense System combining with Honeypot and Predictive Intrusion Detection System

A dissertation by

Akalanka Hewawasam| 2015254

Supervised by

Dr. Randil Pushpananda

Submitted in partial fulfillment of the requirements for the

BSc (Hons) Software Engineering

Department of Computing

May 2019

Abstract

Within the centralized and inter-connected architecture of network, vulnerabilities are always possible even with the supreme of security reliance. In cyber security, there are many approaches to obstruct these attacks by setting up security layers and predetermined set of rules by examining the previous attacks such as firewalls and Intrusion Detection Systems. But no one cannot assure and guarantee a total secure network since there is always a possibility for an adversary to breach in. Therefore in the battle between intruder and defender, one needs to think step ahead to gain the advantage over the attacker. One such tool is called “Honeypot”.

Similar to any other technologies, honeypots also have their drawbacks, the greatest one being their limited field of view. Honeypots capture only activity that's directed against them and will miss attacks against other systems. Finger printing is another disadvantages mostly facing in commercial versions of honeypot where the attacker reveal the true identity of the honeypot. Even though honeypot is an exciting buzz word in deception technology over a decade, it still contains some significant deficiencies.

Quicksand is a novel hybrid architecture combining the best features of honeypots and Intrusion Detection systems for achieving better accuracy and scope. It contains several distinct components and act interchangeably to achieve its objective. Basically the system consist of rule based intrusion detection system which initially distinguish the knows attacks and redirect them towards the honeypot, then the predictive Intrusion Detection System, which predict the incoming request as malicious or not and in the case of being malicious it redirect the request towards the honeypot as well and the rest of traffic will be considered as legitimate and divert to the actual server. If any false positives are diagnosed in the honeypot the state changes will be reverted to the actual system

After the completion of the project it has been evaluated by the target audience who experienced in deception technology and tech-savvy inexperienced personnel in deception