Initial Plan: Hardware Testbed for Operational Security within Large Scale Cloud Infrastructure

Author: William Sims

Supervisor: Jenny Highfield

Project Description

Datacentres have recently been labelled as the 14th sector within Critical National Infrastructure (CNI). They are now critical systems for day to day life, and control how most of society functions and operates with minimal downtime and efficient operation being crucial. This factor in mind makes these systems a valuable target and attacks can cause incredibly damage to a nation or even several when performed correctly. These large instalments requires well designed and effective mitigation and defence protocols to ensure operation impact is as minimal as possible, with more and more of these systems built every year to scale to the ever increasing demand of cloud utilities.

My project aims to replicate a small scale datacentre in a testbed environment and allow simulating day to day operation as well as attacks on it. The testbed system will contain a typical if simplified setup of a centre and have multiple entry and exit points allowing for both generic and tailored attacks which should in theory be applicable to a larger centre.

Datacentres are increasingly interconnected, requiring complex chains of networks and pipelines that are highly vulnerable to attacks both directly and indirectly. Effective testing and simulation tools are vital to develop strategies to prepare for and respond to these attacks.

Aims and Objectives

The aim is to develop a simplified testbed that can simulate the flow of resources and data within a datacentre and its pipelines, allowing for the testing of attack scenarios and response strategies to minimise damage and improve incident response without requiring a live attack on a full scale centre. The system will be many interconnected subsystems communicating via networks and buses, with potential for energy usage and cooling requirements to also be an avenue of attack.

My objectives are to:

- Produce a simplified yet accurate testbed of a datacentre
  - Comprising of sensors, actuators and controllers
  - Can respond to both external and internal state change
- Have the capacity to perform different forms of attacks on the testbed
  - Through internal methods and potentially external attacks
  - Which could be potentially detected and mitigated

- Log the data produced from the state of the testbed to a connected device for analysis

Feasibility

The project's main risk is issues with the necessary hardware. Due to the potential complexity of the system several different pieces will be needed to allow for a proper simulation. Issues with this include:

- Understanding what hardware is actually necessitated
- Acquisition of initial hardware
- Acquisition of extra hardware later on in case of changing requirements and faults
- Remaining as faithful as possible to the wider context of a datacentre when simplifying my model
- Implementing safe and efficient simulations of more complex phenomenon (such as temperature and cooling)

My main mitigation plan for these issues is all in my early on planning in which within the first few weeks I aim to have a exhaustive plan of all hardware I'll need, outlining which are necessary and which are not as crucial allowing me the ability to scale as time allows.

Work Plan