Department	School of Computing
Supervisors	Dr Gordon Russell, Richard Macfarlane
Project Title	Introspection of Virtualised Services using AI

PROJECT DESCRIPTION

There has been a huge growth in the use of virtualised technologies for computing. This includes fully virtualised servers in the cloud, as well as more lightweight solutions such as containers or docker. As customers own and maintain such endpoints, there is no guarantee that such systems will be secure. If such systems are attacked by malware or other offensive technologies, the shared nature of the environment means other customers on the same hardware could also be affected.

In cloud-computing environments, each customer's virtual processing node will be one of many nodes on a physical server. From the server, it is possible to examine each virtual node and gain an understanding of what is running there. This could, for instance, allow the server to detect malware running on a virtual node, or gain an understanding of what is running there generally, or to examine the live data being processed on that node. This type of examination, often referred to as introspection, can generally be done using memory snapshots with a framework which well-understands the operating system running there. However, such introspection can slow and expensive, and generally does not consider containers such as docker.

This PhD is concerned with real-time introspection of virtual nodes with a focus on finding particular types of data. Such data could include the data which is associated with a malware attack, such as the shellcode or exploit code. Other pieces of useful data might be the discovery of encryption keys in memory which are being used to encode command and control channels for bots. Such data could in theory reside almost anywhere in memory, Although in some cases knowledge of the node operating system metadata can be helpful, the focus is on categorising data areas without reliance of the OS in a way that a prioritised list of productive memory blocks can be identified in each node which would be the best candidates to look at in order to find the data of interest. In this way, discovering malware could happen in real time with a reasonable probability from outside the virtual node and without needing to scan the whole of memory.

Through the use of AI, it is envisaged that the memory of each node can be categorised into different types, such as "kernel space", "disk cache", "dynamic libraries", "process heap space". By considering each area, a prioritised list of likely productive areas to investigate can be produced. Such areas could be further labelled by considering where within those areas the data of interest is most likely located. Fast scanning techniques can then be employed looking for the teltale signatures of the data of interest, before finally performing a more detailed scan on a small subset of those. As a result, things can be detected in memory much faster than using traditional techniques.

Perspective applicants are encouraged to contact the Supervisor before submitting their applications. Applications should make it clear the project you are applying for and the name of the supervisors.

Academic qualifications

A first degree (at least a 2.1) ideally in Computing with a good fundamental knowledge of Operating Systems.

English language requirement

IELTS score must be at least 6.5 (with not less than 6.0 in each of the four components). Other, equivalent qualifications will be accepted. Full details of the University's policy are available online.

Essential attributes:

- Experience of fundamental Computing
- Competent in Operating Systems and Virtualisation
- Knowledge of Cybersecurity
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:
Containers, Docker, Artificial Intelligence, Software Engineering, Python

Indicative Bibliography	https://link.springer.com/article/10.1007/s12083-021-01281-5 https://par.nsf.gov/servlets/purl/10093193
Enquiries	For informal enquiries about this PhD project, please contact g.russell@napier.ac.uk
Web page	https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process