School of Computing, Engineering, and the Built Environment
Edinburgh Napier University

PHD STUDENT PROJECT

Application instructions:
Detailed instructions are available at :
https://www.napier.ac.uk/research-and-innovation/doctoral-college/how-to-apply

Prospective candidates are encouraged to contact the Director of Studies (see details below) to discuss the project and their suitability for it.

Project details

Supervisory Team:

- DIRECTOR OF STUDY: Dr Gordon Russell (Email: G.Russell@napier.ac.uk)
- 2ND SUPERVISOR: Prof. Richard Macfarlane

Subject Group: Cyber Security and System Engineering

Research Areas: Cyber Security, Artificial Intelligence, Computer Architecture, Machine Learning

Project Title: Introspection of Virtual Machines 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 and docker. As such system are used, various flaws in software and operating systems means that there is no guarantee that these will be secure. If they 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 machine will be one of many machines running on a physical server. From the physical 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.

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 virtual machine operating system's metadata can be helpful, the focus in this research is on categorising data areas without reliance of the OS. For instance, methods could be created to generate a prioritised list of productive memory blocks 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 telltale 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.

References:

[1] https://link.springer.com/article/10.1007/s12083-021-01281-5
[2] https://par.nsf.gov/servlets/purl/10093193

Candidate characteristics

Education:

A second class honour degree or equivalent qualification in Computing

Subject knowledge:

- Good knowledge of operating systems and storage devices.
- Strong motivation, with a keen interest in the area of proposed work.

Essential attributes:

- Good written and oral communication skills
- Good time management

Desirable attributes:

- Virtualisation
- Artificial Intelligence
- Software Engineering
- Python