WM00I-15 Cyber Security for Virtualisation Systems

22/23

Department
WMG
Level
Taught Postgraduate Level
Module leader
Peter Norris
Credit value
15
Module duration
1 week
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

This module considers the cyber security consequences of virtualised systems and the opportunities that they offer. Focusing on software containerisation systems such as Docker, and comparing their properties with other virtualisation tools and techniques, the course looks at the trust relationships and the available security controls between the underlying operating system, the container, or other virtualised environment, and the software executing within the container.

Students on the module will explore the consequences of the fact that all software executes in some context and in some sort of container. It may be as an app on a mobile device, it may be the operating system on a laptop, it may be a virtual device hosted on the cloud, or it could be an embedded system. It is the container and the context that determine what a program does and what resources it can access. Getting this regulation correct is a significant challenge, giving away just enough resource to get the job done but limiting the resource to prevent additional undesirable things being possible.

The module provides students with practical experience of containerisation systems together with the insights necessary to think clearly about them in the context of cyber security. The course will equip them with the understanding they need to be able to hold meaningful conversations with experts in the field and will allow them to more effectively contribute to informed decision-making

about cyber security.

Module aims

To enable students to regulate the various security relationships between components of a virtualised ecosystem.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

Overall context:

- why is virtualisation and containment needed?

Development of containment in computing:

- bare metal evolution, instruction sets, clock speed, storage, multicore
- operating system, multitasking, scheduling, sharing and isolation
- root jails, virtualisation, containers
- resources: cpu cycles, storage, communications bandwidth, entropy, input, output.

Containment ecosystem:

- host, container (guest) and sibling containers (guests)
- virtualisation vs containerisation

Lifecycle of the provision of a service:

- concept, specification, design, development, versioning, signing, testing, deployment, maintenance, evolution, decommissioning, timescales

Security in virtualisation and containment:

- threats, sources, agents, vulnerabilities, exploits, vectors,
- controls, privilege, capabilities – in host and container (guest)
- resource separation, storage, execution, networking – in host and container (guest)

Learning outcomes

By the end of the module, students should be able to:

- Analyse the security relationships within a virtualised ecosystem between a virtualised container and its sibling containers
- Analyse the security relationships within a virtualised ecosystem between a virtualised container and the underlying host
- Evaluate the extent to which a virtualised container ecosystem satisfies its desired security properties

- Configure a virtualised container ecosystem to achieve the desired security properties from the perspective of both the container and the underlying host.

Indicative reading list

Turnbull J; The Docker Book: Containerization is the new Virtualization; Turnbull / Amazon Media
Matthias K, Kane S P; Docker: Up & Running Kindle Edition; O'Reilly (2015)
Docker; [https://docs.docker.com/] accessed 2016-01-04

Subject specific skills

Configure security components

Transferable skills

Problem solving, critical thinking

Study

Study time

Type	Required
Lectures	15 sessions of 1 hour (10%)
Practical classes	15 sessions of 1 hour (10%)
Online learning (independent)	10 sessions of 1 hour (7%)
Assessment	110 hours (73%)
Total	150 hours

Private study description

No private study requirements defined for this module.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A2

	Weighting	Study time	Eligible for self-certification
Coursework	100%	110 hours	Yes (extension)

Practical security configuration of smallscale virtual ecosystem with associated critical evaluation of the process and outcome of the practical activity.

Assessment group R1

	Weighting	Study time	Eligible for self-certification
Coursework	100%		Yes (extension)

100% Assignment

Feedback on assessment

Written feedback provided with the mark via tabula.

Availability

Anti-requisite modules

If you take this module, you cannot also take:

- WM00I-10 Cyber Security for Virtualisation Systems

Courses

This module is Core optional for:

- Year 1 of TWMA-H6C7 Postgraduate Taught Cyber Security Engineering