WM9PG-15 Cloud & Virtualisation Security

24/25

Department
WMG
Level
Taught Postgraduate Level
Module leader
Christo Panchev
Credit value
15
Module duration
4 weeks
Assessment
100% coursework
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 (AHEP 3.1.1, 3.1.2, 3.1.3, 3.2.3, M1., M2.)
- Analyse the security relationships within a virtualised ecosystem between a virtualised container and the underlying host (AHEP 3.1.1, 3.1.2, 3.2.3, M1., M2.)
- Evaluate the extent to which a virtualised container ecosystem satisfies its desired security properties (AHEP 3.1.1, 3.1.2, 3.2.3, 3.3.6, M2., M3.)

- Configure a virtualised container ecosystem to achieve the desired security properties from the perspective of both the container and the underlying host. (AHEP 3.1.1, 3.1.2, 3.1.3, 3.2.3, 3.3.6, M1., M3.)

Indicative reading list

Turnbull J; The Docker Book: Containerization is the new Virtualization, 2014
Matthias K, Kane S P; Docker: Up & Running, O'Reilly, 2015
Docker Documentation, [https://docs.docker.com] accessed 2016-01-04

Research element

There is a strong emphasis on the development, growth and enhancement of individual research skills so as to provide participants with the high level research knowledge, skills and competencies needed to undertake an independent, original piece of research. The module content draws upon and highlights research within the domain and the module assessment requires participants to perform further research before preparing a response to the assessment task.

Subject specific skills

Assessing security of cloud-based and virtualised systems.
Secure containerised systems design and deployment
Secure deployment of cloud-based systems

Transferable skills

Problem solving, critical thinking

Study

Study time

Type	Required
Supervised practical classes	30 sessions of 1 hour (20%)
Online learning (independent)	10 sessions of 1 hour (7%)
Private study	50 hours (33%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Further practical lab work and research.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A

	Weighting	Study time	Eligible for self-certification
Coursework	100%	60 hours	Yes (extension)

Practical work involving security configuration of small scale virtual ecosystem with associated critical evaluation of the process and outcome of the practical activity.

Feedback on assessment

Feedback will be provided as annotated commentary within the submitted work. High level feedback will be provided on a standard WMG feedback sheet. Students will have an opportunity to get further feedback and support directly from the module tutor.

Availability

There is currently no information about the courses for which this module is core or optional.