WM389-15 Network Security

24/25

Department
WMG
Level
Undergraduate Level 3
Module leader
Hany Atlam
Credit value
15
Module duration
11 weeks
Assessment
100% coursework
Study locations
University of Warwick main campus, Coventry Primary
Distance or Online Delivery

Description

Introductory description

Computer automation, the integration of cyber-physical systems and the exponential increase of devices, software and applications increased the security implications that underpin everything we do on the cyberspace. Assessing these cyberinfrastructures for security and resilience necessitates hybrid and proactive approaches to help us to enhance our understanding or baselines of our current systems' security resistance. Cyber Defence has become one of the biggest business priorities in an attempt to deal with dynamic attack vectors while still relying on static controls and measures. It is a systematic approach to help organisation to better articulate, manage and change threat thresholds and improve the effectiveness of security controls. This module seeks to address the core principles, methods, tools and products available used in proactive cyber operations with the aim of preventing cyber-attacks or decreasing the time taken to discover them.

Frameworks to help better understand and conceptualize how adversaries move through the stages of a cyber-attack have come to the forefront of the cyber security industry. Examples of the frameworks currently in use today are the MITRE ATT&CK, Cyber Kill Chain, Diamond Model. Visual methods include attack trees and attack graphs. Collectively, these are effective techniques which can be used to convey the sometimes-complex tactics, techniques and procedures associated with different stages of a cyberattack.

This module equips students to better understand the stages and concepts of a cyber-attack contextualized by some of these frameworks. Additionally, the module will equip and allow students to develop a practical understanding, as well as applying a range of tools, techniques and procedures utilised by adversaries and attackers during each phase of a cyber attack in a manner that is both legal and ethical. Core concepts of cyber security (confidentiality, integrity, availability, identity, authentication, freshness, authorisation) will be introduced in the contexts of several, generic asset configurations and potential threats (malware, phishing, social engineering, man-in-the-middle).

Module aims

The module guides the students through the fundamentals of building and evaluating successful and secure network communication platforms with focus on all strategic, tactical and operational aspects.

This module seeks to address the core principles, methods, tools and products available used in information gathering and analytics so as to aid decision making with the aim of preventing targeted cyber-attacks.

It also provides an overview of network security mechanisms, tools and techniques to better articulate approaches in informed cyber defence.

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.

Cyber Landscape
Honeypots
Threat modelling processes
Network based attacks
intrusion and multi-stage attack analysis
Lockheed Martin Cyber Kill Chain
Diamond Model
MITRE ATT&CK
Active Reconnaissance
Passive Reconnaissance
Re-purposing
Delivery
Exploitation
Installation
Command & Control(C2)
Action on objectives
Legal and Ethical considerations

Learning outcomes

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

- Provide an advanced understanding of knowledge and awareness of frameworks, methodologies, tools and techniques for cyber defence and network attack analysis in terms of their effectiveness and suitability in different organisational contexts and threat and mitigations in ICT systems and the enterprise environment.
- Apply analytical and critical thinking to security technology solutions development and to systematically analyse and apply structured problem solving against business impact due to cyber attacks
- Correlate tools, techniques and procedures within popular cyber attack analysis frameworks with common attacks within the context of cyber-space.
- Examine and evaluate tools, techniques and measures to provide systems and network hardening against pre-defined security baselines in different organisational contexts

Indicative reading list

Bejtlich, Richard, “The Practice of Network Security Monitoring; understanding incident detection and response”, No Starch Press (2013), ISBN : 9781593275341.
Stallings, William, “Cryptography and Network Security: Principles and Practice”, Pearson (2014), ISBN: 9780273793359.
Anderson, R; “Security Engineering”, Wiley (2008), ISBN : 978-0-470-06852-6.
Hamid Jahankhani et. al.; "Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity", Springer (2020), ISBN: 978-3-030-35745-0

Subject specific skills

You will develop skills and actively be engaged in enquiry during the learning process in network security mechanisms, tools and techniques to real-world scenarios, evaluating and comparing their performance, and analysing the results.

You will look at ethics, risk, governance, compliance, the law, and regulations in relation to intelligence gathering in terms of real-world cybersecurity scenarios, to gain an understanding of the underpinning concepts of network defence, and the techniques and systems used to operate them

You will further develop collaborative abilities through practical sessions and seminars as part of the task to cross-fertilise and discuss ideas about the technologies, challenges and opportunities in the domain of enquiry. Information sharing is highly recommended and promoted so as to present news ways of tackling with these security challenges and issues in our modern cyberspace. Students will further develop their collaborative abilities by working closely with employers and academics.

You will work creatively with new ideas and approaches. It will challenge your ability to intellectually, pragmatically and systematically determine the needs in terms of producing appropriate solutions to address aspects of operational information security management based on existing knowledge in the target discipline suitably balanced with your workplace duties and activities

Transferable skills

Communication Research and Analytical Skills Team Work Personal Motivation, Organisation and Time Management

---

Study

Study time

Type	Required
Lectures	12 sessions of 1 hour (13%)
Practical classes	20 sessions of 1 hour (22%)
Work-based learning	32 sessions of 1 hour (36%)
Private study	26 hours (29%)
Total	90 hours

Private study description

Pre-block exercises given on Moodle.
Post-block problem sets released on Moodle.
Free open source virtual environment in which to conduct experiments

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Assessment group A1

	Weighting	Study time	Eligible for self-certification
Individual Report 3000 word report	100%	60 hours	Yes (extension)

Feedback on assessment

Feedback will be given as appropriate to the assessment type:

- verbal formative feedback on lab activities related to in-module assessment.
- written summative feedback on post module assessments.

Availability

Courses

This module is Core for:

- Year 3 of DWMS-H655 Undergraduate Digital and Technology Solutions (Cyber) (Degree Apprenticeship)
- Year 3 of DWMS-H653 Undergraduate Digital and Technology Solutions (Network Engineering) (Degree Apprenticeship)