WM9C2-15 Proactive Cyber Defence

22/23

Department
WMG
Level
Taught Postgraduate Level
Module leader
Christo Panchev
Credit value
15
Module duration
2 weeks
Assessment
100% coursework
Study locations
University of Warwick main campus, Coventry Primary
Singapore Institute of Management, Singapore

Description

Introductory description

The rapid developments in information technology and the proliferation of devices and applications have enabled digital communications at a scale never seen before. The issue of securing the cyberinfrastructures that facilitate these communications has attracted the same level of attention as natural disasters and significant stock market crises. This is because unforeseen security challenges in our networked technologies manifest catastrophic impact on human-to-human, human-to-machine, and machine-to-machine activities carried out over the cyberspace. This module seeks to introduce the students to the state-of-the-art in effective and proactive cyberattack deterrents, including tools and techniques that can have long-term benefits in organisational policies while maintaining the resilience of our agile and delicate cyberinfrastructures.

Module aims

This module aims to introduce the students in the fundamental strategies and emerging tools, techniques and approaches to deter orchestrated cyberattacks and mitigate their impact. Students will be introduced in network security engineering principles and fundamentals in CIAA and AAA while building their understanding of cyber incidents, including their effects, actors and drivers.

The module equips the participants with an in-depth understanding of the fail-safe capabilities of

different systems and mechanisms used to analyse targeted and multi-stage cyber attacks. Students will establish a firm and in-depth knowledge in network security protocols, including their design philosophy and their weaknesses exploited by motivated and resourceful adversaries.

The module also seeks to equip students with the technical explication of threat modelling in identifying and ranking threats against a variety of scenarios using industry-led and experimental approaches. Students are expected to critically synthesise tools and approaches to adequately model threat landscapes against efficient and autonomous information systems while transferring these skills in different areas where potential threats to business operations might be present.

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.

- Confidentiality, integrity, availability.Applied cryptography with applications to confidentiality, integrity; privacy vs confidentiality, trustworthiness and accuracy of data; business continuity and disaster recovery principles.
- Authentication, authorisation and accounting (the AAA of cyber security).Public key infrastructure and Identity management; Protocols for authentication and key establishment;. Access control, Network Access Controls, (NAC); Network Access Protection (NAP); Kerberos; Firewall Technologies, IDPS; HoneyPots; VoIP security
- Vulnerabilities. Constituent elements of a vulnerability: pre-conditions, pre-condition logic, exploits, post-conditions. Vulnerability inventories, disclosure and mitigation; Standard Security Description references; Cyber mission system development frameworks; Cyber defence measurables & evaluation criteria. Virtualisation and the challenges it brings; Threat modelling and vulnerability analysis.
- standard security descriptors, DDoS, EDoS and its variations; Intelligence gathering for adaptive network defence; Kill-chain model and the APTs paradigm; STIX and CybOX; Threat actors. Cyber criminals, hacktivists, state-sponsored attackers (advanced persistent threats) and insider threats (malicious, incompetence, negligence); Cyber threat analytics
- Semantic network and threat modelling techniques. Attack graphs, attack trees and fault trees. The application of attack modelling techniques in aiding attack analysis, event prediction, outlining of mitigation strategies. investigation of incidents and system hardening; STRIDE; DREAD; Experimental approaches; Threat Model Validation & DFDs; Diagram types & Trust Boundaries
- Cyber security in industrial contexts. Supply-chain, autonomous vehicles, cyber physical systems, IoT.

Learning outcomes

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

- Critically synthesise and apply knowledge of different domains in information security in building an understanding of denying, disrupting, destroying, and manipulating capabilities of adversarial actors.
- Provide an in-depth and systematic understanding of methodologies, tools and techniques used in network defence and attack analysis in terms of their effectiveness and suitability in

different organisational contexts and threat landscapes.
- Quantify the probability and impact of cyber-attack using modelling techniques such as attack trees, attack graphs and fault trees and present them to key stakeholders of all levels in an organisation in an easily understood manner
- Flexibly and autonomously apply knowledge on the creation of innovative and pragmatic solutions in network defence as a response to multi-faced, sophisticated and destructive cyber attacks

Indicative reading list

Anderson, R., 2008. Security engineering. John Wiley & Sons.
Caravelli, J. and Jones, N., 2019. Cyber Security: Threats and Responses for Government and Business. ABC-CLIO.
Wang, C. and Lu, Z. eds., 2019. Proactive and Dynamic Network Defense. Springer International Publishing.
Stalling, 2017 Cryptography and Network Security: Principles and Practice, 7th Edition

View reading list on Talis Aspire

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.

Interdisciplinary

This module has been designed to be accessible to both the cyber security management degree and non cyber-security related WMG programmes. Students from selected WMG programmes will be able to develop their understanding of how cyber security affects their discipline by attending this module.

International

The module is designed in such a way that it can be taught anywhere in the world. Learning materials and examples will be drawn from a range of disciplines, cultures and countries covering the whole range of subjects and disciplines taught in WMG.

Subject specific skills

Participants will develop an advanced understanding of a number of network and computer security principles, strategies techniques and concepts through lectures, in-class discussion and case studies outlining a number of real-world practical issues and scenarios.

Transferable skills

Problem solving, self-awareness, communication, information literacy, professionalism

---

Study

Study time

Type	Required
Lectures	15 sessions of 1 hour (10%)
Tutorials	15 sessions of 1 hour (10%)
Online learning (independent)	40 sessions of 1 hour (27%)
Assessment	80 hours (53%)
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 A1

	Weighting	Study time
Case Study on Threat Identification and System Hardening	100%	80 hours

The work will involve the use of open source tools, methods and techniques for network hardening, attack analysis and projection in a given real-life case study related to security breaches and incidents. This work will enable participants to actively reflect upon the given case, critically analyse the techniques used, evaluate threats, benefits and limitations and propose alternative (optimal) solutions. Participants will be asked to demonstrate certain solutions as part of their hands-on work and evidence of protection against network-based attacks in a given case using appropriate forms of reporting. This will be formally communicated through the assessment brief.

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

Courses

This module is Core for:

- Cyber Security Management (new degree)