# WM9PD-15 Network Security

## 25/26

**Department**
WMG
**Level**
Taught Postgraduate Level
**Module leader**
Hany Atlam
**Credit value**
15
**Module duration**
4 weeks
**Assessment**
Multiple
**Study location**
University of Warwick main campus, Coventry

## Description

## Introductory description

Organisations and networks have changed significantly in recent years. Due to the spread of cloud technologies, the development of edge computing, and the emergence of the Internet of Things (IoT), the modern IT environment is characterised by dispersal. Additionally, the expanding use of remote work practices has created new security challenges that demand increased focus. By lowering the attack surface and thwarting complex attempts, network security is essential for protecting valuable assets as well as business-critical equipment. Network security solutions use a tiered approach that covers both internal and external network domains to provide complete protection. Given their presence across numerous domains, including end-point devices, users, applications, and data pipelines, identifying vulnerabilities is essential.
This module equips students with the necessary knowledge and skills to utilize various tools and methods for examining, creating, executing, and overseeing secure network infrastructures. It is assumed that students will already have some background in conventional, potentially insecure, data networks that is patchy and worthy of review. In particular, IPv4, and TCP / UDP are thoroughly covered, supported by extensive analysis of traffic flows using visualisation tools such as Wireshark.

## Module aims

This module aims to equip students with the knowledge and skills necessary to use tools and techniques to analyse, design, implement, and manage secure network infrastructures to improve the security of an organisation's network.

## 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.

The cyber security landscape:
terminology (CIA, AAA, asset, threat, vulnerability, exploit, mitigation)
threats (malware, phishing, pharming, social engineering, insider)
attack surfaces (people, processes, technology, physical).

Network defence:
IPv4 networks, addressing, routing, network architecture, trust domains,
TCP/UDP, packet capture and analysis using wireshark,
experimentation with virtual networks, dual-use tools (nmap, ettercap)
ingress and egress filtering via (stateful) packet firewalls
patterns of attack and related intervention, detection and prevention techniques,
network security testing, concepts, tools, issues,
network security monitoring, passive, proactive, technical, non-technical, consequences
network security audit.

## Learning outcomes

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

- Critically evaluate the security posture of a network
- Recommend security configuration adjustments to achieve a desired security posture
- Apply security configuration adjustments to achieve a desired security posture
- Verify the extent to which configuration adjustments achieve the intended security posture.

## Indicative reading list

IETF, “IETF Request for Comments (RFC)”, https://www.ietf.org/rfc/ [accessed 26 May 2020]

Pfleeger, C. P. and Pfleeger S. L. , "Security in Computing", 4 ed. vol. 604: Prentice Hall, 2007.

Anderson R. , "Security Engineering: A guide to building dependable distributed systems", 2 ed.: Wiley, 2008.

Donahue, Gary A., “Network Warrior”, O'Reilly (2011)

Kozeriok, Charles M., “TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference”, No Starch Press (2005)

## Subject specific skills

Network Security Assessment

## Transferable skills

Problem solving
Critical Thinking
Organisatonal Awareness
Teamwork and collaboration

## Study

## Study time

| Type | Required |
|---|---|
| Supervised practical classes | 30 sessions of 1 hour (20%) |
| Private study | 60 hours (40%) |
| Assessment | 60 hours (40%) |
| Total | 150 hours |

## Private study description

Independent study between workshops

## 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) |

A written report will be required to discuss and explain the implementation of a network design scenario with a primary emphasis on establishing verifiable security solutions.

### Assessment group R

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

A written report will be required to discuss and explain the implementation of a network design scenario with a primary emphasis on establishing verifiable security solutions.

### 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 1 of TWMS-H1S1 Postgraduate Taught Cyber Security Engineering (Full-time)
- Year 1 of TWMS-H1SH Postgraduate Taught Cyber Security Management (Full-time)