UNSW Course Outline

ZEIT8023 Wireless, Mobile and Internet of Things Security - 2024

Published on the 27 Jun 2024

General Course Information

Course Code : ZEIT8023
Year : 2024
Term : Semester 2
Teaching Period : Z2
Is a multi-term course? : No
Faculty : UNSW Canberra
Academic Unit : School of Systems and Computing
Delivery Mode : Online
Delivery Format : Standard
Delivery Location : UNSW Canberra at ADFA
Campus : UNSW Canberra
Study Level : Postgraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

Wireless technologies are ubiquitous in modern systems yet pose unique challenges. This course combines a theoretical knowledge of wireless defence with a practical approach. This course covers current wireless network protocols and the systems typically deployed in network environments, their weaknesses, practical attack methodologies and mechanisms for their defence.

Course Aims

The last few years have seen a dramatic growth in the use of a vast variety of wireless and mobile network devices. It had been hoped that development in security infrastructure would have afforded the necessary protection to safely operate such a significant infrastructure of integrated services. Regrettably this has not been the case. Mariposa botnet, Conficker, Stuxnet, and Zeus (together with variants) have spelt disaster along with botnets, spam, zeroday attacks, trojans, spyware, spoofing, session hijacking, denial of service and many more as well as blended versions of these network attacks – even though the majority of these stacks are not specific to just wireless and mobile networks. Mobile devices once thought to be largely unaffected have seen dramatic changes with over 40 families of mobile malware threats appearing over the last couple of years.

Many of the techniques used to attack networks 10 years ago are still causing considerable damage today. These techniques have been reinvented and are frequently based on variations of basic themes or combinations of these used to form multi-vector and multi-payload attacks. The scale of interconnectivity that has evolved further compounds the damage that such attacks can cause. Further, wireless and mobile network access can bring with it the opportunity for hackers to exploit many of these attacks, all be it in different forms – many of which were not possible with wired networks. As networks have scaled in size and complexity so have attack vectors.

This course will examine the characteristics of a variety of wireless and mobile personal, local and wide area networks, including Bluetooth, NFC/RFID, Android, and IEEE802.11 variants of WLANs. The manner in which

Course Learning Outcomes

Course Learning Outcomes
CLO1 : At the successful conclusion of this course, students will, at a minimum, be able to: undertake defensive and offensive activities as they apply to wireless technologies.
CLO2 : At the successful conclusion of this course, students will, at a minimum, be able to: evaluate the security implications of wireless technologies and environments.
CLO3 : At the successful conclusion of this course, students will, at a minimum, be able to: analyse current issues in wireless technologies and communicate risks and mitigations to technical and non-technical audiences.

Course Learning Outcomes	Assessment Item
CLO1 : At the successful conclusion of this course, students will, at a minimum, be able to: undertake defensive and offensive activities as they apply to wireless technologies.	• Online Learning Activities
CLO2 : At the successful conclusion of this course, students will, at a minimum, be able to: evaluate the security implications of wireless technologies and environments.	• Essay • Online Quiz • Online Learning Activities
CLO3 : At the successful conclusion of this course, students will, at a minimum, be able to: analyse current issues in wireless technologies and communicate risks and mitigations to technical and non-technical audiences.	• Essay • Online Learning Activities

Learning and Teaching Technologies

Moodle - Learning Management System | 802.11 take home lab. Online resources for training to be provided.

Other Professional Outcomes

Wireless technologies are ubiquitous in modern systems yet pose unique challenges. This course combines a theoretical knowledge of wireless defence with a practical approach. ZEIT8023- Wireless, Mobile and Internet of Things Security covers current wireless network protocols and the systems typically deployed in network environments, their weaknesses, practical attack methodologies and mechanisms to defend against such attacks.

At the successful conclusion of this course, students will, at a minimum, be able to:

CLO.1 Undertake defensive and offensive activities as they apply to wireless technologies.

CLO.2 Evaluate the security implications of wireless technologies and environments.

CLO.3 Analyse current issues in wireless technologies and communicate risks and mitigations to technical and non-technical audiences.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Essay Assessment Format: Individual Short Extension: Yes (5 days)	40%	Start Date: Not Applicable Due Date: 20/10/2024 12:00 AM
Online Quiz Assessment Format: Individual	10%	Start Date: Not Applicable Due Date: 14/08/2024 12:00 AM
Online Learning Activities Assessment Format: Individual	50%	Start Date: Not Applicable Due Date: 18/10/2024 12:00 AM

Assessment Details

Essay

Course Learning Outcomes

- CLO2 : At the successful conclusion of this course, students will, at a minimum, be able to: evaluate the security implications of wireless technologies and environments.
- CLO3 : At the successful conclusion of this course, students will, at a minimum, be able to: analyse current issues in wireless technologies and communicate risks and mitigations to technical and non-technical audiences.

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students can see Turnitin similarity reports.

Online Quiz

Course Learning Outcomes

- CLO2 : At the successful conclusion of this course, students will, at a minimum, be able to: evaluate the security implications of wireless technologies and environments.

Assignment submission Turnitin type

This is not a Turnitin assignment

Online Learning Activities

Assessment Overview

written notes encompassing the learning outcomes of the practical lab sessions combined with evidence of individual learning and critical analysis .

Course Learning Outcomes

- CLO1 : At the successful conclusion of this course, students will, at a minimum, be able to:

undertake defensive and offensive activities as they apply to wireless technologies.

- CLO2 : At the successful conclusion of this course, students will, at a minimum, be able to: evaluate the security implications of wireless technologies and environments.
- CLO3 : At the successful conclusion of this course, students will, at a minimum, be able to: analyse current issues in wireless technologies and communicate risks and mitigations to technical and non-technical audiences.

Assignment submission Turnitin type

This is not a Turnitin assignment

General Assessment Information

For all assessment tasks, you are permitted to use standard editing and referencing functions in word processing software. You must not use any functions that generate or paraphrase [or translate] passages of text, whether based on your own work or not. Please note that your submission will be passed through an AI-generated text detection tool. If your marker has concerns that your answer contains passages of AI-generated text you may be asked to explain your work. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.

Grading Basis

Standard

Requirements to pass course

Students will be required to recieve a minimum pass conceced in all assessments.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 15 July - 19 July	Lecture	Week 1 will focus on an introduction to the course and wireless security. This will involve the lecuturer providing an overview of the course and in introduction to the topics that will be the focus of our discussion activities.
Week 2 : 22 July - 26 July	Online Activity	Week two will be in introduction to privacy. Students will be perscribed reading activities and will be required to contribute to online discussions.
Week 3 : 29 July - 2 August	Online Activity	During week three, students will be introduced to the concept of ethics through a number of activities and events that have taken place over the past twenty years in wireless technologies and research.
Week 4 : 5 August - 9 August	Tutorial	In week four, students will be introduced to Wireless reconnisance as part of an individual tutorial activity.
Week 5 : 12 August - 16 August	Tutorial	Week 5 will see students engage in their tutorial on 802.11 attack and defence, including client based systems.
Week 6 : 19 August - 23 August	Tutorial	Week 6 will be a continuation of the 802.11 attack and defence tutorial.
Week 7 : 9 September - 13 September	Online Activity	Week 7 will be in introduction and online demonstration of Software Defined Radio.
Week 8 : 16 September - 20 September	Online Activity	Week 8 will be in introduction to IOT systems and security considerations.
Week 9 : 23 September - 27 September	Tutorial	Week 9 will be a continuation of our exploration of IOT systems and security considerations.
Week 10 : 30 September - 4 October	Online Activity	Week 10 will explore national security and critical infrastructure, and the role & risks of wireless technologies in this domain.
Week 11 : 7 October - 11 October	Tutorial	Week 11 will continue our exploration of national security and infrasturcutre.
Week 12 : 14 October - 18 October	Activity	Week 12 will wrap up and look to finalise any lab activities, disucssions or tutorial contents.

Attendance Requirements

Not Applicable - as no class attendance is required

Course Resources

Prescribed Resources

None

Recommended Resources

None

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
	Kieran Deale					No	No
	Edward Farrel l					No	Yes

Other Useful Information

School-specific Information

The Leaning Management System

Moodle is the Learning Management System used at UNSW Canberra. All courses have a Moodle site which will become available to students at least one week before the start of semester. Please find all help and documentation (including Blackboard Collaborate) at the Moodle Support page.

UNSW Moodle supports the following web browsers:
- Google Chrome 50+
- Safari 10+

Internet Explorer is not recommended. Addons and Toolbars can affect any browser's performance.

Operating systems recommended are:
- Windows 10,
- Mac OSX Sierra,
- iPad IOS10

Further details:
Moodle System Requirements
Moodle Log In

If you need further assistance with Moodle:

For enrolment and login issues please contact:
IT Service Centre
Email: itservicecentre@unsw.edu.au
Phone: (02) 9385-1333
International: +61 2 9385 1333

For all other Moodle issues please contact:
External TELT Support
Email: externalteltsupport@unsw.edu.au
Phone: (02) 9385-3331

International: +61 2 938 53331

Opening hours:

Monday – Friday 7:30am – 9:30 pm

Saturday & Sunday 8:30 am – 4:30pm

Study at UNSW Canberra

Study at UNSW Canberra has lots of useful information regarding:

- Where to get help
- Administrative matters
- Getting your passwords set up
- How to log on to Moodle
- Accessing the Library and other areas.

UNSW Canberra Student Hub

For News and Notices, Student Services and Support, Campus Comminity, Quick Links, Important Dates and Upcoming Events

School Contact Information

Deputy Head of School (Education): Dr Erandi Hene Kankanamge

E: e.henekankanamge@adfa.edu.au

T: 02 5114 5157

Syscom Admin Support: syscom@unsw.edu.au

T: 02 5114 5284

Syscom Admin Office: Building 15, Level 1, Room 101 (open 10am to 4pm, Mon to Fri)