Design of Computer Networking Courses with Major in Cyber Security

SAVITRI BEVINAKOPPA, AMMAR ALAZAB, TONY JAN
School of Information Technology and Engineering
Melbourne Institute of Technology
288 La Trobe St, Melbourne, VICTORIA
AUSTRALIA
sbevinakoppa@mit.edu.au, aalazab@mit.edu.au, tjan@mit.edu.au   http://www.mit.edu.au

Abstract: - Melbourne Institute of Technology (MIT) is leading private provider that is offering course in Information Technology, Engineering and Business area. MIT is the only private provider in Australia to obtain accreditation from Australian government agency: Tertiary Education Quality and Standards Agency (TEQSA), International professional bodies such as Engineers Australia, Australian Computer Society and Accounting bodies. MIT expanded number of course offers along with current courses in Cyber Security area particularly Bachelor of Networking (BNet) and Master of Networking (MNet) courses Major in Cyber Security. These two courses are designed carefully by benchmarking with other higher educational institutes and current trends in industry. Currently students have expressed interest in enrolling in these new courses as they can have two areas of expertise: Computer Networking and Cyber Security.

Key-Words: Course Design, Computer Networking, Cyber Security, Bachelor degree, Master degree

1 Introduction

Melbourne Institute of Technology (MIT) is offering a Bachelor of Networking (BNet) and Master of Networking (MNet) courses Major in Cyber Security, in addition to the existing general BNet and MNet courses. The purpose of this paper is to outline the concept for introducing Networking courses with Cyber Security Major.

Section 2 provides background information on the concept of new course design. Course design based on conceptual level to advanced level for BNet and MNet are explained in section 3. Conclusion is given in section 4.

2 Background

The Bachelor of Networking degree with Cyber Security Major is targeted at candidates with a successful completion of Australian Year 12 or equivalent, looking at their tertiary course with a view to build their career as expert Cyber Security professionals. Graduates with a Bachelor of Networking in Cyber Security will have the skills and expertise required to protect critical information stored in an organisation’s computer and network systems. In deciding the course structure, the aim is to leverage BNet’s existing Cyber Security units with the introduction of some new units.

The Master of Networking with Cyber Security Major is targeted at graduates of an Australian Bachelor degree or equivalent in and IT or related discipline who wish to build their career as expert Cyber Security professionals. Graduates with a Master of Networking in Cyber Security will have the skills and expertise required to protect critical information stored in an organisation’s computer and networked systems. In deciding the course structure, the aim is to leverage MNet existing Cyber Security units with the introduction of some new units if required.

3.1 Bachelor of Networking Major in Cyber Security

Bachelor of Networking Major in Cyber Security course has two components: Computer Networking and Cyber Security. The following sections explain how these two areas are covered in the new course curriculum.

3.1.1 Coverage of networking from fundamentals to advanced theory and practice

The topics of networking will be introduced at three sequential levels identified by OSI layers:

- Fundamentals of Computer Networks (units BN103, BN106)
- Data Link and Network layers (units BN202, BN321)
- Application Layer (unit BN206)
- Wireless Networks (unit BN303)

Enterprise networks comprise a corporation's communications backbone, connecting computers and related devices across complex workgroup networks. Networking courses will cover operation, configuration and verification of an organisation's network technologies. These courses will combine lectures with hands-on real laboratory scenarios.

Fundamentals of Computer Network (BN103, BN106)

BN103 Platform Technologies and BN106 Networking Fundamentals are first year units in BNet course. The primary objective at this level is for students to learn the fundamental principles underlying computer networks and digital communication. These units covers basic understanding of the computer organisation, Local Area Networks (LAN), Wide Area Networks (WAN), transmission media and concepts of data communications.

Data Link and Network layer (BN202, BN321)

BN202 Internetworking Technologies and BN321 Advanced Network Design units cover understanding of Open Systems Interconnections (OSI) layers of data communications, protocols used in each layer and advanced networking design approach based on various real world case scenario. Networking and switching techniques have been covered. Switching techniques are extensively discussed that was used in circuit switching for voice and packet switching for data. This course focuses on packet switching for computer networks and protocol design. In summary topics in the course include: computer networks over-view; OSI layers, queuing theory; data link layer protocols; flow control; congestion control; routing; local area networks; transport layer.

Application Layer (BN206)

BN206 System Administration unit covers system application such as Linux and Microsoft Server. The Application layer supplies network services to end-user applications. Network services are typically protocols that work with user's data.

Wireless networks (BN303)

BN303 Wireless Networks and Security unit covers wireless network communication technology and security issues. Students learn how to configure wireless routers for local and remote workers. They will gain skill in securing wireless networks. The content of this unit will cover the following areas:

- Wireless communication architecture
- Wireless networks and protocols
- Security vulnerabilities, attacks, mitigation technique.
- Wireless LAN and WLAN architecture and privacy methods
- Implementation and management of WLAN security.

2.1.1 Coverage of cyber security from fundamentals to advanced theory and practice

The topics of cyber security will be introduced in three sequential levels

- Conceptual level (BN200, BN223)
- Technical level (BN303, BN309)
- Application level (BN323, BN309)
- Enterprise Level (BN324)

In the conceptual layer, students will be exposed to the necessity of cyber security for businesses. The students will gain the basic knowledge of confidentiality, integrity, and availability. The students will learn about the cyber threats and attacks followed by their basic mitigation mechanisms. Students will learn the basic mechanism of elementary security tools such as firewall and access control list (router based) for computer network. In addition, students will learn how to perform business contingency planning to support the small to medium enterprises. Overall, students will gain knowledge and skills in SFIA level 1 in which they can apply technical skills and participate in cyber security projects with significant contributions.

At the technical level, students will learn the actual technical solutions for wireless networks and cyber security architectures. Students will gain in-depth understanding of existing attacks and threats including Denial of Service attacks and other sabotages stemming from their understanding from conceptual level. Students will also learn the technical solutions such as advanced firewall, router security, layer 2 switch security followed by introduction to basic Intrusion Detection System. Students will be equipped with the knowledge of cyber network security architecture and solutions equipping them to be able to design and deploy the cyber security solutions, as required in SFIA level 1-2.

At the application level, students will use their technical knowledge to advice and recommend cyber security solutions to businesses. The students will be exposed to the ethical hacking and penetration testing followed by the case studies of past business failures involving cyber security. Students will learn the best business practices in cyber security followed by the standards, legal and professional requirements. Students will be equipped with the knowledge and skills to recommend and lead cyber security projects, equivalent to SFIA level 3.

Description of Cyber Security Major units

BN200 Network Security unit provides students with a comprehensive overview of the field of network security, security risks and countermeasures associated with network connectivity. Students will gain knowledge and skills to understand, apply and manage network security. There are some activities designed to protect network data that include protecting the usability, reliability, integrity, and safety of network and data.

The unit will help students to identify common security vulnerabilities, threats and in depth analysis of these threats that network users often face. It will help students to respond to and recover from security incidents through exercises.

BN223 Cyber Security Principles: Students will be able to provide security solutions to businesses with in-depth knowledge of cyber threats and corresponding security protocols [1, 2]. Students will also be able to provide security solutions to businesses with in-depth knowledge of cyber threats and its corresponding security protocols. Students will also be able to plan and implement operational assurance program for enterprise information infrastructure.

BN303 Wireless Networks and Security: In this unit, students will gain knowledge of wireless network communication technology and security issues. Students will learn how to configure wireless routers for local and remote workers. They will gain skill in securing wireless networks [3].

BN309 Computer Forensics: This unit provides students with an understanding and appreciation of the discipline of Computer Forensics. They will also learn how Computer Forensics interacts with other organisational groups, especially with general management and with other forensics groups [4].

BN323 Ethical Hacking and Security Governance: Students will be able to perform ethical hacking and vulnerability testing on enterprise systems with demonstrated knowledge of network vulnerabilities and security protocols. They will be able to provide cybersecurity solutions with in-depth knowledge of ethical, legal, and professional governance and standards [5].

BN324 Enterprise Cyber Security and Management: Students will be able to identify cyber issues to a board in terms that are relevant to enterprise organisations. 'Identity' will be addressed; especially the challenges that are associated with access control in a federated environment during times of transition such as during merger and acquisition. The highly interconnected nature of Cyber-Physical systems are analysed to help provide a framework to reason about consequences (and their mitigation) in the face of cyber threat. Trends in cloud, IOT, analytics, mobile and social are looked at from the cyber perspective [6, 7].

As explained above, each unit is scaffolded with basic level to advanced level units offering comprehensive overview of cyber security.

3.2 Master of Networking Major in Cyber Security

Master of Networking Major in Cyber Security course has two components: Computer Networking and Cyber Security. The following sections explain how these two areas are covered in new course curriculum.

3.2.1 Coverage of networking from fundamentals to advanced theory and practice

The topics of networking will be introduced in three sequential levels

- Fundamentals of Computer Network (MN503)
- Data Link and Network layers (MN621)
- Wireless Networks (MN603)

Enterprise networks comprise a corporation's communications backbone, connecting computers and related devices across complex workgroup networks. Networking courses will cover operation, configuration and verification of network technologies. The course will combine lectures with hands-on real lab scenarios.

Fundamentals of Computer Network (MN503)

MN503 Overview of Internetworking covers the fundamental principles of computer networks and digital communication. This unit provides students with the knowledge and skills to specify, configure, and manage a medium sized network. The unit provides an overview of internetworking topologies and technologies. The unit topics are:

- Overview of internetworking topologies and technologies
- Internetworking components and network protocols
- OSI model, top-down design
- Internetworking architectural infrastructure in application and transport layers.
- Emerging trends and real world case studies [8].

Data Link and Network layer (MN621)

MN621 Advanced Network Design will focus on plan, design, configure, test and troubleshoot both local area networks and wide area networks. Students will gain knowledge thorough switching, routing concepts and practical knowledge of the use and configuration of network elements such as routers and switches. Students will also be able to effectively administer both local area networks and wide area networks [9].

This unit will cover the following topics:

- LAN design concepts and configuration, virtual LANs
- WAN design concepts and configurations: routing protocols
- LAN and WAN networks testing and troubleshooting
- Enterprise Networks: Software Defined Networking (SDN), Internet of Things (IOT)

Wireless networks (MN603)

MN603 Wireless and Network Security unit enables students to gain in-depth knowledge of wireless network communication technology and security issues. Students learn how to configure wireless routers for local and remote sites. The content of this unit will cover the following areas:

- Wireless communication architecture
- Wireless networks and protocols
- Wireless LAN architecture and security methods
- Implementation and management of WLAN security
- Ethical implications of wireless networks

3.2.2 Coverage of cyber security from fundamentals to advanced theory and practice

The topics of cyber security will be introduced in three sequential layers

- Conceptual level (MN502)
- Technical layer (MN603, MN623)
- Application layer (MN624)

In conceptual layer, students will be exposed to the necessity of cyber security for enterprises. The students will gain the basic knowledge of confidentiality, integrity, and availability. The students will learn about the cyber threats and attacks followed by their basic mitigation mechanisms. Students will learn the basic mechanism of elementary security tools such as firewall and access control list (router based) for computer network. In addition, students will learn how to perform business contingency planning to support small to medium enterprises. Overall, students will gain knowledge and skills in SFIA level 2 in which they can apply technical skills and participate in cyber security projects with significant contributions.

In technical layer, students will learn the actual technical solution for the cyber security architecture. Students will gain in-depth understanding of existing attacks and threats including Denial of Service attacks and other sabotages stemming from their understanding from conceptual layer. Students will also learn the technical solutions such as advanced firewall, router security, layer 2 switch security followed by introduction to basic Intrusion Detection System. Students will be equipped with the knowledge of cyber network security architecture and solutions equipping them to be able to design and deploy the cyber security solutions, as required in SFIA level 2-3.

In application level, students will use their technical knowledge to advice and recommend cyber security solutions to business grade. The students will be exposed to the ethical hacking and penetration testing followed by the case studies of past business failures involving cyber security. Students will learn the best business practices in cyber security followed by the standards, legal and professional requirements. Students will be equipped with the knowledge and skills to recommend and lead cyber security projects, equivalent to SFIA level 3.

Description of Cyber Security Major units

MN502 Overview of Network Security provides a comprehensive overview of the field of network security, security risks and countermeasures associated with network connectivity. This unit covers threats, attacks, and vulnerabilities; technologies and tools for combating attacks, architecture, and design; identity and access management; risk management; and cryptography. Student will learn essential skills for collecting packets from networks. This knowledge will lead students to be able to undertake analysis of network traffic data, with the intention of preventing, or quickly identifying malicious activity in later unit such as MN603.

MN603 Wireless Networks and Security provides in-depth knowledge of wireless network communication technology and security protocols. Students will be exposed to a wide range of techniques, tools and policies to secure wireless networks and wireless connected appliances. In this unit, students can apply appropriate security tools and auditing techniques to protect wireless computing environments.

MN623 Cyber Security and Analytics unit has been designed to enable students to gain knowledge and understanding of the range of advanced threats, vulnerabilities and risks that impact on both individuals and organizations [10]. This unit evaluates and applies contemporary intelligent cyber security solutions for enterprise use. Students will be able to provide advanced security solutions to the business enterprises with in-depth knowledge of cyber threats and its corresponding security protocols.

The students will exercise their skills and knowledge of data analytics in selecting and deploying advanced and intelligent cybersecurity systems for enterprise security.

This unit will cover the following topics:

- Advanced threats and attacks on enterprise systems (cracking, spoofing, hijacking, and resource attacks)
- Security technologies (Access control, Firewalls, VPNs, and Intrusion Detection System)
- Data classification and management for risk assessment
- Decision support system for security control
- Intelligent security management systems

MN624 Digital Forensics provides in-depth understanding of digital forensics principles as well as the forensics tools [11]. Students will be able to develop an in-depth understanding of digital forensics principles as well as the tools and configurations available for the same. Students will also be able to perform ethical hacking and vulnerability testing on enterprise systems with demonstrated knowledge of network vulnerabilities and security protocols.

This unit will cover the following topics:

- Security threats facing modern network infrastructures
- Implementation of forensic analysis on network devices
- Administration of effective security policies in social media
- Penetration and intrusion testing (red teaming)
- Collection of forensics materials for specialist analysis
- Legal, ethical, and professional issues in information security
- Information security architecture planning and governance

As explained above, each unit is scaffolded using basic level to advanced level units offering comprehensive overview of cyber security.

4 Conclusion

Currently both BNet and MNet Major in Cyber Security courses have been offered at Melbourne Institute of Technology (MIT). Materials are being prepared by expertise in these areas with current technology and recent published textbooks and research papers.

The laboratory software includes virtualized instances of popular operating systems and a set of cybersecurity apparatus. Students are exposed to the offensive technologies that allow them to realize the impacts of cyber attacks. The newfound knowledge and realization of vulnerability are to encourage and stimulate the students learning in learning defensive technologies.

5 Acknowledgement

Authors would like to acknowledge all academic staff at Melbourne Institute of Technology (MIT) [12] who contributes ideas in designing these courses.

References:

[1] M. E. Whitman, H. J. Mattord, Principles of Information Security, Cengage, USA, 6th Ed., 2018

[2] M. Dawson, M. Omar, New Threats and Countermeasures in Digital Crime and Cyber Terrorism, 1st ed., IGI Global, USA, 2015

[3] O. Jorge, *Guide to wireless communications*. Cengage Learning, 2016.

[4] B. Nelson, A. Phillips, C. Steuart, *Guide to Computer Forensics and Investigations,* 5th ed., Course Technology Cengage Learning, 2016.

[5] M. T. Simpson, N. Antill, Hands-On Ethical Hacking and Network Defense, Cengage, 3rd Ed., 2018

[6] S. Donaldson, S. Siegel, C. K. Williams, Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program against Advanced Threats, Apress, USA, 2015

[7] W. R. Simpson, Enterprise Level Security: Finding Security in an Uncertain Environment, Auerbach Publishers, USA, 2016

[8] W. Stallings and T. L. Case, Business Data Communications-Infrastructure, Networking and Security, 7th ed., Pearson, 2013.

[9] J. Kurose, K. Ross, *Computer Networking: A Top-Down Approach*. 7th ed., Pearson, 2016.

[10] C. Chio, D. Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms, O'Reilly Media Inc., 1st Ed., 2018.

[11] B. Nelson, A. Phillips, C. Steuart, *Guide to Computer Forensics and Investigations*, Cengage Learning, 5th Ed., 2018.

[12] http://www.mit.edu.au/