Assessment Details and Submission Guidelines	
Trimester	T3, 2018
Unit Code	MN502
Unit Title	Overview of Network Security
Assessment Type	Individual Assignment
Assessment Title	Security Challenges in Emerging Networks (Assignment 2)
Purpose of the assessment (with ULO Mapping)	The purpose of this assignment is to develop skills to independently think of innovation. Students will be able to complete the following ULOs: c. Explain the major methodologies for secure networks and what threats they address; d. Identify and report network threats, select and implement appropriate countermeasures for network security.
Weight	20%
Total Marks	70
Word limit	1500 - 2000
Due Date	11:55PM, Wednesday 30/01/2019
Submission Guidelines	• All work must be submitted on Moodle by the due date along with a title Page. • The assignment must be in MS Word format, 1.5 spacing, 11-pt Calibri (Body) font and 2.54 cm margins on all four sides of your page with appropriate section headings. • Reference sources must be cited in the text of the report, and listed appropriately at the end in a reference list using IEEE referencing style.
Extension	• If an extension of time to submit work is required, a Special Consideration Application must be submitted directly to the School's Administration Officer, in Melbourne on Level 6 or in Sydney on Level 7. You must submit this application three working days prior to the due date of the assignment. Further information is available at: http://www.mit.edu.au/about-mit/institute-publications/policies-procedures-and-guidelines/specialconsiderationdeferment
Academic Misconduct	• Academic Misconduct is a serious offence. Depending on the seriousness of the case, penalties can vary from a written warning or zero marks to exclusion from the course or rescinding the degree. Students should make themselves familiar with the full policy and procedure available at: **http://www.mit.edu.au/about-mit/institute-publications/policies-procedures-and-guidelines/Plagiarism-Academic-Misconduct-Policy-Procedure**. For further information, please refer to the Academic Integrity Section in your Unit Description.

Assignment Description

The purpose of this assignment is to develop skills to independently think of innovation. In this assignment students will first learn how to develop knowledge based on current state of the art of an emerging knowledge domain. Then they will learn how to identify plausible security issues in this emerging network-based applications, and finally learn the skill of adding knowledge to existing domain by theoretically developing the corresponding protection mechanism for a particular issue.

Cyber-Physical Systems (CPS) are based on the interaction between digital, analog, physical, and human components engineered for function using integrated physics and logic. These systems aim to provide the basis of our critical infrastructure which results in the basis of emerging and future smart services, and improve our quality of life in many areas [1].

Smart Grid is one of the CPS technologies, which develops and implements measurement science underpinning modernisation of the Nation's electrical power system (electric grid) in order to improve system efficiency, reliability and sustainability, by incorporating distributed intelligence, bi-directional communications and power flows, and additional advancements. For a smart grid network, communications infrastructure/protocols and wireless networking will play an important role in achieving these objectives. As Smart grid adopts new technologies, this emerging field also faces new security threats. Security of Smart Grid networks is a prime concern in today's World.

This assignment includes **five** parts

1. Literature review on Smart Grid Networks.

   The literature review should be supported by at least three (3) academic (Journal/Conference) papers chosen from the current state of the art.

   Your discussion should include:
   - i. Smart Grid network architecture (System Component and Network Components)
   - ii. Recent developments in Smart Grid networks
   - iii. The importance of cyber security in Smart Grid networks

2. Analyse critically, three current or possible future security issues in Smart Grid networks.

   In this section you will analyse critically, three security issues in Smart Grid networks. These issues should be taken from the current state of the art. This section must be supported by at least three (3) references.

3. Propose a possible solution for one of the threats identified in section-2.

   In this part you need to choose one of the issues identified in the previous section and propose a possible solution to this particular security issue.

4. Analyse and discuss a case study related to recent attack on power systems.

   In this section, students will analyse and discuss a recent attack on the networked power system with proper reference.

5. Create a 3 - 5 minutes presentation and present your work during the Lab.

   You have to create a 3 - 5 minutes presentation to present your work in front of your class fellows and tutor during the Lab in **Week 11**.

[1] *Framework for Cyber-Physical Systems: Volume 1, Overview*. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf, accessed December 06, 2018.

Submission Guidelines

- The assignment should be submitted on the Moodle in **two** separate files:
  - The report should be submitted as a Word file
  - The presentation should be submitted as a PPT file
- **Do not use** Wikipedia as a source or a reference.
- Make sure you properly reference any **diagram/graphics** used in the assignment.

Marking criteria:

Section to be included in the report	Description of the section	Marks
Introduction	Introduction of Smart Grid Networks. Introduction should also discusses the report outline.	5
Literature Review	Literature review of Smart Grid Networks • Smart Grid network architecture (System Component and Network Components) • Recent developments in Smart Grid networks • The importance of cyber security in Smart Grid networks	15
Analyse Critically	Analyse critically, **three security issues** in Smart Grid Networks.	12
Threat Mitigation Technique	Discuss in detail a **threat mitigation technique** for one of the security threat	10
Case Study	Analyse and discuss a case study related to recent attack on power systems with proper reference.	10
Report layout	The report layout should be appropriate (following the submission guidelines and containing all the sections mentioned above)	3
Reference Style	Follow IEEE reference style	5
Presentation Slides	The presentation slides should be well organised and clear.	5
Oral Presentation	Delivery of the presentation (quality of the presentation, depth of knowledge on the material presented and ability to answer questions asked by the audience)	5
	Total	**70**

Marking Rubric for Assignment *#2:* Total Marks 70

Grade Mark	HD 80% +	D 70%-79%	CR 60%-69%	P 50%-59%	Fail <50%
	Excellent	**Very Good**	**Good**	**Satisfactory**	**Unsatisfactory**
Introduction /5	Introduction is very well written and the report outline is also discussed	Introduction is well written and the report outline is also discussed	Introduction is generally presented along with the report outline	Introduction is presented briefly and is missing the report outline	Poor Introduction with irrelevant details
Literature review /15	Excellent literature review with proper referencing	Well written literature review presented with correct references	Good literature review presented with references	Brief literature review with proper referencing	Poorly written literature review
Analyse critically /12	Exceptional discussion on security issues in Smart Grid networks. Identifying highly sophisticated and well referenced vulnerabilities	Exceptional discussion on security issues in Smart Grid networks.	Good Discussion on three security issues	Discussion on Two security issues	Unable to identify security issues
Threat Mitigation Technique /10	A very clear and in-depth discussion about threat mitigation technique	Very clear discussion about threat mitigation technique	Generally good discussion threat mitigation technique	Brief discussion about threat mitigation technique	Poor discussion about threat mitigation technique with irrelevant information
Case Study /10	Excellent discussion about the case study	Very Good discussion about the case study	Good discussion about the case study	Brief discussion about the case study	Poor discussion
Report Layout /3	Well-designed layout and proper formatting following the submission guidelines and containing all the sections	Well-designed layout following the submission guidelines and containing all the sections	Good layout following the submission guidelines and containing all the sections	Report layout following the submission guidelines and missing some sections	Report lacks a proper layout
Reference Style /5	Clear styles with excellent source of references	Clear referencing style	Generally good referencing style	Sometimes clear referencing style	Lacks consistency with many errors
Presentation slides /5	Well organised and resourceful	Organised and resourceful	Resourceful but could be better organised	Resourceful slides	Neither resourceful nor well organised
Oral Presentation /5	Good delivery, easy to follow and good interaction	Delivered, easy to follow and provided a level of interaction	Delivered and provided a level of interaction	Delivered	No oral presentation