

IoT & Network Security

Basic Course Information			
Course Number	01005081	Subject Category	Compulsory IM
Class Format	Lecture	Credit Type and Number of Credits	1
Department	Mechatronics	Student Category	Year 4
Period of Study	Semester 2	Classes per Week	2
Required Materials	Cisco Networking Academy		
Instructor	Prasad Tarasudinundorn	Mo Kobayashi	Taraporn Kasattamam

Course Objective
 The course provides students with introduction and basic knowledge of Cloud system, Web application, Introduction of information security, protocol, Authentication techniques, Security measure.

Evaluation/Rubric	Ideal Level of Achievement (Very Good)	Standard Level of Achievement (Good)	Unacceptable Level of Achievement (Fail)
Understanding the CIA	Explain the meaning and specific examples of each of the CIA in cybersecurity.	Explain the meaning of each of the CIA in cybersecurity.	Cannot explain CIA in cybersecurity.
Explain Firewalls	Explain the function and purpose of each layer of the firewall.	Explain the function and purpose of several firewalls.	Cannot explain about any firewalls.
Understanding Security Vulnerabilities	Explain each Security Vulnerabilities.	Explain some Security Vulnerabilities.	Cannot Explain any Security Vulnerabilities.

Relationship with Learning Outcomes
MCI1 Ability to design, propose and develop network systems to control robots/ mechatronic systems.
 Please change
 Please change

Teaching Method
 Using CISCO Networking Academy
 Lecture and some experiment
 Contents can be adjusted depending on the situation

Course Plan	Semester 2	Contents and Method of Course	Goals	Related MOC
1st week		Guidance (Online)	Understanding how to use CISCO Networking Academy	
2nd week		The Need for Cybersecurity Quiz (Online)	Understanding needs for cybersecurity, Understanding CIA, Hackers, Threat, Personal data, Organizational data and Cyberwarefare.	
3rd week		The Need for Cybersecurity Labwork	Check your computer status for example, health and MCG, Understanding Security breach.	
4th week		Attacks, Concepts and Techniques lecture	Understanding Security Vulnerabilities, Malware, Phishing, DDoS, Social Engineering and SEO Poisoning.	
5th week		Attacks, Concepts and Techniques lecture and Quiz	Experiment the process for Attacks, Concepts and Techniques, Understanding Branded Attack and tool kits.	
6th week		Protecting Your Data and Privacy Lecture	Experiment the process for Attacks, Concepts and Techniques	
7th week		Protecting Your Data and Privacy Lecture and Quiz	Understanding Public Key Infrastructure	
8th week		Midterm Exam	Midterm Exam	
9th week		No class (School Event)	No class (School Event)	
10th week		No class (Monday Class)	No class (Monday Class)	
11th week		Protecting Your Data and Privacy Lecture and Labwork	Experiment protect methods on cloud and Understanding Public Key Infrastructure	
12th week		Protecting Your Data and Privacy Labwork	Experiment protect methods	
13th week		Will Your Future Be in Cybersecurity Quiz	Understanding Firewall, Port scanning	
14th week		Will Your Future Be in Cybersecurity Labwork	Understanding OSI and TCP/IP layer model	
15th week		Will Your Future Be in Cybersecurity Labwork	Experiment OSI reference model and each layer firewalls	
16th week		Will Your Future Be in Cybersecurity Labwork	Experiment cybersecurity techniques IDS and IPS	
17th week		Will Your Future Be in Cybersecurity Labwork	Wrap up and do cybersecurity	
18th week		Prepare for Final Exam	Prepare for Final Exam	
19th week		Final Exam	Final Exam	
20th week		Return Exam sheet and feedback	Return Exam sheet and feedback	

Do not

	Examination	Quiz	Midterm Evaluation between students	Report	Portfolio	Other
Basic Ability	10	10		10		
Technical Ability	10	10		10		
Interdisciplinary Ability	20	10		10		