Curriculum Committee Approval: 04/07/2020

*Lecture Contact Hours: 32-36; Homework Hours: 64-72; Total Student Learning Hours: 96-108*
*Laboratory Contact Hours: 48-54; Homework Hours: 0; Total Student Learning Hours: 48-54*

# CUYAMACA COLLEGE
COURSE OUTLINE OF RECORD

## COMPUTER AND INFORMATION SCIENCE 172 – INTERNET OF THINGS (IoT) SECURITY

2 hours lecture, 3 hours laboratory, 3 units

### Catalog Description
The explosive growth of connected IoT devices enables the world's digitization, but also increases the exposure to security threats. You will use the latest technologies to perform vulnerability and risk assessments, then research and recommend risk mitigation strategies for common security threats in IoT systems. The world needs more skilled cybersecurity professionals. Adding IoT Security to your skillset differentiates you from other job candidates. Consider becoming an IoT Specialist in Network Security by combining this course with your CCENT/CCNA Routing & Switching and CCNA Security certifications. Or pair IoT Security with the CCNA Cybersecurity Operations certification and increase your employability with a deeper understanding of the anatomy of an attack and how to mitigate it.

### Prerequisite:
Successful completion of CIS 170

### Entrance Skills
Without the following skills, competencies and/or knowledge, students entering this course will be highly unlikely to succeed:
1) Describe the use of Sensors, Actuators and Microcontrollers
2) Assemble appropriate Sensors, Actuators and Microcontrollers to apply to a specific project in IoT
3) Program microcontrollers
4) Define and analyze an IoT problem
5) Design and implement a solution for an IoT problem

### Course Content
1) IoT Under Attack
2) IoT Systems and Architectures
3) IoT Device Layer Attack Surface
4) IoT Communication Layer Attack Surface
5) IoT Application Layer Attack Surface
6) Vulnerability and Risk Assessment in an IoT System

### Course Objectives
Students will be able to:
1) Conduct end-to-end security assessments of IoT systems to demonstrate vulnerabilities.
2) Recommend threat mitigation measure to minimize the risk in IoT solutions and networks.
3) Gain hands-on experience with IoT prototypes using a Raspberry Pi
4) Become proficient using real-world penetration and vulnerability testing tools such a Kali Linux.

### Method of Evaluation
A grading system will be established by the instructor and implemented uniformly. Grades will be based on demonstrated proficiency in the subject matter determined by multiple measurements for evaluation, one of which must be essay exams, skills demonstration or, where appropriate, the symbol system. The following tools will be utilized to assess the student's proficiency:
1) Assignments
2) Quizzes

3) Final Project
4) Exams.

**Special Materials Required of Student**

None

**Out-of-Class Assignments**

Using Cisco Netacad and Cisco Packet Tracer as a virtualized environment to complete labs designed to reinforce concepts learned in the curriculum

**Minimum Instructional Facilities**

Classroom with computer availability and Internet access

**Method of Instruction**

Lecture, Demonstration, Labs, and Out-of-Class Assignments

**Texts and References**

1) Required (representative example): Cisco Academy IoT Security Curriculum (Online), 2020.
2) Supplemental: None

**Student Learning Outcomes**

Upon successful completion of this course, students will be able to:

1) Demonstrate “White Hat Hacker” skills to perform vulnerability and risk assessment.
2) Research and recommend risk mitigation strategies for common security threats in IoT systems.