



# C-ID Descriptor

## IoT Security

### Descriptor Details

- **Descriptor Title:** IoT Security
- **C-ID Number:** 168
- **Units:** 3
- **Date of Last Revision:** 2/26/2025 07:24:11 PM GMT+0000

### General Description

The Internet of Things (IoT), where people, processes, things, and data are connected via emerging Internet technologies will be introduced. A variety of networking and computer hardware devices will be integrated into end-to-end systems to solve practical problems. Students will develop introductory skills to perform Vulnerability and Risk Assessment of IoT solutions in a specific business context and be able to assess, research, and provide risk mitigation strategies for common security vulnerabilities in IoT systems.

### Prerequisites

None

### Corequisites

None

### Advisories

ITIS 150 - Computer Network Fundamentals (3)  
ITIS 160 – Introduction to Information Systems Security (3)

## Content

1. The things and connections that make up the IoT.
  - a. "Things" that make up the IoT.
  - b. How things connect to other things and to the IoT.
2. Networking devices as part of end-to-end IoT systems.
  - a. How components and devices are needed to build an end-to-end IoT system.
  - b. How Packet Tracer models IoT systems.
3. Scripts that provide IoT functionality to simple network devices
  - a. The value of computer networking.
  - b. Simple network devices for simple applications.
  - c. How Packet Tracer models single-board computers
4. An end-to-end IoT system.
  - a. How the network supports the IoT.
  - b. An IoT system for the Cloud.
5. Example Internet of Things (IoT) Systems
  - a. How Cisco equipment, software, and services enable IoT systems.
  - b. An abstract business model using a diagram that includes product, customer interface, infrastructure management, and financial aspects.
  - c. How IoT systems solve real world problems in healthcare, cities, energy systems, and manufacturing systems.
6. IoT solutions that address real-world social and environmental problems.
7. IoT Security
  - a. The IoT Under Attack
  - b. Explain the unique security challenges in different IoT sectors.
8. IoT Systems and Architectures. Use industry-standard models to explain security requirements in IoT systems.
9. The IoT Physical Device Attack Surface. Perform threat modeling activities to evaluate physical security vulnerabilities in IoT systems.
10. IoT Communication Layer Vulnerabilities. Perform threat modeling activities to evaluate local access security vulnerabilities in IoT systems.
11. IoT Application Security. Perform threat modeling activities to evaluate remote access security vulnerabilities in IoT systems.
12. Assessing Vulnerability and Risk in an IoT System. Use threat modeling and risk management frameworks to recommend threat mitigation measures.

## **Lab Activities**

No information provided

## **Objectives**

*At the conclusion of this course, the student should be able to:*

1. Analyze the things and connections that make up the Internet of Things (IoT), and its connection to the physical world.
2. Build sensor/actuator systems using a variety of computer and networking hardware
3. Use scripts that provide IoT functionality to a single board computer
4. Create an end-to-end IoT system.
5. Design an IoT in solution in that addresses a real-world social or environmental problem.
6. Interconnect end nodes using IP networks and cloud applications.
7. Explain the unique security challenges in different IoT sectors.
8. Perform threat modeling activities to evaluate physical security vulnerabilities in IoT systems.
9. Perform threat modeling activities to evaluate local access security vulnerabilities in IoT systems.
10. Perform threat modeling activities to evaluate remote access security vulnerabilities in IoT systems.
11. Use penetration testing tools to identify vulnerabilities in IoT systems.
12. Use threat modeling and risk assessment frameworks to recommend threat mitigation measures.
13. Explain the impact of emerging technologies on IoT Security.

## **Evaluation Methods**

Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments.

## **Textbooks**

- NetAcad IoT Fundamentals: Connecting Things
- NetAcad IoT Security