| Course Code | Course Title | L | T | P | C |
|---|---|---|---|---|---|
| 1156EC415 | EMBEDDED SYSTEM SECURITY | 0 | 0 | 0 | 2 |

**a) Course Category**

Independent Learning – Self Learning Course

**b) Preamble**

The development of security-hardened embedded systems is a challenge. Vulnerabilities in products ranging from medical devices to industrial control systems and automobiles are being exploited by attackers. However, these systems can be secured by following a variety of best practices. This course provides an overview of unique challenges of building security into embedded devices and discusses state-of-the-art solutions

**c) Prerequisite**

**d) Related Courses**

**e) Course Outcomes**

| CO Nos. | Course Outcomes | Knowledge Level (Based on Revised Bloom's Taxonomy) |
|---|---|---|
| CO1 | Categorize the types of attacks and vulnerabilities leading towards security in embedded system. | K2 |
| CO2 | Understand various implementations of hardware security. | K2 |
| CO3 | Explain security countermeasures and modular exponentiation fundamentals. | K2 |
| CO4 | Understand various implementations of software security. | K2 |
| CO5 | Describe the fundamentals of cloud security. | K2 |

**f) Course Content**

**UNIT I Embedded Hardware Security**

Introduction to system security, vulnerabilities in digital design, testing for vulnerabilities, types of threat – confidentiality threat, integrity threat, availability threat, fraud threat, types of attacks – physical attack, side channel attack, cache attack

**UNIT II Secure Hardware Design**

Building secure systems,Hardware Trojans, hardware Trojan detection, IC design with hardware Trojan prevention, secure FPGA implementation, physically unclonable functions, physically unclonable functions implementation

**UNIT III Countermeasures**

Countermeasures for physical attacks, other counter measures, Modular exponentiation,Modular exponentiation implementation and vulnerability, Modular exponentiation in Cryptography, Montgomery reduction, modified modular exponentiation

**UNIT IV Embedded Software Security**

Introduction to software security, low level security, memory layout, buffer overflow, code injection, other memory exploits, defense against low level attacks, memory safety, secure coding

**UNIT V Network & Cloud Security**

Web security basics, cloud security basics, Network based attacks, denial of service attacks, wireless based attacks, Cloud Security architectures, Isolated server security

**g) Learning Resources**

**Reference Books**


1. https://www.coursera.org/learn/hardware-security
2. https://www.coursera.org/learn/software-security
3. https://www.coursera.org/learn/intro-cyber-attacks/
4. https://www.coursera.org/learn/it-security
5. https://www.coursera.org/learn/cyber-threats-attack-vectors
6. https://www.coursera.org/learn/enterprise-infrastructure-security
7. http://cse.iitkgp.ac.in/~debdeep/courses_iitkgp/HardSec/index.htm
8. https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/index.htm