**[4859]-1079**

# B.E. (Computer Engineering)
# EMBEDDED SECURITY
## (2012 Pattern) (End Sem.) (Elective - II) (Semester - I) (410445 C)

*Time :2½ Hours.]*                                                    *[Max. Marks :70*

***Instructions to the candidates:***

*1) Solve Q. 1 or Q. 2, Q. 3 or Q.4, Q. 5 or Q. 6, Q. 7 or Q. 8, Q. 9 or Q. 10.*

*2) Neat diagrams must be drawn wherever necessary.*

*3) Figures to right indicate full marks.*

**Q1)** a)  Explain in brief eBay data breach.                                    **[5]**

b)  Comment on: Open source software best practice as a counter measures to Heartbleed attack.                                                       **[5]**

**OR**

**Q2)** a)  Explain architecture of Intel AMT.                                    **[5]**

b)  Explain advantages and drawbacks of embedded security and management engine.                                                          **[5]**

**Q3)** a)  Explain load integrity for threat analysis and mitigation.           **[6]**

b)  Write a short notes on next generation EPID.                              **[4]**

**OR**

**Q4)** a)  Explain working of SIGMA protocol in detail.                          **[6]**

b)  Explain in detail security requirements of security and management engine.                                                              **[4]**

**Q5)** a)  Explain in detail Architecture for Embedded IPT (Intel Platform Trust Technology).                                                      **[8]**

b)  Explain Rooting/Jailbreaking attacks with its type.                       **[8]**

**OR**

*Q6)* a) Write a short notes on: [8]

      i) Boot attack

      ii) Evil Maid attack

   b) Compare Integrated vs. Discrete TPM. [8]

*Q7)* a) Explain in detail Digital Rights Management (DRM). [8]

   b) What is the role of following in software based end to end protection.[8]

      i) Content Server

      ii) License Server

      iii) Software Stack

      iv) External Display

<div align="center">OR</div>

*Q8)* a) Explain in detail HDCP (High banwidth digital content protection). [8]

   b) Explain Dynamic Application Loader with neat diagram. [8]

*Q9)* a) Explain how embedded security is provided for IOT (Internet of Things). [9]

   b) Write a short note on: [9]

      i) Trusted Platform Module (TPM)

      ii) Software Guard Extension

<div align="center">OR</div>

*Q10)* a) Explain in detail IOT reference architecture. [9]

   b) Write a short note on: [9]

      i) Protected Input and Output.

      ii) Anonymous Authentication and Secure Session Establishment.

<div align="center">ℰ ℰ ℰ</div>