Gömülü Sistem Güvenli Yazılım Geliştirme Eğitimi

Süre: 3 Gün

Açıklama

Gömülü Sistem Güvenli Yazılım Geliştirme Eğitimi, gömülü sistemlerin yazılım ve donanım bileşenlerini, haberleşme altyapılarını ve güvenlik gereksinimlerini bütüncül bir yaklaşımla ele alarak katılımcılara güvenli yazılım geliştirme konusunda bilgi ve uygulama becerileri kazandırmayı amaçlamaktadır.

Eğitim kapsamında, gömülü sistemlere yönelik siber güvenlik tehditleri, zafiyetler ve riskler değerlendirilerek güvenli yazılım geliştirme modelleri, standartları ve en iyi uygulamalar incelenmektedir. C/C++ ile güvenli kodlama, gömülü sistem mimarileri, firmware güvenliği, haberleşme protokolleri, kriptografi temelleri ve yazılım güvenlik analizleri üzerinde durulmaktadır.

Programda ayrıca Bluetooth, Wi-Fi, Zigbee, LoRa ve MQTT gibi haberleşme teknolojileri, güvenli veri iletişimi, sensör ve eyleyici kullanımı ile statik ve dinamik kod analizi konuları ele alınmaktadır. ESP32 ve ESP8266 NodeMCU platformları üzerinde C dili kullanılarak gerçekleştirilecek donanım tabanlı laboratuvar uygulamalarıyla teorik bilgilerin pekiştirilmesi hedeflenmektedir.

Eğitim sonunda katılımcıların, gömülü sistemlerde karşılaşılabilecek güvenlik risklerini değerlendirebilmeleri, güvenli yazılım geliştirme yaklaşımlarını tanımaları ve gömülü sistemlerin güvenli haberleşme altyapıları hakkında bilgi sahibi olmaları hedeflenmektedir.

Kimler Katılmalı

Gömülü sistemler ve gömülü sistem güvenli yazılım geliştirme model ve süreçlerini öğrenmek isteyen yazılım geliştiricileri e sistem tasarımcıları, yazılım güvenlik testi yapanlar, endüstriyel kontrol sistem ve IoT güvenlik testi yapanlar katılabilirler.

Eğitim İçeriği

1. Yazılım ve gömülü sistemlere yönelik tehditler ve riskler

- Siber güvenlik gerçekleri
- Yazılım güvenliği neden kritik
- Yazılım atak örnekleri

2. Bilgi güvenliği temelleri

- Korumamız gereken bilgi varlıkları
- Zafiyetler ve tehditler
- Risk analizi

3. Güvenli yazılım geliştirme modelleri ve anaçatıları

- Yazılım geliştirme modelleri
- CMMI, SSE-CMM, Microsoft Secure SDLC, OWASP OpenSAMM
- IEC 62443, Common Criteria

4. Zafiyet Veritabanları

- CWE, CVE, CERT, DISA, OWASP Top 10 vb.

5. Endüstri 4.0 ve Dijital Dönüşüm

6. Internetworking Altyapısı ve TCP/IP Protokol Haberleşmesi

7. Güvenli C/C++ kodlama

8. Gömülü Sistemlerden Veri Toplama, İşleme ve Kullanıcıya Sunma

9. Gömülü Sistemlerin Haberleşme Protokolleri

- Gömülü sistem protokol karakteristikleri
- Gömülü sistem protokolleri ve TCP/IP karşılaştırması
- Gömülü sistem haberleşme protokolleri ve kullanım alanları (Bluetooth, Wi-Fi, Zigbee, LoRa, MQTT vb.)
- Gömülü sistem haberleşme uygulamaları

10. Gömülü Sistem Sensör ve Eyleyicileri

11. Firmware güvenliği

12. Kriptografi temelleri

- Simetrik ve Asimetrik kripto sistemleri
- Şifreleme algoritmaları
- Özetleme algoritmaları
- Güvenli haberleşme protokolleri

13. Gömülü Sistemlerde Yazılım Güvenlik Analizi

- Statik kod analizi
- Dinamik kod analizi

14. Sosyal Mühendislik

Ön Koşullar

C veya C++ programlama dilini başlangıç düzeyinde bilmek. Uygulamalar C dilinde ve ESP32 ve ESP8266 NodeMCU gömülü sistemler üzerinde yapılacaktır.