Main References:


Course Purpose & Objectives: The aim of the course is to cover the underlying principles and techniques used in securing CIS and to give examples of how they are applied in practice.

Learning Outcomes: At the end of the course, a student will have an understanding of the themes and challenges of CIS security and the current state of the art. The student will have developed a critical approach to the analysis of CIS security and will be able to bring this approach to bear on future decisions regarding security. Specific learning outcomes include:

• An appreciation of the main threats, attack techniques and defences relevant to the security of CIS

• An ability to identify potential vulnerabilities and propose countermeasures

• An ability to design secure CIS

Topics Overview – Course Content:

1. A general introduction to Cyber Security

2. Anatomy of attacks – including the two stage kill chain and possible interventions to detect, deny, disrupt attacks; an introduction to the CWE, CVE and CAPEC nomenclature

3. Introduction to Industrial Control Systems (ICS) – the effect of interdependences and consideration of non-IP protocols

4. Risk Assessment & Risk Management

5. ICS Security Architecture
6. Security Controls including the ICS-CERT top 7 controls

7. Case studies – Stuxnet, Ukraine 2015 and 2016, and TRITON

8. Future Trends and Research Topics:
   (a) Intrusion Detection and Machine Learning
   (b) Diversity as Defence
   (c) Security Metrics

**Evaluation Methods – Grade Distribution:**

- Homework (40%) ......................... During Course
- Final Exam (60%) ............... Monday 16 December 2019

**Academic Honesty:** It is acceptable to work together in small groups for study and discussing the lab assignments. However, work that you turn in under your name must be your own. **Cheating will not be tolerated; neither during homework nor during exams.** Note that all rules set by the University of Cyprus and the Department of Electrical and Computer Engineering apply.