ISSC480

Course Summary

Course : ISSC480 **Title :**
Length of Course : 8 **Faculty :**
Prerequisites : N/A **Credit Hours :**

Description

Course Description:

This course provides a peek into the latest threats to Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. Students will explore historical attacks against critical infrastructures across the world to develop an understanding of the challenges faced in securing these systems. Key topics such as malware threats, insider attacks, denial of service, hacker attacks, and terrorism will be reviewed. (Prerequisite: ISSC479)

Objectives

O-1: Understand both the historical and current attacks against ICS and SCADA systems.
O-2: Explore the source code of malware that has attacked these systems before to gain insight into how these
malicious programs infect and propagate
O-3: Understand the role that a single individual with access to the internal systems can affect these systems
both digitally and kinetically
O-4: Recognize the vulnerabilities that exist with ICS and SCADA systems not being air gapped and how online
interfaces can expose your network to digital attacks
O-5: Design a security solution that includes incident response, awareness and training, and information sharing with industry groups

Outline

Week 1: Introduction

Learning Outcomes

O-1: Understand both the historical and current attacks against ICS and SCADA systems.
O-3: Understand the role that a single individual with access to the internal systems can affect these systems both digitally and kinetically
O-5: Design a security solution that includes incident response, awareness and training, and information sharing
with industry groups

Required Readings

https://apus.libguides.com/er.php?course_id=87448.

Assignments

Welcome Discussion

Recommended Optional Reading
Recommended Media

Week 2: Threats

Learning Outcomes

O-1: Understand both the historical and current attacks against ICS and SCADA systems.
O-2: Explore the source code of malware that has attacked these systems before to gain insight into how these
malicious programs infect and propagate
O-3: Understand the role that a single individual with access to the internal systems can affect these systems both digitally and kinetically

Required Readings

https://apus.libguides.com/er.php?course_id=87448.

Assignments

Week 2 Discussion

Week 2 Assignment

Recommended Optional Reading
Recommended Media

Week 3: Assessing Threats

Learning Outcomes

O-1: Understand both the historical and current attacks against ICS and SCADA systems.
O-4: Recognize the vulnerabilities that exist with ICS and SCADA systems not being air gapped and how online
interfaces can expose your network to digital attacks
O-5: Design a security solution that includes incident response, awareness and training, and information sharing
with industry groups

Required Readings

https://apus.libguides.com/er.php?course_id=87448.

Assignments

Week 3 Discussion

Week 3 Assignment

Recommended Optional Reading
Recommended Media

Week 4: Vulnerabilities

Learning Outcomes

O-1: Understand both the historical and current attacks against ICS and SCADA systems.
O-3: Understand the role that a single individual with access to the internal systems can affect these systems both digitally and kinetically

Required Readings

https://apus.libguides.com/er.php?course_id=87448.

Assignments

Week 4 Discussion

Week 4 Assignment

Recommended Optional Reading
Recommended Media

Week 5: Security Frameworks

Learning Outcomes

O-3: Understand the role that a single individual with access to the internal systems can affect these systems both digitally and kinetically
O-4: Recognize the vulnerabilities that exist with ICS and SCADA systems not being air gapped and how online
interfaces can expose your network to digital attacks
O-5: Design a security solution that includes incident response, awareness and training, and information sharing
with industry groups

Required Readings

https://apus.libguides.com/er.php?course_id=87448.

Assignments

Week 5 Discussion

Week 5 Assignment

Recommended Optional Reading
Recommended Media

Week 6: Incident Response

Learning Outcomes

O-3: Understand the role that a single individual with access to the internal systems can affect these systems both digitally and kinetically
O-5: Design a security solution that includes incident response, awareness and training, and information sharing
with industry groups

Required Readings

https://apus.libguides.com/er.php?course_id=87448.

Assignments

Week 6 Discussion

Week 6 Assignment

Recommended Optional Reading
Recommended Media

Week 7: Trends

Learning Outcomes

O-1: Understand both the historical and current attacks against ICS and SCADA systems.
O-2: Explore the source code of malware that has attacked these systems before to gain insight into how these
malicious programs infect and propagate
O-3: Understand the role that a single individual with access to the internal systems can affect these systems both digitally and kinetically
O-5: Design a security solution that includes incident response, awareness and training, and information sharing
with industry groups

Required Readings

https://apus.libguides.com/er.php?course_id=87448.

Assignments

Week 7 Discussion

Begin on Week 8 Assignment (Due at end of course)

Recommended Optional Reading
Recommended Media

Week 8: Critical Infrastructure Wrap-up

Learning Outcomes

O-1: Understand both the historical and current attacks against ICS and SCADA systems.
O-3: Understand the role that a single individual with access to the internal systems can affect these systems both digitally and kinetically
O-5: Design a security solution that includes incident response, awareness and training, and information sharing
with industry groups

Required Readings

https://apus.libguides.com/er.php?course_id=87448.

Assignments

Week 8 Discussion

Week 8 Assignment

Recommended Optional Reading
Recommended Media

Evaluation

Grading:

Name	Grade %
Discussions	20.00 %
Welcome Discussion	2.50 %
Week 2 Discussion	2.50 %
Week 3 Discussion	2.50 %
Week 4 Discussion	2.50 %
Week 5 Discussion	2.50 %
Week 6 Discussion	2.50 %
Week 7 Discussion	2.50 %
Week 8 Discussion	2.50 %
Assignments	56.00 %
Assignment #1	14.00 %
Assignment #2	14.00 %
Assignment #3	14.00 %
Assignment #4	14.00 %
Final Assignment	24.00 %
Assignment #5	24.00 %

Materials

Book Title: Various resources from Trefry Library and/or the Open Web are used. Links provided inside the classroom.

Author:

Publication Info:

ISBN: D2L Note

ISSC480 Library eReserves - https://apus.libguides.com/er.php?course_id=87448.

Course Guidelines

Citation and Reference Style

Attention Please: Students will follow the APA Format as the sole citation and reference style used in written work submitted as part of coursework to the University. Assignments completed in a narrative essay or composition format must follow the citation style cited in the APA Format.

Tutoring

Tutor.com offers online homework help and learning resources by connecting students to certified tutors for one-on-one help. AMU and APU students are eligible for 10 free hours* of tutoring provided by APUS. Tutors are available 24/7 unless otherwise noted. Tutor.com also has a SkillCenter Resource Library offering educational resources, worksheets, videos, websites and career help. Accessing these resources does not count against tutoring hours and is also available 24/7. Please visit the APUS Library and search for 'Tutor' to create an account.

Late Assignments

Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. The due date for each assignment is listed under each Assignment.
Generally speaking, late work may result in a deduction up to 10% of the grade for each day late, not to exceed 50% after 5 days.
As a working adult I know your time is limited and often out of your control. Faculty may be more flexible if they know ahead of time of any potential late assignments.

Turn It In

Faculty may require assignments be submitted to Turnitin.com. Turnitin.com will analyze a paper and report instances of potential plagiarism for the student to edit before submitting it for a grade. In some cases professors may require students to use Turnitin.com. This is automatically processed through the Assignments area of the course.

Academic Dishonesty

Academic Dishonesty incorporates more than plagiarism, which is using the work of others without citation. Academic dishonesty includes any use of content purchased or retrieved from web services such as CourseHero.com. Additionally, allowing your work to be placed on such web services is academic dishonesty, as it is enabling the dishonesty of others. The copy and pasting of content from any web page, without citation as a direct quote, is academic dishonesty. When in doubt, do not copy/paste, and always cite.

Submission Guidelines

Some assignments may have very specific requirements for formatting (such as font, margins, etc) and submission file type (such as .docx, .pdf, etc) See the assignment instructions for details. In general, standard file types such as those associated with Microsoft Office are preferred, unless otherwise specified.

Communicating on the Discussion

Discussions are the heart of the interaction in this course. The more engaged and lively the exchanges, the more interesting and fun the course will be. Only substantive comments will receive credit. Although there is a final posting time after which the instructor will grade comments, it is not sufficient to wait until the last day to contribute your comments/questions on the discussion. The purpose of the discussions is to actively participate in an on-going discussion about the assigned

content.

“Substantive” means comments that contribute something new and hopefully important to the discussion. Thus a message that simply says “I agree” is not substantive. A substantive comment contributes a new idea or perspective, a good follow-up question to a point made, offers a response to a question, provides an example or illustration of a key point, points out an inconsistency in an argument, etc.

As a class, if we run into conflicting view points, we must respect each individual's own opinion. Hateful and hurtful comments towards other individuals, students, groups, peoples, and/or societies will not be tolerated.

Communications

Student Communication

To reach the instructor, please communicate through the MyClassroom email function accessible from the Classlist of the Course Tools menu, where the instructor and students email addresses are listed, or via the Office 365 tool on the Course homepage.

- In emails to instructors, it’s important to note the specific course in which you are enrolled. The name of the course is at the top center of all pages.
- Students and instructors communicate in Discussion posts and other learning activities.
- All interactions should follow APUS guidelines, as noted in the Student Handbook, and maintain a professional, courteous tone.
- Students should review writing for spelling and grammar.
- Tips on Using the Office 365 Email Tool

Instructor Communication

The instructor will post announcements on communications preferences involving email and Instant Messaging and any changes in the class schedule or activities.

- Instructors will periodically post information on the expectations of students and will provide feedback on assignments, Discussion posts, quizzes, and exams.
- Instructors will generally acknowledge student communications within 24 hours and respond within 48 hours, except in unusual circumstances (e.g., illness).
- The APUS standard for grading of all assessments (assignments, Discussions, quizzes, exams) is five days or fewer from the due date.
- Final course grades are submitted by faculty no later than seven days after the end date of the course or the end of the extension period.

University Policies

Consult the Student Handbook for processes and policies at APUS. Notable policies:

- Drop/Withdrawal Policy
- Extension Requests
- Academic Probation
- Appeals
- Academic Dishonesty / Plagiarism

- Disability Accommodations
- Student Deadlines
- Video Conference Policy

Mission

The mission of American Public University System is to provide high quality higher education with emphasis on educating the nation's military and public service communities by offering respected, relevant, accessible, affordable, and student-focused online programs that prepare students for service and leadership in a diverse, global society.

Minimum Technology Requirements

- Please consult the catalog for the minimum hardware and software required for undergraduate and graduate courses.
- Although students are encouraged to use the Pulse mobile app with any course, please note that not all course work can be completed via a mobile device.

Disclaimers

- Please note that course content – and, thus, the syllabus – may change between when a student registers for a course and when the course starts.
- Course content may vary from the syllabus' schedule to meet the needs of a particular group.