USAID CYBERSECURITY FOR CRITICAL INFRASTRUCURE IN UKRAINE

Cyber Physical Systems Security (CPSS)

Dr. Kemal Akkaya

Florida International University

COURSE OVERVIEW
DESCRIPTION

- The main objective of this course is to provide the foundations of threats and security in CPS and present some of the solutions. The course covers introductory topics in cyber-physical systems (CPS), cybersecurity and their intersection.

- The goal is to expose students to fundamental security primitives specific to CPS and to apply them to a broad range of current and future security challenges. The topics will cover the cyber and physical attacks, security of CPS specific communication protocols.

OUTCOMES

- Introducing the foundations of threats and security in CPS and its applications.
- Understanding the fundamental security primitives specific to CPS.
- Knowledge on device security, key management, and privacy.
- Know the increasing threat scape in CPS with some basic hands-on experience.
- Understand the cyber and physical attacks, security of CPS specific communication protocols.

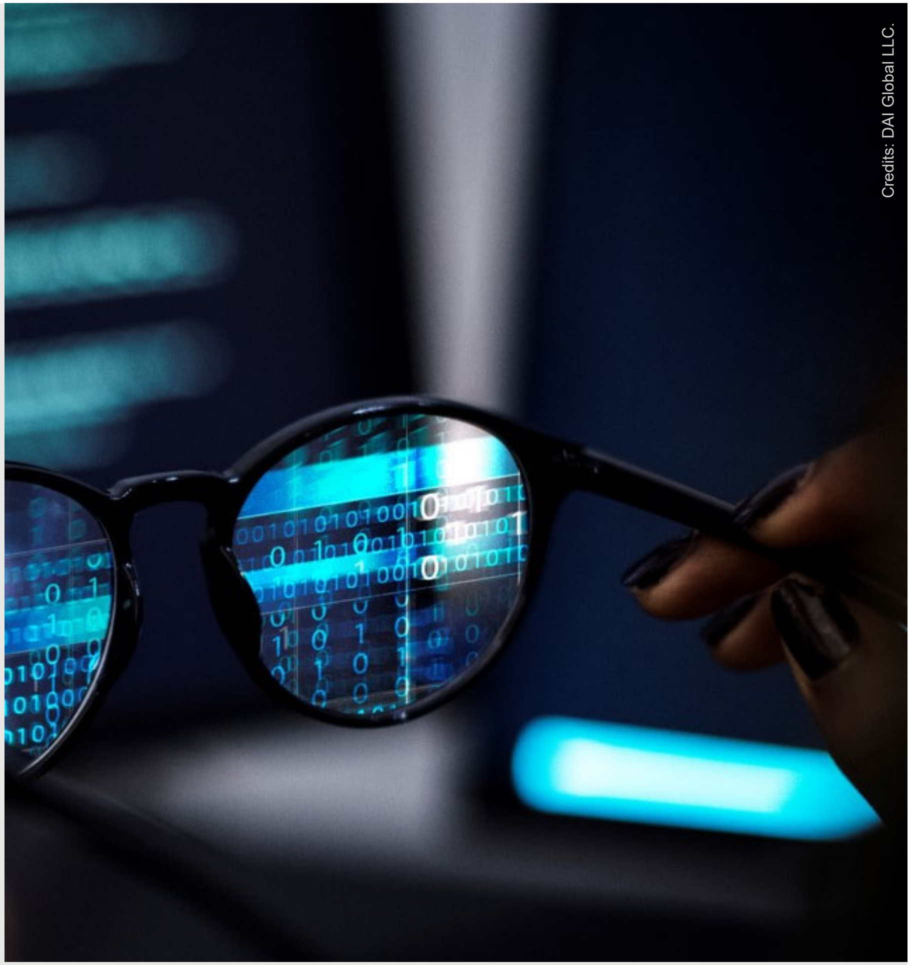
EVALUATION

- There will be 2 quizzes
- The first one (40 points)
- The second one (60 points)

WEEK I
INTRODUCTION TO THE DEFINITION OF CPS

- Review of Cyber Physical Systems Security, Industrial control, SCADA, Applications of CPS.

- Review of Networking topics and Control Theory, TCP/IP, Protocols, system modeling.



Credits: DAI Global LLC.

WEEK 2
ELEMENTS OF A CPS INCLUDING SCADA SYSTEMS

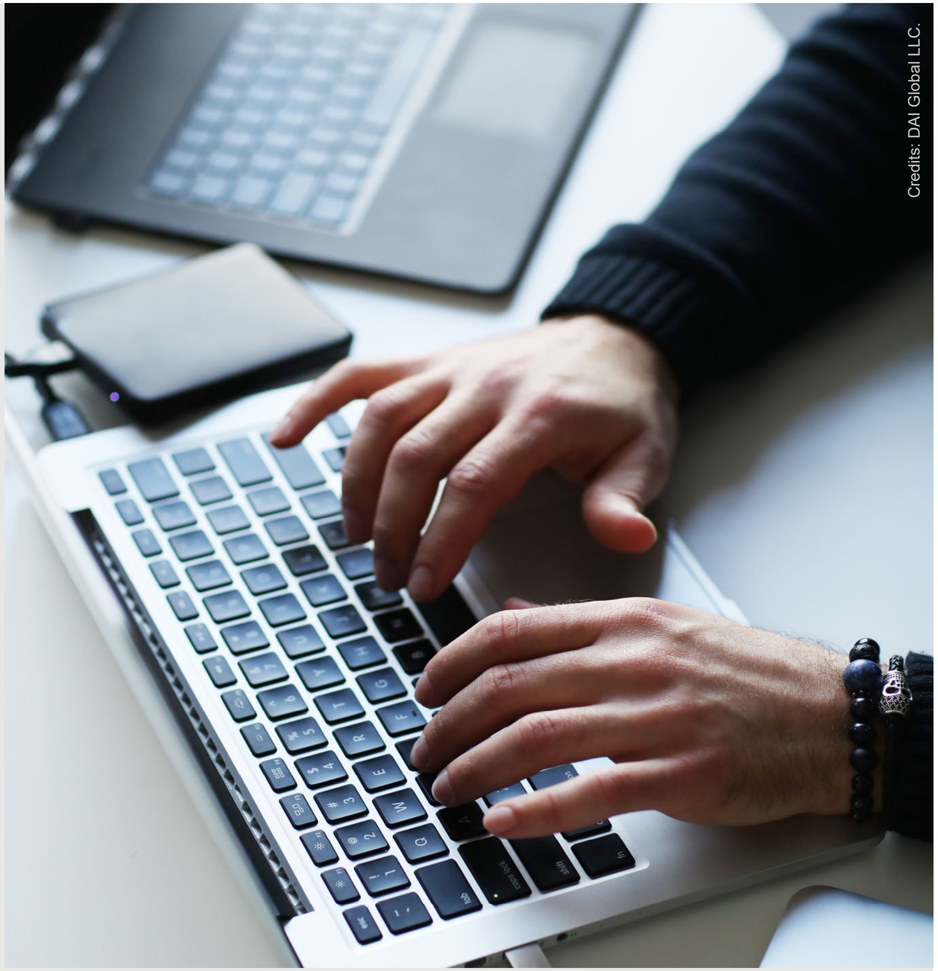
- Industrial Control Systems (ICS), SCADA Features & Functions, SCADA Components.

- Supervisory Workstations, System Architectures, SCADA Topologies, Alarm Handling.

Credits: DAI Global LLC.

WEEK 3
PROTOCOLS FOR CPS

- Industrial Network Protocols, Modbus protocol, ICCP, DNP3, IEC 61850.
- Security aspects, Security Issues & Solutions.



Credits: DAI Global LLC.

WEEK 4
BASICS ELEMENTS OF CYBERSECURITY

- Overview of Cybersecurity Basics, Vulnerabilities, Threats, Attacks.
- Security Services, Security Policies & Mechanism, Cryptography.
- Symmetric/Asymmetric key systems, Cryptoanalysis, Hash functions.

Credits: DAI Global LLC.

WEEK 5
KEY MANAGEMENT

- Types of Key Management, Session Key Distributions, Key Distribution Center, Diffie-Hellman Key Exchange.
- Elliptic Curve, Ephemeral, Certificates, Certificate Revocation Mechanisms.

Credits: DAI Global LLC.

WEEK 6
ATTACKS ON CPS PROTOCOLS

- Reviewing the major security issues, SCADA Network Access.

- Unauthorized Access to SCADA, Field Control Network Access, Protocols Vulnerabilities, DNP3 Vulnerabilities & Attacks.

Credits: DAI Global LLC.

WEEK 7
SAMPLE SECURITY PROTOCOLS FOR CPS

- Secure Versions of Legacy Protocols, Secure Modbus, Message Queuing Telemetry Transport (MQTT).
- Distributed Network Protocol (DNP3), Vulnerabilities, Performance & Security tradeoffs.

```
            airlinesPartnersNetwork.add( newAirline );
        }
        System.out.println(airlinesPartnersNetwork);
        Scanner keyboard = new Scanner(System.in);
        System.out.print("Enter airline miles are on: ");
        String start = keyboard.nextLine();
        System.out.print("Enter goal airline: ");
        String goal = keyboard.nextLine();
        ArrayList<String> pathForMiles = new ArrayList<String>();
        ArrayList<String> airlinesVisited = new ArrayList<String>();
        if( canRedeem(start, goal, pathForMiles, airlinesVisited, airlinesPartnersNetwork))
            System.out.println("Path to redeem miles: " + pathForMiles);
        else
            System.out.println("Cannot convert miles from " + start + " to " + goal + ".");
    }
}
private static boolean canRedeem(String current, String goal,
        ArrayList<String> pathForMiles, ArrayList<String> airlinesVisited,
        ArrayList<Airline> network){
    if(current.equals(goal)){
        //base case 1, I have found a path!
        pathForMiles.add(current);
        return true;
    }
    else if(airlinesVisited.contains(current))
        // base case 2, I have already been here
        // don't go into a cycle
        return false;
    else{
        // I have not bee
```

Credits: DAI Global LLC.

LABS
BASIC HANDS-ON EXPERIENCEDESCRIPTION

1. Setting Up Virtual Machine | Ubuntu
   - The goal of this lab is to provide the necessary steps to setup a virtual machine and use it to the upcoming labs.

2. Executing Modbus Protocol
   - The purpose of this lab is to introduce a Modbus data communication protocol by using Pymodbus Server/Client application to program devices and monitor.

3. Encrypting/Decrypting Data using OpenSSL
   - The objective of this lab is to expose the students to various crypto algorithms using an open-source cryptographic toolkit on UNIX based systems.

4. Diffie-Hellman Key Exchange using OpenSSL
    - The objective of this lab is to show the students a secure method such as Diffie Hellman Key exchange that is widely used for exchange cryptographic keys over a public channel.

5. Executing a secure Modbus communication
    - The purpose of this lab is to implement the secure version of Modbus data communication protocol by using the Transport Layer Security (TLS) and Modbus Client/Server.

6. Secure MQTT with TLS standard
    - The objective of this lab is to learn how to establish a secure/encrypted MQTT connection between an MQTT clients and Mosquitto Broker running on a machine using an OpenSSL.

Hardware/Software

1. **Hardware**

- PC/Laptop

2. **Software**

- Oracle VirtualBox | https://www.virtualbox.org/wiki/Downloads
- Linux OS (Ubuntu) | https://ubuntu.com/download/desktop
- Pymodbus Tool | https://github.com/pymodbus-dev/pymodbus
- OpenSSL Library | https://github.com/openssl/openssl
- Mosquitto Broker | https://github.com/eclipse/mosquitto

Thank You | Questions?

Dr. Kemal Akkaya

kakkaya@fiu.edu

USAID
FROM THE AMERICAN PEOPLE