International Symposium on Cybersecurity in Industry
List of Workshops

Workshop 1 (16 seats, priority to UDST students)

Operational Technology Adversary Emulation by *National Cyber Security Agency, Qatar*

In the evolving landscape of cybersecurity, understanding and countering threats to Operational Technology (OT) systems is crucial. These systems, which manage industrial operations, are increasingly targeted by sophisticated cyber adversaries. The upcoming workshop, designed for cybersecurity and network design students, will focus on Operational Technology Adversary Emulation using MITRE Caldera, an advanced framework for automating adversary behaviors based on real-world observations. Adversary emulation is a cybersecurity technique where defenders simulate real-world attackers' Tactics, Techniques, and Procedures (TTPs). This simulation helps understand how an adversary might compromise a network and allows defenders to test and improve their defenses effectively. In the context of OT systems, which include critical infrastructure like power plants, water treatment facilities, and manufacturing units, such emulation is vital to ensure uninterrupted and safe operations. MITRE Caldera, a tool developed by MITRE Corporation, is a standout resource in this area. It automates adversary behaviors based on MITRE's ATT&CK framework, a globally accessible knowledge base of adversary tactics and techniques. Caldera enables users to replicate a range of attack scenarios in a controlled environment, thus providing a practical, hands-on experience in understanding and countering cyber threats. The workshop will begin with an introduction to OT systems, emphasizing their significance and their unique security challenges. Students will learn about the basic architecture of OT networks, their integration with IT systems, and the potential vulnerabilities that arise from this integration. The workshop will then delve into the MITRE ATT&CK framework, guiding students through its various components and how it categorizes and describes cyber adversary behavior. Understanding this framework is critical for developing effective adversary emulation and cybersecurity defense strategy. The hands-on sessions will involve setting up and using MITRE Caldera. Students will be guided through configuring Caldera for OT network environments, creating and executing emulation plans, and interpreting the results. These exercises will strengthen their understanding of cyber threats and enhance their skills in using advanced cybersecurity tools. The workshop aims to achieve several key objectives:

1. Enhance Understanding of OT Systems: Students will comprehensively understand OT systems, their importance, and their vulnerabilities.
2. Develop Skills in Adversary Emulation: Through practical exercises, students will learn how to emulate adversaries using MITRE Caldera, gaining insights into attacker tactics and strategies.

3. Apply MITRE ATT&CK Framework: Students will learn to apply this framework in an OT context, understanding how to categorize and analyze cyber threats.
4. Improve Cyber Defense Capabilities: The knowledge and skills gained will enable students to improve the cyber defenses of OT systems, crucial for protecting critical infrastructure.
5. Encourage Critical Thinking and Problem Solving: The workshop will challenge students to think critically and solve complex problems, skills essential in cybersecurity.

This workshop is an excellent opportunity for students specializing in network and cybersecurity disciplines to gain practical experience in a vital area of cyber defense. It will equip them with the knowledge and skills to protect OT systems against the ever-evolving landscape of cyber threats. Some preferred requirements include technical Cyber security basics knowledge, ICS Cyber security (optional), and cyber security tools (Kali and Metasploit).

Workshop 2 (24 seats)

Ethical Wireless Hacking by *Dr. Abdelhak Belhi & Dr. Nabil Litayem, Joaan Bin Jassim Academy for Defence Studies, Qatar*

Get ready to immerse yourself in the world of cybersecurity at our upcoming hands-on workshop on Wireless Ethical Hacking! Join us for an exhilarating experience where you will learn and experience how various attacks on wireless communications occur. In term of format, we will use a hybrid format where we briefly explain the attacks from a theoretical point of view and then do a live demonstration. Some of the attacks involving special devices like the Flipper Zero, OM.G cable, Wi-Fi Pineapple, and others will only be demonstrated by the organizers. Other attacks such as Wi-Fi cracking can be experienced by participants. Signing an ETHICAL HACKING WORKSHOP DISCHARGE FORM is a must.

Workshop 3 (24 seats, priority to UDST students)

Networks Cortex XDR Threat Hunting by *Palo Alto Networks, Qatar*

Workshop 4

An Introduction to Vehicle Digital Forensics by *Prof. Christos Papadopoulos, The University of Memphis, USA*

In this workshop we will begin with a general introduction to Digital Forensics. We will then investigate how digital forensics is evolving to meet the demands of the new electronic systems in vehicles and discuss new approaches suitable for vehicle forensics. We will start with the Controller Area Network (CAN) and CAN-FD (Flexible Data) and other automotive networks, and touch on newer systems that use Automotive Ethernet. We will cover both passenger and heavy vehicles, which have different communication architectures. We will also discuss the type of information found in modern vehicles, both in the vehicle itself and what is sent to the cloud, and discuss privacy issues. At the end of the workshop the audience will have a general understanding of vehicle digital forensics and the differences with traditional digital forensics.

Workshop 5

The History of Attestation, Current Landscape, and Challenges *by Prof. Gene Tsudik, University of California, Irvine, CA, USA & Prof. Dr.-Ing. Ahmad-Reza Sadeghi, Technical University of Darmstadt, Germany*