ERIGrid Test Description Canvas

'Title: HTD canvas for CTiCPM project

Author: Abbas Ahmadi
Date: 2/6/2023

**Test Objectives**

The primary goal of this project is to identify various cyberattack models that can be used on data transmitted between senders and receivers in cyber physical systems. Specifically, we will be studying three potential types of cyberattacks:

1. Developing a model for source IP tampering
2. Identifying a model for destination IP tampering
3. Discovering a model for data flooding

By examining these attack scenarios, we hope to gain a better understanding of the vulnerabilities present in these systems and develop strategies for defending against such attacks in the future.

**Purpose of Investigation** *(PoI)*

1. Validating new models for various types of cyber attacks. This will allow us to better understand and prepare for potential threats, ultimately enhancing our overall security measures.
2. Analyzing data packet traffic for a cyber-physical system that is currently under attack. By closely examining this traffic, we can gain valuable insights into the nature and severity of the attack, which will help us develop effective countermeasures to prevent future incidents.

**Object under Investigation** (*OuI*)

The Object under Investigation comprises four key components: two data senders located on one side of the network, two destinations situated on the other side of the network, a communication emulator, and ICT monitoring tools. These components work together to enable the investigation and analysis of network traffic between the two endpoints.

**Function(s) under Investigation** (*FuI*)

This test consists of three distinct parts. In Part One, two senders are required to be set up with identical IP/MAC addresses and send two numerical values to a specific destination. Part Two involves setting up two destinations with the same IP/MAC address for a single sender. Finally, in Part Three, a large amount of data should be injected into the communication infrastructure. A routing algorithm must also be configured for each scenario. The goal of the investigation is to analyze the behavior of the data packets as they traverse the network under various scenarios.

**Domain under Investigation** (*DuI*)

Data senders- receivers and communication infrastructure.

**System under Test** (*SuT*)

Communication infrastructure from sender to receiver includes a variety of components, such as the data packet source, RTU, communication emulator, ICT monitoring tools and data packets receiver.

**Functions under Test** (*FuT*)

For safety reasons, it's crucial that the data sender and receiver are physically separated at the network's physical layer. Currently, our focus is on studying the routing algorithm and analyzing the behavior of both injected and original data packets as they traverse the network.

**Test criteria** *(TCR)*

This test focuses on evaluating real-time communication between devices, involving the exchange of numerical values at predefined sample times. Specifically, the data exchanged consists of predefined numerical values and is transmitted with a specific sampling time.

**target metrics**

The impact of attack scenarios on normal data flow.

**variability attributes**

Our investigation also includes analyzing how an attacker may modify the original data in different scenarios. We are monitoring the impact of these attacks and developing models to better understand them.

**quality attributes**

In this case, there are no established thresholds.

K. Heussen 08-06-2023