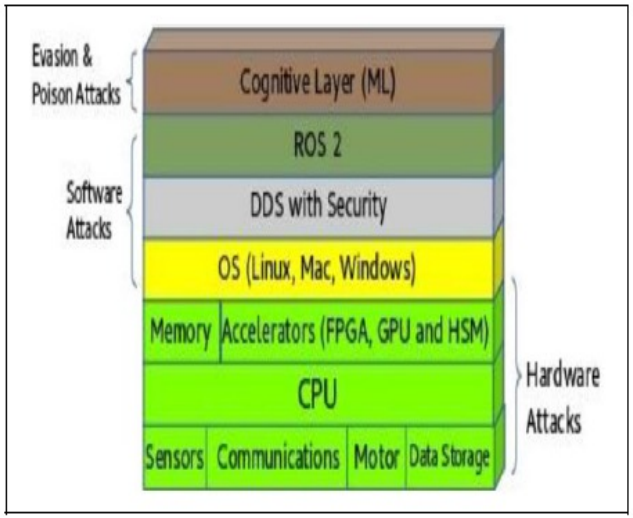
Cybersecurity Evaluation and Testing of the ROS 2 Architecture for Networked UAV Networks

CRUSER
Consortium for Robotics and Unmanned Systems Education and Research



Network stack of a ROS 2 robotic system and its associated vulnerabilities

How

- Step 1: ROS 2 and DDS testing
  - Test with a small UAV network (3-5 UAVs) and ground station. We will use Gazebo on a Ubuntu/Linux workstation along with Matlab
    - 1) Denial of Service (DoS): consider different attack levels (benign, intermediate and severe); quantify time to launch attack and ROS 2 mitigation
    - 2) Man-In-The-Middle (MITM): quantify how an MITM attacker overtakes the communication either between two UAVs or between the UAV and ground station; quantify how ROS 2 provides mitigation against MITM attack
- Step 2: Performance and Security Tradeoff
  - Analyze network performance metrics including any delays, overhead and scalability issues associated with the ROS 2/DDS

What/Deliverables

- Scope of this work is focused on the testing and evaluation ROS 2 and DDS in networked UAV systems, focusing on software attacks
- Provide formal verification and validation of ROS 2 security to enable faster transition to the fleet
- We define several adversarial models for ROS 2/DDS and determine how ROS2/DDS react and mitigate against different threat vectors
- Deliverable 1: Evaluation and results of DDS/ROS 2 performance against the stipulated attacks (Denial of Service and Man in the Middle)
- Deliverable 2: Evaluation of DDS/ROS 2 in terms of network performance compared to ROS 1 in terms of scalability and latency
- At least one MS EE student thesis in FY19 that supports this work. A presentation by the study at a CRUSER monthly meeting and/or TechCon

Why/Objective

- ROS 2 is a critical technology that supports rapid innovation of UxS and can be leveraged for military applications.
- ROS 2 has not been easily accepted into the fleet in part due to a lack of proof of the quality of the system (i.e., formal verification and validation)
- Evaluating ROS 2 from a security perspective will have an immediate impact on its implementation and transition to the fleet
- The proposed research is operationally relevant and will contribute to relevant thesis study for NPS students
- Cybersecurity is an important research and curricular component at NPS and thus furthers the mission of the school, Navy and DoD

NPS PRAESTANTIA PER SCIENTIAM

FY19 Call for Proposals

Dr. Preetha Thulasiraman, Associate Professor
Department of Electrical and Computer Engineering
pthulas1@nps.edu, Office Ph: 831-656-3456