RY26-8

DAGSI Research Topic

1. **Research Title:** Context-aware Malware Detection for Autonomous Air Vehicle Operations
2. **Individual Sponsor:**

Dr. David A. Kapp, AFRL/RYWA
2241 Avionics Circle
WPAFB, OH 45433-7333
david.kapp@us.af.mil

3. **Academic Area/Field and Education Level**

Electrical Engineering, Computer Engineering, Computer Science,
Software and Systems Engineering (MS or PhD level)

4. **Objectives:** Autonomous air operations in a contested environment requires the ability to detect and respond to cyber threats. In order to develop cyber resilient systems, threats due to malicious insiders, remote exploitation, and supply chain compromises must be mitigated. Of these threats, malware that has been implanted into the weapon system supply chain is of high strategic importance since *it can act as a surrogate for a malicious insider on-board the aircraft during mission operations*. On-going research in avionics malware detection has focused on anomaly and behavior-based detection, but a key gap in both these approaches is a lack of contextual awareness necessary to distinguish malicious software implants from the legitimate surrounding code. Given that sophisticated adversaries will likely attempt to blend in with the surrounding code to avoid detection, examination of the code (in the absence of knowledge concerning the function and operation of the legitimate software) may not reveal overt malicious behavior. Therefore, the goal of the proposed research project is to (1) develop a contextual model for a representative software program running on an embedded system, (2) design a means to automate the creation of such a model so the process can be scaled to other software applications, (3) use that model as the basis for identifying malicious behavior within the context of the expected program behavior, and (4) develop test cases that demonstrate the effectiveness of the approach.

5. **Description:** Autonomous air operations requires the ability to detect and respond to cyber threats in flight. One important threat vector that would provide an adversary universal (namely, access to all aircraft of the same type) and persistent access to air vehicles is the software supply chain. Commercial-off-the-shelf (COTS) software is of particular concern since it can be easily acquired by our adversaries and will enable our adversaries to thoroughly test out their attacks prior to deployment. The use of COTS software extends trust to those individuals who developed that software or had access to the software development environment and its toolset. Malicious software implants are particularly challenging to

counteract since malware detection tools must differentiate the malware from the legitimate surrounding code. The problem is that nation-state adversaries who gain access to the software supply chain can develop stealthy implants that do not contain any inherently malicious behavior (i.e., behavior that is exclusive to malware). The root cause of the problem is the lack of a contextual model by the malware detection tools relative to the target software and system in which it executes. The definition of malware can only be made within the context of the software and system in which it executes. Therefore, understanding and developing a model that contains this contextual information and using it in connection with existing malware detection techniques is essential to providing cyber resiliency and in-turn mission assurance to our warfighters.

6. **Research Classification/Restrictions:** Basic Fundamental research, no restrictions anticipated.

7. **Eligible Research Institutions:** University of Cincinnati, University of Dayton, Wright-State University, or other state universities with a suitable research background.

   PA clearance for DAGSI Topic "Context-aware Malware Detection for Autonomous Air Vehicle Operations": 88ABW-2019-3940