RY18-12

DAGSI Research Topic

1. **Research Title:** Bio-Inspired Self-Evolving Hardware and Software Platform for Cyber Security
2. **Individual Sponsor:**

Dr. David A. Kapp, AFRL/RYWA
AFRL/RYR Bldg 620, 3CZ75
2241 Avionics Circle
WPAFB, OH 45433-7333
david.kapp@us.af.mil

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

Electrical Engineering, Computer Science, or Computer Engineering (MS or PhD level)

4. **Objectives:** The objective of the proposed research is to understand the defense mechanisms of biological organisms against viral attacks and to develop self-evolving hardware and software platforms that can implement these schemes to combat man-made malware targeting real-time embedded systems.
5. **Description:** Novel solutions to detecting and responding to malware that has been introduced via a supply chain attack into embedded system software are needed to provide cyber security. One difficulty in detecting malicious Trojans is the inability of current malware detection algorithms to differentiate zero-day malware from the software in which it is embedded (i.e., to distinguish self vs. non-self). This is a particularly challenging problem given that in many cases there is a lack of a trusted baseline for the embedded system software. Interestingly, the self-evolutionary mechanisms of biological organisms, such as bacteria, are equipped with diverse defenses to combat invasion by viruses and other foreign nucleic acids. One such defense mechanism that has spurred significant biological research is called Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR) which, when coupled with CRISPR Associated Proteins (Cas), provide immunity to viral infections. CRISPR/Cas is an adaptive-immune system of certain bacteria that identifies foreign DNA/RNA and incorporates pieces of viral genome into the bacteria's own genome. These sequences are then subsequently used in conjunction with Cas proteins to unwind new viral DNA, compare the previously stored viral sequences with the new viral DNA, and then (when a match occurs) cut or destroy those new viral sequences to prevent reproduction. Based on this or a similar biological immune system, the purpose of the proposed research is to (1) understand the mechanisms that biological organisms, such as bacteria, use to distinguish self vs. non-self and determine whether those mechanisms can be used or adapted to differentiate malware from the host software, (2) develop bio-inspired adaptive immunity models that can be used to design self-evolving hardware and software platforms, (3) validate such systems using simulations to understand its efficacy in producing secured hardware-software platforms, and (4) study the cost, size, weight, and power (SWAP)

performance-metrics of such self-evolving hardware and software platforms to understand its applicability in developing secured embedded systems for avionics applications. The end goal of the project is to develop an embedded immune system to defend against zero-day malware.

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.