RY19-14

DAGSI Research Topic

1. **Research Title:** Automated generation of attacks against x86-based embedded system platforms
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 Engineering, Computer Science,
Software and Systems Engineering (MS or PhD level)

4. **Objectives:** In x86-based embedded systems, such as Intelligence, Surveillance, and Reconnaissance (ISR) platforms, software plays an integral role in performing mission specific tasks as well as keeping critical data protected. One concern is that nation-state adversaries will repurpose x86 malware and exploits developed for Enterprise systems to target military platforms. However, there is currently a lack of *available* malware samples that target these systems and as a result it is difficult to develop and test protection technologies that detect, respond, and adapt to zero-day attacks. The overarching goal of the proposed research project is to develop automated methodologies to generate attacks against the software running on x86 computer platforms so as to enable the development and testing of self-adaptive cyber protection systems. To that end, this project will have the following research objectives: (1) model the domain knowledge required for carrying out attacks, such as tampering, denial-of-service, and exfiltration, (2) develop a capability to evolve malware samples targeting a representative domain, and (3) equip software with self-adapting capabilities to better defend against unanticipated attacks.

5. **Description:** Mission-critical applications and services running on x86-based computing architectures must exhibit high resiliency and endure a broad class of attacks. However, there is currently a lack of malware samples that can be used to develop self-adaptable protection systems. The lack of an embedded system malware repository impacts our ability to both develop effective malware detection algorithms for these platforms as well as test existing cyber security solutions against malicious payloads. A major impediment to solving this problem is the fact that the effectiveness of cyber security solutions is a function of the adversary's knowledge about the security flaws in the system and their ability to gain access to those flaws, both of which require domain knowledge. Hence domain modeling is an essential component to developing attack simulations. However, modeling the attacker is also necessary in order to

determine their ability to exploit those flaws. A co-evolutionary model of evolvable malware (which simulates an attacker and incorporates domain knowledge) with a corresponding self-adaptive cyber protection system would enable protection systems to be built to adapt to evolving threats and objectively test existing cyber security solutions.

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.