RY19-13

DAGSI Research Topic

1. **Research Title:** Low SWAP Techniques for Malware Detection
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 or Computer Engineering (PhD level)

4. **Objectives:** The objective of this research is to develop highly efficient pattern matching circuits for runtime malware detection and to evaluate their integration into a RISC processor pipeline. Efficient pattern matching circuits could include, as an example, resistive memory based Ternary Content Addressable Memory (TCAMs). In this project, the integration of circuits into appropriate sections of a RISC processor pipeline for runtime malware detection should be investigated and the overall system evaluated through detailed simulations.

5. **Description:** With the use of complex software in microprocessor-based systems for mission specific applications, malicious software and firmware is expected to become increasingly prevalent on platforms of interest to the Air Force, such as avionics and sensor systems. Furthermore, there is concern that adversaries will leverage the underlying methodologies used by malware that have been developed for Enterprise systems, such as stealth, polymorphism, and code obfuscation to target real-time embedded systems, which currently have limited malware detection capability. Research is currently underway to develop malware detection algorithms for embedded avionics and sensor systems, however, these algorithms are likely to be significantly constrained to minimize the performance impact as well as size, weight, and power (SWAP) requirements of the host system. The proposed research project should investigate the application of efficient pattern matching circuits, such as TCAMs, to malicious pattern recognition on embedded avionics or sensor systems. The goal of this project is to minimize the runtime impact of malicious pattern search algorithms on microprocessors, and develop efficient malware pattern detection circuits that could be incorporated into the pipeline of a RISC processor.

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.