RY19-17

DAGSI Research Topic

1. **Research Title:** Anti-spoofing of Messages In a Publish-Subscribe Open Architecture
2. **Individual Sponsor:**

Alexander Paxton, AFRL/RYWA
AFRL/RYR Bldg 620, 3CX103
2241 Avionics Circle
WPAFB, OH 45433-7333
Alexander.paxton@us.af.mil

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

   Electrical Engineering, Computer Engineering, Computer Science, or related field at the following education levels BA/BS, MS or PhD level, though MS is preferred.

4. **Objectives:** Determine methods and techniques to allow services that run on publish-subscribe architecture the ability to authenticate a message's origins without impacting throughput significantly. The goals include:
   a. **Low latency and Real-time** – little overhead from processing is desired and reduction in jitter with deterministic worst case timing known
   b. **Network Architecture Agnostic** – centralized or federated
   c. **High-speed networks** – networking speeds up to and exceeding 100GB/s
5. **Description:** Current publish subscribe transport methods do not incorporate authentication of message data beyond correct formatting when sending messages to subscribed services. This leads to the potential of malicious spoofing of messages that could potentially cause degraded mission effectiveness or possibly even causing systems or services to become inoperable. In order to provide anti-spoofing capability without impacting an existing system, it may be necessary to correlate multiple types of network traffic. Tools such as Wireshark, Snort, and Sniffers may be useful but are not required in implementation. Once that more detailed information is acquired the correlation between the message and the origin of that message should be done at near real-time to allow for negligible loss of performance on high speed traffic. The developed methods should allow services in the network to with a degree of confidence know that the messages and data are coming from a trusted source.

6. **Research Classification/Restrictions:** US citizens only.
7. **Eligible Research Institutions:** Any organization with a suitable research background.