

Information Assurance (IA) Issues Common to Unmanned Vehicles

John Yen

Space and Naval Systems Command

Abstract:

Code 5.8 has been providing information assurance and systems engineering support to several programs dealing with unmanned vehicles:

- Broad Area Maritime Surveillance Unmanned Aircraft System (BAMS UAS, NAVAIR PMA 262)
- Littoral Combat Ship Mission Modules (LCS MM, NAVSEA PMS 420) – Surface Unmanned Vehicle (SUV) and Remote Multimission Minehunting Vehicle (RMMV)
- Unmanned Cooperative Cueing & Intervention (UCCI, ONR) - Underwater Vehicle

Among these different unmanned vehicles, several common security issues have arisen and their solutions will be a challenge to implementers of DoD unmanned vehicles. These issues are:

- Most cryptographic devices previously certified by NSA were based on expectations that they will be operated in controlled environments, so the use of these certified cryptography must be revisited with NSA.
- There is a specific DoD policy dealing with cryptographic methods for protection of unmanned aircraft wireless communications
- There is a common desire to control unclassified devices (such as radio or antenna) from the unmanned vehicle's classified network.
- Need to protect classified data at rest collected and stored on unmanned vehicle.

Over the past year, we have recognized these security issues and started on their resolution. This presentation will discuss these issues and the lessons learned in working through them.