CASE STUDY:

MSi's Secure Sentinel Platform Protects Unmanned Aerial Vehicles Against Cyber Attacks

(APT, Insider and Supply Chain Attacks)

BUSINESS SITUATION

Unmanned systems are widely used in the military. They're also becoming increasingly popular in commercial applications as technology in sensors, imaging and data collection continues to improve and drive efficiencies. In addition, significant advances in materials, power sources and utilization techniques allow unmanned systems to perform increasingly protracted and more diverse missions. While drones and unmanned systems are valuable assets, the control systems that manage them present real opportunities for cyber adversaries to sabotage missions and hijack proprietary data.

TECHNICAL SITUATION

The U.S. Department of Defense (DoD) understood this critical vulnerability in the control systems of unmanned aerial vehicles and funded a research initiative to identify mechanisms to mitigate risks. Conducted over a two-year period, the study culminated in 2014 with four days of flight tests emulating real-life threat scenarios that could be faced in commercial and military applications. They included ground-based advanced persistent threat cyber attacks, insider-initiated attacks, and supply chain interdictions.

Multiple attack scenarios were carried out against system areas critical to an unmanned aerial vehicle's (UAV) mission, including:

NAVIGATION: GPS system data and flight plan waypoint manipulations emanating from ground and/or onboard sources

PAYLOAD: manipulation of critical metadata related to transmitted imagery and onboard surveillance and payload system control breaches

The inflight testing gauged the effectiveness of the countermeasure technology to harden the mission critical functions of an unmanned system and provide cyber agility and resiliency under attack conditions.

MSi CYBER PHYSICAL SOLUTION PROVES BENEFICIAL

The inflight test was conducted on the Modified Griffon Aerospace Outlaw MQM-170 running with a Cloud Cap Technologies Piccolo II autopilot and a Tase Gimbal system. The testing proved successful in providing enhanced cyber protections using MSi's "System Aware" cyber security technology and a combination of MSi Secure Sentinels. The Sentinels monitored the systems onboard the UAV as well as in the operator's command center. MSi's Secure Sentinel Platform restored key functions of the UAV to an operational state in the face of various cyber attacks carried out against the MQM-170 and its systems.

In particular, the demonstration enabled mission operators to:

MAINTAIN AIRCRAFT CONTROL: Airborne and ground-based detection of attacker waypoint changes, classifying the nature of the attack as a cyber attack, and automatically restoring the plane to a pre-determined flight path

CONTINUE THE MISSION: Airborne detection of an embedded attack against the plane's GPS system, automatically switching to alternative navigation and enabling continuation of the mission on its designated flight plan and providing assurance of location data throughout the payload systems including image metadata

ENSURE SENSOR AND DATA INTEGRITY: Airborne detection of attack on Gimbal camera control preventing camera tracking and automatically correcting camera to enable proper function and block efforts to disable the camera

ADDITIONAL FEATURES:

- Onboard system remains active in the event communication is lost or jammed
- Compact, lightweight form fits a variety of UAV classes
- Monitors, detects, and informs the operator and takes automatic corrective actions against a cyber attack
- Provides capability to address the situation or allow the attack to occur while monitoring it closely
- Informs the operator, mission commander, and designated personnel when an incident occurs and what actions were taken
- Delivers forensic tracking information for post cyber attack analysis
- Allows for additional protections to be easily loaded on the Sentinel for enhanced cyber and mission assurance
- Delivers mission flexibility when a cyber attack or other problems occur
- Provides a system health monitor for critical system functions
- Configurable and scalable to both legacy and newly fielded systems
- Deployable across multiple UAVs, command centers and other designated facilities for fleet-wide cyber assurance

MSi's innovative technology protects drone and UVa control systems to ensure reliability and productivity - even during a cyber attack. The Secure Sentinel Platform gives operators greater flexibility to achieve mission success.

MSi is a specialized cyber defense company focused on protecting physical assets and control systems in energy and defense. The company's patent-pending Secure Sentinel Platform includes a dual protection system:

- MSi's Sentinel appliance (hardware and software) embeds within physical systems to protect critical assets and controls
- MSi Console manages and extends the Sentinel's protection capabilities throughout a facility

MSi's patent pending Secure Sentinel Platform was built on technology originally developed by the University of Virginia in collaboration with the U.S. Department of Defense. The Platform is unique to the industry and is designed to be vastly more secure than the assets and systems it protects. It **monitors**, **detects**, **informs**, and **corrects** automatically to mitigate cyber physical attacks. Further, the Platform **collects** incident data for forensics and analysis – a critically important feature not offered in other cyber physical defense solutions.

CONTACT

To learn more, view a video of the flight tests, or speak with one of our cyber security experts, please contact **Stephanie J. Dixon,** Director of Marketing at 832.581.2187 or email Stephanie@MissionSecure.com.