## C27 An Effective Security Assessment Framework for Drone as a Service (DaaS): A Digital Forensic Technique

*Fahad Salamh, PhD**, Kokomo, IN 46901-5879; Umit Karabiyik, PhD, Purdue University, Knoy Hall, Lafayette, IN 47907-2021; Marcus Rogers, PhD, Purdue University, West Lafayette, IN 47907*

**Learning Overview:** After attending this presentation, attendees will be able to clarify security risks of drones, determine the best practices of security assessment, and make decisions related to the security of drones during operation.

**Impact on the Forensic Science Community:** This presentation will impact the forensic science community by exploring the best practice techniques related to drone penetration testing, including an effective methodology to keep continuity of risk-free drone operation, especially drones used for emergency purposes, such as safety and rescue.

This presentation will raise awareness in the forensic science community as it draws the importance of securely operated drones for first responders. This presentation will cover various aspects of security, including data transmission, software restrictions, and embedded system-related events. In order to propose a security assessment for drones, they incorporate digital forensics and penetration testing techniques to suggest secure methods related to drone operations. Therefore, this research enhances the security level of flying devices and the overall digital forensics procedure in case of a disruption incident.

Firmware analysis and penetration testing on embedded devices is crucial today. Firmware is used in most emerging technologies, which make them an important factor in securing these embedded devices, such as drones. This presentation will cover aspects of security assessment conducted on three different types of drones used by safety and rescue organizations. The presenters focus on the analysis of firmware to determine both security vulnerabilities that could expose threats to the activity of drones, software restrictions that could limit the operation of drones, such as No Fly Zone (NFA), and operational communication commands. The use of DaaS is rapidly increasing, and risk assessment of software-related issues is important to support the adoption of DaaS in a secure operational manner.

The analysis in this work will be performed based on well-known security measures, such as the Open Web Application Security Project (OWASP) Internet of Things (IoT) top 10, the National Fire Protection Association (NFPA) 2400, standard for Small Unmanned Aircraft Systems (sUAS) used for public safety operations, and the National Institute of Standards and Technology (NIST) security guidelines, and develop a recommendation on the attack resistance based on conducted security auditing of the firmware.[1] Finally, this work will be conducted on DJI Matric, DJI Mavic, and Parrot Bebop, which are currently used by most of the safety and rescue organizations.

**Reference(s):**

[1] Miessler, D. (2015). Securing the internet of things: Mapping attack surface areas using the OWASP IoT top 10. In *RSA Conference*.

**DaaS, Penteration Testing, Firmware Analysis**

*Presenting Author