2:30 p.m. – 3:00 p.m.
Securing Mobile Technologies in the Battlefield

Charlie Stone
VP Federal Business
Mocana

Perimeter-based defenses and threat detection technologies are not enough to defend against modern cyber-attacks in mobile ad-hoc networks. The reality of modern warfighting necessitates lightweight, mobile technologies that integrate devices controlling ever more technologies, very likely including cell-phones and other mobile wireless devices as nodes. In this new environment, enemies seeking to cause harm will not only look to extract and/or corrupt sensitive data and information being transferred through devices, but also leverage command and control capabilities against the devices themselves. Securing devices in the field will require transparent, lightweight solutions that enable multiple protected mobile gateways – not only a handful of nodes - to affiliate quickly and maintain network resilience. Rather than chase network vulnerabilities or simply seek to detect real-time threats against devices, there are two basic ways to address the long-term resilience: 1) harden the code within the devices themselves to make them more resistant to manipulation and virtual tampering; and 2) protect the integrity of the data being transmitted between these devices to ensure authenticity and reliability of the information. In its solutions brief, Mocana will discuss creating trustworthy environments for MANET that lead to resilient and tamper-resistant solutions. Used by more than 200 OEMs to protect more than 100 million devices, Mocana's IoT Security Platform is a FIPS 140-2 validated embedded cybersecurity software solution that ensures device trustworthiness and secure communications across devices by: • Hardening devices with multi-factor authentication using X.509 certificates and trust chaining • Securing the boot process to validate the firmware, OS and applications • Enabling secure, cryptographically-signed over-the-air (OTA) and over-the-wire (OTW) firmware updates • Integrating hardware or software-based roots of trust such as TPM, SGX, TrustZone, HSMs, SIMs, and MIMs • Replacing open source crypto software such as OpenSSL.