Mobile Security Architecture (MSA)

At a Glance

What it is

- Mobile Security Architecture (MSA) is an S&T effort to research, design, test and accredit a lower-cost, COTS-based, NSA Suite B-enabled, non-Controlled Cryptographic Item (CCI) Wi-Fi 'add-on' comms capability that extends tactical SIPRNet with reduced operational controls compared to traditional Type-1 (CCI) COMSEC.

How it works

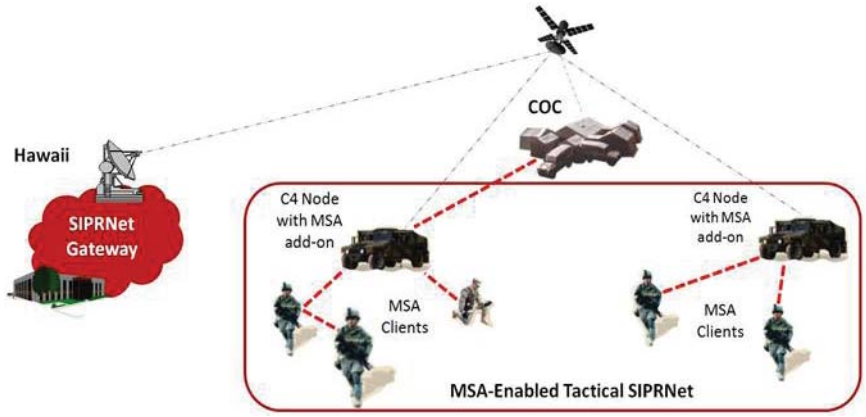
- Multi-layered Suite B cipher design operating at OSI layers two (Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)) and layer three (Internet Protocol Security (IPSec)) between MSA-enabled client devices and C4 Nodes.
- Locally generated certs provide user/device authentication and seeding material for encryption between MSA clients and C4 node-located MSA Wi-Fi APs and VPN concentrator.
- Suite B cipher protocol extensions/options and associated IA technologies optimized for MANET/tactical operations.
- MSA client/device access control managed via local 'white list" vice tactically-inefficient Certificate Revocation Lists (CRL) methods.
- Real-time/distributed MSA device rekeying accomplished via Elliptical Curve (EC) Diffie Hellman negotiation vice device administrator manually installing symmetric keys on all devices.

What it will achieve

- Improved security and increased speed of security mechanisms for users operating in intermittent, and low bandwidth environments
- Provides secure network up to the secret level with less hardware and accountable devices

Point of Contact

John Moniz
john.moniz@navy.mil



Tactical communications networks traditionally employ NSA-approved, Type-1 communications security (COMSEC) equipment that, in turn, employs NSA-generated keying materials. Type-1 COMSEC systems/users must follow stringent (and many times operationally limiting) operational control to protect the Controlled Cryptographic Items (CCI) and the keying material. In addition to being expensive, the Type-1 CCI COMSEC products are generally a number of functional generations behind their COTS-based equivalents (Wi-Fi offerings being a prime example) because the NSA approval processes delay the CCI COMSEC products' time to market.

Recognizing the cost impacts and technical/operational limitations, in 2005 NSA announced Suite B cryptography (which is a suite of four interdependent ciphers) and their Cryptographic Interoperability Strategy (CIS) which built on the National Policy on the use of the Advanced Encryption Standard (AES) to protect National Security Systems and Information (CNSSP-15). Suite B encryption may be provided in the link layer (Layer 2 of the OSI stack), in the network layer (Layer 3), in the transport layer (Layer 4), and in the application layer (Layer 7). Per NSA's CIS, COTS products/systems that properly implement Suite B satisfy COMSEC requirements to support US Secret and Top Secret communications. The problem is that although NSA established an high level Suite B system evaluation/approval process (known as Commercial Solution for Classified (CSfC)) they have not defined all system designs and/or operational controls associated with Suite B enabled systems.

The objective of MSA effort is to identify, research, design and implement the specific IA-supporting technologies operational controls which will provide a secure and scalable 'add on capability' that enables the NSA Suite B algorithms to protect a secret network in a tactical MANET environment, without the use of controlled cryptographic items (CCI), and obtain NSA approval of MSA via the NSA CSfC process.

Research Challenges and Opportunities:

- Optimizing multi-layer encryption over Wi-Fi/MANET communications
- Establishing baseline technical requirements and operational controls for tactical communications systems
- Establishing USMC/Naval operational requirements & system design considerations into developing HAIPESEC and IPsec Minimum Essential Interoperability Requirements (IPMEIR) specifications