Wednesday, August 17, 2022
11:30 AM – 11:50 AM
Phantom

Tim Solie
SISO and Executive Cyber Consultant
Phase II

Abstract:

For years the Army has focused on developing the perfect waveform. By the time the waveform is ready for use, it is normally 5 to 10 years behind the threat or commercial capabilities have out-paced the developmental program. Phantom offers a shift in paradigm in a ready-now solution focused not on development but on providing immediate impact.

A combination of three existing products, Phantom is ready for testing and employment immediately, and delivers a transport environment that is waveform agnostic, lightweight, secure, and randomly diverse in path selection providing a true multi-path, hiding in plain sight networking capability. It enables the rapid insertion of commercially developed waveforms (e.g. 3G/LTE/5G, Satcom) reducing costs and getting the capability in the hands of the Commander now with visibility and extensibility to all endpoints and connections at every layer of Mission Command and Multi-Domain Operations.

NOOB is a commercially available product, providing protection through use of a holomorphic blockchain platform leveraging non-Euclidean geometries and quaternions. NOOB is unique in is approach to create and utilize multiple flexible ledgers, tailorable to mission structures or security requirements. The ledgers define roles allowing or denying the end-user authorization to see/input data, define types of data, establish data functions, tokenize the data, and securely transmit the token in unsecure environments. The data in the token is ciphertext protected. The ciphertext is discarded if a single bit is corrupt protecting the data in motion and at rest. The end recipient will only be able to open the data packets and assemble the message if they possess the base credentials and the unique security credentials. The multiple ledgers support data taxonomies to deliver multi-level classification environments (e.g. coalition). Ridgeback elevates the role of a network defender to network warrior allowing them to see a block and maneuver against adversaries in the network.

Operating at the Data-Link Layer (Layer 2) and Internet Protocol (Layer 3) of the OSI model, Ridgeback sees all network traffic and characterizes intent based on packet protocols, network intentions, and packet function. Ridgeback provides IOT device visibility for everything connected to the network, continuous attack surface scanning and risk assessment, policy enforcement and reporting, and automatic policy enforcement. Ridgeback is agent-less with no bandwidth overhead, allowing defenders to see all IOT devices in the environment, clearly identifying blue space, authorized devices, adversarial probing of the network, and identification, investigation, and detachment of unwanted devices. Ridgeback network defenders fight in the network by blocking adversary reconnaissance and lateral movement, and placing phantoms and decoys, to force adversaries to identify their intentions in reconnaissance. Defenders either disconnect or maneuver them to an observation area by meaconing or deception targets.

cQure is a HEMP protected path diversifier utilizing a unique bonding algorithm to scramble tokenized sensitive data bit-by-bit across up to 4 seemingly randomized communication pathways (any ethernet-based medium available) transmitted through VPN tunnels virtually eliminating any man-in-the-middle data interceptions or manipulation. Phantom’s algorithm then reassembles the data at known, trusted endpoint(s) (e.g. Regional Hub Nodes).