Rajant Kinetic Mesh® Security Is on the Front Line in the Cyber War to **Protect Your Sensitive Communications**

Introduction

The use of technology is growing exponentially in virtually every segment of the industrial marketplace, including mining, oil and gas, agriculture, transportation, heavy construction, military, municipalities, and government. Today's industrial organizations have made, and continue to make, substantial capital investments in equipment and vehicle automation, Supervisory Control and Data Acquisition (SCADA), process control systems (PCS), and communications infrastructure to increase productivity, control costs, and streamline delivery of products and services.

As a result, operations and assets are becoming increasingly interconnected. Massive amounts of data are being processed and stored electronically. Autonomy, the Internet of Things (IoT), and machine-to-machine (M2M) communications are generating volumes of critical information, and personnel are accessing applications and data wherever and whenever needed.

Information Technology: More Benefits, More Risks

Information technology is truly a strategic business asset. Information systems have helped industrial enterprises implement more efficient, agile, and profitable business practices. However, they have also left their information systems vulnerable to persistent, well-organized, and constantly-evolving cyber attacks. Consequently, industrial organizations have had to strengthen security measures to protect against and respond to potential threats.

Today's highly-targeted, difficult to detect, and dynamic cyber attacks can cause serious communication outages, damage physical assets, threaten personnel and customer safety, damage an organization's brand, erode customer confidence, and violate compliance directives. Depending on the size of the organization, the financial impact alone can reach millions of dollars, leading many organizations to make the cyber war a top priority. While there is no defense method or system that can guarantee absolute security, implementing best-in-class security solutions is critical to detect and defeat attacks and safeguard people, data, and operations.

Rajant: Your Partner in the Cyber War

At Rajant, we know how absolutely essential security is. So, we have made significant investments in providing multi-level, robust security to protect your Kinetic Mesh network traffic, even as network topologies evolve. As you add, move, or remove nodes, your mesh network automatically adapts to the changes in real time, while keeping the network available and secure.

Rajant BreadCrumb® wireless nodes powered by our patented[1] InstaMesh® networking protocol offer several firmware-embedded security features, including data and MAC address encryption as well as per-hop and per-packet authentication. Securing your mesh network traffic is accomplished by specifying the security features that fit your organization's information security strategy. All security features can be easily configured and managed using BCICommander® management and monitoring software, which is included with BreadCrumb nodes. In addition, BreadCrumb security features will integrate with the network security systems residing on your non-Rajant network infrastructure.

[1] U.S. Patent 8341289B2

Powerful Cryptographic Options

All BreadCrumb® nodes are configured with 256-bit Advanced Encryption Standard (AES) using BCICommander®.

The first layer of security is a cryptographic handshake that always occurs whenever two BreadCrumb nodes establish a connection with one another, regardless of any other security settings. To protect from malicious activities, this function cannot be disabled. If nodes do not share the same cryptographic settings, they will not mesh.

- **Packet Cipher:** The packet cipher is used to encrypt all data as it flows between BreadCrumb nodes, providing privacy from wireless eavesdroppers. Encryption occurs on a per-packet basis when packets enter the mesh (encounter their first BreadCrumb node) and are decrypted when they leave the mesh. Several options are available, including 128/192/256-bit AES CTR (counter mode), 128/192/256-bit AES GCM (Galois/Counter Mode), and XSalsa-20.
- **Per-Hop Authentication:** To ensure that each data packet received is in its original, unmodified, and authorized state, per-hop authentication provides protection from packet injection, MAC spoofing, and replay attacks. You have several authentication options, including 128/192/256-bit AES GMAC (Galois Message Authentication Code) and HMAC- (hash-based message authentication code-) SHA 1/224/256/384/512.
- **MAC Address Cipher:** This cipher is used to encrypt the source and destination MAC (media access control) addresses of each packet that flows through the network. MAC encryption provides protection from traffic analysis, which could otherwise be used to identify the most important devices on the network in order to target attacks. All of the options available as a Packet Cipher (above) are also available here.
- **Client Traffic Cipher:** Wireless client traffic to and from BreadCrumb nodes can be secured via WEP (Wired Equivalent Privacy), WPA (Wireless Protected Access), WPA Enterprise (Remote Authentication Dial-In User Service or RADIUS), WPA2, and WPA2 Enterprise (RADIUS). Several Extensible Authentication Protocol (EAP) methods are supported for RADIUS as well as Counter Mode CBC-MAC Protocol (CCMP) and Temporal Key Integrity Protocol (TKIP) encryption.
- **Access Control Lists (ACLs):** MAC-address-based ACLs can be applied to Ethernet and radio interfaces to specify the users or system processes that are granted access to objects as well as the operations that are allowed on given objects. You can deny access to specific items such as email addresses, users, URLs, etc., with a blacklist. Conversely, you can create a whitelist and allow only those items that are included in the whitelist to access your network.
- **Virtual Local Area Networks (VLANs):** VLANs allow segmentation of multiple virtual networks on a single mesh and are configured on a per-port basis, where a port is a BreadCrumb node, one of its Ethernet interfaces, or a radio interface-ESSID combination. Clients with access to one set of VLANs cannot receive or send traffic to other VLANs even if they are on the same BreadCrumb mesh.
- **Quality of Service (QoS):** VLANs may have QoS settings applied to prioritize critical traffic. This can provide a security benefit in certain applications.
- **Disabling Interfaces:** In addition, unused Ethernet and Radio interfaces can be disabled remotely.

Security Beyond Network Traffic

Additional security capabilities are provided to protect communications beyond the mesh network, including:

- **Encrypted Firmware Updates:** To protect the integrity of our firmware, updates are encrypted using 256-bit AES in CBC mode and cryptographically signed using a 4096-bit RSA key-pair. Non-Rajant firmware cannot be installed.
- **Administrative Communications:** BCICommander administrative and management communications are secured using TLSv1 with an RSA or ECC key that is configurable and unique to each BreadCrumb.
- **BreadCrumb Administration:** All BreadCrumb configurations, passwords, and critical security parameters are remotely zeroizable via BCICommander or via a button on the device with physical access to a BreadCrumb node. A zeroized BreadCrumb device cannot join a secured mesh network.

Securing Your Inter-Connected World

The global cyber war will continue as long as there are bad guys who engage in seemingly relentless assaults on the information systems that are so integral to the success of industrial enterprises. Equally important to providing you the best-in-class mesh is providing the best-in-class security for that mesh. Our ongoing security objective is to continue our persistent campaign against malicious intruders to stop them from penetrating your wireless mesh network and getting access to your sensitive information. So, you have one less worry when it comes to securing your information systems.

Tel: 484.595.0233 | **www.rajant.com**

Updated 2/7/2018

RAJANT