Assure the Security and Integrity of Information **Traversing Your IoT Networks with Rajant**

Introduction

Are You Prepared to Protect Your Industrial Network Infrastructure? Today's network infrastructures continue to grow in size, complexity, and functionality.

The ever-increasing number of interconnected devices, cameras, laptops, sensors and other assets that traverse a network has placed more pressure on those responsible for ensuring the security and authenticity of the communications traffic moving in, out, and across the network. Moreover, network users are placing greater demands on these infrastructures to support more applications and services, with expectations that the network will accommodate and extend mobility to employees and contractors anytime, anywhere. As network size and scope expands, network operators and security officers are tasked with the difficult job of assuring their enterprise communications remain protected and that their information systems are not compromised by a variety of attack vehicles.

For industrial sectors such as utilities, automobile, oil and gas companies, chemical plants, railways, and ports, the consequences of a network security breach can be severe, including everything from significant business and service disruption to financial systems collapses, and even catastrophic situations that impact human safety and well-being. Needless to say, network security is a top priority for mission-critical networks—if not the highest priority.

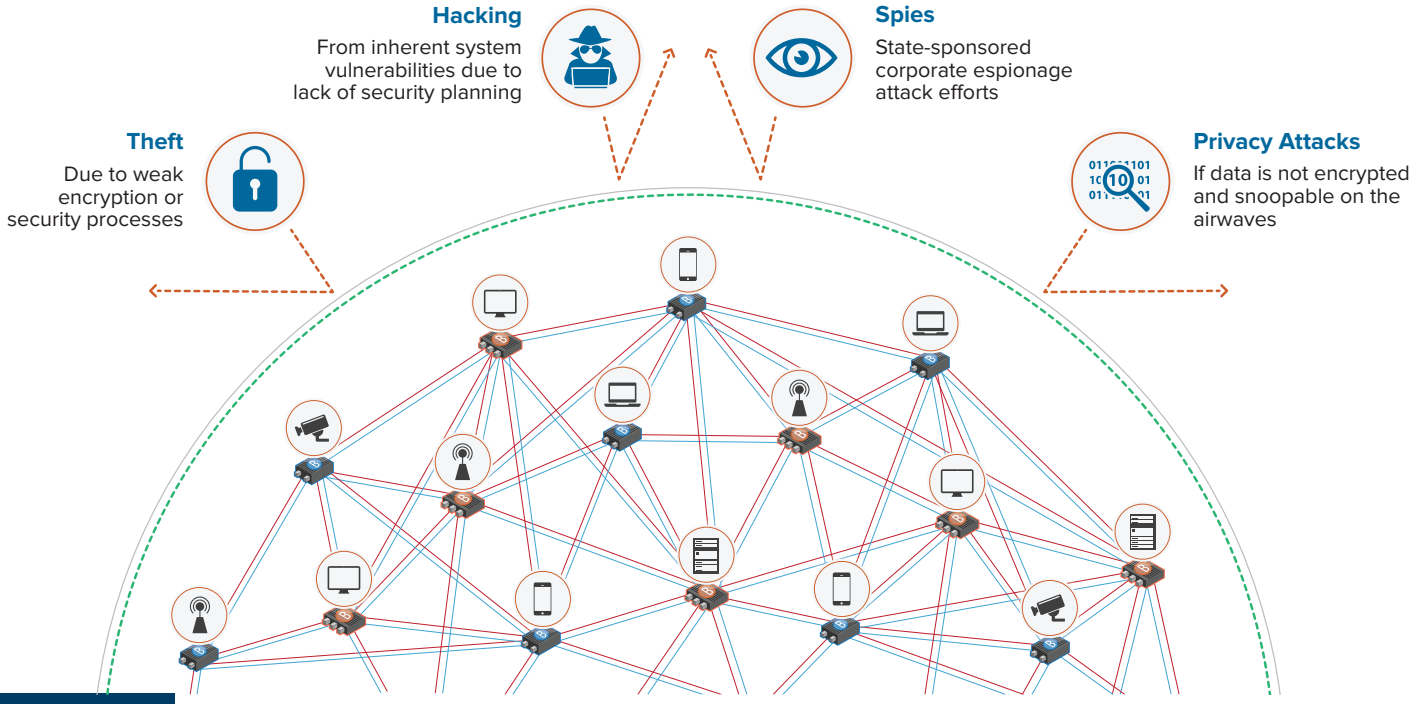
This white paper explores how the increase of interconnected devices, cameras, laptops, sensors and other assets have placed more pressure on those responsible for ensuring the security and authenticity of the communications traffic moving in, out, and across the network.

Understanding Security Prioritization

How to Identify, Organize and Remediate Security

Prior to the seemingly relentless assaults on communications and information systems, it was not uncommon for enterprises to build networks first and plan for security after the fact. This approach creates inherent weaknesses in the network infrastructure and makes it much harder to protect against new and evolving security threats from hackers as they continue to become more advanced. At Rajant, the core of our knowledge and depth of our security expertise is founded in the recognition that before you build a network infrastructure, you must assess and plan for its security. That involves vulnerability assessment, design, and implementation of a comprehensive Information Assurance plan. Rajant has been building secure, private wireless networks for military and industrial customers for 15 years. Our technology is active today in numerous defense programs across the globe, ensuring critical and classified communications are reaching their destination without compromise and ultimately safeguarding troops and personnel. For these obvious reasons, stringent network security has always been a core priority in the defense space, but more and more commercial and industrial operators are now realizing that they too need a more robust approach to information assurance, as they connect more diverse assets across their IoT networks. We leverage our extensive experience supporting the high security requirements of defense customers to enable industrial customers to architect a network with fail-safe security.

PROTECT AGAINST DIVERSE NETWORK SECURITY THREATS WITH RAJANT KINETIC MESH® SECURITY



Meeting the Unique Security Requirements of IoT Networks

Rajant understands that IoT enterprise networks have unique requirements that must be accounted for in the design and integration of their security. At the top of the list is the requirement to improve or otherwise enhance network efficiency while providing the highest level of security possible. Our leadership in this market is directly tied to the significant investment we have made in the provision of multi-level, robust security across the entire wireless platform. Rajant BreadCrumb® wireless nodes powered by our InstaMesh® networking software offer several firmware-embedded security features, including data and MAC address encryption as well as per-hop, 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 our BCICommander® management and monitoring software. In addition, BreadCrumb security features can integrate with the network security systems residing on your non-Rajant network infrastructure. All of our BreadCrumb nodes can be configured with a number of powerful cryptographic options up to 256-bit AES GCM.

These Networks Require:

- Advanced encryption algorithms
- Improved processing power
- Reduced power consumption
- Small form factor chip

Deep Information Assurance Expertise

With a dedicated team of highly experienced cryptographic engineers and information assurance experts, Rajant's team can help commercial and IoT enterprises successfully develop:

- **Fail-safe designs**
- **System level security architectures**
- **Cryptomodule designs**
- **Security certification processes and accreditation readiness programs**
- **Data at Rest (DAR)encryption solutions**
- **Support for embedded, Field Programmable Gate Array (FPGA) and network-based secure software communications**
- **Trust anchor and certificate authentication**
- **Key management solutions (EKMS, KMI, OTAR)**

Our security teams can establish trust chains within a system to assure operational state at all times, while still allowing field software upgrade capabilities. The Data at Rest protection mechanism and encryption schemes deployed by Rajant ensures that the data stored, which is becoming increasingly important to withstand industry and legal scrutiny, is authentic. This expertise, paired with the robust security features built into our BreadCrumb nodes, enables us to provide reliable radio security and encryption without impacting the efficiency and performance of the network.

Rajant Active Security Certifications:

- FIPS 140-2 Level 2
- Suite A – Classified
- AES Suite B – Secret

Information Technology:

More Benefits, More Risk – Be Prepared with Rajant

Information systems have helped industrial enterprises implement more efficient, agile, and profitable business practices.

However, it has also left their information systems vulnerable to persistent, well-organized, and constantly-evolving security attacks. Consequently, industrial organizations have had to strengthen security measures to protect against and respond to potential threats. 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's 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, all while continuing to deliver the high level of network performance your operations demand.

RAJANT

*If it's **moving,** it's Rajant.*
*Industrial Wireless Networks **Unleashed.***

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

Learn why utilities, ports, mines, agriculture, and more industries rely on Rajant Kinetic Mesh networks for the continuous, fully mobile connectivity required to power today's data-driven operations. Visit www.rajant.com or contact a representative to learn more.