SECURING FUTURE PORTS

WITH MULTI-LEVEL CYBER SECURITY

Chad Mercer, Vice President, Information Assurance,
Rajant Corporation, Malvern, US

With about 90% of world trade carried by the international shipping industry. Ports are vital to the flow of commodities and capital worldwide. Terrorism that interrupts the flow of goods may have a severe effect on the global economy. When the US government shut down US seaports and airports in response to the events of 9/11, container shipping lost a billion US dollars a day during the months spent disentangling freight traffic. Robust port security is one way in which to safeguard global trade.

What is the best security strategy for a particular port? The answer is complex because port information networks have evolved significantly over time as new technologies have emerged. Operations have been added or modified to address customer and tenant requirements, and cyber threats continually increase in number and sophistication. This paper examines one security strategy for IT networks and the challenge of how to deter intruders while protecting people and assets.

SECURITY CHALLENGES

Typically, ports use a massive network of technologies – some of which were not designed with the sophistication needed to safeguard them from today's hackers, criminals and terrorists. As a result, port security is often limited by outdated, diverse systems with limited ability to expand to reach the scale and mobility needed to create a truly connected, secure port.

While many ports have implemented layered security systems using devices such as fences, cameras, sensors, access control, CCTV, radar, and patrols, they still may be lacking the robust network security needed to adequately protect data and communications.

Many ports have outgrown the capacity of the wired network, and wired build-outs in concrete and water are not feasible. These port operators are looking to wireless systems to increase network connectivity and security. However, workers, ships, containers, equipment, and vehicles roaming throughout a port can create interference and restrict signal range for many wireless networks.

One challenge is that port environments are exposed to extreme weather conditions and temperature fluctuations, so any new equipment has to withstand these conditions and perform at an optimal level.

It can also be challenging to convince port operators and ship owners that security enhancements are worth the investment, especially if an attack has not yet occurred. Plus, they may need to be convinced that integrating an advanced, secure communication system can be done without interfering with daily operations.

PROACTIVE STRATEGY

Ports need a multi-level security strategy to prevent and detect threats because both physical security and cyber security are vitally important. An active port also relies on constant communications to operate effectively. Even the shortest period of downtime can result in the loss of information needed for emergency response.

Today many ships, vehicles, and pieces of equipment are autonomous, driving themselves via a large number of connected computer systems with humans monitoring performance. Imagine the havoc that could result from a cyber attack on autonomous vehicles, causing serious injuries to people and massive vehicle and cargo damage. To protect operational integrity, autonomous vehicles and equipment need ultra-reliable, ultra-secure people-to-machine and machine-to-machine connectivity.

Physical security, cyber security, and redundant communications need to be integrated into a multi-level security program that:

- Supports surveillance and real-time tracking of port assets
- Enhances situational awareness, which evaluates both risk and incidence of threats
- Promotes collaboration across various populations, networks, and processes
- Processes and shares intelligence appropriately
- Protects information confidentiality
- Maintains operational integrity for autonomous vehicles and equipment
- Scales to accommodate future expansion

CONNECTED DEVICES

The Internet of Things (IoT) helps increase productivity and safety through a myriad of devices. Forecasts predict that across several sectors we will see a 31% increase in connected “things”, such as Unmanned Ground Vehicles (UGVs), drones, and Unmanned Aerial Vehicles (UAVs), from 2016 to 2017.

At present, drones are not actively being used as part of ports’ security ecosystems. However, due to their ability to be quickly deployed to provide situational awareness for first responders, we can expect to see drones being used effectively in port security applications in the near term.

These devices generate enormous volumes of data, making redundancy and confidentiality even more important. To realize the benefits of automation, IoT, and other emerging technologies, the security strategy needs to address their unique requirements such as mobility, continuous connectivity, and bandwidth for transfer of high volumes of voice, video, and productivity data.

Intruders have an ever-increasing number of highly sophisticated cyber tools, making security an ever-moving target. AV-TEST, an independent IT-security institute, registers over 390,000 new malicious programs appearing online every day. As a result, the strategy must also address the need for ongoing security management, maintenance, and upgrades.

BUILDING A SECURE, REDUNDANT NETWORK

A Rajant Kinetic Mesh peer-to-peer, private wireless network can provide port operators with fully mobile, redundant, secure communications.

In traditional wireless networks, additional access points or infrastructure nodes must be purchased to serve as backups, inflating the overall deployment cost significantly. With a Kinetic Mesh network, the multi-radio mesh forms a fully redundant web of connectivity without the added cost of purchasing “backup nodes”. Kinetic Mesh networks are inherently redundant because each wireless node includes multiple radios and automatically forms connections with numerous other

Rajant BreadCrumb LX5 is a wireless device that can fit to a quay crane to form a mesh network

wireless nodes within the mesh, and Rajant software InstaMesh automatically directs data over the most efficient path, enabling mobility for networked equipment. This capability greatly mitigates radio-frequency interference and bottlenecks.

The network supports Wi-Fi and uses Ethernet for integration with satellite, fiber, copper, cellular, LTE, 3G/4G, point-to-point wireless, and point-to-multipoint wireless. As a result, port operators can use legacy systems while still expanding network connectivity and security. The system is designed to be quickly deployed on virtually any assets such as vehicles, quay cranes, surveillance cameras, drones, and buildings.

MILITARY-GRADE SECURITY

Born from military applications, Rajant networks offer robust security capabilities throughout the mesh, for example multiple cryptographic options.

As encrypted information flows through the mesh, it stays encrypted all the way through and is not decrypted until it is delivered to its final destination. This encryption also helps protect communications from attacks that try to pinpoint which nodes are communicating with other devices. The authentication provides protection from packet injection or replay attacks.

It is recommended that network management software be used to isolate and separate configuration roles, for example, administrators and cryptographic administrators, to provide an added layer of security.

PHOTO-SURVEILLANCE

A kinetic mesh network can provide high-bandwidth to support video surveillance – from streaming live remote camera video to maintaining visual communications with patrolling unmanned aerial or ground vehicles. Fully redundant mobile communications let security officers access the real-time information and respond quickly and safely.

Recently, ransomware has become a top security concern. One such cyber attack cost Maersk up to US$300 million and disrupted operations for two weeks. A ransomware attack is an exposed vulnerability that resides within Windows PCs and is related to leaked back-door access methods that reside in out-of-date operating system versions. To prevent ransomware attacks such as Petya, the best solution is to ensure that the Windows system operating within the port's network has all the latest security patches installed and that it runs a current version of antivirus software. Additionally, network monitoring appliances or applications can be used to identify ransomware within a network so that its ability to spread is minimized.

Ultimately, the best protection against ransomware and other attacks is to backup data often on a remote storage device that is firewalled away from the main port operations network.

PROTECT PRODUCTIVITY ENABLERS

Think of cyber attacks as trade warfare with ports on the front line. Whether deploying a new security network or expanding an existing one, it is best to implement a solution that addresses a specific port's application requirements as well as the unique requirements of emerging productivity enablers such as autonomy and IoT. Physical security, cyber security, and redundant connectivity should be combined into a multi-level, secure network to safeguard global trade.

It is important to deploy a network solution that can bridge the gap between current infrastructure and a secure, connected port. A Rajant Kinetic Mesh network with military-grade security can give port operators the deployment ease, flexibility, reliability, and scalability to meet today's requirements for secure communications and to grow as needed.

ABOUT THE AUTHOR

Chad Mercer joined Rajant Corporation as a Senior Systems Engineer in July, 2016 before his appointment as Vice President of the Information Assurance Division in July, 2017. In his current role, Chad acts as a team lead and System Security Architect for Rajant's Cryptographic Module design efforts. Chad has more than 20 years of experience in network security and software development, having previously worked as a Senior Principal Systems Architect Engineer at Harris Corporation and as Software Manager, Developer, and Test Engineer at Intel.

ABOUT THE ORGANISATION

Rajant Corporation is the exclusive provider of private Kinetic Mesh wireless networks powered by BreadCrumb network nodes and InstaMesh networking software. Rajant networks are fully mobile, secure, scalable networks and are used across a broad array of industries, including military, mining, transportation, utilities, and all levels of government.

ENQUIRIES

Rajant Corporation
400 East King Street
Malvern, PA 19355
tel: (484) 595.0233
Email: cmercer@rajant.com
Website: http://www.rajant.com

REFERENCES

[1] International Chamber of Shipping, http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade
[2] Abt Associates, "The Economic Impacts of Bioterrorist Attacks on Freight Transport", 2013
[3] Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016
[4] AV-TEST Institute, https://www.av-test.org/en/statistics/malware/
[5] US patent 8341289B2
[6] Los Angeles Times, "Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks," 2017