NOKIA

Are You Prepared for New Threats to Your Railway?

A new era of security: quantum-safe networking in action

Digital technologies, like automation, Internet of Things, digital twins and newer initiatives in artificial intelligence, continue to bring crucial benefits to railway operators and their customers.

But with railways being prime public targets and digital systems becoming more widespread, they face escalating cyber threats — including the emerging risks with advances in quantum computing. With that in mind, what's the best way for railway operators to protect their assets and their communities, now and in the future?

The first step is to gain a thorough understanding of some of the current and emerging risks, so you can maintain a comprehensive security framework to minimise dangers.

New Vulnerabilities and Targets

The digitalisation of railway operations creates more complexity and inter-dependencies between systems, and that offers hackers more ways to intrude. The most vulnerable links are often found in communications systems, as noted in a March 2023 report by the European Union Agency for Cybersecurity (ENISA). But the report also predicted that groups would soon target operational technology (OT) systems, which proved to be true within six months.

For example, in September 2023, the electrical infrastructure of Israel's railroad network was attacked by state-sponsored hackers using a phishing campaign. And one month earlier, the integrity of the Polish national railway network's radio signalling system was compromised by another group of state-sponsored hackers who issued a false command that stopped 20 trains.

Variations on Familiar Exploits

Hackers are developing new twists on three standard types of attack.

- Eavesdropping is common in IT-based intrusions, where sensitive data is collected, such as login information, operating commands and system control messages. This data isn't always acted on immediately. Hostile groups can simply use it to learn more about how the systems work for devastating attacks later. Or, in the quantum era, it can be part of a 'harvest-now-decrypt-later' exploit. That means encrypted data is held until hackers possess quantum computing powers that can decrypt what they've collected.

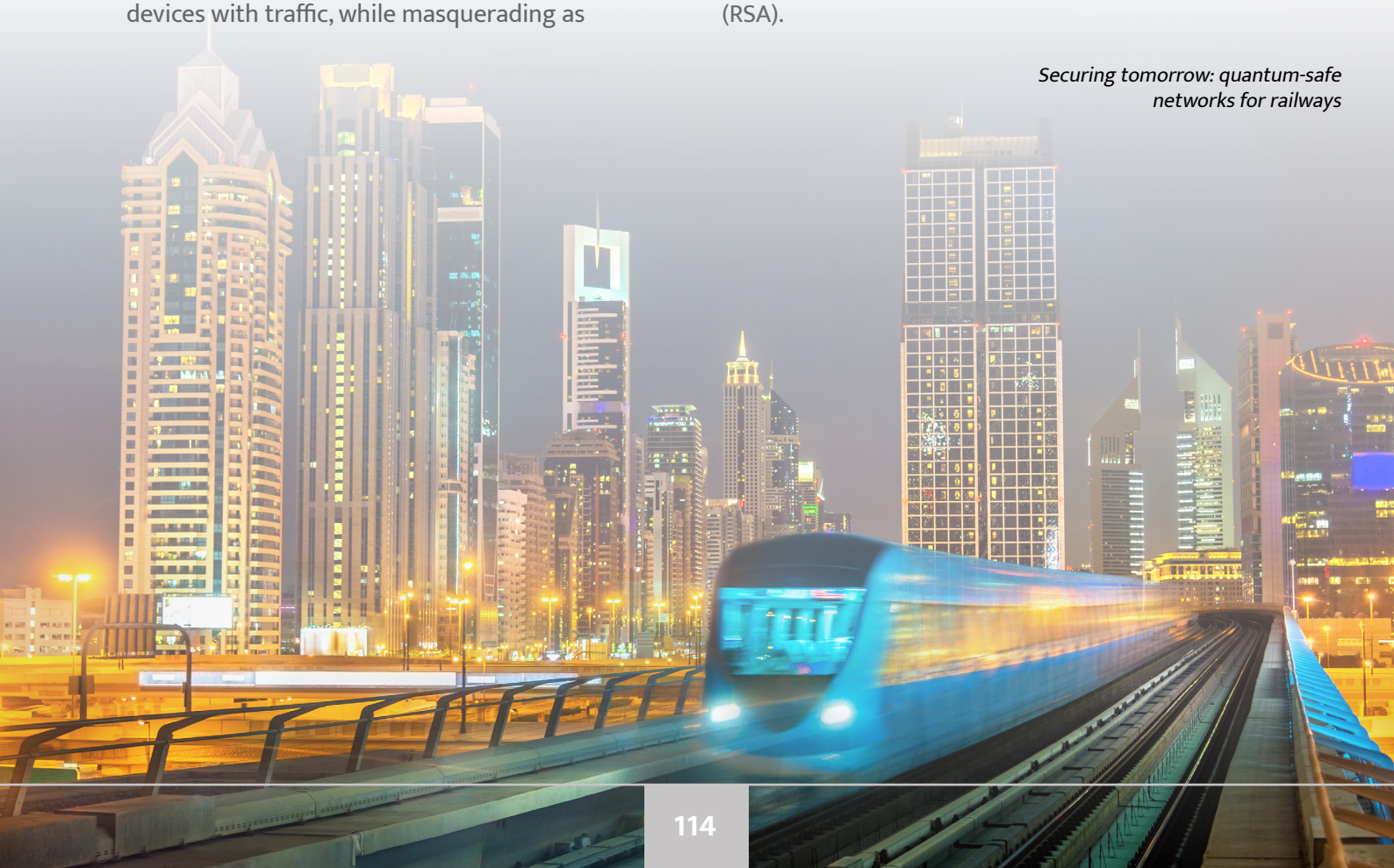
- Man-in-the-middle attacks take eavesdropping to the next level. That is, they not only monitor communications, they also modify them. The attack on the Polish rail system reported by ENISA would have worked this way, by modifying system commands to stop 20 trains. Anything is possible if the signalling system is compromised, which includes sending conflicting interlocking (IXL) signals to cause a head-on collision.

- Denial of service (DoS) attacks compromise the availability of critical systems by flooding targeted devices with traffic, while masquerading as legitimate senders. The sheer volume of traffic overwhelms the systems, leaving them unable to execute essential tasks. For example, a DoS attack could overwhelm a railway's traffic management system in a control centre, so that it's unable to effectively control train movements across the network.

Encryption's Growing Importance — And Limits

As hackers probe for weaknesses in complex and interdependent systems, encryption offers a fundamental tool for protecting data integrity. In the simplest terms, it scrambles messages when they're sent and unscrambles them when they're received. If hackers capture this data 'in flight', they will find it meaningless, without the decoding scheme.

The security level of these schemes (or algorithms) depends solely on the intense computational efforts required to decode them. The goal is to make the effort and money required to break the code so great that it outweighs the potential reward of having the data. Unfortunately, however, the speed of quantum computing may render many of today's most popular public key encryption algorithms ineffective, including Diffie-Hellman and Rivest-Shamir-Adleman (RSA).



Securing tomorrow: quantum-safe networks for railways

Comprehensive Cyber Security in the Quantum Age

While cyber security for individual network elements is essential, comprehensive in-depth security needs to be considered just as carefully. That's because many of the most vulnerable points of a railway system are in the interstices and communications between sub-systems. Therefore, a holistic defence-in-depth security framework is required.

To secure data transport, rail operators must meet well-established standards already set out by regulators — as OT data flows through the various dense wavelength-division multiplexing (DWDM) switches, Ethernet switches and Internet Protocol (IP) and Internet Protocol Multi-Protocol Label Switching (IP/MPLS) routers.

In addition, traffic encryption must be strengthened, using a robust key distribution server and symmetric key encryption. For example, advanced encryption standard (AES) with a session key length of at least 256 bits currently offers robust initial protection against quantum attacks at the network transport layers.

Post-quantum cryptography algorithms designed to scale easily at the application layer will come later, providing further protection for network users. To establish a quantum-safe communications network, defence-in-depth requires implementation of multiple protection mechanisms.

While digitalisation brings many rewards, security is a pressing concern. By taking a holistic and conservative approach, rail operators can help ensure the safety of our transport by protecting sensitive data, maintaining the integrity of operations and safeguarding against potential disruptions.

www.nokia.com

For more detailed information on how to boost railway security in the quantum era, download our white paper, **Strengthening railway communications network security**.