RAILWAY INTERNATIONAL

IS YOUR RAILWAY STILL SECURE IN THE QUANTUM ERA?

By Benoit Leridon, Head of Transportation Business Network Infrastructure at Nokia.

Crucial lifelines for the communities they serve, railways confront escalating risks in the digital era as they become prime targets for bad actors seeking to destabilize critical transportation systems. Digital technologies such as artificial intelligence (AI), Internet of Things (IoT) and digital twins are enabling railways to automate systems for train control, operations and monitoring.

As they evolve from traditional operational technology (OT) systems to advanced cloud-based digital systems, their vulnerability grows. While cybersecurity for individual elements is essential, comprehensive in-depth security is all-too often an afterthought. And with the advent of quantum computing, new kinds of security threats loom.

Growing cyber threats

With the digitalization of railway operations, it is natural that cybersecurity issues are multiplying. With more complexity and inter-dependencies between systems, the number of ways that hackers can intrude increases. They often exploit the interstices between sub-systems, searching for the weakest links, often found in communications systems.

In March 2023, a report by the European Union Agency for Cybersecurity (ENISA), examined recent cyberattacks on the transport sector. It noted that while most attacks had up to that point targeted railway IT systems, they predicted that groups would soon be targeting OT systems, and within six months this proved true.

The electrical infrastructure of Israel's railroad network was attacked by state-sponsored hackers using a phishing campaign in September 2023. Additionally, just a month before, the integrity of the Polish national railway network's radio signaling system was compromised by another group of state-sponsored hackers who issued a false command that stopped 20 trains.

Threats to confidentiality, integrity and availability

Cyber threats may take many different forms, but they can generally be reduced to three types. The first is eavesdropping, which is quite common in IT-type intrusions, where intruders collect sensitive data such as login and authentication data, operation commands and system control messages. These breaches in confidentiality might not be used immediately. Instead, they allow hostile groups to monitor activities, learn more about how the systems work, and use the information for later, more devastating attacks.

The integrity of the in-flight data is most often threatened by man-in-the-middle attacks, which take eavesdropping to the next level, not only monitoring communications, but modifying them. The attack on the Polish rail system would have done this, modifying commands to order to stop the trains. Anything is possible if the signalling system is compromised including generating conflicting interlocking (IXL) signals to cause a head-on collision.

The third kind of attack is probably the most common these days, distributed denial of service (DDoS), which impacts the availability of critical systems. In this kind of exploit, the attacker floods targeted devices or systems with traffic, masquerading as legitimate senders. The sheer volume overwhelms these systems, making them unable to execute essential tasks. Consequently, crucial traffic management systems or edge servers used by an automation system can be taken off-line at critical junctures.

Encryption and the quantum threat

Protecting the communications between sub-systems and the confidentiality, integrity and availability of critical systems, requires data to be encrypted. Cryptography in these advanced

digital systems requires the message to be scrambled when sent and unscrambled when received. Any intrusion that captures the data 'in-flight' finds it meaningless, without access to the decoding scheme.

The idea behind coding and decoding schemes or algorithms is to make the mathematical challenge of breaking the code so computationally intense that the money and effort required isn't worth the potential reward. The advent of quantum computing, unfortunately, may render many of today's most popular public key encryption algorithms, such as Diffie-Hellman and Rivest-Shamir-Adleman (RSA), ineffective.

Bad actors with access to a cryptographically relevant quantum computer (CRQC) can break today's public key encryption schemes exponentially faster than with the most powerful classical (non-quantum) computer. Even without access to a CRQC today, they can collect and store encrypted railway communication data and messages for decryption later when they have a CRQC. This is commonly known as the harvest-now-decrypt-later (HNDL) threat.

Defense-in-depth

Since many of the most vulnerable points of the entire railway system are in the interstices and communications between sub-systems, it is essential to include robust communication network security in the holistic defense-in-depth security framework. This means meeting well-established standards already set out by regulators for securing data transport 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 the pre-dawn of the quantum age, traffic encryption schemes must utilize a robust key distribution server and symmetric key encryption, such as advanced encryption standard (AES) with a session key length of at least 256 bits to ensure an effective defense against quantum attacks. Utilizing AES-256 at the network transport layers will provide robust initial protection.

New post quantum cryptography (PQC) algorithms that are designed to scale easily for use at the application layer will come later, providing additional protection for every network user. Defense-in-depth requires doubling or tripling protections to this formidable threat, forming a quantum-safe communications network.

Digitalization will bring many rewards for both railways and their customers in efficiency and safety. The security of these new systems is a pressing concern, but taking a holistic and conservative approach will ensure the future security and advancement of our railways. Quantum safe encryption is an important part of the complete security framework.