The 451 Take (continued)

Despite these limitations, there are still methods available to manufacturers for enforcing strong authentication in their operational networks. Newer endpoints are often built with sufficient hardware to implement PKI-based authentication, while gateways can be leveraged to offload authentication functionality for brownfield devices. Elliptic curve cryptography has grown in popularity among PKI-based methods for its ability to provide a security level equivalent to RSA with shorter key lengths, requiring less computing power and storage capacity to generate and protect keys. This makes it ideal for relatively constrained endpoints such as those in manufacturing environments. Frameworks and standards have also emerged to provide guidance to manufacturers rolling out broader device authentication, including NIST SP 800-53, the Industrial Internet Consortium's (IIC) Industrial Internet Security Framework, and the IIC's Endpoint Security Best Practices document. Regardless of the methods or frameworks manufacturers choose, cryptographic techniques can help meet the growing need for strong authentication in manufacturing networks.

Business Impact

TAKE STEPS TO UNDERSTAND EXPOSURE. Knowing the devices that send and receive mission-critical communications – and the potential damages that a motivated attacker could cause by impersonating devices or control systems in order to send false commands – can help to build an understanding of where the need for authentication may be most significant in the network.

LEVERAGE GATEWAYS TO PROXY FOR AUTHENTICATION ON BEHALF OF BROWNFIELD DEVICES. Gateways bring datacenter-class functionality to the edge with the ability to securely store device credentials within HSMs, perform cryptographic functions and enable mutual authentication of constrained devices without impacting network performance.

ASSESS NEW PURCHASING DECISIONS IN THE CONTEXT OF A DEVICE'S SECURITY CAPABILITIES. Organizations should determine whether a device was manufactured with considerations such as hardware-based root of trust in mind to support essential cryptographic functions related to authentication – including secure boot, validated firmware updates and encrypted communications – throughout its useful life.

Looking Ahead

Over the long term, we expect cryptographic authentication to become more widespread in manufacturing environments.