451 Research

S&P Global
Market Intelligence **Business Impact Brief**

The Role of Authentication in Manufacturing IoT

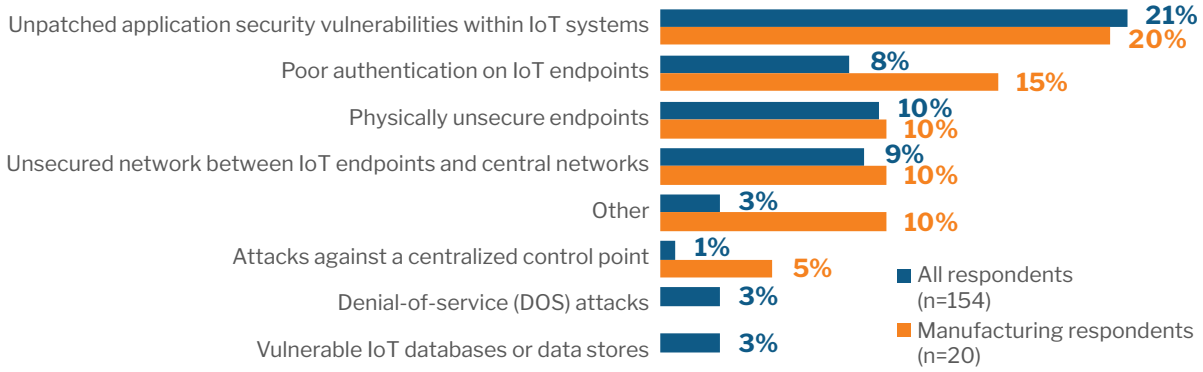
The 451 Take

Internet of Things (IoT) technologies are now being deployed throughout the manufacturing sector to improve operational efficiencies across a variety of use cases. According to a 451 Research operational technology survey, top IoT use cases include production monitoring, inventory management, predictive maintenance and intelligent logistics. As connectivity becomes the norm in a manufacturer's operational networks – many of which were often assumed to be air-gapped – the need for more robust security, specifically authentication, is paramount in an industry where it was once an afterthought. Indeed, in 451 Research's Voice of the Enterprise survey data, 39.5% of manufacturing-specific respondents said they view security as the top impediment to IoT initiatives. Drilling deeper, unpatched application security vulnerabilities with IoT systems was cited as the greatest security threat to IoT initiatives by respondents across all industries and by manufacturing-specific respondents (20.8% and 20%, respectively). However, manufacturing respondents are also quite concerned about poor authentication on IoT endpoints, cited as the next greatest threat (15%), although it ranked fourth as a primary threat for all respondents (8.4%).

Device Authentication a Primary Concern for Manufacturing IoT Initiatives

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2019

Q: Which of the following is the greatest security threat for your organization's IoT initiatives?



While device authentication is essential to validating the identity of devices and ensuring the integrity of data in any industry due to the possibility for data and IP theft, it carries added significance in manufacturing, where weak authentication has the potential to impact safety. There are significant cyber-physical risks present in manufacturing control systems – especially those in the chemical, steel and petroleum industries, where manufacturing processes can involve potentially unstable chemicals and extremely high temperatures. Without proper authentication practices, a skilled adversary could potentially send false commands to the endpoints controlling these processes and cause critical failures leading to injury, significant downtime or even loss of life. This is no doubt an extreme case, but it illustrates the potential risks imposed by poor authentication.

Unfortunately, strong authentication is not as common as it should be in manufacturing, for several reasons. One is that many communications protocols don't require authentication. Modbus, one of the most commonly used industrial automation protocols, typically lacks any form of device authentication, leaving the integrity of communications in question. What's more, manufacturing equipment often has long replacement cycles, which can reach 10-20 years. Older equipment nearing the end of its depreciation schedule is less likely to have been manufactured with security in mind or to have the computing capabilities necessary to implement cryptographic authentication. Manufacturing networks also require low latency to ensure real-time operations of critical processes. Engineering teams can be hesitant to implement any security measures that introduce latency, including authentication.

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. However, the pace of adoption could be slowed throughout the next few years by long replacement cycles of manufacturing endpoints and the need to evaluate alternate forms of authentication in order to minimize latency and cost while optimizing protection. During this interim period, we will likely see attacks carried out against manufacturing and other industrial systems that could have been prevented by stronger authentication.

Given the focus of recent industry standards on authentication, we also expect government regulation around the security of operational systems to recommend or require that manufacturing organizations adopt cryptographically secure authentication methods in some cases. Device authentication is a critical component of any security strategy, and this should prove to be no different in the manufacturing sector.