White Paper

IoT Device Security Risks Prompt Manufacturers to Adopt PKI Security, Provisioning Certificates During Production

Sponsored by: DigiCert

Robyn Westervelt
July 2020

EXECUTIVE SUMMARY

Internet of Things (IoT) is delivering great value, but the proliferation of IoT devices that provides rich data and services to users also brings new risks. Attackers seize on devices that contain security vulnerabilities or are inadequately deployed, configured, or managed. Simple methods for surreptitiously sniffing RFID, Bluetooth, and NFC communications are widely available. And there are countless news reports documenting manufacturing shortcomings. For example, digital picture frames have been mistakenly shipped with embedded malware and smart locks have been shipped with improperly configured electronic components designed to support data encryption. IDC's surveys have consistently found security of paramount concern to IoT device buyers. Security-minded buyers have realized usage scenarios can be affected by compromises to the confidentiality, integrity, and availability of the data and the proper implementation of the components of the device.

This IDC White Paper provides guidance to device manufacturers that are considering utilizing public key infrastructure (PKI) management platforms to provision certificates during production. Key takeaways from this white paper are:

- Device manufacturers are being increasingly held accountable by customers and regulators for implementing mechanisms that assist in monitoring, securing, and maintaining a baseline set of information about each IoT device connected to the network.
- To achieve the level of data integrity required by buyers of IoT devices, manufacturers must adopt PKI to support encryption and authentication and ensure the authenticity of the device firmware, operating system, and applications.
- Digital certificates can efficiently secure data transmitted by IoT devices and protect the hardware, firmware, and software intellectual property (IP); prevent cloning of unauthorized devices; and provide a secure way to update firmware in the field.
- To keep costs in line while improving the security outcome, countless studies have shown that security should be planned for and employed as early as possible including during the design phase of an IoT product.

Manufacturers must satisfy the security concerns of buyers. In part, this means "building security in" through strong software development and engineering practices, aligning their products to support PKI, and conducting in-depth code reviews prior to shipping. Digital certificates applied at manufacturing become the first trust anchor establishing device identity.

SITUATION OVERVIEW

IDC studies have found that digital transformation (DX) investments can enable enterprises to achieve as much as a 40% increase in productivity. Manufacturers are often buyers of IoT devices as well as producers of IoT devices. In many cases, manufacturers have deployed modern smart sensor components in production to gain greater insight into equipment and processes. From the procurement perspective, manufacturers vet the confidentiality, security, and integrity of smart sensors. The data gleaned from these IoT devices promise to help manufacturers conduct preemptive maintenance and reduce costly downtime. The data gleaned from these devices is also analyzed to make business decisions and create new products and services.

The same vetting takes place by buyers of modern manufactured devices that contain components for wireless connectivity and sensors for data collection. If these IoT devices contain the right level of support for secure connectivity and data protection, buyers can reach the level of cohesion with the interconnected physical/operational and virtual environments that allows them to create and adapt and respond to virtual or physical events effectively. While this creates operational resiliency by supporting intelligent operational systems such as robotics, it requires a high level of data integrity from IoT devices. To achieve that level of data integrity, manufacturers of these IoT devices should also align many of their products to support PKI for encryption, authentication, and the integrity of the device firmware, operating system, and applications.

Data proliferation is driving much of the interest in stronger device security mechanisms. The number of IoT devices collecting and transmitting data is expected to skyrocket, prompted in part by the promise of highly scalable 5G wireless connectivity. As devices are deployed, security rapidly rises as a key requirement. Security ranked first, selected by more than 40% of respondents of IDC's 2019 *Global IoT Decision-Maker Survey,* as the type of expertise required of IoT device manufacturers and service providers. Security was followed by requirements for data privacy and solution performance, and these demands are growing. IDC projects at least 55.9 billion internet- or network-enabled devices by 2025, with connected IoT devices accounting for almost 72% (or 35.2 billion) in 2023 and increasing to 75% (or 41.6 billion) in 2025. Nearly 80ZB of data is expected to be created by those newly connected IoT devices, according to *Worldwide Global DataSphere IoT Device and Data Forecast, 2019–2023* (IDC #US45066919, May 2019). Most of the data will be generated by video surveillance applications, but other categories such as industrial and medical sources will increasingly generate more data over time.

Enterprises Seek Embedded Security with IoT Devices

Manufacturers of IoT devices must maintain a security strategy that enables operational continuity and a digitally secure environment to produce products that meet rising buyer security requirements. For example, manufacturers of network-connected refrigeration units are addressing the rising need to secure components from external attacks. The need for PKI for encryption, authentication, and device integrity is paramount to save lives in hospitals where network-connected refrigeration units must keep medications and vaccines at a constant temperature.

Chief security officers, under continued pressure to thwart cyberattacks, increasingly seek manufacturers of IoT devices that demonstrate strong security best practices. When asked about IoT supplier criteria, "proven security capabilities" was overwhelmingly the top choice of respondents to IDC's 2019 *Global IoT Decision-Maker Survey,* followed by solution cost and integration. This focus on security was partially driven by the Mirai botnet, which was notable for targeting digital video recorders and webcams to carry out massive denial-of-service attacks. Attackers are seizing on rampant

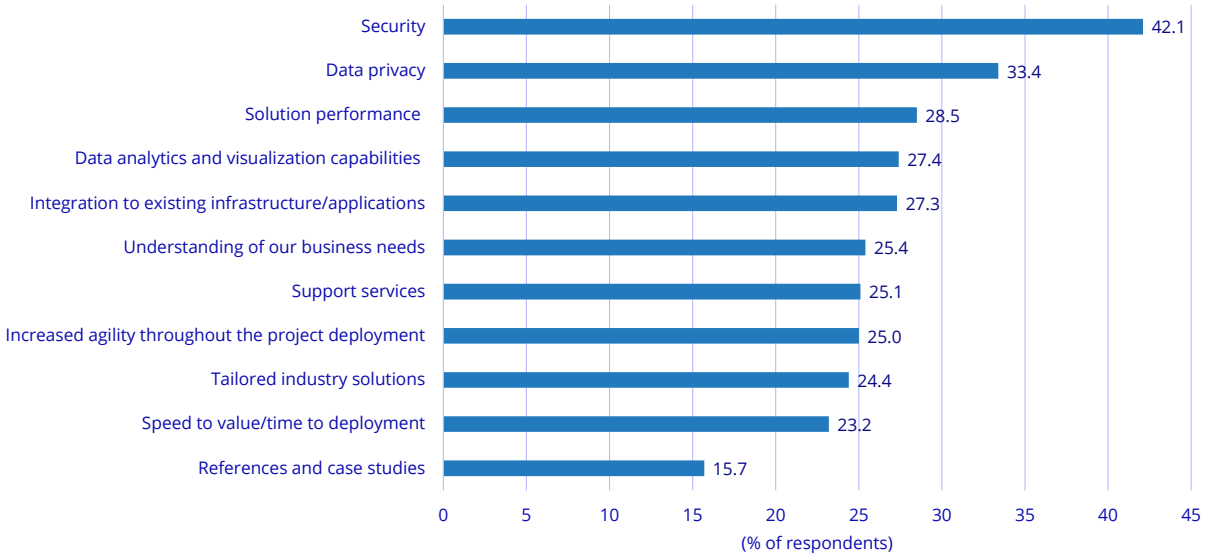
credential reuse and an ever-growing number of unpatched vulnerabilities. Several reports documented a significant increase in attacks against industrial control systems (ICSs) and operational technology (OT) infrastructure in 2019. At the start of 2020, security researchers warned of widespread vulnerability in popular routers, switches, IP phones, and IP cameras that can be remotely exploited by attackers to gain access to sensitive data or cause the devices to crash.

In IDC's 2019 *Global IoT Decision-Maker Survey,* security (42.1%) and data privacy (33.4%) ranked top when respondents were asked what type of expertise they would like to see existing IoT vendors and service providers improve (see Figure 1).

FIGURE 1

Desired IoT Solution Provider Improvements

Q. Which types of expertise would you like to see existing IoT vendors/service providers improve?



n = 4,480 enterprise decision makers representing global organizations with 100+ employees

Source: IDC's *Global IoT Decision-Maker Survey,* 2019

Manufacturers Must Make Cost-Effective Security Investments

The pressure is on for manufacturers to find and employ a variety of cost-effective security controls such as silicon-based security components. These components can greatly reduce the risk of physical attacks and cyberattacks and help manufacturers achieve a competitive advantage over legacy and insecure solutions. To keep costs in line and improve the security outcome, countless studies have shown that security should be planned for and employed as early as possible including during the design phase of an IoT product.

To address these issues at the device level, manufacturers are investing in product design and development services. These investments are in response to requests from security architects and chief information security officers for emerging hardware- and software-based security components.

As IoT devices are increasingly connected, manufacturers face these key challenges when addressing device risks:

- **Device authentication.** Many devices lack components to identify and verify the device identity before it connects to other systems or users in a secure manner. This results in a lack of visibility and inadequate monitoring of connected resources and could lead to data loss or theft. Certificates can be used to validate identities and authorize connectivity to specific resources.
- **Data and system integrity.** Product engineering teams seek to eradicate or greatly diminish counterfeit devices by incorporating strong device identity at the time of production to support authentication and authorization requirements. Certificates also play a critical role in checking the integrity of device firmware at the time it boots or validating the authenticity of software updates before they are applied.
- **Data encryption.** Once the device is authenticated, it must contain mechanisms to support a secure connection. Certificates play a role in ensuring data is protected when it is transmitted. Encryption must be properly implemented and configured to prevent attackers from spoofing a system with erroneous information or sniffing communications.

Certificate Provisioning: PKI Platforms Must Be Flexible and Address Complexity

The National Institute of Standards and Technology (NIST) cybersecurity framework recommends that enterprise security teams gain an inventory of physical devices and systems within the organization and have mechanisms to issue, manage, verify, revoke, and audit identities and credentials for authorizing devices. Organizations that heed this recommendation often use digital certificates to maintain complete situational awareness over IoT edge devices.

Manufacturers are in a position to enable enterprises to carry out this critical recommendation. IoT-specific PKI platforms are designed to help device manufacturers adopt PKI to improve the security of their IoT device over its life cycle. These platforms can also eliminate some longstanding and questionable security practices such as simply using labels for device identity over the lifetime of a device or hard-coding passwords and encryption keys, which can easily provide a false sense of security.

These IoT PKI platforms are designed to reduce complexity and enable manufacturers to establish a device root of trust using PKI to provide certificates used for authentication, encryption, and integrity. These are the essential ingredients of PKI where digital credentials play a key role in authenticating and validating identities to make sure only authorized users, messages, or servers have access to the device. PKI can also be the mechanism to ensure that over-the-air software updates are valid and free from manipulation before being deployed on an IoT device. At a minimum, PKI platform products should support the ability to dynamically create and provision certificates at scale to many devices and support creation and distribution of the private key without compromise.

The PKI platform should also strengthen the supply chain and simplify the provisioning of certificates during the assembly process. Manufacturers can choose to leverage the PKI platform provider's cloud or integrate with the provider's local certificate authority (CA) service to eliminate the risk of disruption at the time of production caused by poor internet connectivity. Data residency requirements and country-specific regulations as well as an air-gapped environment may also require the PKI platform to be deployed on premises.

DIGICERT PKI SOLUTIONS AND SERVICES

DigiCert is a provider of scalable TLS/SSL, IoT, and PKI solutions for identity and encryption. DigiCert's approach to modernizing PKI management, DigiCert ONE, supports fast and flexible PKI deployments. Based on modern software design and engineering, DigiCert ONE delivers end-to-end centralized user and device certificate management for a variety of deployment models and PKI use cases.

DigiCert IoT Device Manager, purpose built for the management of device identity, authentication, encryption, and integrity, is built on top of DigiCert ONE's container-based architecture.

DigiCert IoT Device Manager simplifies the provisioning and management of certificates to connected devices at scale via a cloud or on-premises PKI service. DigiCert supports the automated creation of flexible certificate profile configuration and enrollment methods. The DigiCert IoT Device Manager also provides IT administrators with a centralized management framework that allows for secure access to manage IoT devices from any location and at any time. The solution is broadly used to authenticate devices to other devices, to services, and to cloud applications and provides organizations with the flexibility to adopt PKI at both speed and scale. In addition, the solution is used to protect connected devices along with applications and their associated data, enabling administrators to automate enrollment and certificate issuance – and ultimately control access to services, monitor privacy controls, and manage application restrictions.

Opportunities, Challenges, and Guidance for Manufacturers Adopting PKI Solutions

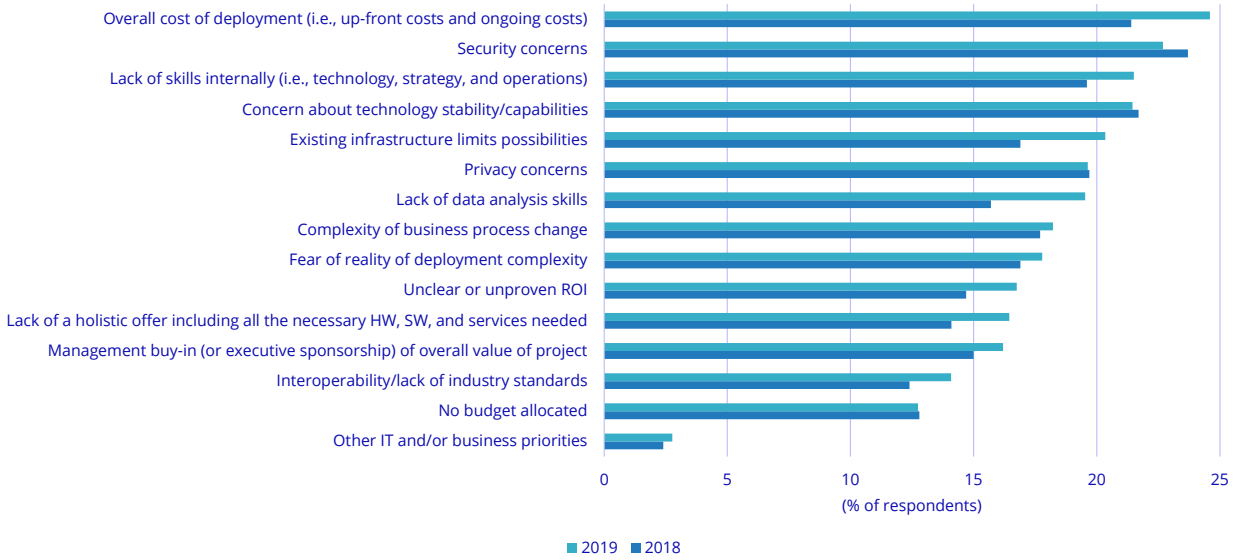
Every manufacturer has unique security and safety requirements that befit its operations and environments. DigiCert and other certificate authorities will have to demonstrate their expertise in the certificate management services that align with the needs of a specific manufacturer. Manufacturers must evaluate the PKI providers on the basis of their familiarity with their industry requirements as well as the system performance and support needed for their operations.

Security is the biggest development area in IoT. As shown in Figure 2, IDC's 2019 *Global IoT Decision-Maker Survey* found that security concerns are the second-ranked top challenge holding back or slowing progress on IoT projects within organizations.

FIGURE 2

Top IoT Project Challenges

Q. What do you think are the top 3 challenges holding back or slowing progress on IoT projects within your organization? (Select up to three.)



n = 3,828 (2018) and 4,480 (2019) enterprise decision makers representing global organizations with 100+ employees

Source: IDC's *Global IoT Decision-Maker Survey,* 2018 and 2019

Buyers are compelling manufacturers to establish security best practices and embed security into their processes. To satisfy these concerns, the process of architecting a modern approach may require on-premises infrastructure to streamline and automate the often complex and fragmented PKI ecosystem that manufacturers are trying to maintain. This is a multipronged, multiyear endeavor. Manufacturers should evaluate DigiCert and its competitors' ability to help architect a PKI strategy as painlessly as possible. Any strategy is more likely to result in the need to manage a hybrid PKI ecosystem consisting of on-premises and cloud-based or remote infrastructure. This effort requires an up-front investment and PKI specialists who are knowledgeable about existing business processes and IT infrastructure, the location of critical resources, and management's existing risk tolerance and growth strategy.
Rapid growth, mergers and acquisitions, the adoption of new technology, business strategy changes, and other external factors can heavily impact and even derail improvement projects if they are not adequately planned and systematically executed.

Recommendations

Baking security into IoT devices gives manufacturers a competitive advantage, but trusted IoT devices require security components that support issuance of device identity at the time of manufacturing or device provisioning. The timing is critical to support authentication and authorization requirements for creating secure network of things ecosystems. Manufacturers must demonstrate a commitment to security by building trust with customers and business partners. This effort begins by "building security in" through

strong software development practices and in-depth code reviews prior to shipping and embedding PKI and digital certificates to support device identity at the manufacturing floor or during device assembly.

Manufacturers can consider the following action items to bolster security:

- **Invest for the future.** Addressing security requirements also requires the implementation of cost-effective measures to raise the bar an attacker must overcome.
- **Establish security by design.** Some IoT device manufacturers are learning the hard lesson that IT software makers learned years ago: bolting on security controls after a product goes to market is costly. IoT device manufacturers should include PKI into the design of their devices. This demonstrates a commitment to security and privacy required by buyers.
- **Shield software vulnerabilities.** Manufacturers must provide a measure of confidence that the device they are producing is free of vulnerabilities and functions in its intended manner. The discovery of new vulnerabilities and threats will require PKI to validate the integrity of updates to device firmware and software.

CONCLUSION

Embedded systems experts interviewed by IDC believe now is the time for manufacturers to address process and design challenges associated with device identity, authentication, data encryption, and secure connectivity. IDC supports this view. Data security and privacy is paramount for enterprises striving to establish long-term trusted relationships with their customers, business partners, and employees.

Manufacturers of IoT devices that gain the greatest competitive advantage have established trust with their customers partly by demonstrating a commitment to security. The security model of the product is one of the top factors in device selection criteria, according to IDC's 2019 *Global IoT Decision-Maker Survey,* which surveyed 4,480 IoT decision makers about their ongoing IoT initiatives. Those respondents involved in projects incorporating IoT devices expect vendors to demonstrate deep industry expertise and offer best-of-breed data management capabilities that support strong security.

Manufacturers must lay the foundation for secure connectivity by leveraging the components that support established security best practices beginning with PKI, which has withstood the test of time. They need to evaluate providers of PKI tools to find a specialist that has the skilled experts and supporting resources to assist manufacturers with laying the foundation for secure connectivity.

Digital certificates applied at manufacturing become the first trust anchor establishing device identity. Device manufacturers are being held increasingly accountable by customers and regulators for implementing mechanisms that assist in monitoring, securing, and maintaining a baseline set of information about each IoT device connected to the network. PKI provides the key elements that enable a baseline level of security for IoT devices. PKI supports encryption and authentication and enables device owners to validate the integrity and authenticity of the device firmware, operating system, and applications.

MESSAGE FROM THE SPONSOR

DigiCert is a leading provider of scalable TLS/SSL, IoT and PKI solutions for identity and encryption. The most innovative companies, including 89% of the Fortune 500 and 97 of the 100 top global banks, choose DigiCert for its expertise in identity and encryption for web servers, enterprise and Internet of Things devices. The company is recognized for its enterprise-grade certificate management platform, fast and knowledgeable customer support, and market-leading security solutions. For the latest DigiCert news and updates, visit digicert.com or follow @digicert.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com