Security in the age of IoT

by Lantronix

Executive summary

In 1965, Intel Corporation co-founder, Gordon Moore, predicted that overall computer processing power would nearly double every two years as a result of the density and falling costs of transistors and CPUs. More than 50 years later, advancements in chip research and ubiquitous access to a variety of wired and wireless connectivity options have paved the way for OEMs to augment existing systems with innovative technologies such as sensors, compute and storage for big data applications, and streaming edge analytics to the cloud. Although it has been with us in some form and under different names such as M2M, global adoption of the Internet of Things (IoT) and cloud-based technologies is projected to reach more than 20 billion devices by 2020[1].

The rapid transition from closed/private networks to enterprise-wide networks over the public Internet is uncovering security risks that went previously unnoticed—and justifiably raising alarms about the future of cybersecurity in the age of IoT. Moreover, as enterprises become increasingly reliant on intelligent, interconnected devices in every aspect of their business, OEMs must ask themselves if they are doing enough to protect vulnerable systems that could compromise sensitive data, personal privacy or threaten public safety.

As a global leader in embedded technology solutions and IoT, Lantronix is dedicated to assisting our OEM customer base with securing their business-critical assets and ensuring compliance with stringent regulations such as Federal Information Protection Standard 140-2 (FIPS 140-2). This white paper will examine the constraints and security challenges posed by connected devices in the IoT as well as the various approaches to addressing them.

The challenge

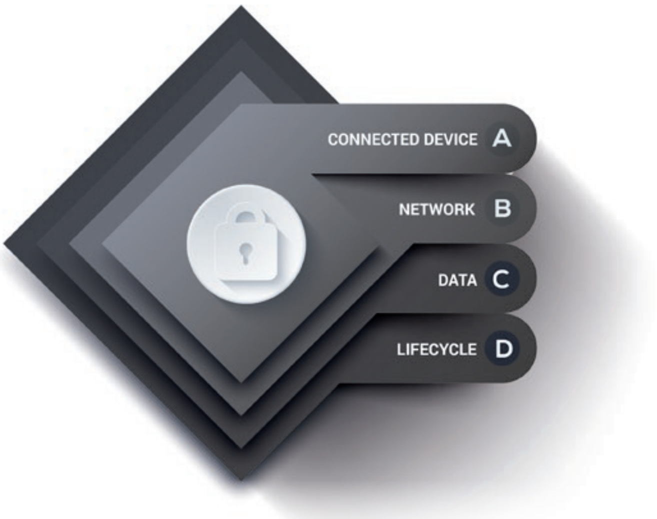
The increased yield and economic benefit of IoT are projected to add as much as $14.2 trillion to 20 of the world's major economies over the next 15 years, according to the latest analysis from Accenture[2]. Future value creation for enterprises, cities, and government verticals will primarily come from monetising hidden data locked away in legacy industrial devices and brownfield equipment such as motors, pumps, control systems and heavy machinery. This exponential increase in data throughput will create the need for various IT departments to monitor and manage millions of different devices, many of which were designed and deployed decades ago and never intended to connect to any network.

The sheer quantity, diversity and age of these devices will grow the potential attack surface considerably and present high-value targets for hackers if proper IoT security best practices are overlooked. A primary concern is that many of these connected devices are a part of a country's critical infrastructure such as electrical grids and communication infrastructure. Therefore, any intrusion into these networks could have potentially devastating effects on national security.

The challenge of preventing future cyber-attacks is also compounded by the complex value chain of IoT product deployments where many parties are involved in the manufacturing process and operation once deployed in the field. This is especially apparent in organisations that lack technical and networking expertise such as small businesses. So how do the various players in the complex IoT ecosystem ensure that connected devices remain secure so critical infrastructure, enterprises and most importantly, the well-being of people are not compromised?

The multi-layered approach to IoT device security

There is no silver bullet to solving the cybersecurity challenge. Increased deployments of connected devices over the past few years have caused common tried-and-true IT security controls to evolve and adapt to the unique constraints of embedded devices. OEMs, solution providers, system integrators, and end users need to establish a comprehensive, multi-layered strategy that ensures the end-to-end protection of their IoT deployments. Traditional solutions that use network firewalls and protocols only offer protection against high-level Internet traffic as opposed to embedded endpoint devices. Guaranteeing maximum protection throughout an IoT product's lifecycle requires securing the device's hardware and software, the data at rest and data in motion, as well as the communication network itself.



Securing the connected devices

The first layer in an end-to-end IoT security strategy begins by protecting the hardware and software of the connected device itself. Concerns over the authenticity of software and the protection of intellectual property have precipitated various software verification and attestation techniques explained on the next page.

Trusted boot/secure boot

Over the past decade, hardware-based, anti-malware technologies have emerged to address security problems shared by multiple parties. Trusted or secure boot requires devices to verify firmware and software packages at boot time through cryptography. When a connected device is powered on, the authenticity and integrity of the software on the device is verified using encrypted digital signatures. These digital signatures are attached to the software image and confirmed by the device to ensure only authorised software signed by the designated device entities will be loaded to run on the machine.

Embedded devices should have secure certificate storage, which is programmed during manufacturing to establish the root of trust.

Application whitelisting

Once a foundation of trust is established, the connected device still needs protection from various run-time threats and malicious parties. Many IoT device manufacturers have begun to use application whitelisting on their new connected products to ensure machines are not compromised at the application level. Device manufacturers have used whitelisting techniques in place of blacklisting to preserve the real-time operation of legacy devices that are unable to run traditional antivirus applications. For centrally managed environments, application whitelisting stops the execution of malware and other unauthorised software by only allowing indexed applications the chance to run on the device. Conventional antivirus software and other PC security technologies block known bad activity while permitting all other. On the other hand, application whitelisting conserves valuable bandwidth by allowing known good activity and preventing all other.

Access control

Proper access control is based on the principle of least privilege, which dictates that only the minimal amount of access required to perform a function should be authorised to curtail the impact of any breach of security. Access control safeguards are typically mandatory or role-based controls built into the operating system that limits the access of device components and applications to the resources they need to do their tasks. Device-based access control mechanisms are analogous to network-based access control systems. If any component is compromised, access control ensures that the intruder has as limited access to other parts of the system as possible.

OEMs should select devices that allow them to configure multiple users and assign them granular permissions to access various functions of the device.

Securing the network

Once a device is connected to the network, the device should authenticate itself before receiving or transmitting data. Embedded devices often must support multiple ways of having their network credentials stored in their secure storage.

The network administrator might pre-provision them in a central location before deployment, or an end user can use a mobile application to configure the device. Supporting multiple ways to configure the device ensures ease of deployment as well as compliance with the best security practices such as changing default passwords.

Given that embedded and industrial IoT devices have unique protocols that are different from traditional IT protocols, firewalls or deep packet inspection capabilities are needed to control traffic that is destined to terminate at the device. For example, industrial devices used in manufacturing have their own set of protocols governing how devices communicate with each other and the various control systems that require industry-specific protocol filtering and deep packet inspection capabilities to identify malicious payloads.

Beyond protocol and application-aware firewalls, intrusion detection and prevention systems (IDS/IPS), plus security incident and event management (SIEM) solutions are also required to keep malicious activity off corporate networks. If malware managed to breach a firewall, antivirus techniques based on signature matching and blacklisting would identify and remedy the problem.

Establishing a secure connection to legacy devices that lack many of the new security measures implemented is another obstacle. A new category of devices called IoT gateways help ensure that legacy devices connect with proper security measures to any network. To learn more about IoT gateways, please refer to the Lantronix Industrial IoT Gateway Solution Brief.

Securing the data

Data privacy and confidentiality remains the primary concern for the enterprise and individuals. It is essential that the data be secured and encrypted in storage locations on the device and while traveling through the network – commonly referred to as security of data at rest and data in motion respectively. Various security measures such as virtual private networks (VPN) or physical media encryption, such as 802.11i (WPA2) or 802.1AE (MACsec), have been developed to ensure the security of data in motion.

Securing the lifecycle

One of the most often overlooked layers of IoT is device security lifecycle. Security must be addressed throughout the device lifecycle, from the initial design by the device manufacturer, to the operational environment handled by the end user or a system integrator, and final decommissioning. After the device is deployed in the field and securely provisioned onto the network, continual firmware patches and software updates must be loaded onto the device to make sure each security layer stays intact even if already infected with malware.

Devices need enough storage to carry out an automatic rollback in the event of an update failure, but malicious rollback to older versions of the firmware or software with critical vulnerabilities must be prevented. End users and operators of IoT devices need a method of rolling out and authenticating patches that do not consume bandwidth or impair the functional safety of the device. Since security vulnerabilities are discovered by OEMs and technology providers regularly, end users and operators must use best practices throughout the lifecycle of their device. These include:

- Always enabling password protection where offered and changing any default passwords
- Always use the strongest passwords possible
- Shutting down any unused services/ports on embedded devices
- Always keeping products up-to-date with the latest firmware to capture the latest updates and security patches from the device manufacturer
- Paying attention to the device manufacturer's end-of-life (EOL) notices that may affect their products as they could affect software patches including those related to security updates.

Conclusion

The rapid adoption of IoT over the coming years will generate massive global economic value but also poses new security risks as more devices are connected to the Internet. The Internet of Things is unprecedented in its interaction with the physical world, and the critical infrastructure systems that impact the safety and privacy of enterprises and individuals. As discussed, implementation of IoT security needs to be multilayered and evolve throughout a product's lifecycle – at the data, device, and network layers. Fortunately, this does not require a revolutionary approach, but rather applying measures that have proven successful in IT networks to the challenges of IoT and the constraints of connected embedded devices.

Furthermore, the complex value chain of IoT requires all entities involved in the deployment and operation of an IoT solution to remain vigilant in all security matters. A comprehensive device security framework includes the following components:

OEMs deploying secure connectivity within their products must consider the requirements of the environment in which their products will be deployed. Since these can vary based on their customer's network, OEMs need to dig deeper into the features and capabilities of the secure connectivity stack offered by vendors. Examples of the types of checks needed would be:

- Check to make sure that support for Enterprise Wi-Fi security is not limited to one or two EAP methods while not supporting other EAP methods that could be deployed within their customer's infrastructure
- Check to make sure that at least three levels of the PKI certificate chain are configurable (This has become the minimum requirement for Industry 4.0[3] deployments as well)
- Check to make sure that the latest hash/crypto algorithms and security protocol versions are supported

ENCRYPTION

Data encryption technologies such as Secure Socket Layer (SSL) and Transport Layer Security (TLS) and X.509 PKI for data encryption throughout the network (data in motion)

AUTHENTICATION

Standard and Enterprise Wi-Fi security such as PSK, Wi-Fi Protected Access 2 (WPA2)-Enterprise and Extensible Authentication Protocol (EAP) for secure Wi-Fi network connectivity

VERIFICATION

Secure Boot that cryptographically verifies firmware and software packages at boot time and Secure Firmware-Over-The-Air (FOTA) update ensures only authorised firmware gets programmed

Secure credential storage that protects critical key and password information on the device (data at rest)

COMPLIANCE

The Federal Information Processing Standard 140-2 (FIPS 140-2) certification, which is a U.S. and Canadian co-sponsored security standard for hardware, software, and firmware solutions that ensure end users receive a high degree of security, assurance, and dependability

Products and solutions deployed in industrial IoT and enterprise environments remain active for 7-10 years. Besides component and supply chain availability, OEMs and SIs need to ensure that vendors provide regular security vulnerability updates and software patches throughout the active life of the product. Vendors that have a history of supporting and delivering products can be an extension of the OEM/SI teams working to ensure their deployed products and solutions remain relevant and up to date.

Vendors that work closely with the networking and IT users in the enterprise bring a fresh perspective into the needs and challenges of these users. OEMs building securely connected products that are asked to comply with varying IT security and network policies can leverage this unique expertise and gain a competitive advantage for their products and solutions. Lantronix IoT building blocks, modules, gateways, and IT network appliances provide various integrated technologies to help OEMs build secure connected devices, as well as solutions for solution providers, system integrators, and end users to implement end-to-end IoT security for their applications with complete device lifecycle security.

References

[1] Gartner, Securing the Internet of Things, available at: https://www.gartner.com/doc/3316617/securing-internet-things

[2] Accenture, Transforming Economic Growth with The Industrial Internet of Things, available at: https://www.forbes.com/sites/valleyvoices/2015/01/21/transforming-economic-growth-with-the-industrial-internet-of-things/

[3] Wikipedia, Industrie 4.0, available at: https://en.wikipedia.org/wiki/Industry_4.0

For more information, see wwww.lantronix.com