The challenges of IoT security and how to harden the edge

By Andrew Bickley, Arrow Electronics

Securing data and devices on the IoT is essential but extremely challenging. Assets can be distributed over a large geographical area, left unattended, and subjected to all manner of attacks by devious and determined hackers. IoT security is a multi-faceted challenge. Clear frameworks and best practices, developed by security experts, can help device designers and network planners to put the right security measures in the right places

■ Security has quickly become a key concern in the world of the IoT. While digital transformation has made clear to organisations the value of data, there are also high risks surrounding the potential misuse of data. This misuse highlights the absolute necessity for strong cyber security. IoT technologies introduce numerous attack surfaces that hackers can exploit to steal data or launch other exploits. Going forward, more and more companies will be affected: Gartner predicts that over half of major new business processes and systems will incorporate some element of the IoT by 2020.

There is no doubting the power IoT applications can deliver, to help improve business efficiency and raise quality of service. Deploying huge numbers of connected sensors and actuators enables organisations to gather massive quantities of data to drive continuous improvement including: control processes remotely to streamline staffing and maximise yield, track the locations of assets to increase operational efficiency, and anticipate maintenance requirements in remote equipment to minimise downtime and utilise staff efficiently, to name just a few. As a tool to support activities like business, commerce, and environmental management, the IoT is just at the beginning of its evolutionary cycle; many more as yet unimagined applications can be expected to emerge in the future. The imagination of application developers will likely be matched only by that of hackers intent on subverting the IoT for their own ends.

Organisations will come to rely heavily on their IoT-based applications, to respond quickly to events in the field and make the right long-term business decisions. They will need a high level of trust in the data from connected assets. Hence preventing unauthorised access to this data is extremely important, to prevent eavesdropping or sabotage; if malicious agents can intercept data or gain access to connected devices, they can exploit numerous opportunities to cause damage by selling or publishing the data illegally, altering the data to misinform or misdirect, loading bogus code to take over or block the devices, or gain access to more sensitive assets within the organisation. These could be security cameras, access-control systems, drives containing confidential information, or others. If any such exploits are successful, victims may suffer direct financial losses or other harm such as reputational damage or lost market opportunities.

By their nature, IoT devices often operate autonomously for long periods, in remote locations, without being regularly inspected for signs of physical tampering. Moreover, being connected to the Internet gives online hackers the opportunity to launch attacks over the Internet without needing to go anywhere near the physical location of the device. Software that scours the Internet for vulnerable connected devices is already readily available on the Internet. Moreover, Gartner – in the same report that predicts the future pervasiveness of the IoT – has said there will be a $5 billion black market by 2020 for fake sensor and video data that can be used to compromise the integrity of data from legitimate IoT devices.

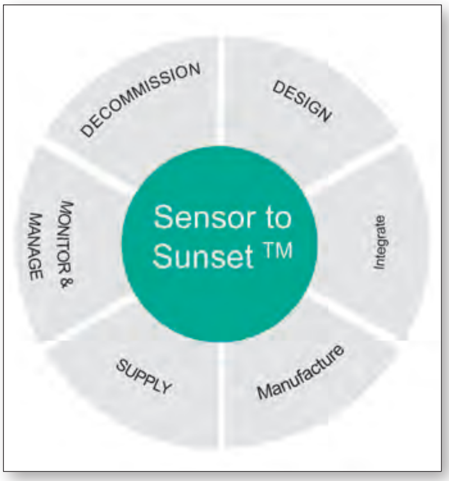
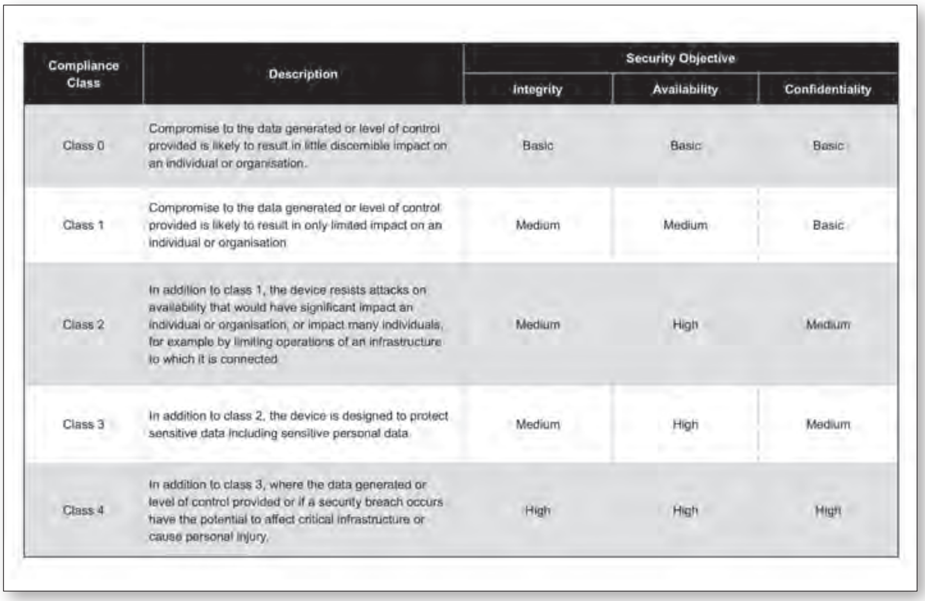


Figure 1. Security concerns over product lifecycle



Compliance Class	Description	Security Objective		
		Integrity	Availability	Confidentiality
Class 0	Compromise to the data generated or level of control provided is likely to result in little discernible impact on an individual or organisation.	Basic	Basic	Basic
Class 1	Compromise to the data generated or level of control provided is likely to result in only limited impact on an individual or organisation	Medium	Medium	Basic
Class 2	In addition to class 1, the device resists attacks on availability that would have significant impact an individual or organisation, or impact many individuals, for example by limiting operations of an infrastructure to which it is connected	Medium	High	Medium
Class 3	In addition to class 2, the device is designed to protect sensitive data including sensitive personal data	Medium	High	Medium
Class 4	In addition to class 3, where the data generated or level of control provided or if a security breach occurs have the potential to affect critical infrastructure or cause personal injury.	High	High	High

Table 1. IoT Security Foundation compliance framework for IoT end nodes

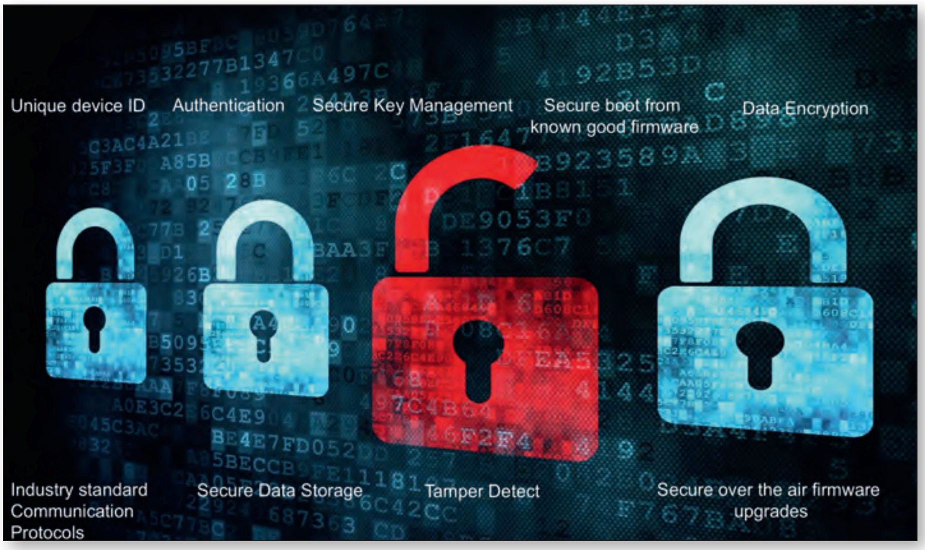

Unique device ID
Authentication
Secure Key Management
Secure boot from known good firmware
Data Encryption
Industry standard Communication Protocols
Secure Data Storage
Tamper Detect
Secure over the air firmware upgrades

Figure 2. Security strategy for edge-node designs

Clearly, the threat is real and significant, and organisations understand the key areas of vulnerability that present barriers to adoption of IoT-based business solutions. Businesses surveyed by 451 Research expressed concern about weaknesses throughout the IoT infrastructure, particularly at the network edge including IoT endpoints and their connections to other devices and the central network.

The most important concerns are the physical security of endpoints, authentication of connected devices, the security of application software, and the connections between IoT devices and the central network. Issues like the security of IoT data stores and vulnerability to denial of service attacks rank below the challenges related to the more vulnerable edge devices and infrastructure. Securing assets connected to the IoT is a huge challenge. Devices are not only vulnerable to physical attacks as well as online exploits, but also typically have only limited resources like processor cycles, power, and memory, to support electronic security. Suitable security must also be unobtrusive, so as not to obstruct authorised users or detract from the overall efficiency and business value of the application. To help implement adequate security, within the prevailing constraints, it is valuable to analyse the potential threats facing various types of device, and the possible implications of a breach in each case, and so develop coherent security policies and best practice guidelines.

The IoT Security Foundation has comprehensively studied device and data security breaches, and their impact on privacy, business activity, infrastructure and safety, to formulate a set of security compliance classes. This analysis can help ensure that IoT devices are designed with adequate security for their intended use and deployed appropriately by network planners. Table 1 describes these compliance classes, in relation to device integrity, device availability, and data confidentiality.

Any approach to IoT security must also recognise that hackers will seek to target the weakest links in the network and use the smallest and lowest-cost nodes as entry points or stepping stones to reach higher-value assets and/or penetrate core networks. A structured approach is needed when designing IoT devices, and when setting up networks, to ensure that all available security techniques are assessed and implemented according to need and within the capabilities of the host system. Security measures applicable to IoT devices include: tamper detection, secure data storage, securing data transmission, authentication, secure boot, secure firmware updates, secure manufacturing of IoT devices, secure decommissioning of IoT end nodes and proper handling of associated assets (data), and security policies and procedures.

These considerations span the complete IoT-device lifecycle (figure 1), from the earliest stages of designing the embedded system – such as selecting a microcontroller with integrated cryptographic coprocessing, or a discrete hardware secure element – through manufacture, commissioning and maintaining while in the field, to removal from the network and disposal at end of life. Even with the aid of a rigorous compliance framework such as that developed by the IoT Security Foundation, and a clear grasp of applicable hardware and software-based security techniques, the fact remains: IoT data faces a huge diversity of security challenges between network endpoints and the core, whether this is a private corporate network, or the Cloud. A wide range of security solutions is available, from many providers, but developers need help to evaluate, select, and combine the chosen elements into a coherent whole that covers all potential vulnerabilities optimally. Figure 2 suggests a security strategy for IoT-endpoint designs, to protect against physical and online attacks.

The Arrow Connect offering aims to provide such a resource, by bringing together solutions for managing IoT devices including endpoints and gateways. It encompasses both a Software Development Kit (SDK) for gateways and endpoints, and the design of device to Cloud management. It includes solutions for provisioning devices on the network securely, authentication, handling security keys, device identification, device management, endpoint priorities, groupings and hierarchies, data ingestion, data storage, data access, and Over-The-Air (OTA) software update. ■