Generic iOT Guide

Securing an Internet of Things (IoT) infrastructure requires a rigorous security-in-depth strategy. This strategy requires you to secure data in the cloud, protect data integrity while in transit over the public internet, and securely provision devices. Each layer builds greater security assurance in the overall infrastructure.

Secure an IoT infrastructure

This security-in-depth strategy can be developed and executed with active participation of various players involved with the manufacturing, development, and deployment of IoT devices and infrastructure. Following is a high-level description of these players.

- **IoT hardware manufacturer/integrator**: Typically, these players are the manufacturers of IoT hardware being deployed, integrators assembling hardware from various manufacturers, or suppliers providing hardware for an IoT deployment manufactured or integrated by other suppliers.
- **IoT solution developer**: The development of an IoT solution is typically done by a solution developer. This developer may part of an in-house team or a system integrator (SI) specializing in this activity. The IoT solution developer can develop various components of the IoT solution from scratch, or integrate various off-the-shelf or open-source components.
- **IoT solution deployer**: After an IoT solution is developed, it needs to be deployed in the field. This process involves deployment of hardware, interconnection of devices, and deployment of solutions in hardware devices or the cloud.
- **IoT solution operator**: After the IoT solution is deployed, it requires long-term operations, monitoring, upgrades, and maintenance. These tasks can be done by an in-house team that comprises information technology specialists, hardware operations and maintenance teams, and domain specialists who monitor the correct behavior of overall IoT infrastructure.

The sections that follow provide best practices for each of these players to help develop, deploy, and operate a secure IoT infrastructure.

IoT hardware manufacturer/integrator

The following are the best practices for IoT hardware manufacturers and hardware integrators.

- **Scope hardware to minimum requirements**: The hardware design should include the minimum features required for operation of the hardware, and nothing more. An example is to include USB ports only if necessary for the operation of the device. These additional features open the device for unwanted attack vectors that should be avoided.
- **Make hardware tamper proof**: Build in mechanisms to detect physical tampering, such as opening of the device cover or removing a part of the device. These tamper signals may be part of the data stream uploaded to the cloud, which could alert operators of these events.
- **Build around secure hardware**: If COGS permits, build security features such as secure and encrypted storage, or boot functionality based on Trusted Platform Module (TPM). These features make devices more secure and help protect the overall IoT infrastructure.
- **Make upgrades secure**: Firmware upgrades during the lifetime of the device are inevitable. Building devices with secure paths for upgrades and cryptographic assurance of firmware versions will allow the device to be secure during and after upgrades.

IoT solution developer

The following are the best practices for IoT solution developers:

- **Follow secure software development methodology**: Development of secure software requires ground-up thinking about security, from the inception of the project all the way to its implementation, testing, and deployment. The choices of platforms, languages, and tools are all influenced with this methodology. The Microsoft Security Development Lifecycle provides a step-by-step approach to building secure software.
- **Choose open-source software with care**: Open-source software provides an opportunity to quickly develop solutions. When you're choosing open-source software, consider the activity level of the community for each open-source component. An active community ensures that software is supported and that issues are discovered and addressed. Alternatively, an obscure and inactive open-source software project might not be supported and issues are not likely be discovered.
- **Integrate with care**: Many software security flaws exist at the boundary of libraries and APIs. Functionality that may not be required for the current deployment might still be available via an API layer. To ensure overall security, make sure to check all interfaces of components being integrated for security flaws.

IoT solution deployer

The following are best practices for IoT solution deployers:

- **Deploy hardware securely**: IoT deployments may require hardware to be deployed in unsecure locations, such as in public spaces or unsupervised locales. In such situations, ensure that hardware deployment is tamper-proof to the maximum extent. If USB or other ports are available on the hardware, ensure that they are covered securely. Many attack vectors can use these as entry points.
- **Keep authentication keys safe**: During deployment, each device requires device IDs and associated authentication keys generated by the cloud service. Keep these keys physically safe even after the deployment. Any compromised key can be used by a malicious device to masquerade as an existing device.

IoT solution operator

The following are the best practices for IoT solution operators:

- **Keep the system up-to-date**: Ensure that device operating systems and all device drivers are upgraded to the latest versions. If you turn on automatic updates in Windows 10 (IoT or other SKUs), Microsoft keeps it up-to-date, providing a secure operating system for IoT devices. Keeping other operating systems (such as Linux) up-to-date helps ensure that they are also protected against malicious attacks.
- **Protect against malicious activity**: If the operating system permits, install the latest antivirus and antimalware capabilities on each device operating system. This practice can help mitigate most external threats. You can protect most modern operating systems against threats by taking appropriate steps.
- **Audit frequently**: Auditing IoT infrastructure for security-related issues is key when responding to security incidents. Most operating systems provide built-in event logging that should be reviewed frequently to make sure no security breach has occurred. Audit information can be sent as a separate telemetry stream to the cloud service where it can be analyzed.
- **Physically protect the IoT infrastructure**: The worst security attacks against IoT infrastructure are launched using physical access to devices. One important safety practice is to protect against malicious use of USB ports and other physical access. One key to uncovering breaches that might have occurred is logging of physical access, such as USB port use.

Again, Windows 10 (IoT and other SKUs) enables detailed logging of these events.

- **Protect cloud credentials**: Cloud authentication credentials used for configuring and operating an IoT deployment are possibly the easiest way to gain access and compromise an IoT system. Protect the credentials by changing the password frequently, and refrain from using these credentials on public machines.

Capabilities of different IoT devices vary. Some devices might be computers running common desktop operating systems, and some devices might be running very light-weight operating systems. The security best practices described previously might be applicable to these devices in varying degrees. If provided, additional security and deployment best practices from the manufacturers of these devices should be followed.

Some legacy and constrained devices might not have been designed specifically for IoT deployment. These devices might lack the capability to encrypt data, connect with the Internet, or provide advanced auditing. In these cases, a modern and secure field gateway can aggregate data from legacy devices and provide the security required for connecting these devices over the Internet. Field gateways can provide secure authentication, negotiation of encrypted sessions, receipt of commands from the cloud, and many other security features.