How to future-proof your IoT device – achieving ‘Secure by Design’ for IoT and connected devices

Developing a secure, smart consumer product from concept all the way through to operation, including manufacture and over the air (OTA) updates, means shifting to a security mindset. You need to think about security early in your IoT projects and product planning process, and invest in a secure development lifecycle, to tick all of the Secure by Design (SbD) boxes.

Here we set out key stages you should go through when considering security in your internet of things device to comply with the UK’s Secure by Design (SbD) principles. It’s worth noting that the UK Government is taking ‘decisive action’ on security; ‘advocating a robust and staged approach to enforcing these principles through regulation’ and ‘leading efforts to create international alignment on IoT security’, for example, working with other territories such as the US (NIST) and the EU (ETSI) to align standards. The SbD Code of practice has been developed to also align with any future Trustmark scheme. In short, the direction of travel is only going one way.

Consult Red’s experience in design and development of smart, connected devices and systems can reduce your time to market and manage cyber security risk to deliver truly secure IoT products.

Cyberattacks on IOT devices surge 300% in 2019, now ‘Measured In Billions’*

// 13 Principles in the UK Government’s Secure by Design Code of Practice

Secure by Design - Guidance

SbD1 No default passwords
All IoT device passwords must be unique and not resettable to any universal factory default value.

SbD2 Implement a vulnerability disclosure policy
Provide a public point of contact in order that security researchers and others are able to report issues.

SbD3 Keep software updated
All software components in internet-connected devices should be securely updatable.

SbD4 Securely store credentials and security-sensitive data
Any credentials must be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable

SbD5 Communicate securely
Security-sensitive data, including any remote management and control, should be encrypted when transiting the internet.

SbD6 Minimise exposed attack surfaces
All devices and services should operate on the ‘principle of least privilege’.

SbD7 Ensure software integrity
Software on IoT devices must be verified using secure boot mechanisms.

SbD8 Ensure personal data is protected
Where devices and/or services process personal data they should do so in accordance with data protection law.

SbD9 Make systems resilient to outages
Resilience must be built in to IoT services where required by the usage or other relying systems.

SbD10 Monitor system telemetry
If collected, all telemetry such as usage and measurement data should be monitored for security anomalies within it.

SbD11 Make it easy for users to delete personal data
Devices and services should be configured such that personal data can easily be removed or deleted by the consumer.

SbD12 Make installation and maintenance of devices easy
Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability.

SbD13 Validate Input data
Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks must be validated.

Access full definitions and details of the UK Government’s Secure by Design principles here:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775539/Secure_by_Design_Report_.pdf

A 7 stage approach to securing your IoT device

//consult.red

1

// The Beginning

Requirements Analysis

It’s important to approach your product design with a security mindset and invest in a secure development lifecycle from the start; if security is not captured at the beginning, don’t expect it to be there at the end!

This starts by ensuring your product and operational requirements comply with the SbD code of practice and includes features such as: easy installation and update, deletion and protection of personal data, resilience to outages, software integrity, secure communication, and other requirements as appropriate.

SbD8 Ensure personal data is protected ✓
SbD9 Make systems resilient to outages ✓
SbD11 Make it easy for consumers to delete personal data ✓
SbD12 Make installation and maintenance easy ✓

2

// Before manufacture

Attack Surface Analysis

IoT expands the attack surface, so you’ll need a system wide review of all physical, electrical and wireless interfaces to understand all vulnerabilities that could be exploited.

The goal of the review is to minimise and mitigate risk, so it needs to include product development, scaling to volume manufacture and product rollouts.

SbD6 Minimise exposed attack surfaces ✓

Reviewing attack surfaces – consider:

Deterrence: What can be done to deter attacks in the first place?

Prevention: This generally drives the implementation, it can involve aspects such as encryption or signing or one time programming.

Detection: How will we know if security is breached?

Correction & Counter Measures: How is a breach managed? This may involve revocation of keys/ certificates, software.

Needs more analysis?

3

// Before manufacture

Design and Development

Incorporate your attack surface analysis into the product design. Our design approach always seeks to leverage proven and approved security technologies.

Implementation can introduce vulnerabilities so review and testing are important at this stage. For instance, this is when negative testing can be used to check input data is being correctly validated or impaired network testing can verify resilience.

In some cases an independent audit may be needed. It’s likely you’ll go back and forth between these stages a few times until you get something that works and is secure.

SbD5 Communicate securely ✓
SbD13 Validate input data ✓

4

// Before manufacture

Production Planning

Planning how you’ll securely manufacture and deploy your device in the field is an important step.

For instance, if you’re considering emailing product security keys to the factory, then your products won’t be secure. If you’re deploying unique passwords to each device, how will you communicate that password?

This is an often overlooked step but taking shortcuts can compromise your device later on (and prove costly to fix).

SbD1 No default passwords ✓
SbD2 Implement a vulnerability disclosure policy ✓

Example: Delivering Secure IoT during Manufacture
An example of how we’ve delivered turn-key, future-proof and secure IoT during manufacture: implementation of a Bluetooth Low Energy board with secure multiple key injection in a smart device.

Keys generation process.
We generated three keys per device using a secure cloud key server. In our experience using separate unique keys and techniques for storage, software & control is good way to achieve future-proofed security.

SbD8 Ensure personal data is protected ✓
SbD7 Ensure software integrity ✓
SbD4 Securely store credentials and security-sensitive data ✓
SbD5 Communicate securely ✓

5

// During manufacture

Secure Key Generation

To be truly secure each device needs at least one (or more) unique keys securing different functions. These keys must never be available in the clear.

In this example, we supplied hardware to the factory in China to ensure chip-to-cloud security. This approach can be adopted for manufacturing sites anywhere in the world and seamlessly scales from PoC to millions of devices.

Three unique keys are written to a one-time programmable secure area on the BLE chip on each board.
This burn process – one-time programming – means once the keys are written they can’t be overwritten. They are also forever hidden within the device itself.

6

// Operation & Updates

Consumer device in the field

Any unprotected device in the field will have its weaknesses – multiple potential attack points, such as interfaces and data exchanges. The ability to disable the device if tampering is detected adds further security in the field.

Keys are never sent in the clear but are asymmetrically encrypted for the target application.
Because of the unique keys per device generated during manufacture, communication between the consumer device and the server are all encrypted.

SbD3 Keep software updated ✓

7

// Operation & Updates

OTA Updates and Data Communication

OTA updates originate from the developer / consumer device manufacturer but are delivered to the consumer device itself via the secure key server, providing secure remote software upgrade to device, with ability to roll back on failure of security.

Data communication between the smart device and any other systems are separately encrypted.

Permissions and role-based access can be implemented for each application.

Software signing service within the cloud which securely generates encryption keys for new images and securely wraps them for individual devices.

SbD7 Ensure software integrity ✓

Each smart device has its own unique keys which means there are no default passwords.

SbD1 No default passwords ✓
SbD5 Communicate securely ✓

Logging: there is an upload logging, decipher and audit function that is used to detect tampering and disable the device which supports the disclosure process.

SbD2 Implement a vulnerability disclosure policy ✓

//Total life cycle

Maintaining trust

Threats emerge over time. Secure by Design requires a vulnerability disclosure policy for your product and you will need to monitor vulnerability disclosures and security updates of any third-party components you have used. This requires ongoing vigilance, monitoring of breach detection, looking for unusual behaviour and active follow up. Maintaining trust requires product life cycle management.

SbD2 Implement a vulnerability disclosure policy ✓
SbD10 Monitor system telemetry data ✓

// Securing your IoT Device

Secure by Design - Is it secure?

If you’re looking to design, develop or deploy a trustworthy, futureproof, secure IoT product, then why not download our Secure by Design product development checklist?

Download your IoT product development checklist
Share with your network
Share with your colleagues

*Source: F-Secure Attack Landscape report H1 2019, as reported in Forbes Sept 2019, for latest report: https://blog.assets.f-secure.com/wp-content/uploads/2020/03/04101313/attack-landscape-h22019-final.pdf