A Handbook for Approaching IoT Security and Why it is Important

“Without trusted and secured endpoints, reliability and sustainability in IoT services and infrastructures are merely a dream”
Ben Cade, Trustonic CEO

Florent Joubert
Sr. Manager, Secure Services & Business Development
florent.joubert@trustonic.com
# Contents

Target Audience & Scope of this Whitepaper ........................................... 2

Introduction – Beliefs and Why the Industry Should Care ......................... 3

Overview of your IoT System ................................................................... 4
  What is a Connected Device? ................................................................. 4
  Why Security within Devices Matters ................................................. 5

Trustonic Security and Positioning in IoT ............................................... 7
  Trustonic Secured Platforms - How Devices Become Trusted ............... 7
  Hardware-backed Security Embedded at the Heart of Devices ............. 7
  Trusted Manufacture ............................................................................. 8
  Application Security with Trustonic Application Protection ................. 10
  Who Can Use Trustonic Security and for What Type of Solutions? ....... 11
  Markets Addressed and Use Case Examples ....................................... 11
  Trustonic Positioning within the IoT Ecosystem ................................... 13
  Proactivity – Design Defensively ......................................................... 13
  Establish Trust ..................................................................................... 13
  Differentiation ..................................................................................... 13
  Scalability & Flexibility ...................................................................... 13
  Cost-Effectiveness .............................................................................. 13

Conclusion: There is Light at the End of the Tunnel ............................... 14

Resources .............................................................................................. 15
  Examples of IoT Initiatives and Opportunities .................................... 15
  Examples of Breaches and Hacks ......................................................... 15
  Examples of Thought Leadership and Market Initiatives for Security in IoT: 16
  About Trustonic and Technical Documentation .................................. 16
Target Audience & Scope of this Whitepaper

This positioning whitepaper is targeted at the key stakeholders of the IoT ecosystem, including:

1. Decision makers and buyers of IoT devices/infrastructures and services
2. System integrators
3. IoT solution/service providers
4. Hardware manufacturers

The purpose is not to provide a deep dive into IoT and endpoint security, but rather to educate and to create awareness around the need to bring security to the forefront of project definition and solution design when building an IoT environment. It is focused primarily on endpoint security, but it is clear that IoT security includes additional multiple layers that need to be considered.

Resources and contact details are located at the end of the document.
Introduction –
Beliefs and Why the Industry Should Care

Operating in the cybersecurity space, Trustonic has deployed its secure platform into well over one billion connected devices to date and currently protects more than 500 million applications. This document is based on Trustonic’s market feedback from various sectors of the IoT industry, including government, financial, healthcare and automotive. This section provides a few facts that will set the basis for this paper.

TRUE – Internet of Things will keep growing

The Internet of Things value proposition is very desirable - cost savings, new/faster/better services, increased revenue, improved operational efficiency, enhanced users’ digital lives - and it’s possible that some of the best benefits haven’t even been imagined yet.

TRUE – There will be more large scale attacks

Large enterprises and consumers have already been targeted and hit by cyber attacks*. Each attack is potentially very damaging to an organization’s brand or reputation.

Massive scale attacks are also finding their way into the business and consumer markets. A popular example is ransomware that take a workstation or mobile device hostage and then demand money to unlock them.

TRUE – There is a lack of knowledge in the industry about the possible threats in the IoT space

Many businesses don’t know about the potential threats and how to mitigate them. There is a strong need for security experts to educate and guide businesses especially during project definition and design.

FALSE - It only happens to others

Those to whom it has happened probably thought the same thing and they are now making the news headlines. Complacency is not an option.

In a perfect world, everything would go smoothly, but the reality is that, if there are weaknesses, someone will try to exploit them. There have already been many security attacks, including data breaches, user impersonation, compromised devices, safety issues, data corruption and distributed denial of service attacks.

FALSE – Security is not yet part of some major IoT plans

Leaders in the IoT industry have already recognized the need to deliver security and, in particular, on endpoints.*

FALSE - Security is too complicated, too expensive and not scalable.

Whilst deploying secure solutions does indeed require expertise and investment, it does not have to be onerous. Security is not a one-size-fits-all approach, and trade-offs can be made, based upon the particular use case.

*See references in resources and contact details page
Overview of your IoT System

To state the obvious, there is, by definition, no Internet of Things without endpoint devices. But this means that all infrastructures and associated services will need to rely on endpoints to manage and deliver what are, in many cases, safety-critical or business-critical services.

Gartner predicts that there will be around 20 billion connected devices by 2020*. This represents 20 billion potential attack surfaces.

What is a Connected Device?

An endpoint, whether it is a small sensor or a large appliance, will consist of a combination of both hardware and software components. This endpoint will then potentially be able to host services and data and to communicate with other endpoints, a cloud environment or a user.

An endpoint device will be designed for a specific given purpose, with a combination of hardware, software, connectivity and application support capabilities.

A smart heart-rate monitor or a pacemaker will not have the same capabilities as a smart car. Nevertheless, they both embed critical software and handle highly sensitive data that it is crucial to protect at all times.

* [http://www.gartner.com/newsroom/id/3598917](http://www.gartner.com/newsroom/id/3598917)
Why Security within Devices Matters

It should be obvious that a connected device is at the heart of an IoT system. Below are some examples of potential risks:

**Scenario 1:** A sensor tells a driver-less car that it is slowing down, when, in reality, it is not.

**Scenario 2:** A hacker remotely alters a pacemaker’s settings

**Scenario 3:** A hacker sends false alert signals to public safety authorities or takes control of CCTV cameras

These situations may sound extreme and may not have happened yet, but they are feasible, as all these IoT use cases either exist or are soon to be deployed.

From a more generic perspective, where could something go wrong with a device?

<table>
<thead>
<tr>
<th>During hardware and software design</th>
<th>During hardware and software integration</th>
<th>During manufacturing</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Introduction of hardware and software design weaknesses that could be exploited</td>
<td>• Improper integration of hardware and software components, thereby introducing exploitable bugs</td>
<td>• Counterfeit devices entering the supply chain</td>
</tr>
<tr>
<td>• Lack of security design review and validation</td>
<td>• Integration of uncertified software</td>
<td>• Lack of reliable device identity/root of trust</td>
</tr>
<tr>
<td>• Lack of security expertise</td>
<td>• Lack of secure app/data management</td>
<td>• Lack of manufacturing-stage tracking</td>
</tr>
<tr>
<td>• Absence of hardware-backed security</td>
<td>• Lack of integration validation</td>
<td></td>
</tr>
</tbody>
</table>
There is a need to be aware of both known and potential upcoming threats, as they will affect all the major IoT segments, such as smart cities, smart homes, industrial, automotive and healthcare. Too often, security in IoT is an afterthought or, even worse, perceived as being irrelevant or less important than the device’s primary function.

While you may not need strong security in your coffee machine, you probably want to have adequate security in your car, house or city. Even then, do you really want your coffee machine to become a weapon, helping to perform denial of service attacks? Some nascent markets can indeed function with limited security. However, the majority of solutions will require strong, adequate security built in from the ground up, i.e. security by design.

Mistakes are not acceptable when you build a smart car, a smart home, a smart warehouse or, on an even bigger scale, a smart city. This is simply because one failure to protect data, or to ensure that services have not been corrupted, can result in loss of life and/or failure of a business.
Trustonic Security and Positioning in IoT

Trustonic helps to deliver security at various stages in IoT ecosystems. Security needs to be applied at the system design stage of the endpoint devices, through the entire manufacturing chain and, finally, to the services that will be executed on and connected to these devices. Trustworthiness requires solutions to address two distinct parts of the value chain:

![Make a device trustworthy with Trustonic Secured Platforms](image)

Make a service trustworthy with Trustonic Application Protection

The reasons for this segregation and the resultant implications on IoT solution design and usage are expanded upon below.

**Trustonic Secured Platforms - How Devices Become Trusted**

**Hardware-backed Security Embedded at the Heart of Devices**

*Trustonic Secured Platforms* includes a range of products suitable for application processors (e.g. for processors integrated within high-resource, demanding devices requiring a lot of memory and computing power to run multiple services, such as in-car infotainment or telematics) to lower-end microcontrollers (typically embedded within small devices with a dedicated purpose or limited capabilities, such as a building temperature sensor).

In particular, it includes a security-certified operating system – Kinibi – that is integrated with chipset and device manufacturers to provide a hardware-based isolated operating environment in endpoint devices.

Kinibi relies on a secure hardware design, widely available in the market, to create a Trusted Execution Environment (TEE) whose integrity can be verified, that can host multiple applications,
that can perform secure data processing and storage and can also obtain privileged access to peripherals (such as a camera, a fingerprint sensor or a touchscreen).

This concept of hardware-based isolation of sensitive software and data applies to most IoT devices and does not require any additional hardware components, as it is part of the processor design.

Hardware isolation is becoming the industry-standard mechanism used to ensure real protection of assets on a device. Software protected by software quickly reaches its limits, as it is more easily broken, requires more frequent updates and maintenance and only mitigates a limited set of attacks.

**Trusted Manufacture**

A. **Device Identity and Root of Trust**

Device manufacture may outsource all or part of the manufacturing process to third parties, thereby breaking the traditional view of “trusted” manufacture where the complete process is managed by one company. How, therefore can a device manufacturer, or indeed a customer, know that only official hardware components, firmware and clean software images have been installed on a given device? Traditional approaches to secure device manufacture and procurement are both expensive
and unscalable. In addition, IoT devices may never be "touched" by their owner(s), so there is a need to attest the trustworthiness of the manufacturing chain when an endpoint becomes live and tries to enroll itself or needs to be enrolled. In addition, many services, especially in M2M, are based on the trustworthiness of data received from one or several endpoint(s) and it is essential to make sure that endpoints themselves are trustworthy, without the need for complex relationships with intermediaries.

Trustonic’s Key Provisioning Host is also part of the Trustonic Secured Platforms product suite. Easily integrated within manufacturing plants, it enables the creation of unique device identities by managing a Root of Trust at the various manufacturing stages, as required.

The Trustonic solution enables administrators of the IoT infrastructure to remotely attest the trustworthiness of devices that are being connected to their IoT infrastructure.

B. Trusted Device Attestation and Device Enrolment

Small or large, an IoT infrastructure will evolve with time, by either adding new devices or replacing old ones. There are different architectures possible for device discovery and enrolment, either managed via a central server, or distributed between the devices themselves. In all scenarios, it is essential to ensure and maintain trustworthiness of the new connected devices that are going to communicate and exchange data with the other endpoints and/or the cloud.

With its security products, Trustonic enables the remote validation of the authenticity of a device. Based on its internal policy, the cloud or other devices may decide to ignore an untrusted device (i.e. that cannot be clearly identified) and not accept any information coming from the device. It may also apply specific rules and countermeasures to make sure that this device is not going to tamper with the whole system. The performance, quality of services and reliability of the whole system will then depend on how much trust can be put into the infrastructure.
Application Security with Trustonic Application Protection

Once platforms and devices are equipped with Trustonic’s security, solution developers can leverage the Trustonic Application Protection software development kit to develop (Client SDK) and securely deploy (Server SDK) their secure services.

The development and deployment of services using Trustonic Application Protection relies on industry standards\(^1\), and enables solutions to scale across devices without having to redevelop for each hardware platform.

Security is a continuous process and business entities may already leverage devices that are not yet fully “hardware-enabled”. To that extent, Trustonic Application Protection also delivers security for solutions that are already designed and deployed on the field. This allows actors in the IoT value chain to enable what they already have and are selling today, while capitalizing on more robust and scalable solutions for the future.

Trustonic also provides resources to support device manufacturers and application providers during the development and deployment phases.

\(^1\) GlobalPlatform [https://www.globalplatform.org/](https://www.globalplatform.org/)
Who Can Use Trustonic Security and for What Type of Solutions?

Whether one builds a whole IoT infrastructure/system or a specific IoT component, there is considerable value to be derived from providing and leveraging the maximum level of security.

| Trustonic Secured Platforms | • Chipset / platforms manufacturers  
|                            | • IoT module manufacturers  
|                            | • Device manufacturers/OEMs  
|                            | • System integrators  

| Trustonic Application Protection | • Hardware manufacturers  
| (for application & service security) | • System integrators  
|                                      | • Application/solution developers  
|                                      | • Service providers  

Trustonic Application Protection offers a unique market capability to either pre-load secure services into a device, or to simply remotely authenticate the device and install secure services (that would include critical assets such as code and data) when the device is deployed in the field. This allows the ecosystem greater flexibility, enabling it to bring innovative services, in a secure manner, to devices that are already shipped and are in the hands of the consumers or businesses.

Markets Addressed and Use Case Examples

If we look at the major IoT verticals, we can see that device security applies to the vast majority of services. Here some examples:

Smart cities
• Public safety, energy, transport

Smart homes
• Surveillance, energy management, smart locks

Industrial
• Production streamlining, inventory management, robotics, building access

Automotive
• Driverless cars, telematics, infotainment, in-car payment

Healthcare
• Telehealth, remote drug prescription and administration
If we look at the solutions themselves that are used in these verticals, here are some key use cases:

- Secure software/firmware management
- User and device enrolment
- Data analytics
- Data transmission
- Device to device communication
- Device to cloud communication
- Device authentication
- Device counterfeit protection
- Device tracking
- Payment
- User authentication
Trustonic Positioning within the IoT Ecosystem

It would be foolish to think that merely securing the endpoint itself could solve every problem (just like only securing an IOT-centric cloud is not enough). This is, of course, not what Trustonic believes. Endpoint security is not the only element to take into consideration, but it is a great start. Security should be built into devices, not added after devices are deployed, as patching a device not designed with security in its foundations will usually an inferior security. With its services and partnerships, Trustonic’s foundations of security rely on the following principles:

**Proactivity – Design Defensively**

Security needs to be anchored and pre-embedded within devices in order to be effective. The larger the software, the more bugs it will have that could be exploited eventually by an attacker. It is essential to leverage environments that are designed for security and to minimize risks by isolating the most sensitive code/data and controlling how they are accessed.

**Establish Trust**

If you cannot ensure the origin of the information, then you should not trust it. If you do not trust it, then the whole system relying on this information becomes irrelevant. There is a need to strongly identify the appropriate devices and services and to validate that they are legitimate. Trust should apply across all IoT infrastructure layers, not only to the endpoints. Building a chain of trust goes beyond just providing some cryptographic routines.

**Differentiation**

Additional security is key to creating differentiation within the hardware, software/applications and services. It both allows safe innovation and prevents irreparable damage.

**Scalability & Flexibility**

In most cases, security should not be a closed environment, as different parties will be necessary to build an end-to-end IOT infrastructure. It is important to have a comprehensive ecosystem of service providers that can access it, so the whole market can benefit. It is also essential for a service provider to have as much control as possible over its own services. This will enable not only faster response-time to incidents, but also a better service to their customers.

**Cost-Effectiveness**

If a security system is well designed at the platform level, the associated costs can be reduced and optimized. Scalability is also a factor that will minimize the effort involved in bringing solutions in the market and then managing them.
Conclusion: There is Light at the End of the Tunnel

Many businesses believe that security hampers a fast go-to-market model and a positive ROI, as it is often perceived as too complicated or expensive.

Security itself is not a simple task.
- However, the IoT industry is full of security experts that can provide advice, assist during projects and provide the necessary proven building blocks for a sustainable IoT environment.

Security has a cost, but it does not have to be prohibitive.
- It is essential for industries to understand that the potential incremental costs involved in bringing security to the appropriate level for their needs will deliver value within the overall ROI.
- Trade-offs can be made deliberately and thoughtfully, based on risk exposure

Security in IoT is a multi-layered approach where endpoint security is critical.
- IoT devices are the link between services and users. Therefore, protecting such devices cannot be an afterthought

Security must be seen as adding essential value and not as detrimental.
Industries are now catching up and increasing numbers of initiatives around security in IoT are being initiated. Trustonic’s recommendation is for businesses to be more proactive in assessing their risks and properly protecting their IoT systems, rather than waiting to react and suffering irreparable damage.

Trustonic’s mission has not changed since its inception. This is to provide hardware-based security in devices and to enable users of these devices to easily develop innovative services while protecting their assets. Being part of the AT&T Cybersecurity Alliance, alongside key security providers IBM, Nokia, Palo Alto Networks, Qualcomm and Symantec opens up exciting and fresh opportunities for the IoT ecosystem.
Resources

Examples of IoT Initiatives and Opportunities

Smart cities

Connected cars

Healthcare and IoT

Smart agriculture

Examples of Breaches and Hacks

Target data breach – Profit Falls 46% On Breach

DDOS Attack – Mirai botnet

Baby monitor hack

Network router backdoors

Network transport vulnerability - Heartbleed bug
- http://heartbleed.com/

Remote device access control
Examples of Thought Leadership and Market Initiatives for Security in IoT:

US Government - Senators Introduce Bipartisan Legislation to Improve Cybersecurity of IoT Devices

AT&T – The CEO’s guide to securing the Internet of Things

GSMA – IoT Security Guidelines for Endpoint Ecosystems

MediaTek and Trustonic – Trustonic, MediaTek Partner to Secure Smart Car Software

Samsung and Trustonic – Samsung Advances Open IoT Ecosystem

About Trustonic and Technical Documentation
- [https://www.trustonic.com/](https://www.trustonic.com/)

Trustonic

At Trustonic, we see both the exciting opportunities and inherent new challenges that come from having to protect and secure individual users and service providers in an increasingly connected world. Our proven foundation of hardware-backed security and Root of Trust forms the basis upon which a secure and trusted IoT infrastructure should be built and provides IoT devices with the robust protection that they will need, long into the future.

As a founding member of the IoT Cybersecurity Alliance, we bring industry-leading expertise in embedding security into the world’s smart devices, collaborating with customers and partners to protect critical IoT applications and assets. Ultimately, Trustonic empowers developers to deliver simpler, safer services that customers expect and demand.

Learn more at [https://www.trustonic.com/markets/iot/](https://www.trustonic.com/markets/iot/)

For more information, please email [enquiries@trustonic.com](mailto:enquiries@trustonic.com)