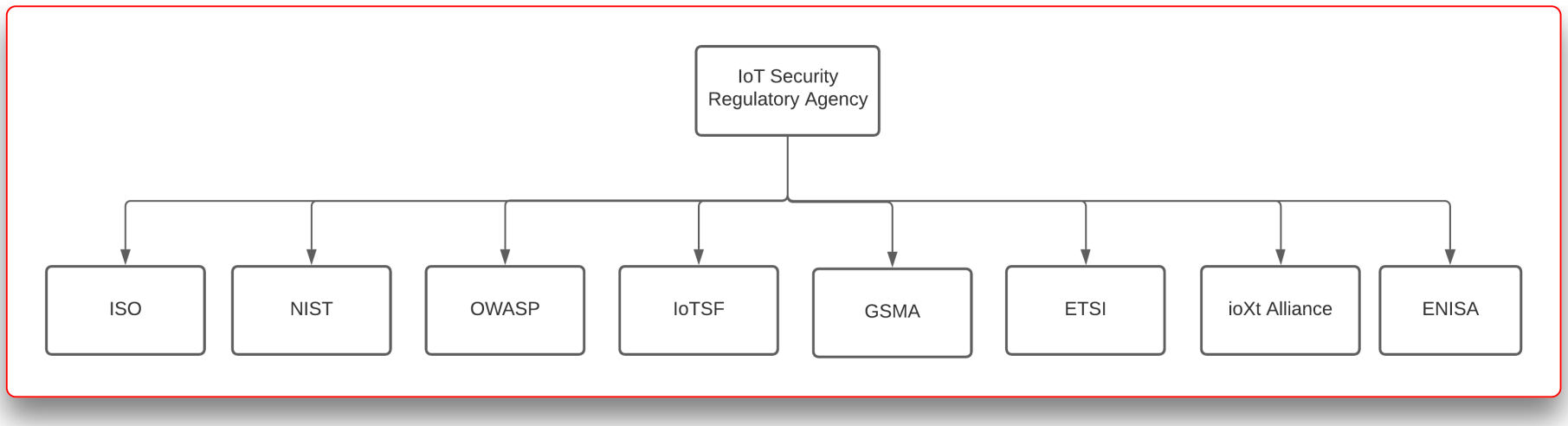
IoT Security- Part 23 (IoT Security Compliance, Guidelines And Recommendations By GSMA Part 1)

Yashodhan
21-February-2021

Introduction

To address the threat and vulnerability issues encountered by IoT devices for consumers,industry and critical infrastructure, a variety of IoT security standards have been developed and there are more standards under development.Globally there are compliances and guidelines for IoT security that helps IoT manufacturers to architect/design secure IoT systems.This gives confidence to the customer to identify secure products.

Following are some the regulatory agencies for globally accepted IoT security compliance and guidelines



ISO : International Organization for Standardization

NIST : National Institute of Standards and Technology

OWASP : Open Web Application Security Project

IoTSF : IoT Security Foundation

GSMA : Global System for Mobile communication Association

ETSI : European Telecommunication Standards Institute

ENISA : European Union Agency for Cybersecurity

ioXt Alliance : Internet of Service Things

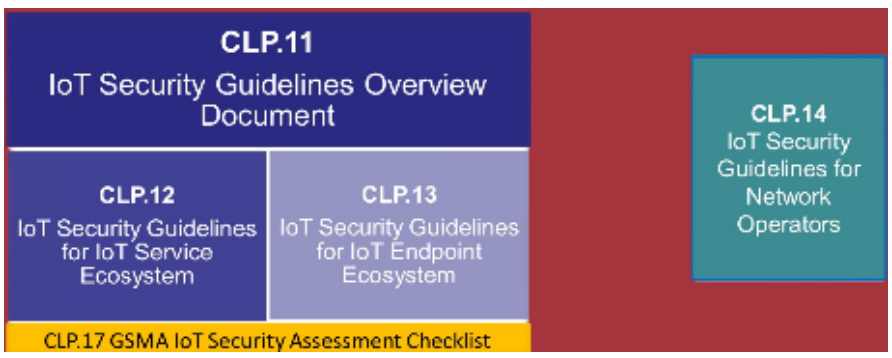
These agencies provide the guidelines regarding secure by design, vulnerability assessment and security testing checklist for IoT systems. Each of these compliance have different viewpoints and methodology addressing the product security.

With this blog we will start exploring these globally accepted IoT compliances. We will begin with GSMA IoT security guidelines overview for IoT ecosystem and in subsequent blogs we will look into specific guidelines by GSMA for IoT security in endpoint devices and IoT services.

GSMA IoT Security Guidelines Overview

The GSMA has created the set of security guidelines for the benefit of service providers who are looking to develop new IoT services and IoT endpoint devices in an entire IoT ecosystem.

As shown in figure 2,the GSMA provides 4 different sets of guidelines specific to IoT architecture viz. IoT ecosystem in general, IoT service ecosystem and IoT endpoint ecosystem alongwith their security assessment checklist. In addition to that it also provides guidelines for network operators. The guideline documents are numbered as CLP.1x where CLP stands for Connected Living Programme.

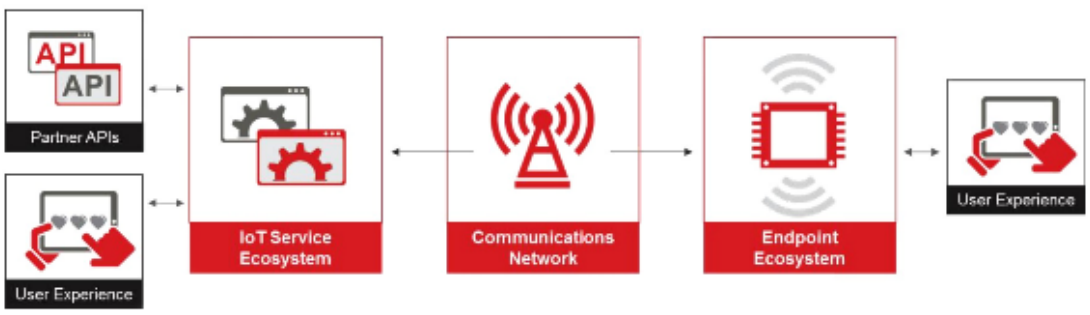


Source :*https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.11-v2.2-GSMA-IoT-Security-Guidelines-Overview-Document.pdf*

For the Internet of Things to evolve effectively, IoT manufacturers must resolve the security challenges nherent to its growth. These challenges are:

1. Availability: Ensuring uninterruptible connectivity between Endpoints and their respective services
2. Identity: Authenticating Endpoint devices and services
3. Privacy: Reducing the risk to individual end-users
4. Security: Ensuring that system integrity can be verified, tracked, and monitored

The GSMA IoT guidelines addresses all of the above challenges for the entire IoT ecosystem. The figure below shows the standard IoT model used throughout the guideline documents by GSMA.It is portrayed as components of the service and endpoint ecosystems. Each component is composed of subcomponents, which are detailed in a document that focuses solely on the primary component.



Source :*https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.11-v2.2-GSMA-IoT-Security-Guidelines-Overview-Document.pdf*

In most of the IoT services and products figure 3 is considered to be primary components deployed in a production environment.

The IoT Service Ecosystem represents the set of services, platforms, protocols, and other technologies required to provide capabilities and collect data from endpoints deployed in the field. This ecosystem typically gathers data from endpoints and stores them within its server environment. This data is available to users either through user interfaces providing visual presentation or accessible as third party API emerging at the service framework.

The IoT Endpoint Ecosystem consists of low complexity devices, high performance devices and gateways that connect the physical world to the digital world via several types of wired and wireless networks. Typical endpoint devices are motion sensors,atmospheric sensors,automotive telematics systems, sensor driven industrial control systems etc. Endpoint devices gather data from sensors or any other physical environment and push that in different formats via a network interface such as local network,short range radio access or cellular network to the IoT service ecosystem, often receiving instructions or actions in response.

The security guidelines for IoT Service ecosystem and IoT Endpoint Ecosystem are described in depth in GSMA IoT security guideline document viz. CLP.12 and CLP.13 respectively. These guidelines will be discussed in our subsequent blogs of the series.

Based on a set of policies,procedures, methodology, mitigation and response to gaps in security in technical contexts the organization evaluates risk assessment to secure overall business. Thus risk assessment becomes a critical part for any organization opting for security.

Considering different stages in IoT ecosystems the IoT services and endpoint devices create,receive and share data at each stage. A key challenge the IoT makers face that there are multiple laws dealing with privacy and data protection. The data privacy regulations vary from different industry sectors to different countries. The GSMA guidelines for both IoT service and endpoint devices addresses risk assessment and privacy consideration at each stage.

GSMA IoT Security Guidelines Effectiveness

The beauty of GSMA IoT security guidelines is that it can help the organization to implement security at any stage i.e whether IoT makers who are in the initial phase of a project or whether the product has already been deployed in the industrial environment. Also while assessing the security measures GSMA has taken a reference of CERT OCTAVE model and NIST Risk Management Framework.

To get most out of these documents there are certain steps GSMA suggests that the organization needs to follow . Those are mentioned below

1. Evaluate the technical model
2. Review the current product or service's Security Model
3. Review and evaluate Recommendations
4. Implementation and Review
5. Ongoing Lifecycle

Let us try to understand each of these steps in brief.

Evaluate the technical model :

It is one of the fundamental steps in understanding the IoT model of service or product. The component of IoT systems can be mapped to model selection guidelines for IoT service and endpoint ecosystem. It simply uses the class of components such as a microcontroller, communication module, or trust anchor, as the context.This process corresponds with the first and second phases of the CERT OCTAVE risk assessment model or the Frame stage of the NIST Risk Management Framework.

Review the current security model :

Second step as per guidelines is review of the security model for endpoint or service being assessed. This section assists an IoT team from the viewpoint of an attacker so as to find out the vulnerabilities.This will help organization to gain understanding of risk and threats to security model. Similar to stage one this process also corresponds with the first and second phase of the CERT OCTAVE risk assessment model or the Frame stage of the NIST Risk Management Framework.

Review and Evaluate Recommendations :

The next stage is to review and evaluate how security tasks can be resolved. For this GSMA has sections viz. Method,Expense and Risk section.

The Method section provide methodologies that assist in the mitigation of the corresponding security risk.An Expense section is provided to discuss, where applicable, extra financial expenses that the organization should prepare for when implementing a particular recommendation.A Risk section is also provided so the reader understands the gaps in security that are likely to result from not implementing a particular recommendation.

This process corresponds to the steps six, seven, and eight of CERT OCTAVE risk assessment model and the Assess step of the NIST Risk Management Framework.

Implementation and Review :

The business shall now create a clear architectural model for each Component being adjusted, and use the Risk Assessment process chosen by the organization to develop a threat model of each Component, incorporating the Recommendations and Risks that are appropriate for each Component and Security Task. When the architectural model is completed, the organization can begin implementing each Recommendation in order to fulfill the Security Tasks.

This process corresponds with the step eight of CERT OCTAVE risk assessment model and the Respond component of the NIST Risk Management Framework.

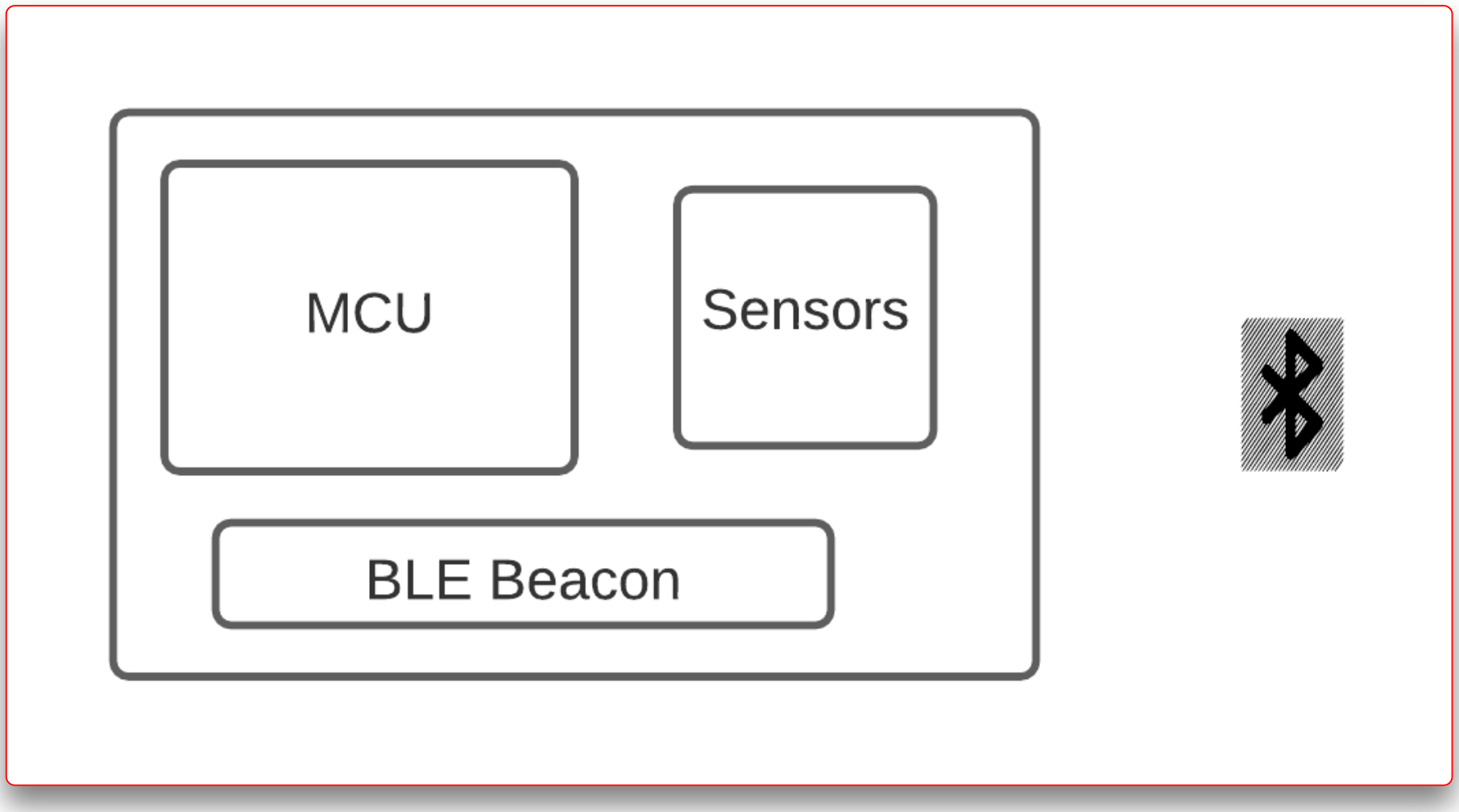
Ongoing Lifecycle :

Both endpoint devices and IoT services have a lifetime and they need to be upgraded over a period of time.Also cryptographic algorithms become out-dated or deprecated.The new protocols and radio technologies must be integrated with the product or service. This ever changing ecosystem when deployed, must be constantly reviewed to ensure that confidentiality, integrity, availability, and authenticity are maintained.This process corresponds with the step one, four, and five of CERT OCTAVE risk assessment model and Monitor and Frame components of the NIST Risk Management Framework.

Use case for IoT Endpoint Device as per GSMA Guidelines

Let’s explore the industrial use case of assets tracking Bluetooth Low Energy (BLE) beacon to evaluate it from the guidelines mentioned by GSMA. Here we have endpoint and service ecosystems both.

The endpoint overview :



First, let’s start by evaluating the hardware design of the endpoint.

The BLE beacon is composed of standard components i.e BLE enabled microcontroller unit (MCU) and sensors such as triaxial accelerometer, temperature and humidity for tracking and monitoring condition of asset.The sensor data is transmitted by built-in BLE . Here BLE stack is considered as version 5.0. The complete hardware is a coin cell battery powered.According to the Endpoint Ecosystem document, this device would fit into the Lightweight Endpoint class of devices.

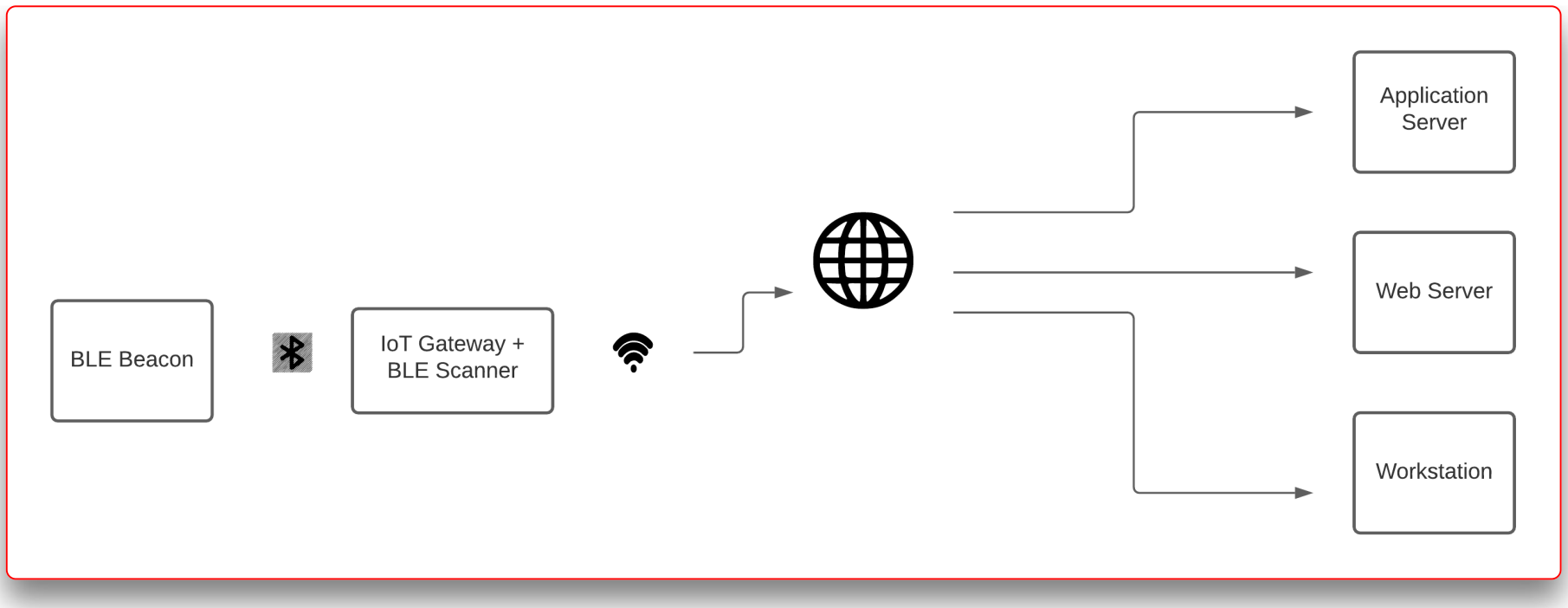
The service overview :

In the context of service ecosystem, the endpoint device gets scanned by IoT gateway and data is pushed to back end service over WiFi. The back end service for the application simply associates the device owner with the data features being captured and stores them in a local database of the application server.

Data visualization can be achieved using either the mobile application or via the service’s

web application. Device users can log into the service provider’s web application to perform more actions with the metrics captured by the endpoint.

According to the Service Ecosystem document of GSMA,this device would fit into the service class of devices.



The security model:

Following the GSMA IoT security guidelines the design team at endpoint and service may come up with following questions in order to secure the product and services.

From an endpoint perspective:

1. Cloning
2. Endpoint impersonation
3. Service impersonation
4. Ensuring privacy

From a service perspective: 1. Cloning 2. Hacked services 3. Identifying anomalous endpoint behavior 4. Reduction in data loss and exploitation 5. Managing user privacy 6. Improving availability

Now after studying the above mentioned issues it may be followed that the endpoint device i.e BLE beacon needs minimal security as it has limited functionality. Unless the firmware of the endpoint is encrypted,there is no real threat of attack against the endpoint within the given use case. To handle privacy issue the organization should ensure that each endpoint device should have unique personalized encryption token so that compromising on a single endpoint will not affect the privacy of other devices. If the unique encryption keys were encoded into the firmware locked microcontroller, it would be feasible to accept that this use case was sufficiently secured from the threat of cloning, impersonation, and privacy issues. The future blogs will address in depth security assessment of such models from a view point of GSMA.

Summary

The IoT standards and guidelines if used effectively make substantial impact on performance of the IoT ecosystem. These compliances provide profound directives for designing and assessing security aspects of IoT products and effectively address the threat.

GSMA has a unique way of evaluating risk assessment by assigning priorities to security recommendations and validating corresponding responses by IoT makers. This helps an organization to implement the security at any stage and ensure end product security.

References

1. CLP.11-v2.2-GSMA-IoT-Security-Guidelines-Overview-Document,
   https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.11-v2.2-GSMA-IoT-Security-Guidelines-Overview-Document.pdf
2. CLP.12-v2.2-GSMA-IoT-Security-Guidelines-for-Service-Ecosystems
   https://www.gsma.com/iot/wp-content/uploads/2020/03/CLP.13-v2.2-GSMA-IoT-Security-Guidelines-for-Endpoint-Ecosystems.pdf
3. CLP.13-v2.2-GSMA-IoT-Security-Guidelines-for-Endpoint-Ecosystems
   https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.13-v2.2-GSMA-IoT-Security-Guidelines-for-Endpoint-Ecosystems.pdf
4. National Institute of Standards and Technology (NIST)'s Risk Management Framework
5. Computer Emergency Response Team (CERT)'s OCTAVE model

About Payatu

Payatu is a research-powered cybersecurity service and training organization specialized in IoT, embedded, mobile, cloud, infrastructure security, and advanced security training. We offer a full IoT/IIoTT ecosystem security assessment, including hardware, firmware, middleware, and application interfaces. If you are looking for security testing services then let's talk, share your requirements: https://payatu.com/#getstarted Payatu is at the front line of IoT security research, with a great team, and in house tools like expliot.io. In the last 8+ years, Payatu has performed, security assessment of 100+ IoT/IIoT product ecosystems and we understand the IoT ecosystem inside out. Get in touch with us. Click on the get started button below.