The GSMA IoT Security Guidelines

Introduction and Purpose

Shashank Murali
PALINDROME TECHNOLGIES
www.palindrometech.com

Introduction

The Internet of Things (IoT) ecosystem is experiencing significant growth, driven by technological advancements, increased connectivity, and an expanding range of applications. IoT application expansion across sectors ranging from healthcare to industrial automation to smart homes/cities has led service providers to innovate and develop a myriad of connected products and services. In addition, 5G wireless deployment is enabling high-speed, low latency, energy-efficient connectivity for an ever-increasing number of IoT devices. 5G networks also offer advanced network management capabilities, supporting the efficient orchestration of resources to meet the specific requirements of each unique IoT use case.

This increase in the deployed base of IoT devices, along with the growing complexity of services offered, has expanded the IoT ecosystem's scope. At this scale, security issues can have broad implications and pose challenges for many IoT service deployments.

While service providers across various sectors, including automotive, healthcare, consumer electronics, and municipal services may perceive their security needs as unique and isolated, the reality is that most IoT services comprise endpoint devices and remote service platforms that often share common components with other communication, computing, and IT solutions. The security threats and potential solutions are often similar, despite the differences in attacker motivations and the impact of security breaches.

To help ensure the security of emerging IoT services, network operators and their service and equipment provider partners are keen to share their security expertise with IoT service and product developers. In support of this industry need, the GSMA has created a set of security

guideline documents that provide a reference for security design principles and considerations for building secure IoT products and services.

The Security Challenges Created by IoT

The IoT ecosystem has expanded into an extensive collection of devices, products, and services that have become ubiquitous. Many of these devices have become elements of mission-critical infrastructure services or services used to collect and process vast amounts personal or sensitive health data. These devices are often operated in constrained environments (power, bandwidth, coverage, data speeds, human management interfaces, etc.) and may not have the best-in-class security features and protection mechanisms found in other traditional networked devices due to scale and cost constraints. IoT endpoints may not offer a straightforward or substantial set of features for user interactivity, control, and secure management. This poses a security challenge for IoT services and customers, especially when considering the large deployment numbers. The GSMA aims to provide a baseline of required security features and mechanisms for all IoT products and services.

To secure IoT solutions effectively, the following challenges must be addressed:

- **Availability**: Networks must be reliable, with minimal downtime to ensure uninterrupted secure connectivity between IoT devices and their respective services.
- **Identity**: Secure and reliable authentication between endpoints and services in an interconnected ecosystem must be assured.
- **Privacy**: Due to the vast amount of personal and/or sensitive data generated by connected devices, protection must be held paramount. Privacy-sensitive information or security-sensitive data (in the case of industrial systems) must be protected both at the endpoint devices and in transit.
- **Security**: Due to the interconnected nature of devices, the massive volumes of data generated, and the diverse range of applications, system security is crucial. Device security features, managed updates and patching mechanisms, and network and data protection mechanisms all play an important role in securing the IoT-based solutions.

The GSMA IoT Security Guideline Document Set

The GSMA IoT security guidelines are designed to:

- Establish a common understanding of IoT security issues.
- Promote a methodology for developing secure IoT services to guide the implementation of security best practices throughout the product lifecycle.

In scope, these documents provide recommendations pertaining to the design and implementation of IoT endpoint devices, products, and services. The structure of the document set is shown in Figure 1 below.

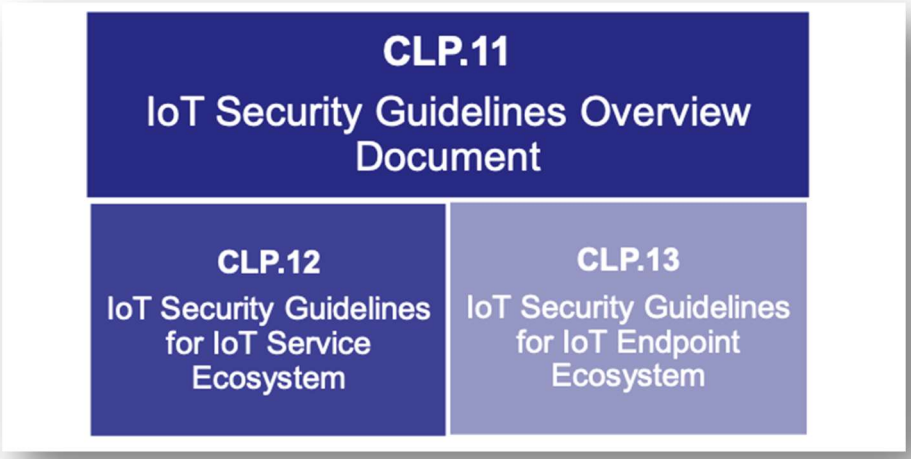

Figure 1 GSMA IoT Security Guidelines Document Structure

"**CLP.11 IoT Security Guidelines Overview**" provides the implementer of an IoT technology or service with a set of design guidelines for building a secure product and serves as an overarching model for interpreting and identifying the relevant aspects of a technology or a service. In addition, it provides guidance on evaluating the risks associated with each aspect / component and creating a remediation plan for these risks. Each risk is to be assigned a priority to help determine the cost of an attack, remediation cost, and the potential costs of not addressing the risk.

"CLP.12 IoT Security Guidelines for IoT Service Ecosystem" is used to evaluate all components in an IoT product or service from a Service Ecosystem perspective. The Service Ecosystem includes all components that make up the core of the IoT infrastructure. Some of the possible components in this ecosystem are services, servers, database clusters, network elements, and other technologies used to drive the internal components of any product or service.

"CLP.13 IoT Security Guidelines for IoT Endpoint Ecosystem" is used to evaluate the components of an IoT Service from the IoT Endpoint Device perspective. An Endpoint, from an IoT perspective, is a physical computing device that performs a function or task as a part of an Internet-connected product or service. An Endpoint, for example, could be a wearable fitness device, an industrial control system, an automotive telematics unit or a personal drone device. All technologies used to drive the physical device are to be evaluated for security risks.

The GSMA IoT Model

The GSMA IoT Model depicted in Figure 2 identifies the standard components of the IoT service and endpoint ecosystems. Each component is further comprised of sub-components with their own security challenges and requirements. The CLP.12 and CLP.13 documents delve

into these specific requirements for the IoT Service Ecosystem and the IoT Endpoint Ecosystem respectively.

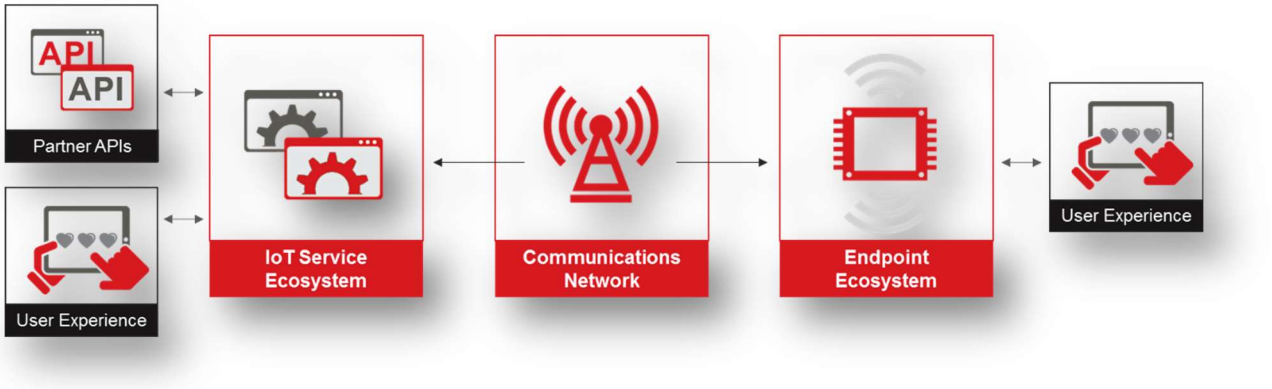

Figure 2: GSMA Standard IoT Model

Communications network components are the primary building blocks of any IoT ecosystem and are inherent to the concept of the Internet of Things. Effective and secure communication is essential for IoT services, and the choice of communication protocols and technologies depends on factors such as the nature of the devices, the range of communication, deployment environment and specific application requirements.

The simplified lifecycle of a typical IoT product or service is shown in Figure 3 below. Ensuring security is an ongoing process, requiring vigilance, innovation, responsiveness, and continuous improvement throughout the IoT product lifecycle. The overall security and risk management process is enhanced by including security baseline requirements and principles from the start, in the design and conceptualization phase. In order to safely retire the devices after their service life, an "End of Life" plan is needed to avoid any sensitive data leakage during the device recycling process.

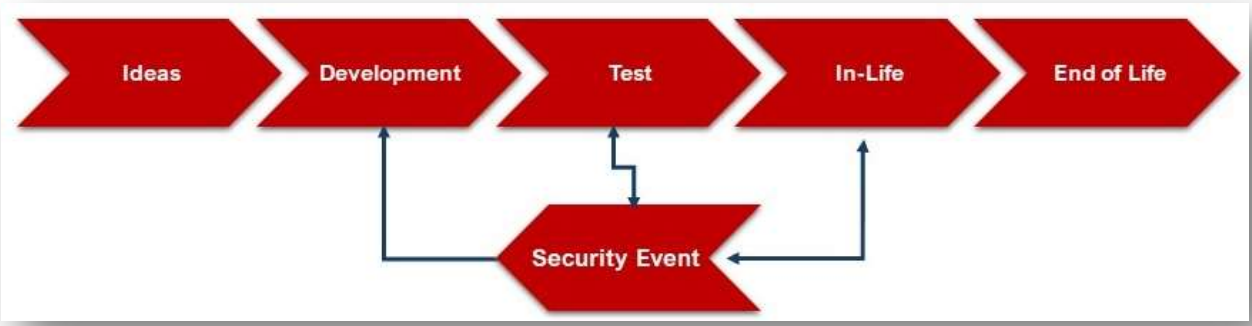

Figure 3 IoT Life Cycle Model - GSMA

Service providers and vendors need to have a vulnerability management and robust security remediation plan in place to address any security vulnerabilities and weaknesses reported throughout the product lifecycle. Furthermore, security evaluation by a qualified independent testing facility provides 3rd party attestation to ensure proper alignment with GSMA security requirements and demonstrate commitment to industry best practices and provide assurance and confidence to stake holders, partners and users.

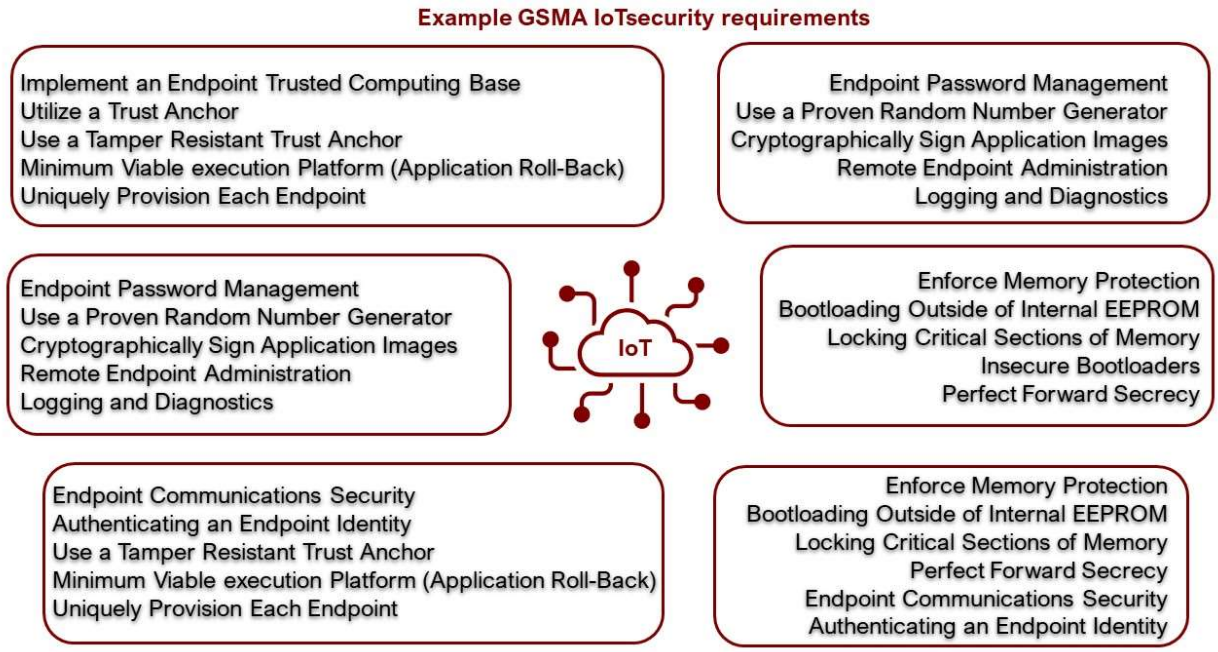

Figure 4 GSMA IoT Security Requirements Examples

The GSMA IoT Security Assessment Checklist

The GSMA IoT security baseline documents, namely CLP.12 and CLP.13 address the security models of the IoT services and endpoints. They focus on security design considerations, challenges, potential attack vectors, threats, and associated risks.

In prior versions of the GSMA IoT Security Guidelines, a self-assessment checklist for the products and services against the baseline GSMA security framework was provided in the form of document CLP.17. However, since 2016, several widely adopted industry baseline security specifications (e.g. ETSI EN 303 645) and associated assurance specifications (e.g. ETSI TS 103 701) have been produced. Hence, while GSMA encourages manufacturers or service providers to use CLP.17 as a means of initial security baselining, the actual industry standard security specifications are recommended for internationally recognized product security conformity assessments.

Summary: The GSMA IoT Security Assessment and Palindrome Technologies

The GSMA IoT Security Assessment provides a flexible security framework that addresses the unique challenges of the rapidly expanding, diverse IoT market.

Palindrome Technologies, a leading Cybersecurity Research firm with years of industry experience in securing IoT platforms, ecosystems and carrier-grade infrastructures, is an active member of the GSMA-IoT Security Working Group and an approved testing facility for GSMA IoT Security Assessments. Palindrome operates an accredited **ISO 17025 Testing Laboratory,** and leverages industry security standards and recommendations, such as the GSMA IoT Security Guidelines, to provide technical expertise in security assurance testing and certification services.

Contact Information

shashank.murali@palindrometech.com

services@palindrometech.com

www.palindrometech.com

GSMA

Network Equipment Security Assurance Scheme

Authorised Test Laboratory