CMSGu2016-02

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Internet of Things (IoT) Security

CERT-MU

National Computer Board
Mauritius

Version 1.0

May 2016

Issue No. 2

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

This document provides a generic set of security controls for security and privacy in the IoT.

1.2 Audience

The target audience for this guideline include early adopters of the IoT and smart devices.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 gives a background on the IoT.

Section 3 presents the risks of IoT to individuals and organisations.

Section 4 gives some rcommendations for security and privacy in the IoT.

Section 5 concludes the document.

Section 6 contains a list of references that have been used in this document.

Appendix A provides a list of acronyms that have been used in the document.

2.0 Background

The Internet of Things ("IoT") refers to the ability of everyday objects to connect to the Internet and to send and receive data.

The marketplace is seeing the beginning of widespread adoption of IoT within the consumer sector. Wearables, smart home appliances, lighting and other smart devices are becoming the typical norm. The popularity of smart consumer devices is anticipated to continue to grow at a frantic pace well into the future.

The IoT introduces large quantities of new devices that will be deployed or embedded throughout an organization or even within a system. Data captured from these devices can then be analyzed and acted upon. In some cases, the deployed devices are capable of performing some tasks. These described edge devices will become ubiquitous and allow for massive data collection activities. The analysis of this data will allow previously unseen linkages to be made which may cause concern for the privacy of individuals or groups of people.

In some cases, individuals may not even be aware that they are being tracked or recorded given the ability for next generation microchips to be embedded in virtually any platform. In all cases, assuring the security of each component within an IoT system is important to keep malicious actors from taking advantage of the power of the IoT in an unauthorized manner.

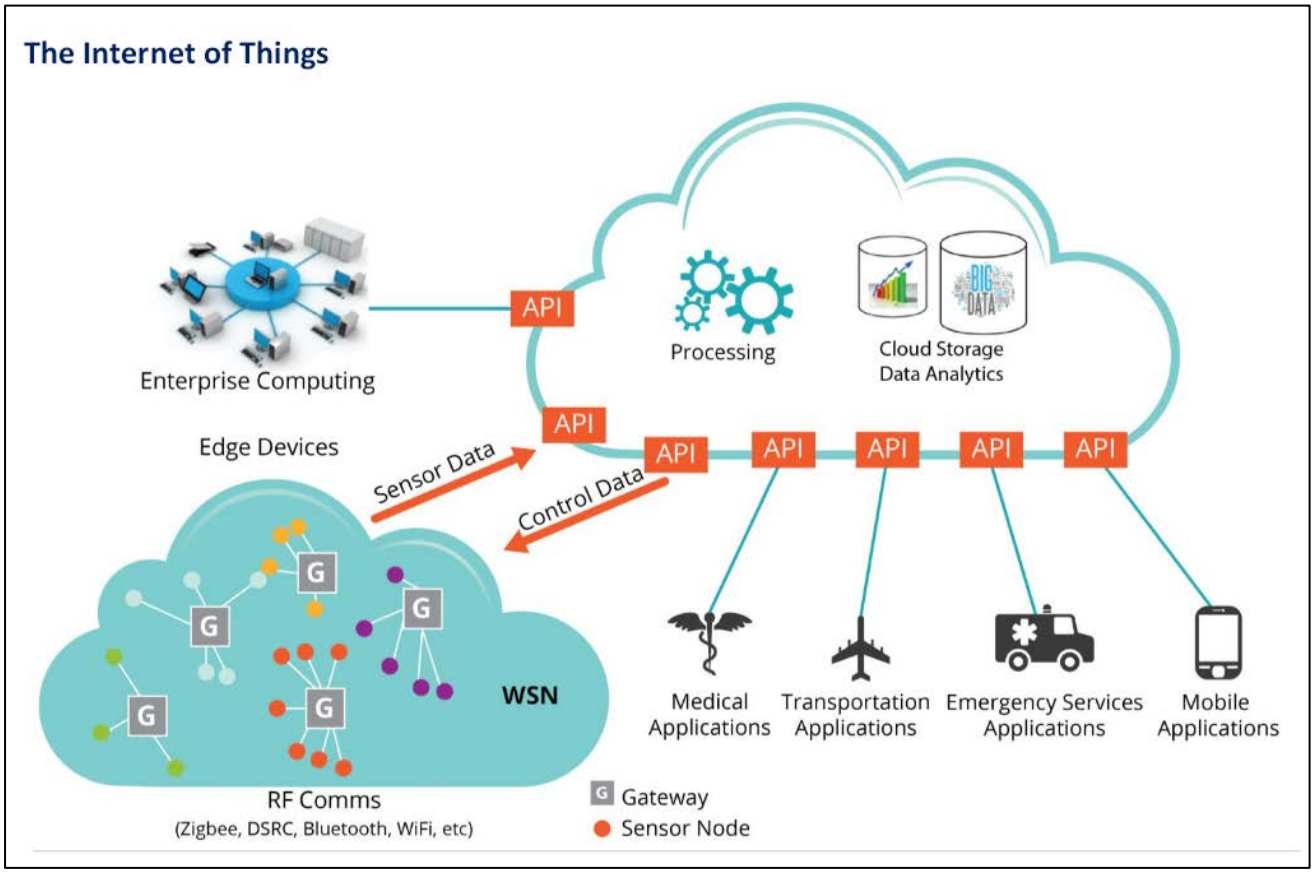
3.0 Risks of IoT To Individuals and Organisations

Some examples of new threats and attack vectors that malicious actors could take advantage of are:

- Control systems, vehicles, and even the human body can be accessed and manipulated causing injury or worse through unauthorized access to physical sensing, actuation and control systems (including vehicle, SCADA, implantable and non-implanted medical devices, manufacturing plants and other cyber-physical implementations of the IoT)
- Health care providers can improperly diagnose and treat patients based on modified health information or manipulated sensor data
- Intruders can gain physical access to homes or commercial businesses through attacks against electronic, remote controlled door lock mechanisms.
- Loss of vehicle control can be caused by denial-of-service against internal bus communications
- Safety-critical information such as warnings of a broken gas line can go unnoticed through DDoS of IoT sensor information
- Critical infrastructure damage can occur through override of safety critical features or power supply /temperature regulation
- Malicious parties can steal identities and money based on leakage of sensitive information including Personal Health Information (PHI)
- Unanticipated leakage of personal or sensitive information can occur by aggregating data from many different systems and sensors, or the merging of personal data that has been collected under differing consumer privacy preferences and expectations
- Unauthorized tracking of people's locations can occur through usage pattern tracking based on asset usage time and duration
- Unauthorized tracking of people's behaviors and activities can occur through examination of location-based sensing data that exposes patterns and allows analysis of activities, often collected without explicit notice to the individual
- Unlawful surveillance through persistent remote monitoring capabilities offered by small-scale IoT devices
- Inappropriate profiles and categorizations of individuals can be created through examination of network and geographic tracking and IoT metadata
- Manipulation of financial transactions through unauthorized POS and mPOS access

- Monetary loss arising from the inability to provide service
- Vandalism, theft or destruction of IoT assets that are deployed in remote locations and lack physical security controls
- Ability to gain unauthorized access to IoT edge devices to manipulate data by taking advantage of the challenges related to updating software and firmware of embedded devices (e.g., embedded in cars, houses, medical devices)
- Ability to gain unauthorized access to the Enterprise network by compromising IoT edge devices and taking advantage of trust relationships
- Ability to create botnets by compromising large quantities of IoT edge devices
- Ability to impersonate IoT devices by gaining access to keying material held in devices that rely up on software-based trust stores
- Unknown fielding of compromised devices based on security issues within the IoT supply chain

The IoT relies upon edge components that collect data or perform some action. These components may take the form of standalone devices, for example smart sensors or smart meters, or be embedded in larger systems, such electronic control units (ECUs) of connected vehicles. These edge components collect, store or process data. They are networked, either together or through some gateway typically using Radio Frequency (RF) communications. This allows for communication with a backend service, oftentimes, hosted within the cloud. Data analytics systems can make sense of data and in some cases instruct the components to perform some action. There will be a number of applications that make use of data collected from IoT edge components, or the resultant analysis derived from edge components.



3.1 Challenges associated with the adoption of the IoT

As the generation and analysis of data is so essential to the IoT, consideration must be given to protecting data throughout its lifecycle. Managing information at this level is complex because data will flow across many administrative boundaries with different policies and intents. Individuals will surely have different privacy goals than corporate entities, which in turn will have different goals than government or other organizations.

Oftentimes, data is processed or stored on edge devices that have highly limited capabilities and are vulnerable to sophisticated attacks. Privacy implications must also be considered to include developing an understanding of potential privacy issues when many different sources aggregate to a single point. Privacy controls are required at various points across the IoT ecosystem, particularly at point of user consent to data capture, transfer of data between IoT partners and at the points within the system that the data is stored and used. Given the various technological and physical components that truly make up an IoT ecosystem, it is good to consider the IoT as a system-of-systems.

The architecting of these systems that provide business value to organizations will often be a complex undertaking, as enterprise architects work to design integrated solutions that include edge devices, applications, transports, protocols, and analytics capabilities that make up a fully functioning IoT system.

This complexity introduces challenges to keeping the IoT secure, and ensuring that a particular instance of the IoT cannot be used as a jumping off point to attack other enterprise information technology (IT) systems.

4.0 Recommendations for Security and Privacy in the IoT

Cloud Security Alliance Recommendations for early business adopters of the IoT:

- Maintain the confidentiality and integrity of both business and personal data collected within the IoT through the provisioning of encryption, authentication and integrity protections throughout the IoT infrastructure

- Understand and address stakeholder privacy concerns prior to the implementation of the IoT capabilities by performing a privacy impact assessment

- Safeguard the infrastructure from attacks that target the IoT as a vector into an organization's assets, through the use of IoT device life cycle controls and a layered security approach

- Initiate a global approach to combat security threats by sharing threat information with security vendors, industry peers and Cloud Security Alliance

5.0 Conclusion

The IoT can potentially change the ways that consumers interact with technology. In the future, the Internet of Things is likely to combine the virtual and physical worlds together in ways that are currently difficult to understand. From a security and privacy perspective, the predicted pervasive introduction of sensors and devices into currently intimate spaces poses particular challenges. As physical objects in our everyday lives increasingly detect and share observations about us, privacy continues to play an important part when it comes to fully or partially adopting the IoT.

5.0 References

- **www.ftc.gov**
- **www.cloudsecurityalliance.org**

Appendix A

List of Acronyms

API	Application Program Interface
DSRC	Dedicated Short Range Communications
ECU	Electronic Control Unit
IoT	Internet of Things
PHI	Personal Health Information
RF	Radio Frequency
SCADA	Supervisory Control And Data Acquisition
WSN	Wireless Sensor Network