CMSGu2017-05

National Computer Board

Mauritian Computer Emergency Response Team
Enhancing Cyber Security in Mauritius

Guideline on Securing your IoT Devices

CERT-MU

National Computer Board
Mauritius

Version 1.0

December 2017

Issue No. 5

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

The purpose of this guideline is to provide a guidance to manufacturers of IoT devices so that they can build more secure products in the Internet of Things space.

1.2 Audience

The targeted audience for this document includes manufacturers of IoT devices as well as security staff and users of IoT devices.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a background on IoT devices and the security implications they carry.

Section 3 explains how you can boost security on your existing IoT devices.

Section 4 provides a set of best practices for manufacturers of IoT devices.

Section 5 concludes the document.

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

2.0 Background

IoT devices are evolving at a rapid pace. It will not be long before a large percentage of the objects in our house or business are connected to the internet. Because these devices are enabled by small computers, they are just as susceptible to hacking as our personal laptops or smart phones. For example, if someone accesses one IoT device in our house, they could gain access to any device on our network.

IoT devices, however, cover a much larger spectrum than just home monitoring systems. For example, a baby monitor that we can view from your phone, or an insulin monitor that we can manage online. These devices are much more important to keep secure from hackers.

Luckily, a lot of the devices we buy off-the-shelf today come with security measures built-in. Unfortunately, some manufacturers do not tell us about the security measures they have put in place.

3.0 Boosting security on IoT devices

1. Make security the default.

Many manufacturers ship hardware or software with generic usernames and passwords like 1234, assuming that these will be changed by the installer or end user. Meanwhile, botnets scan the Internet of Things for these known, factory-default usernames and passwords. For hackers, this is an easy entry point. As such, you have to ensure your internal IT staff check passwords and usernames and changes those that are not secure.

2. Use the most recent operating system possible.

Many IoT devices use Linux OS, but they do not necessarily use the most up-to-date version. The advantage of open-source software is that it is constantly improved by contributors, and these improvements include changes to remove vulnerabilities. That does not make the current OS invulnerable, but at least it will not include well-promulgated holes.

3. Select hardware with security features.

When economically and technically feasible, choose hardware that does include security features, for example, computer chips that integrate security at the transistor level or embedded in the processor that provide encryption and anonymity.

4. Plan for disruption.

System designers should understand the consequences of the failure of a device or part of the network. The best practice is to create a system in which the failure of one IoT device does not disrupt the rest of the system. When this is not possible, understanding the consequences can lead to better decisions about risk.

5. Design in the ability to update and patch.

Even when security is included at the design stage, vulnerabilities may be discovered later on. When devices are upgrade-capable, they can be maintained with the latest security and flaws can be patched as new information is discovered and understood. This results in a system that can adapt to new and changing threats or attacks.

It is also important that the updating mechanisms themselves are secure, tested and use cryptographic signatures because the updating process itself is vulnerable to attack.

6. Plan for the end of device life.

At some point, devices may no longer be able to be patched and will need to be replaced. It is much better to create a schedule for replacing old devices before they fail instead of waiting until they do so. Also, be mindful of when support for hardware and software ends.

7. Participate in information sharing.

You should develop a policy regarding the disclosure of information from your company and form a security team that includes your developers, manufacturers and service providers.

You can also get information and alerts about vulnerabilities and major incidents from the Computer Emergency Response Team of Mauritius (CERT-MU).

4.0 Manufacturer IoT Security Guidance

The goal of this section is to help manufacturers build more secure products in the Internet of Things space. The guidance below is at a basic level, giving builders of products a basic set of guidelines to consider from their perspective. This is not a comprehensive list of considerations, and should not be treated as such, but ensuring that these fundamentals are covered will greatly improve the security of any IoT product.

Category	IoT Security Consideration
Insecure Web Interface	• Ensure that any web interface in the product disallows weak passwords • Ensure that any web interface in the product has an account lockout mechanism • Ensure that any web interface in the product has been tested for XSS, SQLi and CSRF vulnerabilities • Ensure that any web interface has the ability to use HTTPS to protect transmitted information • Include web application firewalls to protect any web interfaces • Ensure that any web interface allows the owner to change the default username and password
Insufficient Authentication/Authorization	• Ensure that any access requiring authentication requires strong passwords • Ensure that user roles can be properly segregated in multi-user environments • Implement two-factor authentication where possible • Ensure password recovery mechanisms are secure • Ensure that users have the option to require strong passwords • Ensure that users have the option to force password expiration after a specific period • Ensure that users have the option to change the default username and password

Insecure Network Services	• Ensure all devices operate with a minimal number of network ports active • Ensure all devices do not make network ports and/or services available to the internet via UPnP for example • Review all required network services for vulnerabilities such as buffer overflows or denial of service
Lack of Transport Encryption	• Ensure all communication between system components is encrypted as well as encrypting traffic between the system or device and the internet • Use recommended and accepted encryption practices and avoid proprietary protocols • Ensure SSL/TLS implementations are up to date and properly configured • Consider making a firewall option available for the product
Privacy Concerns	• Ensure only the minimal amount of personal information is collected from consumers • Ensure all collected personal data is properly protected using encryption at rest and in transit • Ensure only authorized individuals have access to collected personal information • Ensure only less sensitive data is collected • Ensuring data is de-identified or anonymized • Ensuring a data retention policy is in place • Ensuring end-users are given a choice for data collected beyond what is needed for proper operation of the device
Insecure Cloud Interface	• Ensure all cloud interfaces are reviewed for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces)

	• Ensure that any cloud-based web interface disallows weak passwords • Ensure that any cloud-based web interface has an account lockout mechanism • Implement two-factor authentication for cloud-based web interfaces • Ensure that all cloud interfaces use transport encryption • Ensure that any cloud-based web interface has been tested for XSS, SQLi and CSRF vulnerabilities • Ensure that users have the option to require strong passwords • Ensure that users have the option to force password expiration after a specific period • Ensure that users have the option to change the default username and password
Insecure Mobile Interface	• Ensure that any mobile application disallows weak passwords • Ensure that any mobile application has an account lockout mechanism • Implement two-factor authentication for mobile applications (e.g Apple's Touch ID) • Ensure that any mobile application uses transport encryption • Ensure that users have the option to require strong passwords • Ensure that users have the option to force password expiration after a specific period • Ensure that users have the option to change the default username and password
Insufficient Security Configurability	• Ensure password security options are made available (e.g. Enabling 20 character passwords or enabling two-factor authentication) • Ensure encryption options are made available (e.g. Enabling AES-256 where AES-128 is the default setting) • Ensure secure logging is available for security events

	• Ensure alerts and notifications are available to the user for security events
Insecure Software/Firmware	• Ensure all system devices have update capability and can be updated quickly when vulnerabilities are discovered • Ensure update files are encrypted and that the files are also transmitted using encryption • Ensure that update files are signed and then validated by the device before installing • Ensure update servers are secure • Ensure the product has the ability to implement scheduled updates
Poor Physical Security	• Ensure the device is produced with a minimal number of physical external ports (e.g. USB ports) • Ensure the firmware of Operating System cannot be accessed via unintended methods such as through an unnecessary USB port • Ensure the product is tamper resistant • Ensure the product has the ability to limit administrative capabilities in some fashion, possibly by only connecting locally for admin functions • Ensure the product has the ability to disable external ports such as USB

5.0 Conclusion

One of the biggest challenges with IoT devices is the security implicaitons that come with them. That is why security for every IoT device should begin at the initial design process. Incorporating security from the beginning is cheaper and easier than trying to look for security solutions later on.

6.0 References

- **https://www.bluespurs.com**
- **https://hologram.io**
- **https://www.owasp.org**
- **http://www.zdnet.com**