A guide for securing your IoT device

Gonçalo Valério *

December 6, 2015

Date Performed: June 2015

1 Introduction

1.1 Background

This document is the result of a research performed during the internship of the masters degree in Informatics Engineering at Whitesmith [1]. The purpose of the work was initially to study the state of the art of IoT security and other privacy concerns, inspect some popular devices in addition to the in house ones and propose strategies or solutions to improve future releases.
This approach is the reflex of a needed change in the mentality of many manufacturers and the confirmation that the principles and concept of *"security by design"* are in fact important for the success of any IoT offerings.
In addition to the security tests made on some devices a provisioning method was proposed to improve this setup process that was found in many cases insecure. That part of the work is also available publicly at [2].

1.2 Objectives

This document has two main goals, which are to expose the some of the weaknesses found during our research (and their solutions) and to make the bridge to many documents and projects that can help manufacturers improve their offerings.
The research followed mostly a previous work done by OWASP [3] in 2014, that is their "Iot top 10 project" [4], even tough some security concerns were found outside of that scope. These concerns do not only compromise software bugs and the use of outdated and vulnerable implementations, but also were found some security flaws in the design of some processes.
Regarding the second goal, for each security concern we will show what good practices and solutions are described in the existing literature and propose a way to fix them.

2 Why it matters to business

Discussing the business perspective is very important, because much of the decision making in every technology development project is dependent on business. The time frame, the resources, the budget, the features, every one of the previous areas is dependent on the priorities of non technical people focused in maintaining their company floating.
In most cases compromises must be made, but nowadays security shouldn't be in that list. The business impacts of security breaches, data loss, customer privacy violations and damages caused by attacks can lead to serious monetary losses and to the destruction of the company's reputation.
So communicating and making every stakeholder understand the importance of having a *security-by-design mentality* is critical. In this paper we try to cover the possible outcomes in an easy language without lacking in technical aspects and depth, in order to provide both audiences with the information needed to secure certain aspects of the devices and the reason it must be done.

3 What you shouldn't forget to address

3.1 Introduction

During our research, which was done in a relatively small but popular group of devices and included *wearables*, TV Sticks, energy monitors and analysers of several body parameters, we found a diverse number of security problems, that in the vast majority could be easily avoided.
Given that our work was done using the *OWASP Internet of things Top 10 2014* [4] as a reference, the majority of the issues fall into at least one of the categories defined in their "list". However some of them might be a little more complex.
One aspect that you should be aware while reading this document is that it isn't supposed to be the full reference on how to build a secure device and surrounding systems. For that you should check the other referenced materials and consult with a security professional. This document only addresses a subset of all issues that must be kept in mind while building your product.
In the following chapters the most common problems found in the research will be broken down into categories, then discussed separately.

3.2 Transport

Starting with the topic of transport, which means how should the data be transmitted between the device and the cloud, Smartphone or any other device through any channel, which in the majority of the case we should assume as insecure. This is probably the most discussed topic in Internet security in the recent years however some devices still seem to lack any mechanism to safeguard the user's data in this regard.
In our research we found devices that even though they are massively popular, just didn't implement any protection to the shared data. This makes it easy

for any attacker to eavesdrop or do some kind of more complex MITM attack. Other implemented protection mechanisms that are outdated and have been proven insecure.
It is essential that every link between all stakeholders in the system to be encrypted. This encryption should be made using a state of the art standard that as been proven effective [5, 4] given device constrains.
A TLS or DTLS implementation should be used, depending as said on the device constrains. For a generic case, were exists Internet connection, some processing capacity and power is not an issue the mozilla server recommendations [6] should be used. Something like this:

Versions: TLSv1.1, TLSv1.2

RSA key size: 2048

DH Parameter size: 2048

Elliptic curves: secp256r1, secp384r1, secp521r1 (at a minimum)

Certificate signature: SHA-256

DTLS should be used for more constrained devices. Given that all its versions follow the TLS versions described above, the remaining parameters should be matched.
For cases were the use of the above solutions is not possible, check the security specs of the protocol being used or consider using an application layer security protocol.

3.3 Authentication

Following the trend from the previous topic, authentication should not only be addressed when accessing the device but also between all the communications made to and from the device and related services.
It goes several steps further than just saying the user needs stronger password, authentication also means that every stakeholder in the system (servers, devices and users) know and can verify precisely with whom they are "talking" with. For interaction with users this often means passwords but between machines there are several alternatives such as pre-shared keys, raw public keys or certificates [5].
Some devices that were tested had weak authentication mechanisms in some of their actions, making it easy to exploit them in some way. A few examples of the problems found were:

- The server accepted data from a device without checking if it was the right account sending the data.
- The device does not do any kind of identity verification
- Recovery passwords are sent in plain text by email.

So regarding this topic, there are several aspects that a developer/manufacturer should be aware and make sure their device does:

- Use default and widely tested processes for account password recovery in the related web services that communicate with the devices.
- Only accept strong passwords, either on the device or in the related web services/mobile apps.
- Use a string key derivation function to store the passwords (look at scrypt or PBKDF2) [7]
- If possible use a public key infrastructure to assure that all stakeholders verify each others identity.
- Make sure that if any physical action on the device or access to its internal systems is needed, only the manufacturers can perform it.

A good practice would be to use a public key infrastructure so each stakeholder identity would be validated through a certificate [8].

3.4 Provisioning

Another aspect that is very important when developing an IoT solution, is the provisioning method. Not all solutions specially those destined to B2C (Business to Consumer) segment, where is highly probable that the company's engineers will not do the setup for each customer.
This way, for the devices that need wireless connection, a mechanism for the user to easily do the setup and provide access to the network(Internet) generally is developed. This process should ensure 3 main things, that only the owner can run the setup mechanism, the device and the user can authenticate each other and that all the critical information shared between them is well protected.
In our research several devices were in this category and all of them were accompanied with an app that would do the setup either by bluetooth or connection to the device's temporary access point.
All of them failed to secure all 3 aspects mentioned above. Here are the main security issues found:

- Network credentials were transmitted in clear text.
- An attacker could "remotely" initiate the setup process.
- Any person within the reach of the device could connect it to their network.

This issue is very dependent on purposes and constrains of each type of device, but in the case of home and office equipment, this rules should be helpful for developing a more secure mechanism:

- The user should only be able to initiate the setup mechanism with physical access to the device.

- Only allow 1 connection to the device.
- Use standard mechanism to protect the link with the device. For example if the device spawns an access point and a screen, use WPA2 and print the access password on the screen. Otherwise implement the security on the application layer.

With this in mind, we developed a prof of concept setup mechanism, based on some constrains, for a IoT device that would meet all of the 3 aspects. It could be a good starting point is this matter [2].

3.5 Network Services

Since the intent of the Internet of things is to have interconnected devices that interact with the real world, many times this devices need to also accept connections. This is done through exposed network services that are constantly listening for input from other agents in the network. As it is well known, this is one of the major attack vectors for any device, as soon a vulnerability in the software used by these services is found attackers will to exploit any machine that doesn't have been patched.
This is also true for IoT devices, since they typically are updated less frequently than most servers. So the recommendation here (given by almost every security manual out there) is to have the minimum number of services required for the device to work properly actively running. If the device only function is to send information it doesn't need any network service permanently running and listening for connections.
For those services that are essential, frequently check for updated and vulnerabilities so that they an be fixed as soon as possible.

3.6 Firmware Updates

Other aspect that is very important and sometimes is not implemented in a secure matter is the firmware/software update mechanism, this servers not only of major upgrades but also for fixing small bugs and security vulnerabilities. This mechanism should be secure and is recommended to be a base requirement of any new device [9].
During the research we found that the majority of the devices got the this aspect right but yet some fundamental problems still exist as:

- Users downloads a program to his PC to upgrade the device, from a insecure location.
- The mechanism allowed the device to upload, instead of being read-only.

So to have a secure upgrading mechanism it should take care of the following issues:

- The transmission should be encrypted.

- The device should be able to verify (authenticate) the source and the integrity of the code.
- It should be download only.
- The device should automatically check for new updates.

These aspects should be common-sense but is always good to remember as does the OWASP in their recommendations [4].

3.7 Cloud

Even though this aspect was outside of the scope of the study we had some contact with the cloud services that gave support to the devices. Through a normal user utilization it was easy to detect some bad patterns in this services that could throw away most of the security measures implemented in the device level.
If you are exposing a service on the Internet to the user (either through an API or website) you should follow the security best practices of this area. The OWASP website should be good place to start.
Here are some of the critical aspects that were found:

- Cloud services, of a well protected devices, that are only available through HTTP.
- Insecure authentication and mechanisms to recover passwords.

4 Privacy

Privacy is a topic that generally concerns more the users than the manufacturers. In the last decade the trend has been to extract more and more information about the user, from a manufacturer point of view it is great since with more information it is possible to do more and provide *better* services and experiences. However, with the advent of the Internet of things the user's information is expected to be much more available since it is collected automatically and generally without user input.
This fact combined with the overall notion that this devices are, in their vast majority, insecure [10], is everything that is needed to compromise the users privacy more than expected.
Even though this recommendation might go against some business aspects of the product, the development team should try to address it some how. During our tests we've found and confirmed several issues with some devices such as:

- User information is exposed in the network
- Device features allow the user to be tracked by other entities

Given this issues and other concerns manufactures should make sure the development of their device takes the following points into account:

- Inform the user in a clear way about all the data that is being collected
- Do not collect more data than the explicitly needed
- Given the user a change to opt out from the collection of extra data.
- Understand the information that could be indirectly obtained by the collected and aggregated data. Act to minimize the issue.
- Use best practices to protect the data in transit and the one that is stored.

If the above principles are followed and used with a *privacy by design* development process, we are certain that the business goals can be met while protecting the user's privacy.

5 Conclusion

In this small guide we tried to sum in a clear way our main findings when studying how these devices work. The Internet of Things is here to stay and the possibilities are almost limitless, browsing the Internet and reading the newspapers these days will let you with notion of all the excitement in the technology industry about this phenomenon, that while not being new is getting up to speed.
The exposed concerns and suggestions if taken into account, will greatly improve the security and privacy of the users without being restrictive for the manufacturers.
As it as being said in the past [10] the majority of this issues can be described as "low hanging fruit" and can be solved pretty easily, the only requirement being the developers to have a security mindset while designing the whole ecosystem.
The only topic that we have not seen properly addressed, was definitely the provisioning method of the devices. Which given the number of possibilities and usages of this kind of devices, must take into account the local attackers. For this a proof of concept was built to address a common pattern, that is "devices without user interface" that need to connect to a local (and protected) wifi network.
Concluding this guide, we would like to make a call to developers starting new projects to address security from the beginning since it will lead to more secure devices and less troubles along the way. There are many resources and communities trying to get this topic right, with great documentation that could be used [11].

References

[1] "Whitesmith." http://www.whitesmith.co.

[2] "Setup spell - repository." https://bitbucket.org/dethos/setup-spell-device.

[3] "Owasp." https://www.owasp.org.

[4] "Internet of things top 10." https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project.

[5] "Security guidance for early adopters of the internet of things (iot)." https://cloudsecurityalliance.org/media/news/csa-launches-new-security-guidance-for-early-adopters-of-the-iot/.

[6] "Security/server side tls." https://wiki.mozilla.org/Security/Server_Side_TLS#Modern_compatibility.

[7] "Recommendation for password-based key derivation part 1: Storage applications." http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf.

[8] "The challenges of iot security and techniques for mitigating risk." http://nquiringminds.com/files/2015/06/NQM-IOT-Security-4.pdf.

[9] O. Whitehouse, "Security of things: An implementers' guide to cyber-security for internet of things devices and beyond." https://www.nccgroup.com/en/learning-and-research-centre/white-papers/security-of-things-an-implementers-guide-to-cyber-security-for-internet-of-things-devices-and-beyond/.

[10] "Internet of things research study." http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[11] "Builditsecure.ly." http://builditsecure.ly/.