Problem Solving (A3) Report

Topic: Security of IoT

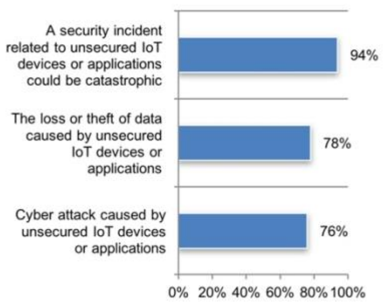
Date: 08/18/2020
Name: Isaac H. López Díaz

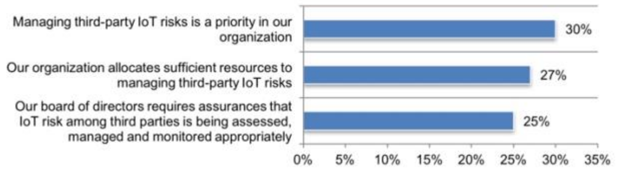
1. Identify a Problem — PLAN

Problem:

- The IoT is a new concept in the software development field, and security for developing these devices has never been a top priority. The idea of networking devices is helpful but most of these devices *severe security issues because manufacturers are interested in marketing and selling their devices.*
- Eg: Hardcoded or default passwords, ability to automatically transfer data over a network, the computer is created with the purpose in mind meaning that security is sometimes even forgotten, companies have a large variety of standards for their devices in addition the use proprietary software that limits the company's input.

Figure 1. IoT risks in the next two years
Very likely, somewhat likely & likely responses combined





2. Set the Target — PLAN

Main Target:

- To start spreading awareness in a more global scale about the lack of security in these devices and the consequences that they bring. Hopefully in a future stop/minimize the number of attacks.

Small Idea:

- A website/app that can start the awareness and inform people on their personal device. What security vulnerabilities the device has, what can he/she do to stop or minimize the vulnerability, point them to experts in the security field, etc.

Deadline could be by the end of the semester hopefully

Big Idea:

- Develop a standard OS for these types of devices that meet some sort of criteria of security measures, one that is also easy to handle to develop the purpose of the device.

Deadline could be by the end of 2022

3. Analyze the Causes — PLAN

Main Cause:

The main cause for the lack of security in IoT devices is the lack of security knowledge and the lack of knowledge of what consequences this brings by the companies.

4. Propose & Implement Countermeasures — PLAN/DO

Small Idea(s):

1. Website/app that could inform customers about their device and help them to make some security adjustments if needed.
2. Website/app that could allow people, that purchased a device (or multiple), to hire an IT, specialized in security, to help with their device(s). I.E. much like baby-sitter websites that allow people to hire baby-sitters, rate their service, and recommend to friends and family, etc.
3. Website that could help IT technicians working on devices for companies (or help even the companies) to ask questions, or answer questions (for example like stackoverflow.com) but specifically for security of IoT. Maybe this could be paired with idea 1 or 2.

These ideas can shed some light to people who use these devices. Hopefully some reports can be done that can be shared with companies that produced the devices so that we can help them build better and more secure devices. This can definitely put some calmness in the customers because they know their information is safe, achieving greater customer satisfaction for both the company and us.

- Implement the idea with the following Stack:
- React-Native for framework: Extensive libraries (pro), great documentation and community (pro), easy to use and learn (pro), JavaScript (pro & con), requires little to no configuration depending on machine (pro), but requires many software (con).
- Nginx as server: Easy to use (pro), extensive documentation and large community (pro), is a standard in Linux requiring minimal configuration (pro), somewhat archaic (con).
- Digital Ocean as hosting service: Have credit (pro), extensive documentation but confusing (pro & con), uses Linux machines (pro), service is never down (pro), great community (pro).

5. Check/Evaluate — CHECK

Questions:

1. Are devices now getting more secure?
2. Are people getting informed about their devices?
3. Are companies addressing/fixing security issues from devices?
4. Do IT techs have the knowledge? And, are they completing their work?
5. Are companies/IT techs doing some reporting on security flaws and countermeasures?

6. Act and/or Standardize — ACT

Questions:

- Can we standardize security measures for IoT?
- Can we address new vulnerabilities while technology is being created? Can we be ahead of hackers?
- Can our service be useful for every corporation and small companies? Is our service just addressing just one specific target or multiples?