Collaborative Threat Mitigation:
Problem Statement

Lucien Armand Tamno

Oregon State University
Fall2017-CS461

08 October 2017

Abstract

This document describes the fact that there is currently no cutting edge technology device that allows Hewlett-Packard company to fully benefit from an open communication environment like the Internet of Things in order to securely and effectively carry out any kind of extensive workflow.Though the company has so far of the advanced digital technology installed in its devices, it hasn't been able to update its technology up to the point where those devices are able to meet the needs of the most recent technology changes.Changes such as the cloud computing, Big data as well as the great move of the Internet of Things.Therefore, the capstone project ***IoT Device collaboration*** was born and that name was recently changed into ***Collaborative Threat Mitigation*** to provide a vital solution to the problem by designing and developing a software that will allow Hewlett-Packard devices to securely work together.

Contents

1 Problem Statement

1.1 Definition and Description of the Problem

Though it's fairly admitted that most of the digital devices produced by the HP company can perform basic tasks such as for an HP printer to print colorful images on plain papers or a scanner storing data with a great precision, still, HP digital devices haven't yet got ways to communicate among themselves. And that lack of communication may stand as a barrier to the company goodwill policy to engage its technology to better provide the most recent services that might get from the Internet of Things. So for the company policy, that environment of devices collaboration has to take place in order to be left behind in century where the world is opened up in all kind of technological changes.To company perspective for example, printers shouldn't be limited anymore to print images but to smartly communicate with others devices as well as its environment. To do so, HP thinks in terms of building a new technology for its devices that is the main reason why the project capstone " IoT Device Collaboration" was devised and which name has recently been changed into " Collaborative Threat Mitigation " just because the project has to embrace a scope of operation that is beyond the sole venue for collaboration.

In order to solve the current problem of no cutting edge technology device in its facilities, the Hewlett-Packard tasked a capstone team of software engineering students from the Oregon State University, to carry out the following steps in order to figure out a vital solution:

- Brainstorm on the pros and cons of having social collaboration technology for digital HP devices
- Define - design and implement the technology that will work the best
- Provide the technology to be devised with a robust system of threats mitigation

While looking at these bullet points, the first question we might likely ask ourselves is whether indeed Hewlett-Packard company needs: social collaboration technology environment or is it others alternatives to that and does the technology that company is looking for can be implemented to mitigate threats in its environment? all have as end point the underneath proposed solution

If the firm doesn't get along with the current technological advancement, the company will certainly miss numerous opportunities offered by the new IoT trend. For example, the company may come to the point where it won't be able to know what its customer needs are for the decision making relying on the information from the market in which the company is no longer part of. Moreover, as this is the Hewlett-Packard's goodwill policy to create an internal-mutual environment of sharing resources across the branches also known as "open door policy", the company won't reach it best allocation resources if the technology can't be improve to be smart enough. Ultimately, even to mitigate threats the company will definitely needs smart devices that could potentially inform decisions makers in real-time so that the most appropriate decision is made.

When the HP company thinks about threats, it can be any from new device introduced in the network or files that can put the normal workflow of companies or people using HP devices. With the rise of the Internet of Things, threats are everywhere and can happen at any time. So in a proposed solution section, we will present one or two solutions to this problem.

1.2 Proposed Solution

To get this project onboard, our mission as the developers'team is to present in six months ahead, a vital solution on how the client technology can still be count as one of the world leading technology to this century, to which people can rely on the carry their routine tasks when it comes to the point to where, they would like to print, to scan documents but also to more than what is currently being offered by those machines. The solution would like be to develop a software with multiple functions. one of the functions will be for instance for a printer to recognize how many pages of a given document it has to print when a user via a microphone speak to that printer to do so.

Among other things, the same printer should be able to talk to any other device in which the software was installed. However, all these transactions are possible if only if, the devices are working in environment void of any kind of threat.Whenever any threat is identified, the software to be implemented has to deal with it by,either sending a signal as a number like 1 being " the work is down" and 10 being the system has recovered from the threat. And the whole process is called the " Threat mitigation".

1.3 Performance Metrics

Metrics which we would like to perform in the project should be specific, measurable, achievable, results-focused and time-bound. And those metrics start primarily with we, as a team will be frequently touch with our client to receive once in awhile feedback from him but more than that, we are planning to use the agile software development methodology which is one of the intense process of software development iteratively taking place between clients and developers. And on top of all these, we will likely use mutation testing to make sure our software is free of major flaws.