Capstone 2017 Problem Statement

Oregon State University

CS 461

Fall 2017-2018

Written By:

Robert Hayden Anderson

October 10, 2017

Abstract

The Collaborative Threat Mitigation (CTM) project focuses on the security issues within the realm of the Internet of Things (IoT). Using this rigid structure ensures the intranet of social devices continue providing optimum service. This will be accomplished by creating an overlay node network comprised of low profile raspberry pis as an add-on to each respective IoT device. These nodes will be the medium for which IoT devices will communicate to ensure security and efficiency among the IoT framework. The nodes will use a collaborative mesh framework that shares relative information and redundantly send previously failed jobs to connected devices that can accomplish the job.

Problem Definition

When Internet of Things (IoT) devices become more prevalent in all consumer households security should be the last thing on the mind of its users. When you have a household chocked full of social devices, the user should know without a doubt that they are there to make life easier. They should require very little, if any, need for interaction to work correctly. Each social device should intercommunicate with each other to reach peak performance and share relevant data within the group.

Security has been a huge problem as of late in the technology world. One of the biggest areas of technology that is lacking in security is the realm of the Internet of Things (IoT). One story even involves a hacker speaking to a napping baby through the use of an IoT capable baby monitor. Another instance showed a blackhat stop the heating unit of a building in Finland causing the temperature in the building to reach well below freezing.

Despite many of these issues popping up over the last couple years during the rise in prevalence of IoT devices, many devices continue to ignore the necessity of better security within their social devices. Ideally, security should be one of the top priorities when creating devices that are so personally linked with their users.

Financial risks from social devices can be very small to astronomical. This would depend on how closely knit the IoT devices are with the users life and finances. For example, if the social device is an insulin pump for a diabetic, a blackhat could increase the dosage causing the user medical harm.

Problem Solution

One way to help keep these devices safe is to keep them on the intranet as much as possible as opposed to accessible from the internet. This would ensure remote infiltration would be magnitudes harder. Another way to increase security in social devices would be on how they interact with each other and mitigate the risks to each separate device on the network would be to instantiate threat levels. As the device finds that it might be infected with a virus, it sends a message to the current leader node who will then decide the best route to take. If the leader decides it is a substantial threat or something they havent seen before, it will broadcast to all members on the net to stop all contact with the infected node. If the node is currently doing a task, the remainder of the task will be sent to another node of the same type to finish the job. For example, If one of your social devices is a printer that receives a job consisting of 100 pages and becomes compromised while 30 pages into the print job. The current leader node would send the remaining 70 pages to another IoT printer within the intranet and notify the user of both the compromised machine as well as where the rest of the pages are.

Fixing these problems could include an Arduino or Raspberry Pi add-on to a current IoT device that are a medium to incoming and outgoing traffic throughout the IoT intranet. The devices will connect to each other dynamically. Each node will work together.

Performance Metrics

This project will be finished when we have IoT devices capable of dealing handling a IoT framework with at least one of each of the following devices; printer, scanner, display, microphone, speaker, and outlet. The display will be used to map the current IoT network to visually represent each node within the network. It will also have connection lines to show that each device is connected to each other. The display will show which node is the current leader and can effectively show when nodes leave, enter, and/or select a new leader node. The nodes will be able to dynamically select a new leader, enter, and leave the network. The nodes will also be capable of sending jobs that were previously assigned to a node to a similar typed node if the original node becomes infected by a virus or shuts down unexpectedly. The nodes are not required to detect a virus.

The nodes will be able to effectively handle other compromised nodes to different levels of security threat. The worst of which will contact the IoT outlet of the infected node and turn the machine off. In the instance of a partially compromised node, the leader will inform the rest of the nodes to cease contact with the node until the leader has established the regained security of said node.

Summary

There currently is not a standard for IoT devices to handle threats such as viruses or malware or other network compromising issues. When a closed network of IoT devices become compromised, there is not a way to keep that infection to be spread to the rest of the devices within that network.

Collaborative Threat Mitigation aims to solve this issue by creating a standard that utilizes Raspberry Pis as a medium of communication for IoT devices to mitigate these security threats within an IoT intranet. Doing so will allow products to keep working as intended and cut off communication to the extent that is necessary when dealing with a compromised social device.

Hayden Anderson

Name

10/9/2017

Date