Identification of Location of Laptop Devices using Raspberry Pi Module

Jibin John[1], Anson Mathew Thomas[1], Abey Varghese[1], Arya Vijayan[1], John T Thomas[1], Dr. Jubilant J Kizhakkethottam[2]

[1]Dept. of Computer Science and Engineering, Saintgits College of Engineering, Kottukulam Hills, Pathamuttom, Kottayam, Kerala 686532, India
[2]Professor, Dept. of Computer Science and Engineering, Saintgits College of Engineering, Kerala, India

---***---

Abstract - *Theft of mobile devices, such as laptops, are the third most frequent computer crime after virus and hacking. While mobiles devices can be located using the built-in GPS module and accompanying software, devices such as laptops are much more difficult to locate. This paper suggests a better method to identify the location by using a Raspberry Pi that identifies the exact coordinates of the laptop and transmits it over to the owner. The coding is done in Python as it is the easiest to implement, though any programming language can be used.*

The proposed system consists of four different phases. This includes auto run terminal, which is the first phase and it turns on along with the CPU. It can be either from charging or just switching on the system.

Once the port for communication is successfully established from GPS module, the coordinates are obtained and stored in a second file. This is the second phase.

The third phase focuses on establishing connection using Wi-Fi/Internet. Since the CPU runs automatically, the geolocation details will have to be sent to the owner. It will search for some open Wi-Fi networks or any other internet connections, before using the built-in GSM module.

Whenever the connection is established, the last phase is executed, sending of the E-mail containing the geolocation. From the coordinates received via this email, the owner can use any map application to identify the location of the device.

***Key Words*: Raspberry Pi, Python, GPS, Geolocation, Wi-Fi**

1. INTRODUCTION

The work focus on a novel method for finding a lost laptop. In the present scenario when a laptop has been stolen it cannot be retrieved so easily unless and until it is informed to the police. The main objective of the device is to locate the whereabouts of the stolen laptop. Laptop Security is a broad term which includes the various products and techniques used to prevent the theft of laptop computers. Laptop security solutions can involve physical lock-and-key systems, locator devices, or other kinds of devices and technologies that make it difficult for an unauthorised person to access the device. This work provides security features to the Laptop. In this paper, we have suggested a better method to increase the security of the laptop devices that lacks features of a mobile device such as smartphone.

2. EXPERIMENTAL SECTION

The number of personal mobile devices like laptops, mobile phones etc... have increased exponentially over the last decade. Many mobile devices that lack a proper location service are stolen because they are harder to track or identify. Once a laptop is lost or stolen, it is almost impossible to physically locate it. There has been no development or very little progress for the identification and location of the misplaced or stolen laptops. Not only in companies but also in universities and colleges, social places it became a major problem for students, staff and people. Even though the laptops are password protected, that type of security is not providing any kind of use in finding the laptops once they are stolen.

2.1 Problem Description

Laptops have become a valuable part of the computing scenario. They allow users powerful mobile computers with the same capacity and software of many desktops. They also allow connectivity, even outside the office, thus freeing people to take their workplace with them. This is extremely valuable for employees who must travel frequently while remaining in continual communication with their offices. Unfortunately, the mobility, technology and information that make laptops so useful to employees and organizations also makes them valuable prizes for thieves.

In 2006, a laptop containing personal and health data of 26,500,000 veterans was stolen from a data analyst working for the US Department of Veterans Affairs. The data contained the names, dates of birth, and some disability ratings of the veterans. It was estimated that the process of preventing and covering possible losses from the theft would cost between USD 100 million and USD 500 million.

One year later, a laptop used by an employee of the UK's largest building society was stolen during a domestic burglary. The laptop contained details of 11 million customers, including but not limited to, names and account numbers. The information was unencrypted. Subsequently, the UK's largest building society was fined with GBP 980,000 by the Financial Services Authority (FSA). The reason for the fine was failing to have effective systems and controls to manage its information security risks.

From above mentioned incidents it can be inferred that laptop theft is a serious problem that concerns both businesses and individuals. Victims of laptop theft can lose not only their software and hardware, but also sensitive data and personal information that have not been backed up. The current methods to protect the data and to prevent theft include alarms, anti-theft technologies utilized in the PC BIOS, laptop locks, and visual deterrents.

2.2 Existing Systems vs. Proposed System

1. Locating devices: The first intention of the concerned person will be to obtain the location of the laptop or mobile device in question. Most antitheft products use Wi-Fi lookup to determine the laptop's geolocation. They check nearby Wi-Fi hotspots against a database to find out where the laptop is. It's also possible to roughly determine the device's location based on the IP address of the network to which it's connected. However, IP-based geolocation doesn't have nearly the accuracy of the Wi-Fi-based technologies. The problem with such technologies are that they rely on an externally available connection to perform a lookup and also require expensive monthly or yearly subscriptions.

   Our proposed system is different because it contains built-in GPS & GSM modules and can connect to externally available Wi-Fi. It also does not require any subscription as it does not rely on any specific company provided database or service.

2. Stealth Tactics: Applications working in stealth, install in stealth mode, deliberately hiding their processes and leaving no visible evidence of their presence. Their aim is to covertly gather information about the unauthorized person without letting the person know that he's under observation.

   Scare tactics take quite the opposite approach. Some services sound a loud alarm if a locked, but running laptop, is disconnected from its power cord while others sound a loud, whooping alarm when the owner remotely sends it a lockdown command.

   They need not work always if the unauthorized person is ready to deal with loud alarms and plan on getting away using force. They also may not provide locating service if the laptop is taken away in such a scenario.

   Our proposed system incorporates both stealth and scare tactics. Even if the person does manage to get away with the device, he can be tracked whenever he attempts to switch on the device or inputs an incorrect password repeatedly. The locating device is activated in stealth mode so that the person never knows it's working in the background.

2.3 Advantages of Proposed System

1. Security: GPS technology also acts as a guard against auto and mobile thefts and if GPS chips are installed then it can be easily traced even if these are stolen and being sent to some other region. It is easy to trace lost or stolen laptops using GPS technology. Hence, our project is a perfect answer for our security concerns against mobile and laptop thefts.

2. No operating system vulnerabilities: In computer security, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. A security risk may be classified as a vulnerability.

3. Modifiable to manufacture: A good manufacturing change process feeds information back into the design process so engineers are informed about problems on the manufacturing line and can apply that information to their current and future design iterations. Manufacturing changes should be documented so that problems can be addressed efficiently. There are many modifications which can be applied to our system. Therefore, this can be designed and manufactured as per modifications.

3. MODULE DESIGN

1. Auto run: A product is being developed in raspberry pi using Wi-Fi module and it turns on whenever it gets a power supply from CPU.

2. Accessing geolocation: Once the port for communication is successfully established from GPS module the latitude and longitude is located and is stored in a file.

3. Establishing connection with Wi-Fi/Internet: To send data to the destination internet is important. Since the CPU is run automatically, after collecting geolocation details we have to send it to the destination. Initially it will search for some open Wi-Fi networks or any other internet connections. Whenever the connection is established, next module will get started.

4. Sending E-mail: Once successfully established connection with internet the next step is to send the current location of the laptop. From the link send to the destination E-mail, the owner will be directed to google map and he/she can view the exact location.

4. RESULTS AND DISCUSSIONS

This paper discusses the possibility of a device that can be developed using Raspberry Pi and programmed in Python programming language. Locating is made possible by the GPS module that is built into the Raspberry Pi. In the scenario when the Laptop is lost, the Raspberry Pi is automatically activated by the Operating System and the current location is obtained by the GPS module. These coordinates are mailed to the owner using a network connection.

The further discussions on the topic Laptop Locator suggests developing the said device so that it is deeply integrated into the Operating System environment and into the hardware. This makes it impossible for the anyone to remove the Raspberry Pi. Also the current size of the implementation is too big to fit inside the laptop. It can be scaled down to fit inside the laptop.

5. FUTURE ENHANCEMENTS

The proposed device is made as simple as possible so that we can further tune it according to user requirements. Some of the features that we can add as future enhancements include:

1. Investigate how to protect the data inside the system which belongs to its owner.
2. Developing a means to show track record of where the laptop has been rather than just the position located.
3. To develop a mobile application for the above proposed system.

6. CONCLUSIONS

The system has been successfully implemented and has been found to be working efficiently. It is very much user friendly and comparatively comfortable to operate. Our project is implemented to give out response to laptop theft and to handle certain situations. The foremost objective of our project is to develop a Laptop Locater that would be used in a real world. The GPS modem will give the data that is, the latitude and longitude indicating position of laptop. This is converted and located on map. And the corresponding link is send to the linked mail. The expected results were obtained as it can be evident as analysed. This project is simple to implement and cost effective and easy to use.

REFERENCES

[1] Graham Glass, King Ables, “Unix for programmers and users”, 3rd edition, Pearson Education

[2] http://opensourceforu.com/2016/10/programming-raspberry-pi-with-python/