Volume 4, Issue 1, January 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Laptop Theft tracking: A Review

Sachin S. Bahade
Student, Mtech,
Department of CSE, India

Lalit Dole
Asst. Prof,
Department of CSE, India

Abstract— The use of number of personal mobile devices like laptop, palmtop increasing day by day. Peoples are addicted for the use this devices. The most popular device is the laptop, which is not only very expensive but also very important for the user because it contain a lot of personal information and data. If this laptop is losted or stoled, then it not only economical loss of user but also loss of very important data. To recover a stolen or lost mobile devices, it is very tedious job to manually locate a lost or stolen device. One of the method is to lounge a police complaint but it take too much time to recover, sometimes it is impossible to return a lost devices. In this paper, the review of available method for theft protection and location tracking analyze finding out which will be best suitable method

Keywords— tracking devices, lost devices, Theft detection, MAC address, Burned-In Address.

I. INTRODUCTION

As the number of computer laptop user increasing day by day, the computer laptop lost or stolen also increasing. Laptop is expensive devices and contain a lots of important information. If the laptop of VIP person get stolen, it will be very dangerous for that person because if the emails are auto login then theft can misuse of their email. It is found that according to FBI, 10 laptop among 100 will be stolen within the next year. Only 3 percent will be return. It is extremely tedious job to physically locate the laptop, its almost impossible. So, some automatic methods require that not only save time for recover the lost or stolen laptop but also protecting the laptop that being stoled [1].

There are a number of computer theft protection products on the market. These generally belong to one of two distinct categories. The first category is theft deterrence products and the second category is theft recovery products[2]. The deterrence product include computer lock which deter theft that laptop being stoled. It include Wirelessly locking computer to discourage theft for stole while mobile platform traveling through distributed channel. A theft prevention system for protecting device contain accelerator sensor to detect acceleration of device and controller to analyze accelerator for detecting the presence of theft. The surveillance of computer device include network surveillance server connected to device. It gives alarm if device fail polling with the network surveillance server.

The theft recovery product offer recovering the device after being stolen. It take the help of email or web connected network or GPS. It also need some unique identifier which identify the device and track the location of device and recover.

II. RELATED WORK

There are a number of computer theft protection products on the market. These generally belong to one of two distinct categories. The first category is theft deterrence products and the second category is theft recovery products[2]. The detail about the is are as below.

1.Theft Recovery

1.1. *Using Encryption Key*

A network system comprises a computer system, a network, and a server module. The computer system has a network interface for connection to the network, a server module address, a secure identifier, and a key. The computer system generates identity information which comprises the secure identifier ID and which is protected using said key k. This identity information is automatically sent via the network interface to a server module which is reachable via the network by using said server address where it is used to determine whether the respective computer system is reported lost or stolen [3].

1.2. Blacklisting mechanism with DHCP server

The chosen mechanism for implementation is a blacklist. It is a lists of cataloging ISPs refusing to control their mail volume. A globally distributed list of MAC addresses tied to missing or stolen hardware would be maintained with accompanying information for each entry. Such a blacklist, in combination with a DHCP server monitoring client MAC addresses could be used to detect any clients on the DHCP server's network that report matching MAC addresses. Detection is, of course, only the first step, beyond this remains the question of tracking down the blacklisted hardware. Is it possible, with only the DHCP data to track down the hardware on the network.

A subscriber's DHCP message goes from the com-puter to the cable modem to the Cable Modem Termination System (CMTS), Making this addition at the CMTS renders the process invisible to the subscriber. The result is that each

subscriber's DHCP is tagged with not only the computer's MAC address, but also the cable modem's MAC address. Videotron registers new subscribers by linking their cable modem's MAC address to their account information. Therefore, if a Videotron subscriber attempted to use a blacklisted computer, then Videotron could use the cable modem's MAC address, found in the DHCP message, to track down the subscriber's account information. This data includes the subscriber's name and address, which could be forwarded to the appropriate authorities.

More generally, ISPs often maintain billing in terms of bandwidth usage and thus it is likely they will maintain a mechanism for linking a customer's IP address given by the DHCP server to the customer's billing data. Beyond this, legal requirements in several jurisdictions demand that ISPs be able to identify customers using IP addresses to facilitate law enforcement activities. We can tie the MAC address to the IP address from the DHCP server's logs, which means there is little doubt that ISPs would be able tie it to their customer records.

2. Theft Protection

2.1. Wireless locking

A computer platform contain chipset, a random access memory (RAM) coupled to the chipset, a central processing unit coupled to the chipset, a protected storage device coupled with the chipset, and a wireless communication device coupled to the chipset. A radio signal having an authentication lock is introduced into the Wireless communication device. The authentication lock is then placed in the protected storage device. The computer platform is placed in the distribution channel. The package set of laptop move along conveyner and past through radio transmitter. The authentication code send by radio transmitter is unique for each package. Radio receiver receive a wake event signal. The wireless communication device receive authentication code at receiver. In this way it verify the authenticity of laptop. Here is prevention of laptop theft [4].

2.2. *Acceleration based detection*

An acceleration of device is monitored and processed to determine wether a condition of theft is present. A theft prevention system for protecting a laptop contain an acceleration sensor, an audio output device, and a controller operatively connected With the acceleration sensor and the audio output device. The acceleration sensor is configured to sense an acceleration of the device and provide an acceleration signal to the controller upon detection of the acceleration. The controller is configured to initiate the production of an alarm signal from the audio output based on the acceleration signal [5].

As a method comprises the acts of monitoring the portable electronic device so as to generate an acceleration signal corresponding to an acceleration of the portable electronic device, the acceleration signal having frequency characteristics of movement of the portable electronic device; filtering the acceleration signal so as to isolate the frequencies characteristic of movement of the device; comparing the acceleration signal to a frequency profile so as to determine a metric measuring a correspondence between the frequency profile and the frequency characteristics of movement of the device; and generating an alarm based upon the metric[6].

2.3. *Surveillance of network connected device*

This system include a surveillance of network connected device, network surveillance server and alarm system. The centre surveillance unit issue an alarm, when device disconnect without notice. Upon joining the communications network, a laptop is required to log-in to NSS. Then, NSS polls the device connected on the communications network so that an alarm can be issued from NSS to a central surveillance unit, When the laptop fails responding to polling. Prior to leaving the communications network, the laptop logs-out from NSS. This allows the laptop to be watched as long as they stay connected onto the communications network [7].

III. PROPOSED WORK

The location tracking of lost laptop or stolen laptop is very important to recover the stoled laptop. The one of the method where with the help of MAC address we are able to track the location of lost laptop. Every laptop contain their own network interface which contain the unique MAC Address, with the help of this MAC Address, we are trying to find the location of stolen laptop but the condition is that at least once the laptop should be connected to the internet. It contain following module.

1. Web Application
2. Console Application
3. Security

Web Application is used to primarily admin login, next is create a user profile and insert the detail about the owner of the laptop. Console application run on the laptop hidden under the task which theft not known. Security is used to check that the user working on laptop is authenticate or not. As soon as the theft start the laptop one pop-up appear on the screen asking about the security code. If the security code is correct the user is authenticate and incorrect, the user is theft. After identify the wrong security code, counter is sent in hidden, and once the laptop is connect to the Internet, the regarding MAC Address and IP Address sent to owner email ID. With this detail the location of lost laptop is tracked.

IV. CONCLUSIONS

This paper described about the laptop location tracking. Here we analyze the two category laptop protection and laptop recovery. In laptop protection, various methods use to deter the theft from the laptop being stolen and in laptop recovery, after stolen of lost laptop, the methods involves to identify the location of lost laptop based on unique identifier.

The method which is most suitable after analyzing is laptop location tracking and recovery based on MAC Address and IP address. With this we can recover the lost or stolen laptop automatically.

REFERENCES

[1] S.-S. Lin, I.-C. Yeh, C.-H. Lin, and T.-Y. Lee, "Theft Detection of Computers using MAC address by Map-Reduce Programming Model on a Cluster," IEEE conference, 2012.
[2] Christian Roy, "An Alternative Approach to Identifying Stolen Network Clients Using DHCP., school of computer science, Christian RoycGill university, http://scholar.google.co.in/scholar
[3] Patric Droz, "DISCOVERING STOLEN OR LOST NETWORK-ATTACHABLE COMPUTER system," patent no. US006950946B1 27 sept 2007,http://scholar.google.co.in/scholar..
[4] Luke E. Girard, Santa Clara, CA (US), "PROTECTION OF LAPTOP COMPUTERS FROM THEFT IN THE STREAM OF COMMERCE,"http://scholar.google.co.in/scholar.
[5] Wehrenberg, Palo Alto, CA "ACCELERATION-BASED THEFT DETECTION SYSTEM FOR PORTABLE ELECTRONIC DEVICES,http://scholar.google.co.in/scholar.
[6] marc,eric, lavy., "ENABLING SURVEILLANCE OF NETWORK CONNECTED DEVICE," http://scholar.google.co.in/scholar.
[7] Kenneth Vernon Westin, Portland, "MOBILE DEVICE OR COMPUTER THEFT lassification,http://scholar.google.co.in/scholar.
[8] METHOD AND APPARATUS FOR AUTOMATIC RECOVERY OF A STOLEN 0B ECT,,....Narayan L- Gehlot, sayrev,http://scholar.google.co.in/scholar.
[9] SYSTEM AND METHOD FOR TRACKING LAPTOP COMPUTERS.....Robert K. Johnson, Detroit, MI (US),http://scholar.google.co.in/scholar.
[10] Privacy-Preserving Location Tracking of Lost or Stolen Devices: Cryptographic Techniques and Replacing Trusted Third Parties ,http://scholar.google.co.in/scholar.
[11] MOBILE DEVICE OR COMPUTER THEFT RECOVERY SYSTEM AND METHOD.....Kenneth Vernon Westin, Portland,http://scholar.google.co.in/scholar.
[12] SYSTEM AND METHOD FOR LOCATING MOBILE DEVICES THROUGH A DIRECT-CONNECTION PROTOCOL.....Janakiraman Gopalan, Cupertino, CA.,http://scholar.google.co.in/scholar.
[13] METHOD AND APPARATUS FOR LOCATION-BASED RECOVERY OF STOLEN MOBILE DEVICES.....David A. Sandage,http://scholar.google.co.in/scholar.
[14] MOBILE DEVICE TRACKING AND LOCATION AWARENESS .....TOIIll Blinnikka,http://scholar.google.co.in/scholar
[15] Trajce Dimkov, Wolter Pieters, Pieter Hartel, "Laptop Theft: A Case Study on the Effectiveness of",CCS'10, October 4–8, 2010, Chicago, Illinois, USA,ACM 978-1-4503-0244-9/10/10.

