Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 60 (2013) 16214-16218

ISSN: 2229-712X

Laptop tracking mechanism using GSM/GPS technology

Venkata Surya Narayana T* and S. Anil Srikanth
ECM Department, K L University, Guntur.

ARTICLE INFO

Article history:
Received: 21 May 2013;
Received in revised form:
17 June 2013;
Accepted: 5 July 2013;

Keywords
Laptop theft,
Case study,
GSM,
GPS modules.

ABSTRACT

In this paper we explain, the need of Organizations facing the real problem on physical, mechanism to protect their IT systems such as Laptops or notebooks and palmtaps. All IT systems ,have become difficult to protect because they can easily be stolen. 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. This is a method which gives better way in finding the laptops and also catching the thieves. In this paper, we are designing an anti-theft security system to track the location of the laptop. By using the GSM/GPS module connected to laptop the current location of the laptop is read and it is sent through message to the owner. By which it is possible to get back our laptops. As result we can reduce the laptop thefts.

© 2013 Elixir All rights reserved.

Introduction

All IT systems, laptops are particularly hard to protect. Laptops are mobile, easily concealable, there is a big market to sell the hardware and there can be many of them in a single building. With the increased data storage capabilities of laptops, the loss of even a single laptop can induce dramatically costs to the organization. Thus, although there can be a large number of laptops in an organization, losing even a single laptop may not be acceptable. Organizations open to the public are particularly at risk from laptop theft. Hospitals and universities, for example, accept hundreds of people that can wander in the premises every day points out that 46% of data breaches occur in institutions open to the public: education, health care and the government. Laptops containing sensitive medical or academic data become highly vulnerable in these environments. The problem security professional's face is how to protect the laptops in such open organizations.

The LAPTOP Tracking System is developed by exploring the applications of various state-of-the-art technologies to overcome the problems of laptop theft. This is a effective and efficient system in order to enhance the laptop security. This system is based on the Data Logging System. The Data Logging System consists of four different elements. They are

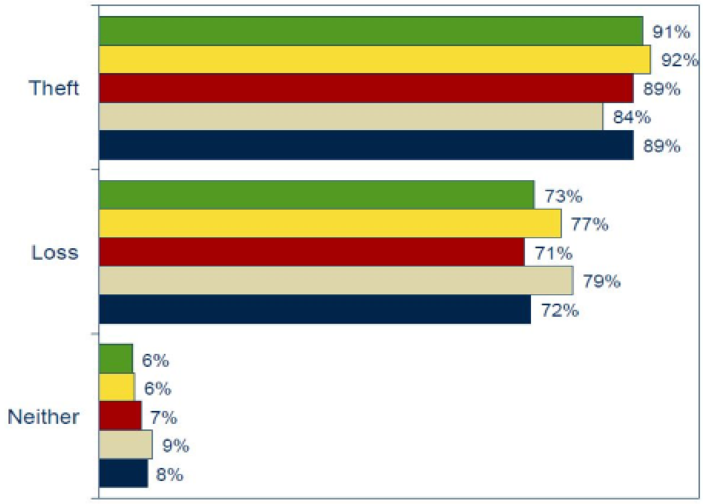
- Measuring the laptop parameters such as position, time, and velocity and so on by the help of sensors. The sensor in this system is GPS sensor.
- Recording the obtained parameters by the temporary logger unit.

Microcontroller acts as temporary logger unit.

- Uploading / accessing the recorded data. The process involved is called telemetry which is performed by GPRS
- Finally, analysis and presentation of recorded data through internet or through the response to the SMS request by the subscriber.

Case study:

Statistics show that as many as one in ten laptops will be stolen or lost from your organisation over the lifetime of each computer. That's 10% of your colleagues and co-workers knocking on your door for a replacement machine. And this dismal scenario is extremely common around 90% of organisations are affected.



Most theft is opportunistic the miscreants usually want the laptop for its resale value rather than for the data. Laptops are easy to sell anonymously over the internet and, once reformatted, stolen hardware is difficult to spot.

Yet it's worrying that most laptops 58% are stolen from work. IDC research shows that the office is the most likely place for a thief to strike. Coffee shops, public transport and hotel lobbies may seem to be the most dangerous places for laptop theft – but your colleagues may actually be more risky than an unknown stranger.

86% of IT security practitioners report that someone in their organization has had a laptop lost or stolen. 89% of companies experience laptop loss. The average total cost to a business from laptop loss is $47,000.

Objectives:

The main objective of the project is foremost building a laptop tracking device that would be used in a real world. The device could be used for wide purposes such as tracking,

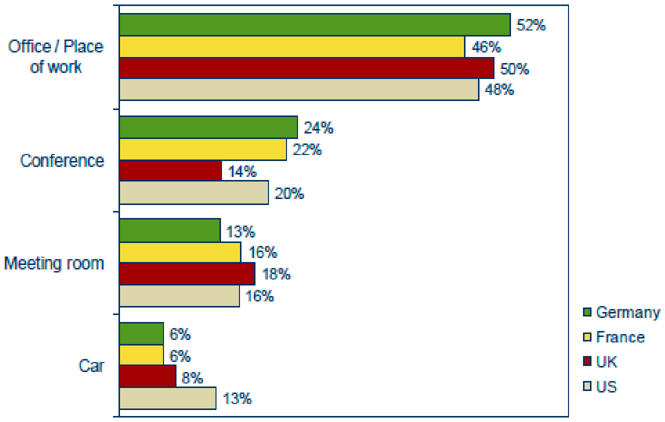
Tele:
E-mail addresses: drsuryanarayana@kluniversity.in

© 2013 Elixir All rights reserved

navigation, fleet and traffic management etc. Also the project helps us to get more familiar with existing GPS and GSM/GPRS networks. So far we have only been able to view the theoretical side of the system but after the project completion we are sure to get familiar with practical side of it. The GPS and GSM/GPRS services have not been fully exploited yet. Therefore we wish to build a base upon which more advanced application of the laptop tracking systems are built in future. Therefore we can say that our project is both research and application based. To be more specific the objectives of the project can be listed as follows.

- To implement a data logging system, which can be used for telemetry
- To show how systems can be combined for the purpose of telemetry.
- To shed light about how new technologies can be exploited for the benefit of human beings.

To understand in detail the electronics behind the GPS and GSM/GPRS



GPS Technology:

GPS is a network of satellites that continuously transmit coded information, which makes it impossible to precisely identify locations on earth by measuring distance from the satellites. As stated in the definition above, GPS stands for Global Positioning System, and refers to a group of U.S. Department of Defense satellite constantly circling the earth. The satellites transmit very low power radio signals allowing anyone with a GPS receiver to determine their location on Earth.

GPS Working:

GPS satellites circle the earth twice a day in a very precise orbit and transmit signal information to earth. GPS receivers take this information and use triangulation to calculate the user's exact location. Essentially, the GPS receiver compares the time a signal was transmitted by a satellite with the time it was received. The time difference tells the GPS receiver how far away the satellite is. Now, with distance measurements from a few more satellites, the receiver can determine the user's position and display it on the unit's electronic map. A GPS receiver must be locked on to the signal of at least three satellites to calculate a 2D position (latitude and longitude) and track movement. With four or more satellites in view, the receiver can determine the user's 3D position (latitude, longitude and altitude). Once the user's position has been determined, the GPS unit can calculate other information, such as speed, distance to destination, sunrise and sunset time and more.

Recent developments in GPS like DGPS have made the positioning even more accurate. The USCG beacons and the WAAS systems are the kinds of DGPS which correct the data from the satellites with appropriate environmental error models.

GPS Sensor:

The GPS receiver used for our purpose is the GARMIN 15L GPS receiver. The sensor first has to be initialized according to the formats in which we required the data. There are certain NMEA (National Marine Electronics Association) sentences that help us to communicate with the receiver. These sentences are the Garmin proprietary NMEA sentences.

Sensor Features:

- 12-channel GPS receiver tracks and uses up to 12 satellites for fast, accurate positioning and low power consumption.
- Differential DGPS capability yielding 3–5 meter position accuracy.
- Compact, rugged design ideal for applications with minimal space.
- Receiver status information can be displayed directly on a PC.
- User initialization is not required. Once installed and a fix is obtained, the unit automatically produces navigation data.
- User-configurable navigation mode (2-dimensional or 3-dimensional fix).
- Built-in backup battery to maintain real-time clock for up to 21 days. Provision for external power to maintain the real-time clock for longer intervals.
- FLASH-based program and non-volatile memory. New software revisions upgradeable through Website download and serial interface. Non-volatile memory does not require battery backup.

Technical Specifications:

- It requires an 8-pinJSTconnector and 1-milimeterpitch.Mating wire harness
- A MCX male antenna has to be connected with the female MCX connector in the sensor
- Required voltage range is 3.3 VDC to 5.4VDC(must have less than 100mV (peak-to-peak ripple)
- Input current is 100 mA peak, 85 mA nominal at 3.3 to 5.0 VDC.

GSM Technology:

GSM (Global System for Mobile communications) is the technology that underpins most of the world's mobile phone networks. The GSM platform is a hugely successful wireless technology and an unprecedented story of global achievement and cooperation. GSM has become the world's fastest growing communications technology of all time and the leading global mobile standard, spanning 218 countries. GSM is an open, digital cellular technology used for transmitting mobile voice and data services. GSM operates in the 900MHz and 1.8GHz bands GSM supports data transfer speeds of up to 9.6 kbps, allowing the transmission of basic data services such as SMS.

A GSM modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. GSM (Global system for mobile) uses a process called circuit switching. This method of communication allows a path to be established between two devices. Once the two devices are connected, a constant stream of digital data is relayed. GSM networks consist of thee major systems the Switching System (SS), The Base Station(BSS) and the Mobile station(MS).

I. The Switching System

The Switching system is very operative system in which many crucial operations are conducted, SS systems holds five databases with in it which performs different functions. If we talk about major tasks of SS system it performs call processing and subscriber related functions. These databases from SS systems are HLR, MSC, VLR, AUC and EIR. The MSC in cooperation with Home Location register (HLR) and Visitor location register (VLR), take care of mobile calls and routing of phone calls. Authentication centre (AUC) is small unit which handles the security end of the system and Equipment identity register (EIR) is another important database which holds crucial information regarding mobile equipments.

II. The Base Station System (BSS):

The base station system have very important role in mobile communication. BSS are basically outdoor units which consist of iron rods and are usually of high length. BSS are responsible for connecting subscribers (MS) to mobile networks. All the communication is made in Radio transmission. The Base station System is further divided in two systems. These two systems, they are BTS and BSC. BTS (Base Transceiver station) handles communication using radio transmission with mobile station and BSC (Base station controller) creates physical link between subscriber (MS) and BTS, then manage and controls functions of it.

III. Mobile Station (Subscriber):

MS consist of a mobile unit and a smart card which is also referred as a subscriber Identity Module (SIM) card. This card fitted with the GSM Modem and gives the user more personal mobility. The equipment itself is identified by a unique number known as the International Mobile Equipment Identity (IMEI).

GSM-GRPS terminal (GM862-GPRS):

Features

The GSM/GPRS device that we are using is Telit GM862 The GM862-GPRS with its EASY GPRS feature is a special device. It embeds and controls the PPP/ (UDP) TCP/IP protocol stack inside itself. In this way the local-host sees a "virtual serial line" connection with the application software on the server machine. Differently from other GPRS devices that embed the TCP/IP protocol stack; an EASY GPRS device, such as the GM862-GPRS, does not provide a set of API functions to interface with the protocol stack but it automatically manages it internally as specified when starting the connection. It also includes all the features of a standard GSM device.

Specifications:

Quad-band 900 / 1800 MHz or 850 / 1900 MHz GSM / GPRS Modem

- Internet, Data, SMS, Voice, Fax, TCP/IP Services and EASY GPRS
- Commands
- Remote Control by AT Commands (according to GSM 07.07 and GSM
- 07.05)
- Input voltage 5.5 V to 12 V DC
- Current 1.8A peak at 5.5 V, 330 mA average at 5.5
- SIM Interface 3V / 5 V
- Weight125 gram

Input/Output Format:

AT Command:

Mobile phone or GSM/GPRS modem are controlled and instructed through commands called AT commands. The AT is an attention commands and is use as a prefix to other parameter in a string. The AT command combine with other parameters can be set up in the communication package or typed in manually as a command line instruction A terminal program's function is like this: It sends the characters you typed to the mobile phone or GSM/GPRS modem. It then displays the response it receives from the mobile phone or GSM/GPRS modem on the screen. The terminal program on Microsoft Windows is called HyperTerminal which was used for the required setting of the GPRS device. The Telit GM862 wireless module can be driven via the serial interface using the standard AT commands. The Telit GM862 wireless module is complaint with Hayes standard AT command set (to maintain compatibility with existing programs), GSM specific AT commands and GPRS specific commands. This module also supports proprietary AT commands for special purposes.

Some AT commands used with Telit GM862 module

The carriage return<CR> and line feed <LF> after every command is implied.

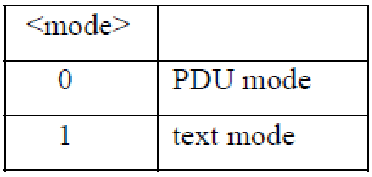
The AT commands used were:

- **AT+CMGF: Message Format**

AT+CMGF=<mode>

Select the SMS format to be used in reading and writing messages.

<mode>



<mode>	
0	PDU mode
1	text mode

Test command:

AT+CMGF=? Reports the supported value of <mode> parameter.

For example:

AT+CMGF=1

The above command will select the SMS format as text mode.

- **AT+CMGS: Send message**

AT+CMGS=<da>

<da>=destination address number.

The device respond to the command with the prompt '>' and waits for message text (max 160 character). To complete the operation send ctrl-Z char (0x1A).

For example:

AT+CMGF=1[Enter]

AT+CMGS="+491711234567"[Enter] >Please call office ^Z

Here +CMGF=1 will set the modem in text mode. After the +CMGS you enterthe number the message is intended to in between quotation signs. The message in ourcase "Please call office" is written in the next line and terminated by ctrl+Z (^Z equals ctrl+Z).

- **AT+CNMI: New message indications to terminal equipment**

AT+CNMI=<mode>[,<mt>[,<bm>[,<ds>[,<bfr>]]]]

The MCU does not require any new message indication. Hence the indications are disabled with the command:

AT+CNMI=0,0,0,0,0

The above command will indicate the first 0 as buffer unsolicited result codes buffering option buffer is full. Second 0- no SMS-deliver indications are reported to the TE. Third 0- Cell broadcast message are not send to the DTE. Forth 0- Status report receiving is not reported to the DTE.

And last 0- TA buffer of unsolicited result codes define within this commands is flushed to the TE.

- **AT+CMGR: Read message**

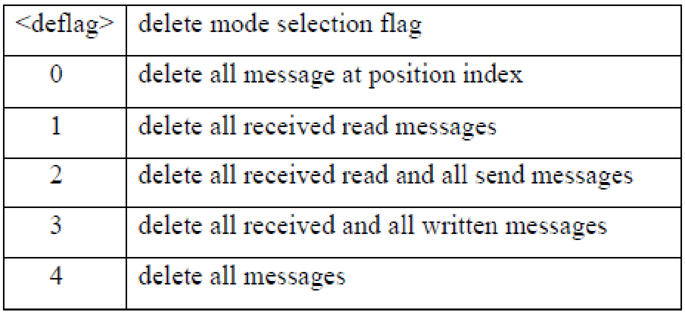
AT+CMGR=<index> Read the message with location value index.

Example:

AT+CMGR=4 This command will read the message on location no 4 of the sim card.

- **AT+CMGD:Delete message**

AT+CMGD=<index>[,<deflag>]
<index>-message position index in the selected storage



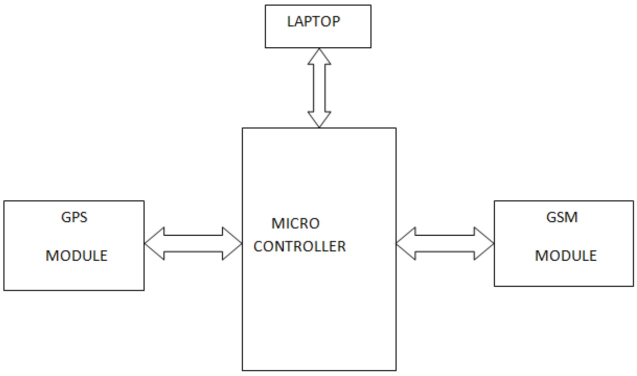
<deflag>	delete mode selection flag
0	delete all message at position index
1	delete all received read messages
2	delete all received read and all send messages
3	delete all received and all written messages
4	delete all messages

Example:
AT+CMGD=1,0
This command will deleted the message of stored location no.1
AT+IPR=4800
This command sets the baud rate of the GPRS device to 4800.

Microcontroller:

The microcontroller is the heart of this device. It is the interface between the GSM module and the GPS receiver. A microcontroller is a small computer on a single integrated circuit containing a processor core, data memory, A/D converter and programmable input/output peripherals. In this device the microcontroller is programmed in such a way that it stimulates the GSM modem in message forwarding when a request is send by the user. Microcontrollers are much smaller and simplified so that they can include all the functions required on a single chip. Having the microcontroller is of great use, as it has low design cost and add intelligence to the system.

Design of tracking system:



Conclusion:

In this paper we evaluate, The current design is an embedded application, which will continuously monitor laptop and report the status of the laptop on demand. For doing so an ARM7 microcontroller is interfaced serially to a GSM Modem and GPS Receiver. The GPS modem will continuously give the data i.e. the latitude and longitude indicating the position of the laptop. The GPS modem gives many parameters as the output, but only the NMEA data coming out and sent to the mobile at the other end from where the position of the laptop is demanded. When the request by user is sent to the number at the modem, the system automatically sends a return reply to that mobile indicating the position of the laptop in terms of latitude and longitude. The block diagram of tracking system using GPS and GSM technology is presented in figure. The project is laptop positioning and navigation system we can locate the laptop around the globe with micro controller, GPS receiver, GSM modem. Microcontroller used is ARM7. The code is written in the internal memory of Microcontroller i.e. ROM. With help of instruction set it processes the instructions and it acts as interface between GSM and GPS with help of serial communication of ARM7. GPS always transmits the data and GSM transmits and receive the data.

References:

1. Trajce Dimkov, Wolter Pieters, Pieter Hartel, “Effectiveness of physical, social and digital mechanisms against laptop theft in open organizations”, 2010 IEEE/ACM International Conference on Green Computing and Communications & 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing.

2. Raj Kishen Moloo, Varun Kumar Digumber, “Low-Cost Mobile GPS Tracking Solution”, 2011 International Conference on Business Computing and Global Informatization.

3. Gps- Gsm based tracking system-International journal of engineering and technology-volume3issue2-2012

4. T. Dimkov, W. Pieters, and P. Hartel. Laptop theft: a case study on the effectiveness of security mechanisms in open organizations. In *CCS ’10: Computer and Communications Security*, pages 666–668, NY, USA,2010. ACM.

5. L. Ponemon. Cost of a lost laptop. Technical report, Ponemon Institute, 2009. communities. intel. com/docs/DOC-3076.

6. M. Marshall, M. Martindale, R. Leaning, and D. Das. *Data Loss Barometer*. KPMG, UK, 2008. www.datalossbarometer.com.4 Seagate Technology. Can your computer keep a secret? 2007.

7. Wayne A. Jansen, Serban I. Gavrila, and Vlad Korolev. Proximity-based authentication for mobile devices. In *Security and Management*, pages 398–404, 2005.

8. T. Ristenpart, G. Maganis, A. Krishnamurthy, and T. Kohno. Privacy-preserving location tracking of lost or stolen devices: cryptographic techniques and replacing trusted third parties with dhts. In *SS’08*, pages 275–290, Berkeley, CA, USA, 2008. USENIX Association.

9. D.J. Scott. *Abstracting Application-Level Security Policy for Ubiquitous Computing*. PhD thesis, University of Cambridge, 2004.

10. D.J. Scott, A. Beresford, and A. Mycroft. Spatial policies for sentient mobile applications. *Policies for Distributed Systems and Networks*, pages 147–157, 2003.

11. L. Cardelli and A.D. Gordon. Mobile ambients. *Theoretical Computer Science*, 240(1):177–213, 2000.

12. B. Dragovic and J. Crowcroft. Information exposure control through data manipulation for ubiquitous computing. In *NSPW ’04: Proceedings of the 2004 workshop on New security paradigms*, pages 57–64. ACM, 2004.

13. B. Dragovic and J. Crowcroft. Containment: from context awareness to contextual effects awareness. In *Proceedings of 2nd Inernational Workshop on Software Aspects of Context*. CEUR Workshop Proceedings, 2005.

14. T Dimkov, W. Pieters, and Hartel P. Portunes: representing attack scenarios spanning through the physical, digital and social domain. In *ARSPA-WITS*, 2010.

15. P. Kleissner. Stoned bootkit. In *Black Hat USA*, 2009.

16. E.M. Chan, J.C. Carlyle, F.M. David, R. Farivar, and R.H. Campbell. Bootjacker: compromising computers using forced restarts. In *CCS ’08: 15th ACM conference on Computer and communications security*, pages 555–564, NY, USA, 2008. ACM.

17. S. Türpe, A. Poller, J. Steffan, J.P. Stotz, and J. Trukenmüller. Attacking the bitlocker boot process. In *Trust '09: Proceedings of the 2nd International Conference on Trusted Computing*, pages 183–196, Berlin, Heidelberg, 2009. Springer-Verlag.

18. L. Ponemon. The human factor in laptop encryption. Technical report, Ponemon Institute, December 2008.

19. D.B. Cornish and R.V. Clarke. Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies*, 16:41–96, 2003.

20. G. Kitteringham. Lost laptops = lost data: Measuringcosts, managing threats. Crisp report, ASIS International Foundation, 2008.