Edith Cowan University
Research Online

Australian Digital Forensics Conference | Security Research Institute Conferences

2009

Satellite Navigation Forensics Techniques

Peter Hannay
Edith Cowan University

Originally published in the Proceedings of the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2009.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/adf/62

Satellite Navigation Forensics Techniques

Peter Hannay
SECAU Security Research Centre
Edith Cowan University
p.hannay@ecu.edu.au

Abstract

Satellite navigation systems are becoming increasingly common for automotive use within the civilian population. This increase in use is of interest to forensic investigators as satellite navigation devices have the potential to provide historical location data to investigators. The research in progress investigates the data sources and encoding on a number of common satellite navigation devices. The aim of this research is to develop a framework for the acquisition and analysis of common satellite navigation systems in a way that valid for multiple devices.

Keywords

Global Positioning System, GPS, forensic methodology, digital forensics, GPS forensics, satellite navigation system, satnav, satnav forensics, TomTom, TomTom forensics.

INTRODUCTION

Global Positioning System (G.P.S.) networks have become a part of everyday life, possibly more than many realise. There are of course the positioning elements of the Global Positioning System (G.P.S.) which beyond assisting drivers in getting to their destination help with a large number of tasks:

- Allows Unmanned Arial Vehicles (U.A.V.) to operate autonomously
- Assists in air and sea navigation
- Provides a way for cargo to be tracked in transit
- Tacking of vehicle fleets
- Tracking of rental vehicles to ensure compliance with the rental contract
- Modern cameras automatically tag photos with location information
- Mobile devices provide location information to tourists based on GPS
- Computer time synchronisation relies on data sent from GPS satellites

With the importance and ubiquity of tasks relying on GPS infrastructure it is worth considering the possible forensic implications of this technology. Devices receiving GPS information have access to precise location information as well as extremely accurate time data. It has already been established that in the case of automotive satellite navigation systems it is possible to retrieve historical location data based on the information received from GPS networks.

In many cases these GPS devices have no in built functionality that would allow their historic locational data to be displayed. Even if it were a feature of a specific device however the forensic implications of using such a feature would need to be questioned. Forensic procedure requires that the original evidence being acquired not be altered or in the situation that the data must be altered that any of these alterations are documented and the impact on potential evidence is understood.

The research will focus on the acquisition and subsequent analysis of historical locational data from a range of GPS aware devices. Many of these units make use of storage in the form of internal flash memory, external flash media and hard disks in order to store operational data, logs and other potentially significant data.

The large number of devices on the market however has lead to a situation where differing acquisition techniques must be developed for each individual device. The research aims to identify the similarities between GPS aware devices and develop a series of forensic procedures that will suit a large number of devices based on these similarities.

History of Global Positioning Systems

The first known satellite navigation network was known as TRANSIT and was developed to provide location data to the US Navy's Polaris submarine forces (Parkinson & Gilbert, 1983, p. 1117). The TRANSIT network became operational in 1963, the use of this network lead to the US Navy and US Air force to consider further use of this technology. At this stage the US government was unable to implement two separate networks due to budget issues. It was due to these issues that the NAVSTAR network was incepted; NAVSTAR was to be a resource that would be shared between US military agencies. The first NAVSTAR satellites were launched in the 1970s (Braunschvig, Garwin, & Marwell, 2003).

NAVSTAR was designed as a dual use system, in that it would be shared between military and civilian users. It was decided however that in order to deny precise locational data to potential enemies of the United States the civilian signal would be degraded. The degradation was to be known as 'selective availability' and would lead to inaccuracies of up to 500m. In 1983 US president Ronald Reagan approved GPS for use in commercial aircraft and subsequently selective availability was altered so that the signal would be accurate within 100m (Parkinson & Spilker, 1996, p. 601).

In May 1st, 2000 Bill Clinton announced that selective availability would be set to zero (Braunschvig, et al., 2003). The result of this was that the civilian GPS signal would no longer be artificially degraded and as such a wide range of commercial uses for the technology became feasible.

Tensions present between the US and the USSR during the cold war lead to the creation of a Soviet owned satellite navigation network known as *ГЛОбальная НАвигационная Спутниковая Система* or GLONASS (Parkinson, 1997, p. 22). The system become operational and available for civilian use in 1995 (Polischuk & Kozlov, 2002, p. 154).

As a result of concerns that the United States controls the NAVSTAR network and has the ability to degrade or tamper with the signal, the European Union (EU) proposed a satellite navigation network named Galileo. The Galileo network is intended to be interoperable with the existing NAVSTAR network provide unprecedented levels of accuracy to both civilian and military users (Braunschvig, et al., 2003).

Global Positioning Devices and Forensics

GPS tracking devices have been used by law enforcement to track offenders who are confined to specific premises during specific hours (Nellis, 2005). There are various implementations of these GPS tracking devices, however one common theme is the combination of GPS and mobile telephone technologies. In these implementations GPS is used in conjunction with the mobile telephone network's assisted global positioning system (AGPS) to provide increased accuracy, this method is particularly useful when indoors, underground or in areas where the GPS signals are weak (Djuknic, 2001). AGPS operates on the principles of triangulation in a similar way to the standard GPS system, however in this case mobile towers are used instead of satellites when determining location. These tracking devices will typically use a data logger component to record location information or alternatively make use of a transmitter and antenna to broadcast real time tracking information (Keith, 2007, p. 25).

Thus far there have been a limited number of published works documenting the use of GPS evidence in legal proceedings. However there are a number of incidents that have been reported on by various news agencies. Significant incidents include those involving Brett Pownceby and Michael Simotas, both of which involve the use of GPS evidence to challenge speeding fines.

An article published by the Australian Broadcasting Authority (ABA) recounts the incidents of Brett Pownceby a Victorian farmer who was issued with a speeding fine for exceeding the speed limit by 21km/h (Watt & Crase, 2007). Supposedly a GPS receiver was turned on and active at the time the alleged infringement occurred. It is stated that Mr Pownceby retrieved records from the GPS device which showed his speed as being within an acceptable range at the specified time. Purportedly the charges against him were dropped when he presented this evidence to an unknown member of law enforcement, however it is stated by the ABA that the case never reached court (Watt & Crase, 2007). It should be noted that an article published by the Herald Sun newspaper reports that a representative of the Traffic Camera Office has stated that "The production of a GPS report alone to avoid any speeding infringement is insufficient" (Whinnett, 2007).

A similar incident involving Michael Simotas, who as it was reported in the Sydney Morning Herald newspaper, was charged for exceeding the speed limit by 25km/h. The article states that Mr Simotas made use of an expert witness and GPS evidence acquired from the satellite navigation unit in his car in an attempt to prove his speed at the time of the incident. Initially the court ruled against Mr Simotas, however the charges were dismissed by the District Court of New South Wales on appeal (Wainwright, 2007). It should be noted that the article does not state that the GPS evidence used was taken into consideration as part of the ruling. The article also reports that the police operating the radar unit at the time of the incident admitted to not using it correctly and instead were making a visual estimation of Mr Simtoas' speed (Wainwright, 2007). The EziTrack website states that the GPS device used was an "EziTrak® GPS Security and Tracking System" which is able to record time, date and vehicle speed ("EziTrak News," 2007). However, it is worth

noting that Michael Simotas is listed as a distributor of the EziTrack product, as such this information may not be impartial ("EziTrak NSW Distributors," 2007; Pye, 2007).

EXISTING GPS FORENSICS RESEARCH

The field of GPS forensics is still quite new and as such there is a limited amount of material published on the topic. The research published so far is focused on forensic analysis of the TomTom navigation devices.

It has been determined that the operating system, data files and settings for the TomTom navigation device are stored on an SD card if present; otherwise these are stored on internal flash media. The media can be acquired through traditional methods, such as using a write blocking SD card reader or USB write blocking device and performing the bit stream acquisition using 'dd' or a similar utility.

The analysis of data acquired from the TomTom devices has also been documented quite heavily. The majority of historical locational data is stored within the MapSettings.cfg file for each map used by the device (as such if there are multiple maps installed, there will be multiple MapSettings.cfg files present). The MapSettings.cfg file contains the last known location, home location, recent destinations and custom locations that have been accessed or saved by the user. The contents of these are shown in table 1 below.

Description	Length	Start	End	Encoding
Header	12 bytes	Indicated by '04 00 XX 00 00 00 04 00 XX 00 00 00'	-	-
Coordinant Set 1	8 bytes	Indicated by '08 00' following header	-	2x signed integer
Coordinant Set 2	8 bytes	Indicated by '08 00' following Coordinant Set 1	-	2x signed integer
Text description of location	Variable	Indicated by end of Coordinant Set 2	Indicated by '08'	ASCII
Coordinant Set 3	8 bytes	Indicated by '03' following Text description of location	-	2x signed integer
Coordinant Set 4	8 bytes	Indicated by '03' following Coordinant Set 3	-	2x signed integer
Footer	5 bytes	Indicated by '04 00 00 00' following Coordinant Set 4	-	-

Table 1 – Contents of MapSettings.cfg Record

SIGNIFICANCE OF RESEARCH

The wide variety of GPS capable devices on the market has led to a situation similar to that of mobile phones, in which a wide variety of forensic techniques and tools are required to make analysis of devices. In many cases there is no documented forensic methodology existing for particular GPS capable devices. In these situations a new methodology would need to be developed, tested and verified prior to a forensic acquisition being able to take place.

The research aims to address this issue through the development of a series of forensic procedures for the acquisition of a range of GPS devices. In the event that this is successful it would become possible to largely eliminate the development of new methodology when analysing GPS devices, allowing devices to be interrogated without lengthily periods of research and development for each individual device. The research differs from previous research conducted in that it attempts to target a wide range of devices based of common hardware components, rather than a single device or line of devices.

RESEARCH METHODOLOGY

Research Questions

The research is designed to answer the question "Is it possible to develop a framework that will allow for the forensic acquisition and analysis of a large range of GPS devices based on their common hardware components?" In order to address this question it has been broken down into the following sub questions:

- What hardware components are common between GPS devices?
- Is it possible to develop a set of procedures that will allow for forensic acquisition from these common hardware components?

Research Design

The research design is split into four main phases:

- Identification & Selection of Devices
- Identification & Analysis of Components
- Data Population & Collection
- Data Analysis

Phase 1 – Identification & Selection of Devices

The selection of devices for research will be made based on two criteria. The first being market penetration, by selecting devices that are widely in use it is hoped that the research will be more relevant for forensic applications. The second criterion is that these devices should represent a good cross section of the devices available. For example if the 3 of the five top devices based on market penetration were all of Brand A, the number of devices selected from Brand A is likely to be limited. This criteria aims to ensure that any developed methodology is indeed able to be employed generally, across a wide variety of devices, not just those of a few choice manufacturers.

Phase 2 – Identification & Analysis of Components

The identification & analysis of components involves the disassembly of the selected devices. Once disassembly is complete the components of these devices will be documented. The aim of this phase is to identify components that are likely to contain data of forensic interest.

Phase 3 – Data Population & Collection

This phase first involves the creation of a forensic image of the device. This image serves two purposes, first it will act as a baseline that will allow for further analysis to be conducted, and secondly it will allow the device to be returned to a base state. The data population will be accomplished by placing the devices into a vehicle and driving a specific route. The data will then be retrieved from the devices and the devices returned to the baseline states. This phase will be repeated a number of times in order to ensure that any results are consistent.

Phase 4 – Data Analysis

This phase will involve the analysis of the images collected previously. Each image will be compared to the established baseline. This comparison will serve as the basis for analysis as it will demonstrate the changes performed by the device during specific scenarios. These changes will be examined in order to determine their forensic relevance; these examinations will be focused on the determination of what historic locational data is present.

CONCLUSION & ONGOING RESEARCH

At this point in time the first phase is nearing completion, with the selection of devices finalised and the sourcing of these devices currently in progress. The data population phase is currently undergoing a trial process in an effort to determine the best way to accomplish a consistent result; this trial is focused on determining the extent of impacts on GPS signal due to varying atmospheric conditions.

In conclusion satellite navigation is a field of increasing importance to law enforcement and other investigative agencies. The magnitude of this importance is amplified by both the increasing number of satellite navigation devices on the market, as well as the increasing number of consumer devices which make use of location aware technologies.

REFERENCES

Braunschvig, D., Garwin, R. L., & Marwell, J. C. (2003). Space Diplomacy. *Foreign Affairs, 82*(4), 156.

Djuknic, G. M. (2001). Geolocation and Assisted GPS. *Computer, 34*(3), 123.

EziTrak News. (2007). *EziTrak* Retrieved 16 Oct, 2007, from http://www.ezitrak.com.au/aa-News.htm

EziTrak NSW Distributors. (2007). *EziTrak* Retrieved 16 Oct, 2007, from http://www.ezitrak.com.au/aa-NSWDistributors.htm

Keith, H. (2007). Tracking "Bad Guys": Legal Considerations in Using GPS. *FBI Law Enforcement Bulletin, 76*(7), 25.

Nellis, M. (2005). Out of this World: The Advent of the Satellite Tracking of Offenders in England and Wales*. *The Howard Journal of Criminal Justice, 44*(2), 125.

Parkinson, B. W. (1997). Origins, evolution, and future of satellite navigation. *Journal of Guidance, Control, and Dynamics, 20*(1), 11-25.

Parkinson, B. W., & Gilbert, S. W. (1983). NAVSTAR: Global positioning system—Ten years later. *Proceedings of the IEEE, 71*(10), 1177-1186.

Parkinson, B. W., & Spilker, J. J. (1996). *Global Positioning System: theory and applications*: Aiaa.

Polischuk, G. M., & Kozlov, V. I. (2002). THE GLOBAL NAVIGATION SATELLITE SYSTEM GLONASS: DEVELOPMENT AND USAGE IN THE 21ST CENTURY. *34th Annual Precise Time and Time Interval Meeting*, 151-160.

Pye, G. (2007, March 14). A Knight With Shining GPS. *Rock Paper Dynamite* Retrieved 16 Oct, 2007, from http://rockpaperdynamite.wordpress.com/2007/03/14/a-knight-with-shining-gps/

Wainwright, R. (2007). Father and son stick to guns to prove radar wrong. *The Sydney Morning Herald* Retrieved 16 Oct, 2007, from http://www.smh.com.au/news/national/father-and-son-stick-to-guns-to-prove-radar-wrong/2007/03/11/1173548023012.html

Watt, J., & Crase, S. (2007, July 2, 2007). How I used my GPS to beat my speeding fine. Retrieved 16th August, 2007, from http://www.abc.net.au/southwestvic/stories/s1967739.htm

Whinnett, E. (2007, 16 Oct 2007). GPS beats radar gun. Retrieved 16 Oct, 2007, from http://www.news.com.au/heraldsun/story/0,21985,21999706-661,00.html

COPYRIGHT

Peter Hannay ©2009 The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.