Legal and Ethical Implications of GPS Vulnerabilities *

Muhammad Usman Iqbal[1] and **Samsung Lim**[2]
PhD Candidate[1], Senior Lecturer[2]
School of Surveying and Spatial Information Systems
The University of New South Wales
m.iqbal@student.unsw.edu.au[1], s.lim@student.unsw.edu.au[2]

Abstract. The Global Positioning System (GPS) has slowly permeated into the civilian community and has become an essential accessory for the modern individual. Various commercial applications heavily rely on GPS technology. GPS has also started receiving attention in court cases, where it has been admissible as evidence leading to convictions or proving innocence. However, GPS is a radio-navigation system and is prone to vulnerabilities that may be introduced intentionally or unintentionally. The legal literature has not debated the possibility of human alteration of GPS data in judicial reasoning which raises the prospect of forged GPS data being presented to courts by individuals who have the motive and the technical knowledge to do so. By exposing the weaknesses present, this paper aims to draw the attention of the legal fraternity to these issues which may put the legal system in a dilemma as over-reliance on GPS technology may produce disastrous results, especially when innocence or guilt largely depends on GPS evidence.

Keywords: Global Positioning System (GPS), Vulnerabilities, Court Cases, Privacy, Surveillance, Tracking, Legal, Mobility-Pricing

1. Introduction

The Global Positioning System (GPS) is a space-based radio-navigation system using a constellation of satellites (currently 31) and provides precise position, velocity and timing information to receivers on the ground that can obtain the signals of four or more satellites simultaneously (FRnP, 1999). Primarily designed for military applications, it has recently seen widespread adoption by the civilian community with an explosive growth in the number of users and applications of this technology. Part of this demand stems from the changes prompted by GPS in the way some industries operate, from construction to emergency services. In fact, GPS is invading all walks of life, from personal navigation in cars and emergency location services for mobile phone users, to location-based charging systems such as GPS-enabled vehicle insurance and friend-finder services (Iqbal & Lim, 2006; Grush, 2005; Vidales & Stajano, 2002; Zhang, Wang, & Hackbarth, 2003).

GPS devices have become pocket-sized, battery operated and commercially available at nominal costs. They are also being embedded into mobile phones, digital cameras, Personal Digital Assistants (PDAs) and watches. This ubiquity of location-determination devices enables tracking and monitoring of individuals by governmental entities, private entities and individuals which raises profound ethical, policy and legal issues for the society. In recent years, the legal system has encountered various cases involving the use of GPS either as evidence collected through surveillance by Law Enforcement Agencies (LEAs), or as a tool for invasion of privacy of individuals in the workplace or private lives. While GPS data has been used to indict and convict individuals for suspicious criminal activity, individuals have also presented GPS data to prove their innocence (ABC News, 2007a; ABC News, 2007b). In the United States, courts have debated whether surreptitious installation of GPS-tracking devices amounts to 'search' or 'seizure' requiring a warrant under the 4th Amendment. Most of these debates have revolved around the notion whether GPS tracking can be an invasion of privacy of individuals; however, there have been minimal discussions about the accuracy of this GPS data in legal contexts and virtually no mention of the vulnerabilities of GPS data as a result of malicious human intervention in judicial reasoning.

GPS is a radio-navigation system and is prone to certain vulnerabilities that may be either intentional or unintentional. This paper comprises of two experiments to highlight two weaknesses of GPS systems which may be introduced intentionally, specifically, malicious editing of GPS data, and spoofing of GPS signals, which means transmission of GPS-like fake signals with false positional data. These issues raise the prospect of forged GPS data being presented to courts by individuals who have the motive and the technical knowledge in an effort to inflict harm, to defame or to exonerate a person of criminal charges. By exposing the weaknesses present, this

* This article was first published in Kierkegaard, Sylvia (2007) Cyberlaw, Security and Privacy , IAITL, pp. 581-558

paper aims to draw the attention of the legal fraternity to these issues which may put the legal system in a dilemma where over-reliance on GPS technology in judicial settings may produce disastrous results, especially when innocence or guilt largely depends on GPS evidence. Therefore, it is imperative for legislators to acknowledge and address this problem.

Before delving into the experiments that expose weaknesses of GPS receivers, it would be worthwhile to review some legal and commercial scenarios where GPS is actively being used.

2. Background

2.1 Legal Scenarios

The United States constitution's fourth amendment protects the right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures (Kilman & George, 2000). The fourth amendment test has been applied in various cases to decide whether privacy rights of individuals were violated. The Supreme Court case that comes closest to the use of GPS tracking is *United States vs. Knotts* (1983), involving a 'beeper'- a battery operated Radio Frequency (RF) transmitter, which was attached to a chloroform container that the defendant had purchased and loaded in his car. The police followed the defendant by a combination of visual surveillance and the use of the beeper to locate the defendant's rural cabin which turned out to be a drugs laboratory. Although a search warrant was obtained to enter the premises, the court held that monitoring the vehicle while it was on public roads without a warrant was permissible because the defendant had no reasonable expectation of privacy when in public. According to the court, the beeper was merely an augmentation to the sensory faculties bestowed upon the police officials at birth and was analogous to using a pair of binoculars while conducting visual surveillance.

The *United States vs. Garcia* (2007) case is a more recent one and directly involves the use of GPS data for surveillance of suspected criminal activity and largely draws from the *Knotts* case. The police were tipped off by an informant that the defendant, who was recently released from prison for methamphetamine offences, had mentioned to him that he intended to produce meth again. The police located the defendant's vehicle on a public street where it was parked and installed a GPS memory tracking unit under the rear bumper. After a few days, when the device was removed, the police were able to learn the car's travel history since installation which led them to a tract of land that the defendant frequented and contained equipment and ingredients to produce meth. The defendant was arrested and charged with drug offences. The defendant contested to suppress this evidence as a fruit of an unconstitutional search because a warrant was not obtained before installing this tracking device. The 7th Circuit Court of Appeals concluded that installation of the GPS tracking device neither constituted seizure nor search because the device did not interfere with the driving qualities of the vehicle and was analogous to a police officer following the vehicle. However, the court did acknowledge that there was a practical difference between following a vehicle and using GPS devices.

The cases discussed above involved surreptitious installation of tracking devices by law enforcement officials. Another extraordinary case that has recently come to light involved the use of a GPS tracking device by a suspicious wife in her husband's vehicle (Finz & Taylor, 2004). The data obtained from the tracking device led to filing of murder charges by the police in the death of the couple's twelve year old baby-sitter. The device was placed by the wife in her husband's truck a few days earlier because she suspected him of having an affair. The husband told the police that he went to drop the baby-sitter to her home when they took a detour to show her some horses, then accidentally ran her over as he turned his truck around on a rural road in central New York. He was initially charged with a felony count of reckless endangerment, but based on data obtained from the GPS unit the charges were raised to second degree murder as data revealed that the defendant did not take the girl to see horses at all. Instead, he drove around other roads and spent more than three hours with her behind an abandoned home. Police believed that the girl had gotten away from him when he drove over her. At the time of writing this paper, this case awaits a decision, but proves that GPS data was the major evidence for indictment.

There has also been a trend to track and locate parolees, and sex-offenders using electronic means. GPS has become the technology of choice for implementing this. At least twenty-three states in the United States use GPS tracking of convicted sex-offenders and some states are even using GPS tracking as an inexpensive transition program for low-risk offenders in order to make more room in the crowded prisons (Mohan, 2006). Usually worn as an anklet or bracelet by the parolee, GPS tracking has proven to be a powerful tool in strengthening the monitoring of high-risk offenders (Newschanel.com, 2007). From real-time and retrospective monitoring of the subject's locations, movement patterns can be developed, and unusual activity may be predicted (Iqbal & Lim, 2007). Additionally, by augmenting the tracking device with additional sensors, future models of these bracelets would also be capable to sense the presence of drugs and alcohol and transmit this information to a monitoring facility in near real-time (QuestGuard, 2007). This careful effort to weave ex-

offenders into the fabric of society requires monitoring, but does it violate the privacy rights and would it motivate them to tamper with these devices is open to debate.

Previous cases discussed the use of GPS tracking as evidence generating convictions, for controlled rehabilitation and ethical monitoring of high-risk offenders. In the context of liability offences, there have been instances where motorists have successfully challenged issuance of speed tickets against them by providing GPS data as evidence (Wainright 2007). Recently, a motorist in New South Wales (NSW) was fined $203 for allegedly driving at 85 km/h in a 60 km/h zone. The motorist challenged the fine in court and presented data from his on-board GPS navigator which showed that he was mostly travelling at a speed of 57 km/h on that particular stretch of the road, which was also corroborated by a GPS expert in court. The motorist challenged the accuracy of the hand-held radar guns questioning how rigorously these guns were calibrated each year. The traffic officials conceded in court that they had not taken the readings on their radar guns for the required length of time and had simultaneously relied on their experience and visual estimates. The fines were overturned in the district court setting a precedent for the admissibility of GPS evidence in NSW.

2.2 Commercial Scenarios

The concept of differentiated-pricing or mobility-pricing is not a new one. It has been identified as a method to accurately charge road-tax or motor-insurance based on actuarial principles of costs reflecting usage (Litman, 2003). GPS technology makes it possible to replace traditional flat fee insurance with an approach where insurance premiums are charged based on mobility. There have been successful pilot studies conducted throughout the world that use GPS technology to offer actuarially accurate insurance products (Tripsense 2007; Norwich Union 2007). In the Australian context, a recent statement by an NRMA (National Roads and Motorists' Association) Insurance official lauded the benefits that GPS-based insurance would offer to motorists but also acknowledged the inherent "Big-Brother-ish" qualities that such a product would implicitly have (NRMA 2007).

Another related area of significant interest is congestion-charging of roads in central business districts which is being employed in various jurisdictions in an effort to curb congestion issues during peak hours (Litman, 2005). These systems typically utilise Automatic Number Plate Recognition (ANPR) technology installed around the charging zone. There is a possibility that these systems may be augmented or replaced by GPS-based road-charging as this approach would curtail maintaining and expanding the ANPR infrastructure, thus offering cost reductions. In the UK, where London congestion charging has been operational for a while, there are suggestions to give additional discounts to motorists who opt for GPS-based charging. There are speculations that the British government has engaged with an insurance company offering mobility-priced insurance in an effort to acquire GPS data of its clients for its own GPS-based congestion-charging research (Hytch 2007). It is unclear whether this data would be exclusively used for future GPS-based congestion charging or augmenting the already pervasive surveillance of roads.

With regards to workplace tracking of employees, both GPS-enabled mobile phones and fleet vehicles equipped with GPS are being used. In the United States, GPS-enabled mobile phones have been employed as a solution to satisfy the E-911 mandate enforced by the Federal Communications Consortium (FCC) requiring locating a caller to the emergency number '911' within 300 metres (E-911, 2004). This availability has naturally drawn the attention of employers for work-related tracking. Employees with company-owned GPS mobile phones can be located by the employer by accessing a website. Similarly, vehicles used by employees for work that have GPS-based telematics systems can be used to locate the vehicle. For instance, taxis have been equipped with GPS tracking for directing them to customers in minimum time (Karni, 2007). GPS data has also been used to maintain electronic travel logs for accounting and tax related purposes when using the vehicle for work. While there are advantages of improving productivity and reducing response times using tracking technology, there are potential privacy issues that need redress.

3. Research Motivation

The previous section reviewed scenarios from the legal,as well as the commercial sector where GPS technology played a significant role. The situations discussed may motivate a person to tamper with or erroneously edit the GPS data contents in order to evade criminal charges, avoid financial liability, cheat mobility-pricing systems, provide false GPS alibis, escape speeding fines, frame another person of committing a crime, or simply misinform employers of their whereabouts. These motivations are significant enough to warrant a critical assessment of GPS vulnerabilities to intentional interference.

The Volpe report (Volpe, 2001) summarises these vulnerabilities ranging from ionospheric interference and Radio Frequency (RF) interference including television broadcasts and VHF interferences in the

unintentional disruptions to jamming, spoofing and meaconing of GPS data in intentional disruptions. The Ionosphere surrounding the earth at approximately 350 kms away refracts GPS signals transmitted from the satellite introducing certain errors in the position solution. Likewise, RF interference from TV and VHF transmitters may interfere with GPS receivers at ground level. Jamming, as the name suggests means emission of radio signals of sufficient power that prevents receivers in the target area from tracking GPS signals. Meaconing is the reception, delay and rebroadcast of the radio-navigation signals to deceive the GPS receiver. Spoofing is a technique to deceive the receiver to lock onto legitimate-appearing false signals and make it believe that it is somewhere else.

Another weakness in current GPS receivers open to exploitation is the design of storage memories where GPS data is saved. GPS devices lack any cryptographic protection for the tracks, routes and waypoints stored on its memory, and a compatible software tool can be easily used to edit the positional data. There is no method to validate, for the purpose of non-repudiation, that the claimed GPS positions on the storage memory were indeed generated as a result of the GPS receiver processing. Volpe (2001) reports that spoofing attacks would most likely be targeted towards individuals instead of large areas. Additionally, editing of GPS logs would also be likely performed by individuals on target receivers making it probable that these attacks would be launched by or against an individual.

With regards to admissibility of GPS data as evidence in court, legal precedents have already been set as discussed earlier. Courts have regarded GPS technology to be 'generally accepted and fundamentally valid' (Fox News, 2004) and waived any doubts about its credibility. Even in a case where a tracking device installed on a murder suspect's vehicle reported speeds of 30,00000 mph, the data was still admitted to the court as evidence. Hugh Roddis, Chief Technology Officer for the Nova-Scotia-based Orion Electronics, which sold the GPS tracking devices to the police in this case acknowledged that GPS was "not exactly perfect", but prosecution argued that inaccuracies accounted for only minutes as compared to days of surveillance data gathered(Finz & Taylor, 2004).

In summary, the legal literature has not debated the possibility of human alteration of the data or more sophisticated attacks like spoofing. Additionally, no evidence has been found of any prescribed standards or practice of assessing vulnerabilities either in law enforcement environments or the commercial sector for the suitability of a GPS device for a specific task. This paper questions the over-reliance on GPS data in legal proceedings and the commercial sector by arguing that these susceptibilities could be exploited to significantly or totally change the positional claims in the stored GPS data. With regards to spoofing, countermeasures exist, but Volpe acknowledges in his report that it would be unlikely that commercial receivers have these defences because of the costs involved in implementing them (Volpe, 2001, pp 39). Using off-the-shelf, commercially available GPS devices, this paper demonstrates that human abuse of GPS is plausible which may have drastic effects both on legal as well as commercial GPS uses.

4. Research Study

4.1 GPS Hardware

Four different commercially available GPS tracking devices were used to conduct the experiments, as shown in figure 1. Two of them had serial flash memories, (figure 1: yellow and red borders) to log the GPS data on the same board as the GPS receiver. One of the devices had a PCMCIA (or PC Card for short) interface to a Personal Digital Assistant (PDA) and stored National Marine Electronics Association (NMEA) format messages on the file system of the device (see figure 1:green border). The last one was a bluetooth GPS receiver that transmitted NMEA messages to any paired bluetooth device, e.g. a bluetooth-enabled mobile phone, laptop or PDA (see figure 1: blue border). With the exception of one of the tracking devices, which utilised power from the cigarette lighter adapter of the vehicle, all other devices had batteries attached to the units (see figure 1: blue border). All the receivers had 12 parallel satellite tracking channels, with accuracies ranged between 15m-22m on the horizontal plane and a price tag of under $250 (USD).

4.2 Editing GPS data

This experiment involved editing of the GPS data and a volunteer was required to install the GPS devices in a vehicle to collect data. An administrative staff member from the school, with little technical knowledge about these devices, was asked to take them with him in the school's car when he left for conducting some work-related tasks. These devices were powered-on and were attached to the front dashboard of the vehicle using double-sided adhesive tape. The antennas of the GPS receivers had line-of-sight to the open sky. The volunteer brought back all the four devices after completion of the trip and reported that he had visited the bank and an office goods supplier before returning back to the university.

Scenario 1: NMEA messages output to the file system:

Two of the GPS receivers generated NMEA output, which were connected to a mobile phone and PDA respectively. The NMEA output was stored as a text file on the file system of the mobile phone and the PDA. The NMEA format was primarily developed as an interface between marine electronic equipment therefore its contents are not intelligible to humans. However, there are software converters available that can easily convert between NMEA and various other data formats (for instance GPX, KML, Shapefile, CSV), which makes this data comprehensible to users. Using editors for these formats, the data variables including positions, speed and the times can be altered and then translated back to NMEA, and the same file can be overwritten with the edited contents. There is no method to verify that the contents of the NMEA file are produced as a result of the GPS receiver's processing.

The same technique was used to edit the contents of the NMEA files created as a result of the volunteer's trip. On the return leg of the vehicle, a fake stop-over was added, right in-front of a sports-bar (see figure 2). The data was edited to report that the vehicle was parked in this compound for 30 minutes before proceeding back to the university. When the volunteer was asked about these embarrassing situations, he rightly denied them, but did not have any answer how it may have occurred. This vulnerability was then explained to the volunteer. He was informed that the deception involved was not to vilify him but rather expose the issues.

Scenario 2: Binary data stored on flash memory

In this scenario, the tracking devices stored the GPS data in proprietary binary format on the flash memory, as shown in figure 3 without casings, which is harder to edit as compared to the previous receivers. These devices have a USB interface that connects them to a computer in order to extract the data (see figure 3: circled red). Both these devices come with software that is used to export data into different formats. The user interfaces provided only gave read-only access to the data on these tracking devices' flash memory (see figure 3: circled yellow).

Further investigation of these flash memory chipsets led to the fact that they were general purpose serial flash memory chips and have been used in a range of devices, including mobile-phones. The data-sheet specifications for them are widely available explaining how to write binary data onto them (Atmel, 2005). These flash memories are not secure, and do not have any measures to indicate if they have been tampered with. If a technically savvy person with basic electronics skills is able to understand the format that the manufacturer used to store GPS data, it is possible to reprogram the contents of the flash memory using the same USB interface that is used to download the data to a computer. Alternatively, as the tracking devices are commercially available,it is not hard to obtain an additional GPS receiver of the same specification and use it in a vehicle to create a desired route so that the flash memory has the required data. Then either a swap of the boards or a swap of the flash memory makes it possible to put different contents on the tracking device.

4.3 Spoofing attacks

Spoofing attack, as explained in the introduction section is a sophisticated attack on an individual GPS receiver where a transmitter is used, that sends signals very similar or identical to what GPS satellites would be transmitting. If transmitted at a slightly higher power than the actual satellite signals, it is possible that the GPS receiver would lock onto these signals and would eliminate the actual satellite signals as interference or noise while computing position solutions as shown in figure 4.

In order to test GPS receivers, various research facilities have access to GPS signal generators. These simulators generate RF (Radio-Frequency) signals for different conditions in order to test receiver algorithms' performance in situations involving interference, e.g. multi-path. These signal simulators can be used to conduct a spoof attack on receivers as they are capable of emulating the same PRN (pseudo-range number) of the existing satellites. A Spirent 6560 multi-channel GPS signal generator was used to generate a high-gain RF signal (see figure 5). This RF signal was outputted to a re-radiator antenna on the ceiling of one of the lab rooms (see figure 6). In order to mimic actual vehicular movement, logged NMEA data obtained by driving a car equipped with a GPS receiver was brought back to the lab, which was used to create a scenario in the signal simulator. This means that the output obtained from the re-radiator antenna would make a GPS receiver believe that it is in motion, and the GPS receiver's processed data can be used to verify that it acquired the spoofed signals showing that the GPS receiver followed the vehicle's track.

With the exception of the tracking device that required power from the cigarette lighter, all 3 GPS receivers were placed beneath the re-radiator antenna. The scenario was then run on the simulator, which sent RF signal output of the satellite signals in such a way that it represented a vehicle's motion on the roads when processed on the receiver. All the three receivers processed the signals emitted from the signal generator and computed false positions, thus validating Volpe's inference about commercial receivers' inability to detect spoof attacks.

5. Discussion

The exercise conducted verifies the hypothesis that it is possible to tweak the GPS data either by physically tampering with it, or by the use of more complicated spoofed signal attacks. Although it would require adequate technical knowledge to perform these hacks, the possibility cannot be ruled out. This research demonstrates that GPS data can be edited to portray a different scenario, which may be used to substantiate that a person was not going over the speed limit, or was at a friend's place at the time of a crime incident, or an employee for a courier company was busy with delivery of orders, whereas in reality a different event may have occurred. The cases and circumstances discussed in section 2 may act as the perfect motive tempting a person to tamper with the GPS devices in order to prove innocence or guilt.

Consider the *Garcia* case in the light of these exposed vulnerabilities. Garcia was under GPS surveillance on suspicion that he had intent to produce meth again. The tracking device was installed under the plastic bumper of his vehicle when it was parked on a public street. Had he known about the presence of the tracking device, he may have not travelled to the drugs laboratory site to raise further suspicion and avoid arrest. It is possible to imagine that he would have shielded the GPS antenna of the tracking device to prevent its operation. It can also be speculated that he would have sought technical assistance in cheating the GPS device by either physically editing the data on the tracking device or by conducting a spoof attack which would have resulted in the GPS device logging motion of the vehicle on roads of his choice resulting in the reversal of these suspicions and eventually misleading the police about his plans. Even if sophisticated tracking devices which transmit locational information in near real-time using the GSM network were used, a carefully planned spoof reporting locations within the same mobile cell would have circumvented precision tracking yielding fewer details. The same analogy can be applied to the other scenarios discussed, for instance, an employee who wants to avoid the employer knowing about a romantic rendezvous during working hours whose proof is in a GPS tracking device in the company car would make all possible attempts to erase or replace it even if it requires utilizing the exposed vulnerabilities. Additionally, financial liability matters, such as evasion of a speeding fine, may motivate a person to edit GPS data contents to prove that no offence occurred. Individuals may also not appreciate the idea of mobility-pricing of roads (insurance or a congestion charge) where a fee is applicable based on the distance covered and may rebel against it by trying to outwit the system by exploiting these weaknesses. This implies that cases where corroborative GPS evidence has been presented should be reviewed in the light of the issues highlighted here to avoid erroneous verdicts.

In order to harden GPS systems against these weaknesses, several countermeasures can be implemented both in terms of policy as well as technology development. With regards to policy, it is clear that GPS output which is not exclusively read-only, whether in the form of NMEA messages or any other standard or proprietary format, should not be admissible in court as evidence due to its high susceptibility to tamper. Tracking devices that store GPS logs in proprietary binary format on the same board as the GPS receiver, and provide read-only access, can still be edited with the correct know-how and tools, therefore expert advice should be sought when assessing these types of devices in court proceedings. One possible solution to this problem may be introducing cryptographic techniques to the storage process, where GPS logs are encrypted and digitally signed (Goldwasser, Micali, & Rivest, 1988) so that it can be verified that the data has been produced exclusively as a result of the GPS receiver processing and no other GPS receiver could produce those same results.

However, building in encryption and non-repudiation into the GPS hardware cannot prevent spoofing attacks. Several countermeasures against spoofing have been proposed in the literature (Volpe, 2001; Lagier, Craig, & Benshoof 2004). These include GPS receivers constantly measuring the received signal strength (RSS) of the satellite signals, and if significant difference beyond a certain threshold is found between the expected and observed signal strengths, the user can be alerted to a possible spoof attack. This countermeasure fails if a sophisticated attacker also monitors the RSS and transmits its signals within the threshold, but slightly higher than the observed RSS. This countermeasure also fails if the person who owns the GPS device is the one tampering with it. Other similar solutions include angle of arrival discrimination, amplitude discrimination, time of arrival discrimination, and cryptographic authentication (Volpe, 2001, pg 39). Military-grade GPS receivers work on encrypted signals known as the Precision Code or P-code. These signals work on top of the Coarse Acquisition (C/A) code available for civilian users and can be unscrambled only by US military GPS receivers providing greater accuracy and robustness. Considering the increased reliance of the civilian transport

infrastructure on GPS, there are suggestions to introduce signal authentication for civilian use too (Hein *et al.*, 2007) in order to mitigate spoofing attacks. However, it is unlikely that these hardware, software and infrastructure extensions would be available to civilian GPS receivers in the imminent future. For applications such as mobility-based charging, tamper-proof hardware can be installed that prevents the owner or user of a vehicle to hack the system. The GPS device can be augmented with other sensors, for instance accelerometers can be installed and the odometer output can be compared to the GPS velocity to verify if the vehicle is actually in motion.

6. Conclusion

This paper addresses an important issue that has not been thoroughly examined before, the vulnerabilities of GPS systems and their implications in judicial reasoning and commercial settings. While GPS data has been used as an effective tool in generating suspects, deterring criminal activities, repressing behaviour, and improving response times, the exposed vulnerabilities question all these scenarios, by highlighting that the seriousness of these issues can be a motive for adversaries to exploit these susceptibilities to their favour. An innocent man may be convicted of a crime he never committed or a person who is the culprit in reality may get away by presenting forged GPS evidence. It is hoped that the results of this research would attract the attention of policy-makers, and rigorous ethical and legal safeguards should be implemented to protect the rights of the public from future abuse. The viewpoint that GPS is generally valid means that there is an implicit over-reliance on this technology, and the experiments conducted have proven that the over-dependence may prove disastrous.

Acknowledgement

The authors wish to acknowledge the assistance provided by the 'Metadata Scholarship' from OMNILINK Pty. Ltd. for this research.

References

1. ABC News, (2007a). GPS evidence clears British sailors of wrongdoing, Vice-Admiral says. Retrieved October 10, 2007, from http://www.abc.net.au/news/stories/2007/03/28/1884174.htm
2. ABC News, (2007b). Commonwealth appeals against green zone GPS ruling. Retrieved October 9, 2007, from http://www.abc.net.au/news/stories/2007/04/26/1906741.htm
3. Atmel (2005). 1 megabit 2.7 Volt only Data Flash AT45DB011B Data Sheet. Retrieved October 25, 2007, from, http://www.atmel-grenoble.com/dyn/resources/prod_documents/doc1984.pdf
4. Dempster, A. (2005). How Vulnerable is GPS? *Position*, no 20, pp64-67.
5. Dornin, R. (2004). Judge allows GPS evidence in Peterson case. CNN.com. Retrieved October 5, 2007, from http://www.cnn.com/2004/LAW/02/17/peterson.trial/
6. Federal Communications Commission, Enhanced 911 – E911 (2004). Retrieved October 15, 2007, from http://www.fcc.gov/911/enhanced/.
7. Federal Radionavigation Plan-FRnP (1999). Interagency GPS Executive Board, Washington, DC.
8. Finz, S. & Taylor, M. (2004). Peterson tracking device called flawed, Defense wants GPS evidence shut out of trial. San Francisco Chronicle. Retrieved October 4, 2007, from , http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/02/12/BAG7P4V69B1.DTL
9. Fox News (2004). GPS Expert Testifies in Peterson Trial. Retrieved September 4, 2007, from, http://www.foxnews.com/story/0,2933,132197,00.html
10. Goldwasser, S., Micali, S., & Rivest, R.(1988). A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. SIAM J. Computing 17(2): 281-308.
11. Grush, B. (2005). Optimizing GNSS-Based Mobility Pricing for Road-Use, Parking, and PAYD Insurance. 4th European Traffic Congress. Salzburg, Austria.
12. Hein, G., Kneissl. F., Ávila-Rodríguez, J.A., Wallner, S. (2007). Authenticating GNSS: Proofs against Spoofs, Part 2. Inside GNSS, October 2007, pp 71-78. Retrieved October 20, 2007, from http://www.insidegnss.com/auto/SepOct07-wkngpapers-proof-spoof.pdf
13. Hytch, D. (2007). Service vendors target traffic-management deals. Computer Business Review Online. Retrieved July 25, 2007, from, http://www.computerbusinessreview.com/article_news.asp?guid=E01E9184-2F51-4B85-9577-D0A6C72AF895
14. Iqbal, M.U., & Lim, S. (2006). A privacy preserving GPS-based Pay-as-You-Drive insurance scheme. Symposium on GPS/GNSS (IGNSS2006). Surfers Paradise, Australia, 17-21 July, CD-ROM proceedings.

15. Iqbal, M.U., & LIM, S. (2007). Privacy implications of automated GPS tracking and profiling. Second Workshop on Social Implications of National Security: From Dataveillance to Uberveillance, Wollongong, Australia, 29 October 2007.
16. Karni, A. (2007). GPS Concerns Taxi Drivers. The New York Sun. Retrieved February 12, 2007, from, http://www.nysun.com/article/46133
17. Kilman, J. & George, C. (Eds). (2000). The Constitution of the United States of America: Analyis and Interpretation.
18. Lagier, E., Craig, D., & Benshoof, P. (2004).JAMFEST - A Cost Effective Solution to GPS Vulnerability Testing. Journal of Global Positioning Systems Vol. 3, No. 1-2: 40-44.
19. Litman, T. (2003). Distance-based Vehicle Insurance. Victoria Transport Policy Institute.
20. Litman, T. (2005). London Congestion Pricing – Implications for Other Cities. Dice Report: Journal of Institutional Comparisons 3(3): pp. 17-21, Retrieved November 12, 2006, from, http://www.cesifogroup.de/portal/page?_pageid=36,34692&_dad=portal&_schema=PORTAL.
21. Mohan, S. (2006). Technology: GPS Keeps Parolees on a Short, Smart Leash. Ziff Davis Media Inc. Retrieved September 12, 2007, from http://findarticles.com/p/articles/mi_zdcis/is_200609/
22. NRMA (2007). NRMA calls for car surveillance via GPS. Ninemsn Science and technology news, Retrieved July 10, 2007, from http://news.ninemsn.com.au/article.aspx?id=59964
23. Newschannel.com (2007). Parolees Monitored by GPS Tracking. Retrieved October 14, 2007, from http://www.newschannel9.com/onset?id=963605&template=article.html
24. Norwich Union (2007). Pay As You Drive Car Insurance, Retrieved June 5, 2007, from http://www.norwichunion.com/pay-as-you-drive/index.htm .
25. Questguard (2007). ActSoft Alcohol and Drug Monitoring. Retrieved October 23, 2007, from, http://questguard.com/ActSoft-Alcohol-and-Drug-Monitoring_.html
26. United States v. Garcia (2007). 474 F.3d 994 (7th Cir. 2007)
27. United States v. Knotts (1983). 103 S. Ct. 1081, 1087.
28. Tripsense (2005). How TripSensor Works, retrieved January 11, from, https://tripsense.progressive.com/about.aspx?Page=HowDeviceWorks
29. Vidales, P., & Stajano, F. (2002). The Sentient Car: Context-Aware Automotive Telematics. Paper presented at the LBS-2002.
30. Volpe, J.A. (2001). Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. National Transportation Systems Center. Retrieved August 12, 2007, from, http://www.navcen.uscg.gov/archive/2001/Oct/FinalReport-v4.6.pdf
31. Wainright, R. (2007). Father and son stick to gins to prove radar wrong. Sydney Morning Herald, Retrieved July 5, 2007, from http://www.smh.com.au/news/national/father-and-son-stick-to-guns-to-prove-radar-wrong/2007/03/11/1173548023012.html
32. Zhang, D., Wang, X.H., Hackbarth, K. (2003). OSGi Based Service Infrastructure for Context Aware Automotive Telematics, Paper presented at the IEEE Vehicular Technology Conference, Italy

Appendix

Figure 1: GPS Receivers used for the experiments

Figure 2: Edited route

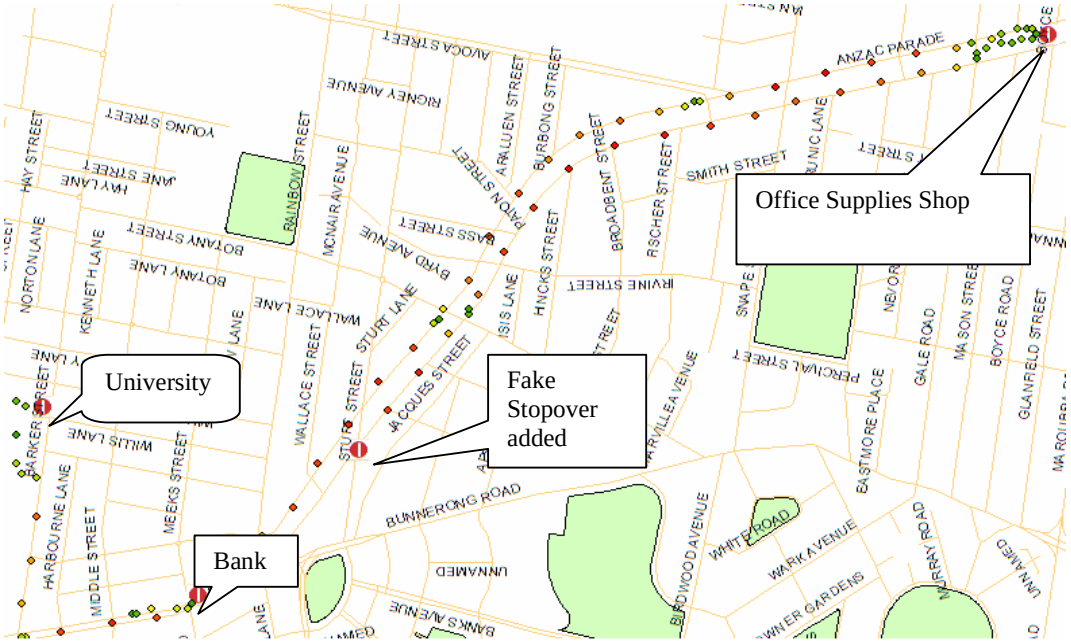

Figure 3: GPS receivers opened

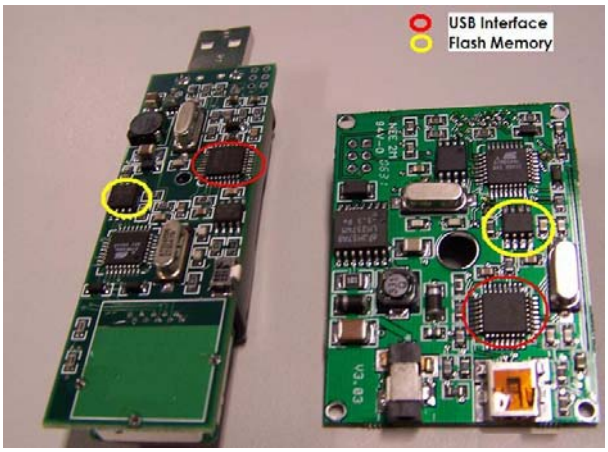

Figure 4: GPS Receiver processing phases, and signal sources source

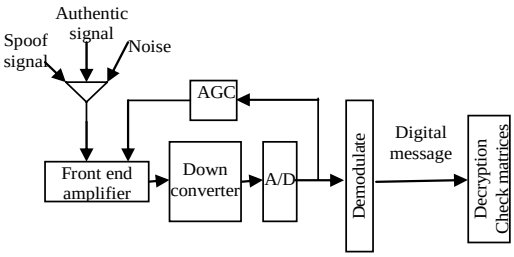

Figure 5: Spirent 5650 Signal Generator

Figure 5: Re-Radiator Antenna