Developing a Self-Powered Vehicle Tracker

(Technical Paper)

Cybersecurity and Privacy Concerns with Location Tracking

(STS Paper)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree

Bachelor of Science, School of Engineering

Malcolm Miller

Spring, 2020

Technical Project Team Members

Jesse Dugan

Nayiri Krzysztofowicz

Vivian Lin

Nojan Sheybani

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature ____ Date __________

Malcolm Miller

Approved ____ Date __________

Harry C. Powell Jr., Department of Electrical and Computer Engineering

Approved ____ Date __________

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction: Modern Location Tracking Devices

With the global positioning system (GPS) being widely available to both individuals and companies, it is now possible to obtain fairly accurate location information from a particular device in real-time. Access to this type of data can help improve productivity and reliability in a variety of industries. In agriculture, location data can be used to associate attributes of a farm such as humidity, irrigation, and soil temperature, with precise locations (Maia et al., 2014). In public transportation, GPS devices help commuters to better plan their trips (Chung, 2019). Despite the widespread use cases of GPS, there are still many situations in which commercially available GPS tracking devices cannot perform reliably. Current GPS trackers are either powered by a battery or through a connection to the electrical system of a vehicle (El Khoury, 2018, p.7). Batteries require recharging periodically, which can make systems less dependable and more expensive to maintain. Connections to external power systems are reliable, but they restrict the compatibility of trackers to specific vehicles. These shortcomings in tracking devices can mean reduced safety and dependability for public transportation systems (Chung, 2019). Additionally, companies that are unable to track the location of their vehicles will likely miss out on opportunities for increased productivity. In order to make GPS tracking services accessible to more problem domains, my capstone team and I are designing and building a solar-powered vehicle tracker that can be easily installed on many types of vehicles. To better understand how location-tracking devices affect society, I will study literature on data privacy and embedded systems to assess their security implications.

Technical Topic: Developing a Self-Powered Vehicle Tracker

As stated in the introduction, there is no commercially available vehicle tracking solution that is both reliable and adaptable to many different types of consumers. Currently, consumers must choose between devices with complex installations that have restricted compatibility and devices that are only guaranteed to work while the battery has charge. A failure to track vehicles can result in consequences such as students being dropped off at the wrong address (Chung, 2019). Additionally, when an unreliable tracking system is used, the information it provides can be less helpful than not receiving any location information whatsoever. For instance, a reporter attempted to track the location of his daughter during her school day. On several occasions, her location didn't update until midway through the day (Ricker, 2018). Instead of providing reassurance, the device caused grief. With this in mind, our group has sought to build significant reliability into our device. By utilizing solar panels, our device harvests its own energy and stays powered without the need to be recharged by a human. Vijay Raghunathan and his colleagues at UCLA (2005) claim that the biggest consideration for solar powered technologies is the duration for which a device is to be in operation. Since our device is intended to run indefinitely, my capstone group and I have designed our product to produce more energy than it consumes.

Low power electronics are key enabling technologies for this project. As electronics fabrication has improved, circuits have decreased significantly in size (shown in Figure 1) and power draw. Makimoto and Sakai discuss in their paper, "Evolutions of Low Power Electronics and its Future Applications" (2003), how these improvements have led to more nomadic devices. They define a figure of merit for such devices as being equal to $\frac{Intelligence}{Size \times Cost \times Power}$. Since our device seeks to eliminate the need for external power, it would have a very large figure of merit with respect to this equation. As seen in Figure 2, our final deliverable will be a module that contains a GPS receiver to acquire location data, a microcontroller to process data, a radio-frequency transceiver to send GPS data, a battery to power the system, and a solar panel to maintain charge within the battery. We believe that the simplicity of our device contributes to its utility. Without the need to connect to an external power supply, our device can be mounted anywhere with sufficient surface area (1 square foot). This means that our product can be used to track many different types of vehicles.

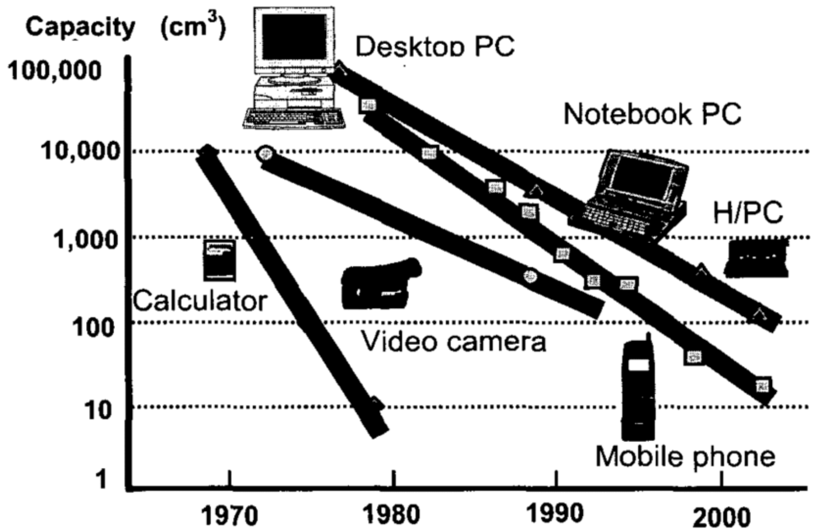

Figure 1: Increased Spatial Efficiency of Computers

As manufacturing technologies have improved, computers have become both smaller and more powerful.

(Makimoto & Sakai, 2003, p.2)

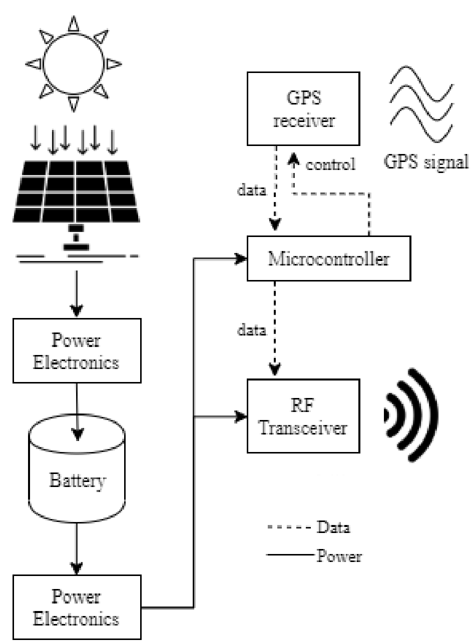

Figure 2: Block Diagram of Device

Solar energy is collected and used to charge a battery, which powers our logic and transceivers. (created by my capstone team)

Commercially available devices do not offer the same versatility as our product. Off-the-shelf GPS trackers that are designed to run for a long time must be connected to the electrical system of a vehicle. This means that different vehicles would require different versions of the device. Additionally, the connection between an internet-enabled device and the electrical system of a vehicle can introduce security vulnerabilities. It has been shown that certain vehicles with internet connectivity are able to be controlled by cyber-intruders (Greenberg, 2015). In some cases, hackers are able to remotely shut off a car, putting its inhabitants in physical danger. By retrofitting a previously offline vehicle with an internet-enabled device, many modern tracking devices are unintentionally introducing potential cyber-threats. Our device eliminates the possibility of such intrusions by decoupling the electrical systems of our tracker and its vehicle. With the two systems electrically isolated, a hacker would have no way of controlling the car through our device.

STS Topic: Cybersecurity and Privacy Concerns in Location Tracking Devices

According to the researchers at the CSIRO ICT Center in Australia, 14 adults are made victims of cyber-attacks every second (Jan-Jaccard & Nepal, 2014). Additionally, embedded processors, which are used in low-power devices such as our GPS tracker, often have significant security vulnerabilities due to their limited processing power (Jan-Jaccard & Nepal, 2014). Thus, many of the computers used for location tracking are unable to adequately defend against hackers; therefore, it is not clear whether the added benefits of expanding location tracking to more vehicles outweighs the cyber threats it opens up. Any location data connected to a person—even if it is intended to be used solely for their work—can be used to link an individual to a church, school, home, or protest (O'Keefe, 2018). As discussed by Michael and Clarke (2013), the ability to extract personal information from individuals using location means that such data collection is deeply intrusive into privacy. Thus, there is clearly a need to find a compromise between using GPS data to augment the utility of an industry and protecting the information of individuals.

Amanda O’Keefe, a privacy, technology and intellectual property lawyer, proposes several steps that can be taken to better protect personal data. She claims that transparency in GPS data collection can better inform consumers as to what data is being shared. This can allow for users to selectively disable certain location features. Additionally, she discusses how companies can practice “data minimization” by only collecting pertinent location data and avoiding collateral data that could compromise the privacy of their users (O’Keefe, 2018). For example, if a shipping company wanted to track the location of their packages, they could minimize their data collection by only recording the position of their employees during the hours of their shift. I believe that a useful alternative to this approach is data decoupling, in which the data that is being collected is not directly associated with a particular individual. Data decoupling is implemented in our tracking device because the tracker itself is attached to a vehicle, not a person. For example, if a van rental company were to use our product to track their fleet, they would only know the location of their customers while they were in the vehicle. Once the rental period ends, the location tracking stops because the customer is no longer in the vehicle. Additionally, the company could increase their privacy protection by associating the vehicle with a customer ID or confirmation number; therefore, the personal information of a customer wouldn’t be directly attached to their car’s location.

Another approach to this issue is to consider whether or not location tracking devices are necessary. As discussed in “Towards an Integrated View of Technology”, engineers must envision the consequences of a device before introducing it into society (Neeley, 2011). This paper discusses the idea of "thintelligence", the action of creating novel technical inventions and releasing them into society without considering their ethical implications. If modern-day companies act "thintelligently" and incorporate GPS tracking into many human activities, perhaps it is up to society itself to regulate what data we allow to be collected. One group that has strictly controlled the introduction of new technologies into their lives is the Amish. As discussed in "Look Who's Talking" (Rheingold, 1999), the Amish community is quite strict with what technology they bring into their lives. While many outsiders believe that the Amish are strictly against innovation, Howard Rheingold uncovered that they are simply against devices that encroach upon their way of life. Perhaps this techno-selectivity employed by the Amish could combat the pervasiveness of location tracking within our society. If we decide to reject certain technologies that we deem overly-invasive, we may be able to influence the development of GPS enabled technologies in order to attain a better balance between utility and privacy.

Conclusion

As discussed above, the deliverables of my technical project are functioning self-powered GPS tracking devices that can transmit data to a common source. This receiving source will then be able to visually display the collected location data in real-time. My STS research seeks to understand how to connect devices to the internet without creating harmful cyber-vulnerabilities or exposing private information. I believe that if this technical project were to be professionally implemented and made available to the public at a reasonable price, many different industries and individuals would have great benefits. With simple installation and vast compatibility, our modules could be deployed on a multitude of vehicles that were previously untracked. This could result in increased security and productivity within businesses. Also, accessibility to reliable tracking technology could open up new opportunities in research, such as tracking the activity of heavy machinery within construction sites.

References

Chung, J. (2019, August 23). Parents will be able to track NYC school buses with an app. *New York Public Radio*

El Khoury, F. (2018). Building a dedicated GSM GPS module tracking system for fleet management: Hardware and software. Taylor & Francis.

Fliev Maia, R., Netto, I., & Lan Ho Tran, A. (2017, December 25). Precision agriculture using remote monitoring systems in Brazil.

Greenberg, A. (2015, July 21). Hackers remotely kill a Jeep on the highway-with me in it. *Wired*

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. doi: 10.1016/j.jcss.2014.02.005

Makimoto, T., & Sakai, Y. (n.d.). Evolution of low power electronics and its future applications. *Proceedings of the 2003 International Symposium on Low Power Electronics and Design, 2003. ISLPED 03.* doi: 10.1109/lpe.2003.1231823

Michael, K., & Clarke, R. (2013). Location and Tracking of Mobile Devices: Überveillance Stalks the Streets. *Computer Law and Security Review: The International Journal of Technology and Practice*, 29(3), 216 - 228.

Neeley, K. A. (2011). Toward and Integrated View of Technology. In *Technology and Democracy: A Sociotechnical Systems Approach* (pp. 37–45). San Diego, CA: Cognella.

O'Keefe, A. (2018, February 6). Balancing the benefits of location data with privacy protection. *International Association of Privacy Professionals*

Raghunathan, V., Kansal, A., Hsu, J., Friedman, J., & Srivastava, M. (n.d.). Design considerations for solar energy harvesting wireless embedded systems. *IPSN 2005. Fourth International Symposium on Information Processing in Sensor Networks, 2005.*, 457–462. doi: 10.1109/ipsn.2005.1440973

Ramadan, M. N., Al-Khedher, M. A., & Al-Kheder, S. A. (2012). Intelligent anti-theft and tracking system for automobiles. *International Journal of Machine Learning and Computing*, 88–92. doi: 10.7763/ijmlc.2012.v2.94

Reingold, H. (1999). Look who’s talking. *Wired*, *7*(01), n.p. Retrieved from https://www.wired.com/1999/01/amish/

Ricker, T. (2018, October 31). Invoxia GPS tracker review: Longevity and range from a new kind of network. *Vox Media*

Sheets, D. (2019, January 2). Architecting cybersecurity into embedded systems. *Armed Forces Communications and Electronics Association*