Thesis Portfolio

Presented to

The Faculty of the
School of Engineering and Applied Science
University of Virginia

In Partial Fulfillment
Of the Requirements for the Degree
Bachelor of Science in Computer Science

By

John Szumski

May 4, 2010

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Wireless communication systems are poised to invade almost all aspects of society in the near future as customers encourage engineers to create products that connect together and to the digital world at large. The primary driver of this newfound use of short-range wireless transmissions is the explosion of the smartphone market and its inclusion of the pervasive Bluetooth protocol. Tracking the Bluetooth signals from the phones of car passengers facilitates personalized and automatic choices for music, radio, and temperature by the car itself without any interaction from the driver, which greatly reduces driver distraction and improves safety. The inclusion of Radio Frequency Identification (RFID) chips in next-generation currency, documents, and retail goods foreshadows a drastically interconnected future that will deliver excellent benefits at the expense of important privacy expectations. Specifically, the creation of an RFID-enabled U.S. passport increases the document's anti-counterfeiting protections, but exposes the holder to wide array of security risks. Both areas of research demonstrate the great potential of tracking objects via short-range wireless communication, but also highlight the unique privacy concerns system designers must consider.

Daily, Americans spend a significant portion of time in automobiles, predominantly commuting or traveling, and improving that experience provides a large benefit to society. Driver distraction is a leading cause of car accidents, and the car software system aims to help this problem by allowing the car to make many common choices automatically. Each rider in the car registers a personalized profile to his or her mobile phone that includes preferences for music artists, radio stations, and indoor temperature. As users enter or exit the car, the software will update its environment choices to options that please the most passengers. An in-car display informs the user of the current choices and allows for the override of incorrect or undesirable ones.

A prototype system employing four Bluetooth sensors was installed in a Honda Civic for real-world testing. Riders' mobile phones were successfully identified in the car with 100% accuracy and placed in the correct seat location with roughly 90% accuracy. A lack of resources precluded extensive tests of driver distraction rates, but informal testing found a decrease in the number of required interactions with the music or climate controls. The development of successful prototype system validates the use of short-range Bluetooth signals to track riders in an automobile and provides a foundation for future uses of personal profiles for car configuration.

The fast pace of RFID adoption across a variety of industries has the promise of faster travel times and more efficient supply chains, but privacy concerns have largely been left behind. Fear mongering is rampant in the media about RFID security, and it is important to understand an RFID chip's technological capabilities and limitations. These background topics are explored and connected to a case study of the new U.S. e-passport, which includes a mandatory RFID chip. Because citizens are forced to accept the new passport in order to travel, it is essential that the public be informed of technical safeguards, legislative protections, and behavioral changes they can make.

Academic security research and government literature were consulted to survey the current state of RFID technology. A variety of proof-of-concept attacks have been published that detail methods to steal private data from an e-passport or track its holder within an airport, train station, or hotel. The government acknowledges that current legislation does not sufficiently protect the government use of RFID data, but does not make specific suggestions for future protections. Security researchers have also discovered non-technical actions, such as increasing the passport's shielding, that citizens can take to protect themselves if they are issued an e-passport. The new U.S. passport is an excellent case study because it exemplifies attacks and defenses that also apply to almost all implementations of RFID technology.

Innovative uses of wireless communication technology can drastically improve society, but are not a panacea for businesses or customers. The same Bluetooth signal that improves driver safety can also be surreptitiously used to track car passengers as they move around the streets of their community. Uses of any specific wireless protocol can usually be generalized to work with all wireless types, which adds an interesting dynamic to beneficial and malicious research in the wireless field.

Automatic Adaptation Of A Vehicle's Environment For Its Current Occupants By Mobile Phone Triangulation

A Technical Report
In STS 4020

Presented to

The Faculty of the
School of Engineering and Applied Science
University of Virginia

In Partial Fulfillment
Of the Requirements for the Degree
Bachelor of Science in Computer Science

By

John Szumski and Matt Beattie

April 26, 2010

On our honor as University of Virginia students, we have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments in the Undergraduate Thesis Manual.

Signed ________________________________ Date ______________________
John Szumski

Signed ________________________________ Date ______________________
Matt Beattie

Approved ________________________________ Date ______________________
Mark Sherriff
Department of Computer Science

TABLE OF CONTENTS

Automatic Adaptation of a Vehicle's Environment for its Current Occupants by Mobile Phone Triangulation

John Szumski, Matt Beattie, and Mark Sherriff
Department of Computer Science
University of Virginia
{ajs7c, mgb4d, mss2x}@virginia.edu

Abstract

The ubiquity of Bluetooth technology in portable computing, primarily mobile phones, opens the door to a number of interesting applications that use it for identification purposes. We have created an in-car software system that automatically sets car preferences, such as the preset radio stations or indoor temperature. These settings are chosen from a pool of preferences for all current riders, who are identified by a Bluetooth-enabled device on their person. When possible, the car will make choices that attempt to please the majority of riders in the car, deferring to the driver's preferences otherwise. The automatic nature of the system eliminates the need to perform common entertainment or climate-control configuration, which drastically cuts driver distraction and improves safety. If a collision does occur, our system enables the car to automatically send important medical data about the current passengers to first-responders to improve their on-the-scene care.

1. Introduction

As the market penetration of smartphones, wireless computing devices, and in-dash digital entertainment systems expands in the next decade, a new market will develop for services that integrate these discrete digital systems into one unified system [1]. Many faults of the current driving experience could be improved or eliminated entirely by connecting the myriad of devices present in the modern car. We envision using software to eliminate driver distraction, increase enjoyment of a car ride for the group of passengers as a whole, and raise survival rates of automobile crashes by improving paramedic's knowledge of the crash victims.

The automobile is one of a few products that have a daily impact on the lives of a majority of Americans. Excluding a few of the largest cities in the country, mass transportation is not a viable option for commuters, which leads to a large reliance on cars to commute to work, run errands, and travel long distances. Because of the sheer amount of time spent behind the wheel or in the passenger seat, even small improvements to the overall car environment can lead to a large net positive outcome when spread across the whole population. The National Highway Traffic Safety Administration estimates over 515,000 car accidents occur in the U.S. each year due to driver distraction alone, and 5,870 of those accidents were fatal [2]. Improving survival rates by only five or ten percent would still save many lives and reduce the severity of post-accident injuries.

We have created an integrated digital entertainment system that will run on the in-dash navigation computers found in many cars today. Our new system provides a personalized experience tailored to the current occupants. Passengers create a customized profile to store preferences for trips in the same car. When their Bluetooth-capable device, usually a mobile phone, is detected in the car, it is matched to the passenger's profile. During a ride, the system takes into account the choices of all the current occupants and makes a fair decision for the entire group. It also features a graphical user interface (GUI) that allows the user to view or override these preferences and displays an overview of the car with each passenger's position clearly marked.

For our first version of this system, we have chosen to begin with preferences for air temperature, radio stations, and artists for a music playlist. However, future work could expand our system to any number of preferences, such as disabling airbags for young children or the ability to unlock the car when the driver's mobile phone comes within a specific range.

This paper is organized as follows: Section 2 investigates related work to car software systems and Bluetooth location technology. Section 3 describes the flaws we have found in today's automobiles and their impact on safety. We then present a detailed, technical analysis of how we designed and implemented the software and hardware of our system in Section 4. Section 5 considers the ethical and social issues that our system raises, focusing primarily on user privacy. Section 6 describes possible areas of focus for future work on our system. Finally, Section 7 summarizes our design and results.

2. Related Work

Research has focused on the use of Bluetooth technology for location sensing, however most efforts have produced inconclusive results. Software companies and car manufacturers have also developed systems that integrate mobile phones with car computer systems, but predominantly only use Bluetooth for hands-free calling. Presently, current products do not combine the two areas of research.

2.1. Microsoft Auto & Ford SYNC

In an effort to bridge the gap between phones and navigation systems, Microsoft began a partnership with the automotive industry to develop Microsoft Auto [1]. Microsoft's motivations are clear: the U.S. Department of Transportation found that Americans spend more than 500 million hours in their vehicles per week. In addition, 73 percent of mobile phone users talk on their phones while driving [1]. Microsoft has entered the market with a strong focus on improving the safety and efficiency of using a mobile phone in an automobile.

Microsoft Auto is based on Windows Embedded CES 6.0 R2, Microsoft's embedded operating system [1]. It provides the underlying operating system for Fiat Blue&Me and Ford SYNC. Auto offers device driver support and the building blocks that developers can use to create a range of features. It uses Bluetooth to connect users' mobile phones with the car's navigation system.

Ford SYNC is a well-known implementation of Microsoft's Auto software. SYNC provides the user with a wide array of features, but its primary one is hands-free calling while driving. Drivers are able to access their mobile phone's options and phonebook using the navigation system's interface or by voice-activated control. In addition, SYNC will also intercept and read incoming text messages, allowing the driver to continue watching the road instead of reading a screen. Ford SYNC supports multiple phones, provided that each is Bluetooth-enabled. Starting in 2010, all Fords will come with SYNC installed standard [1].

2.2. Atlantis: Location Based Services with Bluetooth

Ye at Brown University created a context aware application using a network of Bluetooth sensors [3]. His application provided a location-based service using triangulation. The motivation behind this application is to take something that everyone already has – a Bluetooth-enabled mobile phone – and use it to replace something larger and more expensive like a Global Positioning System (GPS) receiver.

To create his network, Ye used six Cambridge Silicon Radio Class 1 Bluetooth dongles. He was granted the use of one floor of an office building to implement his system. Each of the six base stations was comprised of a Windows laptop hosting a dongle. Though most of his methods were omitted pending a US Patent application, Ye was able to produce data with a precision of about five meters in one dimension, assuming that the path was unobstructed [3].

Although this system shares the common goal of locating Bluetooth devices, Ye uses multiple base stations to cover a large area. Our system only needs to cover the area of a car interior, which allows us to use a single base station with many dongles using USB extension cables.

2.3. A Study of Bluetooth Propagation Using Accurate Indoor Location Mapping

Madhavapeddy and Tse at the University of Cambridge devised an experiment to test the accuracy of Bluetooth location mapping [4]. Their system employed multiple Bluetooth nodes and several Active Bats, which emit a Bluetooth signal

[1] http://www.microsoft.com/auto/default.mspx

at various periods. In their test, Madhavapeddy and Tse simulated an office environment by moving the bats around the nodes at various speeds.

Through a series of complex algorithms, Madhavapeddy and Tse determined that Bluetooth was a poor candidate for accurate location sensing. They noted large fluctuations in signal strengths, particularly at longer distances and at higher movement speeds, as the main hindrance to the accuracy of their Bluetooth system [4].

The Active Bats employed in this system allow base stations to only run the algorithms when active devices are in range. This differs from our implementation, which must poll for new devices, because we do not require additional software on the Bluetooth devices to trigger periodic transmissions.

2.4. Bluetooth Triangulator

Almaula and Cheng at the University of California, San Diego, recognize that while Bluetooth is already widely used for communication, rich software applications could greatly increase the functionality of Bluetooth systems [5]. For example, knowing the position of other Bluetooth devices could be useful for security and social networking applications.

The Bluetooth Triangulator experiment consisted of three master nodes, each collecting Received Signal Strength Indication (RSSI) values from a mobile device. These values represent the signal strength from the node to the device. Rather than being able to pinpoint an exact location, the Triangulator was only able to indicate a certain area in which the device was placed. The experiment resulted in a +/- 5-10 feet accuracy, which got increasingly more accurate as the distance from node to device decreased.

Almaula and Cheng cited the inaccuracy of RSSI measurements as the main deterrent to the reliability of their system. RSSI values fluctuate often, and always vary based on device manufacturer [5].

In light of these findings, we modified our use of RSSI values to consider a range of values instead of a specific target for each seat. Our algorithm judges a sensor's value relative to the values from all other sensors, not an absolute threshold.

3. A Solution to Common Causes of Driver Distraction

Our integrated digital entertainment system provides a personalized experience tailored to the car's current occupants and transmits essential medical data to first responders in the event of a collision with another car or object. Each passenger is identified by his or her Bluetooth-capable mobile phone and located within in the car by triangulation of the Bluetooth signal [6]. Every phone is tied to a previously created profile in which the rider has specified preferences for all aspects of the car environment. The system is easily expanded to almost any user-configurable function; however, we begin with preferences for the air temperature, radio stations, and artists for a music playlist.

The Linux-based software system takes into account the choices of all the current occupants and makes a decision based on a fair selection algorithm. If the driver's phone comes in range of the car sensors, he or she will have the option to have the doors automatically unlock. To address the survivability goal, a rider's profile includes any medical information that would be beneficial to a paramedic arriving at the scene of an accident involving this car. Because the system keeps track of each individual's current seat, the paramedic will be able to more effectively triage the passengers by knowing where the rider with the most urgent pre-existing condition is sitting. Triage information is shown on the in-dash display when the car's collision sensors are triggered and could be transmitted to a 911 operator similar to the OnStar communications system. During normal operation, the display shows an overview of each passenger's location, the currently playing music selection, the temperature, and other statistics about the system.

Drivers and passengers are safer and have a better experience because of this feature . The key benefit is increasing driver independence from entertainment system configuration because many choices are made automatically. The chances of an accident occurring are reduced because the driver can keep his or her eyes on the road instead of fiddling with the knobs on the entertainment console [2]. The passengers also benefit from the fairness quality of the selection algorithm; the system will not make decisions that do not benefit the largest number of riders. Accident statistics for cars utilizing our system should show a drop in the number of accidents and fatalities because of the improved safety characteristics.

4. A Technical Implementation to Reduce Driver Distraction

The project was split into three main deliverables to make it easier to manage. First, a database and web interface was needed to allow the user to enter information such as their name, Bluetooth MAC address, preferences, and medical history. Second, we designed a graphical interface that provides the current riders' information and options about the system. Third, an automated phone locator was developed which used the car's Bluetooth sensors to determine the identity and location of the passengers.

4.1. Hardware and Software Design

In order to simulate an in-dash navigation system, we used a Lenovo X40 laptop running Ubuntu Linux. We chose this because it has a small screen and relatively low computing power, and therefore most representative of the system we were attempting to emulate. We also were highly interested in using the `hcitool` command, which is included with Ubuntu by default. This command interfaces with any Bluetooth devices attached to the computer, and provides tools for checking RSSI and link quality (LQ) values, as well as scanning visible Bluetooth devices in discovery mode. It also allows for multiple Bluetooth sensors (also referred to as dongles) to be connected at the same time, which is essential to any system that requires triangulation.

In order to accurately identify and locate all the passengers in the vehicle, we chose to implement a system of five Bluetooth sensors in specific locations throughout the car. Four would be placed in each of the corners of the vehicle, which allowed each sensor to cover a single seat. See Figure 1 for a top-down view of precisely where in the car we placed the Bluetooth devices. We encountered high variability in the reported RSSI values from these sensors, which prevented a true triangulation calculation from delivering accurate results within the footprint of the car. Instead, we modified our design to match each sensor with the seat closest to it. As an added benefit, the change reduced the computational overhead of our locator algorithm.

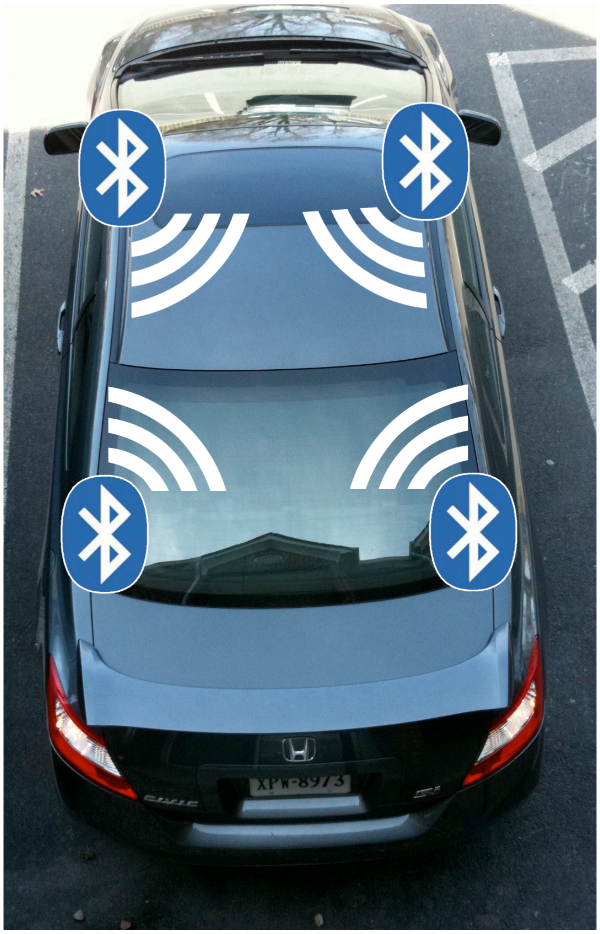

Figure 1. Position of Bluetooth sensors in the car.

4.2. Database and Web Interface

Based on our design, the Bluetooth system only searches for and identifies individuals who have entered their Bluetooth MAC address into a profile. This creates an opt-in program where users are required to give consent before our system can track them. We created a basic profile creator and editor using PHP and MySQL that stores the preference data our application will use.

We designed the interface to be accessed two different ways. The car itself can be configured as a Wi-Fi hotspot, allowing riders to access the system via any web-capable device within range. Ideally, we envision a situation where the car is parked in a garage or driveway, and anyone in the house can access the interface before going on a trip, rather than wasting time at the beginning or during the ride. If this option is unavailable or undesirable, the profile creator can be accessed by a web browser on the in-dash computer.

4.3. Graphical User Interface

We developed the GUI using the Swing toolkit for Java. The interface simulates a real-world display with physical buttons used for input. In our implementation, clicking on these virtual buttons would represent pressing the buttons on an actual navigation system. The inside frame (see Figure 2) represents the actual screen of the in-dash system, and would change depending on which buttons were pressed.

The buttons on the left side of the screen are used to navigate between the top-level sections of the application. The status of the current riders is shown visually on the "Car" screen. The "Climate" section displays the current indoor temperature and the desired temperature as calculated from each rider's preference. Audio options can be set under "Radio" and "Music", but initially the system makes a choice that pleases the majority of riders. "Settings" allows the driver to set options for the system.

Each top-level section has unique functions that are mapped to buttons on the right side of the display. Because the buttons labels are drawn in software, we can easily change their function to suit the current top-level section we are displaying. For example, the same button can increase in the desired temperature under the "Climate" section but also move to the next track under the "Music" section.

4.4. Identity and Location Algorithm

Determining the location and identity of all of the current passengers required a mix of hardware and software. Once the Bluetooth sensor infrastructure was in place, we designed an algorithm to search for an occupant using each sensor and return their seat if he or she was found.

Given a list of all of the Bluetooth MAC addresses in the profile database, the system first needed to determine which riders are present from our pool of profiles. We used a dedicated fifth Bluetooth sensor that was stationed in the middle of the car to continuously scan for new riders. Using this sensor, we were able to split the long pool of profiles into *active* and *inactive* profiles as they were found by the scan. This sensor would periodically search through the *inactive* list, and add any mobile phones it found to the *active* list.

The algorithm was as follows:

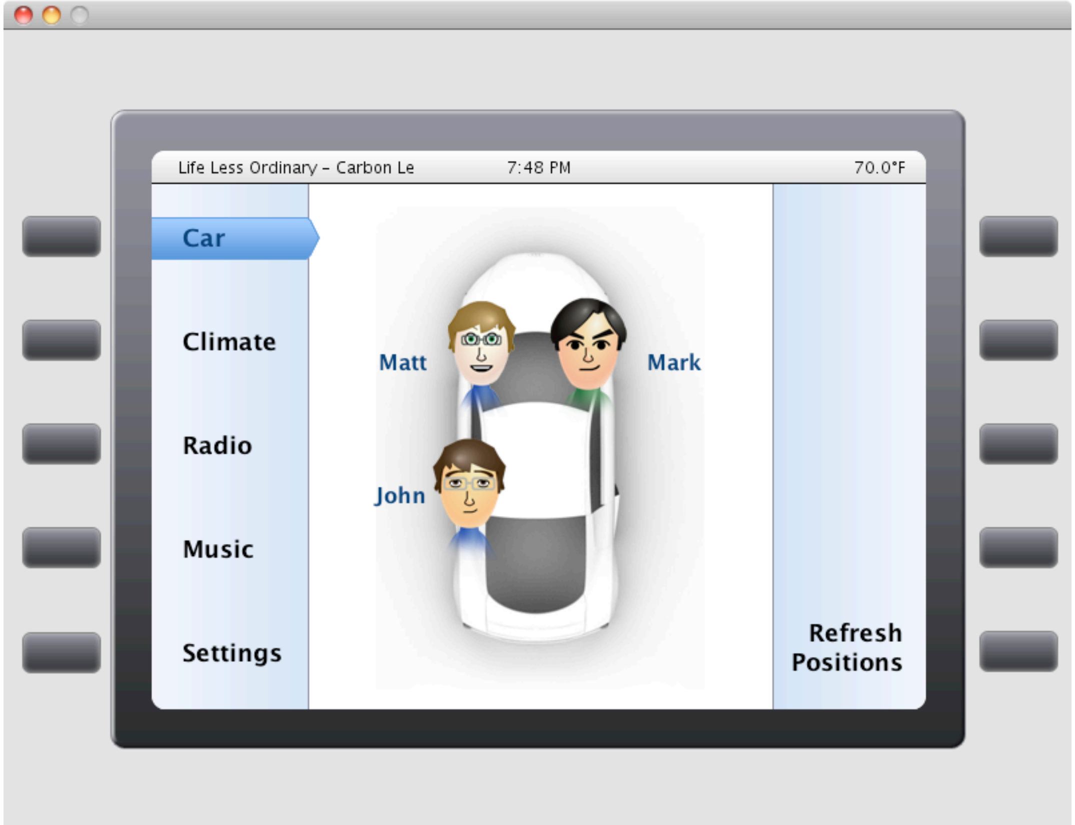

Figure 2. The main section of the system display.

```
For each MAC address in database:
     Get RSSI values from each sensor
     Use values to determine location
     Search inactive for new riders
```

After testing multiple approaches, we settled on an easy, but accurate algorithm for determining the locations of the mobile phones based on the returned RSSI values. Simply placing the occupant at the seat nearest the sensor that returned the lowest RSSI value, which indicates the strongest signal at that sensor, delivered the most accurate location.

4.5. Testing and Problem Resolution

Working with the Bluetooth signals and sensors was arguably the hardest part of our design process. Bluetooth RSSI values always fluctuate greatly and vary based on the device or sensor manufacturer. Therefore, we had to find a way to normalize the values that the system returned. Additionally, the maximum range for Bluetooth is about thirty feet, which was far too large for our sensors to notice any drop in an RSSI value. Because we were working with the inside of a car, which is roughly a six feet by five feet, we needed a way to limit the sensor's reception strength in order to return more accurate results.

Initially, we simply covered the devices with aluminum foil, in an effort to create a Faraday's cage to block some of the incoming signal. While this limited the signal strength at distances over ten feet, it was not effective enough to discern a difference between readings at one and five feet, the essential range within a car.

Next, we investigated hardware modifications that would help limit the signal strength. We found that the Bluetooth antenna was conveniently located at the top of the sensor's printed circuit board (PCB). We attempted to cut the antenna in half, but could not without damaging the PCB itself. Failing that, we decided to drill straight through the PCB where the antenna connects to the rest of the board (see Figure 3). Disconnecting the antenna connection limited the sensor range to roughly 5 feet, a perfect distance for use in a car.

Once we had successfully limited the range of the Bluetooth sensors, we ran extensive tests to ensure that the software and hardware were integrated correctly, and that the system returned the correct seat for each passenger. Once we placed the sensors in the car, we tweaked the sensor locations by a few inches to normalize the RSSI values returned.

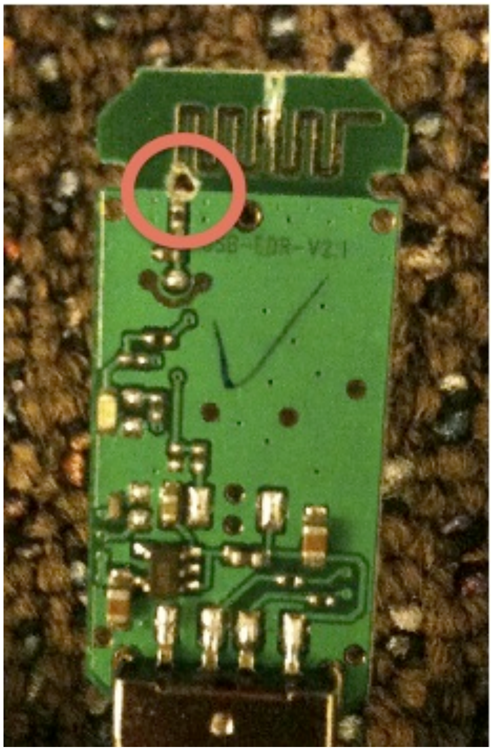

Figure 3. The Bluetooth sensor's circuit board with antenna trace disconnected (shown in red).

5. Ethical Concerns

While our car entertainment system would provide many benefits to society, we realize we must consider a few professional and ethical issues. First, we will be deliberately tracking people using their mobile phones. This could raise a few privacy-related concerns; however, the system is only able to identify and track people if they have registered their phones using the car's web application. This way, users are essentially giving their consent in an opt-in system to having their position tracked and monitored.

A second and more important issue is the security of users' medical information. While providing first responders with relevant medical information can be very beneficial, this information is often very private and confidential. Existing legislation, particularly the Health Insurance Portability and Accountability Act (HIPAA), defines precise policies concerning medical information [7]. Noting these laws, it is important that we be very careful in storage and transmission of medical data.

Connecting our software to the car's internal computer, while outside of the scope of this first version, is the logical next step to a car software system. If this step is taken, there is a risk of third-party software affecting the car's internal systems, negatively impacting safety or functionality. For example, we envision a door unlock feature, which would unlock the car's doors when the driver gets within a range of the sensors. While this feature is certainly desirable, there are certain cases where the driver might not actually want this to happen, perhaps if his or her phone is stolen. Our system cannot identify the person in possession of a particular mobile phone; we can only sense the phone's presence. Thus, we may decrease the security of the car by including a door unlock feature.

6. Future Work

Tighter integration with the onboard car computer system is logical point of expansion for this system. Currently our application only simulates any direct effects on the car's computer; however, the ideal scenario would be to actually embed the application in a real in-dash computer hooked directly to the car's climate controls and sound system. We do not possess the automotive electronics skills to safely create a fully connected system, thus we leave its realization to future researchers.

An easier route for expansion is to increase the user preferences we support. Air temperature, radio stations, and music artists comprise a representative selection of common car features; however, with the infrastructure already in place, it would be simple to add new preferences. For example, seat inclination, legroom adjustments, sound volume, or airbag toggling quickly come to mind. With the addition of each new preference, the safety of the car will improve as more configuration tasks are completely automatically.

7. Conclusion

Driver distraction is a widespread problem that results in many accidents every year. While some forms of distraction, for example using a cell phone, are voluntary, others are more difficult to avoid. Interacting with the controls of the car in order to optimize the entertainment and climate controls is much less preventable.

In response, we designed and built a system to automatically set these preferences for the occupants of the car. The application identifies the passengers and their seat location and then makes a fair choice for radio, music, and temperature. We improve the driving inexperience because the driver spends less time pressing buttons and more time watching the road. Ultimately, this will lead to more attentive drivers, and eventually lower the number of driver distraction accidents per year. In the event of a collision, the system will be able to send medical information and seat location of all the passengers to first responders, resulting in better on-the-scene care and higher survivability rates for patients.

Our combination of hardware and software takes an existing technology in widespread deployment and uses creative software to increase its value. It addresses a common problem that endangers today's drivers, while also providing a new and interesting way to experience a car ride.

8. References

[1] Microsoft, "Microsoft Auto 3.1 Platform Overview," Retrieved from http://www.microsoft.com/auto/ma.mspx, Novemer 2008.

[2] NHTSA. "Traffic Safety Facts: An Examination of Driver Distraction as Recorded in NHTSA Databases," Retrieved from http://www-nrd.nhtsa.dot.gov/Pubs/811216.PDF, October 2009.

[3] Ye, Jason Yipin, "Atlantis: Location Based Services with Bluetooth.," Retrieved from http://www.cs.brown.edu/research/pubs/theses/ugrad/2005/jye.pdf., 2005.

[4] Madhavapeddy, Anil and Alastair Tse, "A Study of Bluetooth Propagation Using Accurate Indoor Location Mapping," Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.3970&rep=rep1&type=pdf, 2005.

[5] Almaula, Varun and David Cheng, "Bluetooth Triangulator," Retrieved from http://cseweb.ucsd.edu/classes/fa06/cse237a/finalproj/almula.pdf, 2006.

[6] Bluetooth SIG, Inc., "Core Specification v2.1 + EDR," Retrieved from http://www.bluetooth.com/NR/rdonlyres/F8E8276A-3898-4EC6-B7DA-E5535258B056/6545/Core_V21__EDR.zip, July 26, 2007.

[7] U.S. Department of Health & Human Services. "The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information," Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/, December 15, 2008

Privacy Implications Of RFID-Enabled Documents

A Research Paper
In STS 4020

Presented to

The Faculty of the
School of Engineering and Applied Science
University of Virginia

In Partial Fulfillment
Of the Requirements for the Degree
Bachelor of Science in Computer Science

By

John Szumski

April 26, 2010

On my honor as a University of Virginia student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments in the Undergraduate Thesis Manual.

Signed ________________________________ Date _____________________
John Szumski

Approved ________________________________ Date _____________________
Catherine Baritaud
Department of Science, Technology and Society

TABLE OF CONTENTS

ABSTRACT

Driver’s licenses, passports, and retail goods are now outfitted with radio frequency identification (RFID) chips that wirelessly identify them as part of the growing interconnectedness the digital revolution has wrought on society. The downside to this wireless capability is that an RFID tag is always transmitting its identity, which means that it has instantly become a very effective tracking device. RFID chips are a direct threat to privacy, and safeguards must be put in place to protect individuals from unintentional disclosure of private data via RFID tags.

RFID-enabled U.S. passports provide an excellent framework to analyze areas where privacy or security is at risk because of the numerous proof-of-concept attacks that already exist. Researchers have used the knowledge learned from these attacks to craft defensive RFID-blocking technology, draft proposed privacy legislation, and recommend steps everyday citizens can take to protect themselves.

The issues raised by e-passports will only become more important as time progresses because their adoption by the U.S. will encourage other nations to follow suit to remain competitive and secure. Once the technology is deployed, it must withstand 10 years of sophisticated attacks supported by an ever-increasing amount of computing power. If privacy safeguards are not proactively applied, the personal data of millions of Americans will be stolen in the coming decade.

AN RFID PRIMER

The digital lifestyle has revolutionized the way Americans communicate, discover new music and television, buy plane tickets, withdraw money, and perform countless other everyday tasks, simplified by the move to digital systems (Brito, 2004, pp. 7-15). With this added convenience comes the threat that digital data can be easily copied, stolen, or deleted entirely. The revolution's next takeover target is the ordinary paper document. Everyday items like driver's licenses, passports, and groceries contain radio frequency identification (RFID) chips, commonly referred to as "tags", that wirelessly identify the object; an improvement on the optical bar codes used to identify most items on store shelves today (Garfinkel, Juels, & Pappu, 2005, pp. 34-37). The downside to this wireless capability is that an RFID tag always transmits its identity, transforming it into a very effective tracking device. Proponents of the RFID initiative will point to the limited range of the wireless signal or the encryption of the broadcast, however trackers easily overcome both of these limitations (Carluccio, Lemke-Rust, Paar, & Sadeghi, 2007, pp. 391-393).

A case study of RFID-enabled U.S. passports provides an excellent framework to analyze areas where privacy or security is at risk. Identification of these weaknesses facilitates discussion of existing and proposed fixes. Technical barriers may block the attack, legislation can protect the private data or shield the victim of the attack, and behavioral changes allow all passport owners to take action themselves. Each separate recommendation on its own is not totally effective, but one hopes that a few approaches taken together will reduce the risk of the attack to an acceptably low level.

MORE THAN JUST A WIRELESS BARCODE

RFID technology is widely deployed throughout the developed world in a variety of different applications. Frequently it tracks items as they move through various stages of a distribution chain (Government Accountability Office, 2005, p. 2). Presently, distributors affix tags to each pallet of goods to keep costs down, but as prices fall below five cents per tag, every individual item will have its own RFID chip. Distribution systems are a perfect fit for the technology because they commonly have well-defined entrances or exits that are easily covered by a small number of RFID readers. For example, if goods from a certain warehouse leave via truck, a reader placed above the loading dock will record each pallet as it moves from the warehouse to the vehicle.

Once tags embedded in individual products become commonplace, RFID proponents have identified many exciting potential uses in the retail sector. Wireless price checkers instantly come to mind, and more sophisticated displays may be placed around the store that allow you to compare features or prices between two competing products. Passing the entire cart under a single RFID reader simplifies the checkout process by eliminating the tedious scanning of black and white bar codes. Although many of these technologies have not yet been deployed, RFID supporters and detractors anticipate widespread use in the near future (Brito, 2004, 7-15).

The same tracking capability used for shipment tracking benefits customer-facing applications as well. The E-ZPass toll collection system quickly identifies and charges cars as they pass through a toll plaza at highway speeds. Concerned pet owners can have an animal tagged with an RFID chip just below its skin to allow an animal shelter to return a lost pet to its owner. Newer automobile keys also include RFID authentication chips within the key fob that prevent the car from starting with a copied key. Each of these implementations delivers a very tangible benefit previously unavailable to consumers nationwide (Garfinkel, Juels, & Pappu, 2005, pp. 34-37).

Currently, students in the Spring, Texas school system participate in a prototype RFID tracking system designed to prevent the kidnapping of a child walking home from school. Although no children were kidnapped before the system was created, it serves to reassure parents who may not be able to meet their children at the bus stop each afternoon. Each student carries an RFID-enabled ID card that is read at each stage of the school day, much like a package making its way through a distribution center. The ID cards automatically take attendance, which provides more time for class instruction. Location accuracy lowers the time required for police to apprehend a kidnapper and provides greater safety to children across the district (Richtel, 2004, pp. 1-3).

RFID chips allow a new dimension to the function of everyday products because designers must take into account the role an individual product plays in our increasingly interconnected world. Historically, the creator of a new product would only consider the physical form and aesthetics. Barry Katz, professor of design at Stanford University, argues that designers today must extend those concerns to the entire experience of using the product: mental and physical responses to its use, its sustainable disposal, and countless other considerations. The modern world is an interconnected network of devices, individuals, and software that has become more than just the sum of its parts. Katz (2006) observes, “the line between products and their users is blurring … in the future the distinction may vanish altogether” (p. 390). RFID chips allow products to identify other objects around them and change their function to complement each other.

IMPLEMENTATION PITFALLS

The soon-to-be ubiquity of RFID chips in everyday items poses many threats to privacy. These threats are classified in two groups: those that allow an eavesdropper to uniquely identify an individual, and those that broadcast private information without an individual's knowledge. Both flaws are inherent to the basic technology used for RFID communication, however certain precautions prevent the disclosure or mitigate its consequences.

A variety of privacy threats exist in the RFID-enabled world because RFID tags transmit wirelessly and unobtrusively. Security researchers Lee and Kim posit that the biggest threat to privacy is the ability to map a unique RFID tag to a specific individual. Such a mapping permits the identification of that person's location and preferences, for example, the brand of clothing they are currently wearing, and observing the addition of a new RFID tag to a person's RFID "constellation" allows the observer to infer financial transactions (Lee & Kim, 2006, p. 2). The constellation of RFID tags contained in ones clothing or credit cards violates personal privacy in an entirely undetectable manner (Garfinkel et al., 2005, p. 38).

Even if an attacker does not have enough information to definitively match a specific tag to a specific person, private information may still leak out into the airwaves as an individual goes shopping, checks out a library book, or many other everyday tasks. Using this leaked information, a database may track purchases, preferences, and locations (Ohkubo, Suzuki, & Kinoshita, 2005, pp. 2-3).

Alarming real world examples demonstrate the dire need for appropriate RFID protections to be created. Juels (2003) posits that if high-value currency includes RFID chips to prevent counterfeiting, it may enable someone passing you on the street to determine how much money you have in your wallet without any visible sign of the scan (p 105). Garfinkel et al. (2005) use the Electronic Product Code, a digital replacement for the black and white barcode, to demonstrate potential problems with RFID deployment. These problems manifest because RFID tags do not "remember" when they are read and cannot differentiate between tag readers. Corporate privacy is at risk when a competitor can read RFID tags exiting a company's warehouse to glean confidential supply chain data (pp. 36-38).

SOCIAL CONTEXT OF RFID TECHNOLOGY SYSTEMS

The development, integration, and use of RFID technology to solve a real world problem requires the collaboration of many different groups of engineers: RFID inventors, system integrators, and developers of the real world system. Even the interaction between the technology creators and attackers attempting to exploit it requires careful consideration. These complex relationships exhibit key characteristics of the System in Context model of technological development.

System in Context models the system, its boundary with the world around it, and the engineering work that must happen to cross that boundary. The inventors of RFID technology reside in the center of the model. They have a marginal effect on the social role of their product because they only created the technology, not any specific implementation of it to solve a problem. System integrators or attackers pierce the boundary surrounding the invention and connect it to a real world use, whether it is a

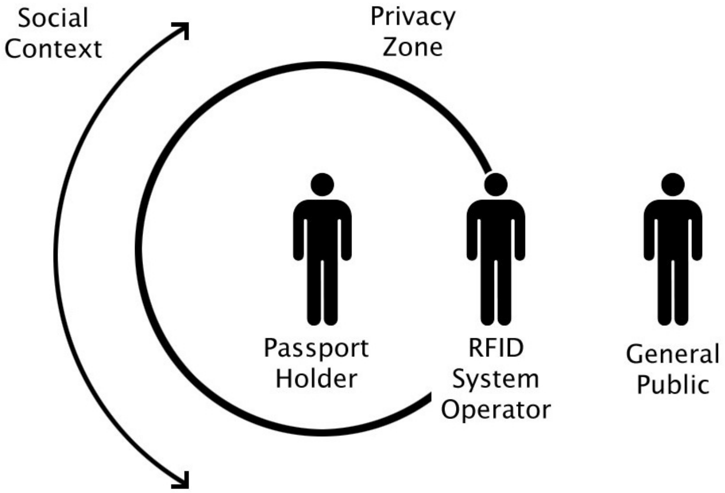

Figure 1. Social context of an RFID technology system (Szumski, 2010).

beneficial or detrimental one. It is the responsibility of those two intermediate groups of engineers to consider the social ramifications of the connection they are making between RFID tags and society (Baritaud, 2010).

It is not readily apparent why an attacker would have any concern for the well being of society; however, he or she must balance violating privacy unobtrusively without alerting authorities and also gaining as much private information as possible. Similarly, system developers who use RFID chips face a balancing act between providing a cheap and quick solution to the customer and providing one that does not put the user's personal privacy at unacceptable risk. The roles of these two separate groups are intertwined and must be modeled accurately to correctly anticipate the full effect of RFID technology and the social context that defines its use.

A CASE STUDY OF E-PASSPORTS

The inclusion of an RFID tag within the newest version of the U.S. passport is the most widespread implementation of RFID technology, yet most of the public knows little about it. It is an excellent choice for a representative study of RFID privacy implications because there is an easily demonstrated benefit to the passport's integrity as an identification document; however, the passport system also harbors security weaknesses that potentially expose the holder's private information. Although the U.S. Government uses RFID technology in 13 of its 24 primary agencies, the majority of these systems

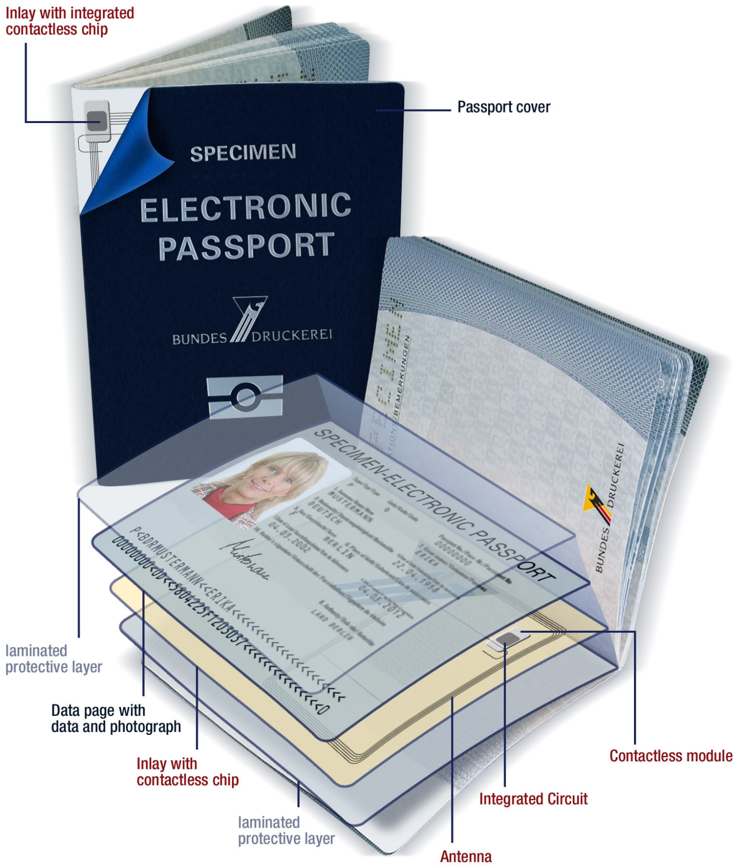

Figure 2. An exploded view of an e-passport (Bundesdruckerei, 2005).

only track shipments or other physical assets, not individuals. The State Department's E-passport program is therefore the first use of RFID tags to track individuals. The Government Accountability Office, in a report charged with ensuring government RFID implementations follow existing privacy regulations, voiced concern in the areas of confidentiality, integrity, and availability of RFID systems. In particular, the report stressed that only authorized readers or personnel should be able to read the contents of an RFID chip. The Federal Information Security Management Act and the E-Government Act of 2002 have strong protections for the use of private information, but new legislation may be necessary because the two laws govern the use of collected data only, not the technology used to collect it (Government Accountability Office, 2005, pp. 1-27).

TECHNICAL ATTACKS AND DEFENSES

E-passports, also known as Machine-readable Travel Documents, have been deployed in limited numbers in the Netherlands and Germany, but the underlying system contains numerous privacy vulnerabilities. These shortcomings can be exploited using two types of attacks: passive and active. Passive attacks permit attackers to read unencrypted data, including the holder's picture, fingerprints or iris scans, from anywhere within range of the passport (Carluccio et al., 2007, p. 393). An active attack breaks the encryption protecting the passport, and requires a significant amount of computing power to do in near-real time. Two examples of proof-of-concept passive attacks will be analyzed, and two defense proposals will describe methods to provide some level of technical protection from those attacks.

Academic security researchers Carluccio et al. (2007) have developed a proof-of-concept attack platform that passively eavesdrops anywhere passports are checked, for example airports or train stations, and reveals the holder's personal information in near real-time. While any attack that reveals passport information is undesirable, this one is particularly harmful because it occurs very quickly. Near real-time means that the computation needed to extract data from the passport's RFID chip can be done fast enough for the attacker to also make a decision about the nearby victim before the passport moves out of range. This leads to a two-pronged threat: the passport holder's private data has been stolen, but also the attacker may potentially take further action, such following the holder home from the airport, if the intercepted data meets some desirable criteria. One can envision a potential terrorist attack where a bomb explodes when an eavesdropping RFID reader intercepts data that indicates the holder is an American citizen. If acquiring the private data took many hours to complete, the data will still be lost, but the physical security of the holder is protected. A distributed network of near-real time readers would be able to pinpoint the location of a passport holder, especially if the readers were placed in passport-dense environments such as transportation hubs, hotels, or convention centers. As this proof-of-concept shows, it is within the realm of feasibility for a malicious attacker to easily track a passport holder (pp. 396-402).

In an effort to be proactive, the State Department amended the original e-passport design to limit eavesdropping by inserting a metal lining in the cover to stop the RFID signals from emanating when it is closed. While this does in some cases limit the passive attack described above, Mahaffey (2005) of Flexilis, a security consulting firm, demonstrates an alarming real-world attack that defeats the updated design. He draws attention to implementation mistakes that allow an RFID reader to access the passport's data even when its protective cover is open only a fraction of an inch. This vulnerability remains even after the State Department overhauled the security model of the e-passport in response to privacy concerns. In a dramatic video demonstration, the company rigged a disguised RFID reader and bomb to explode when the reader could sense any e-passport. The passport survived when fully closed; however, opening it only a fraction of an inch, as could happen in a purse or pocket, successfully triggered the explosive. The firm notes that RFID shielding on both covers, instead of the current front-only design, would help prevent this type of attack (pp. 1-3).

Rieback et al. (2007) have created a defensive product called RFID Guardian, a battery-powered device that serves as a middleman to judge which RFID queries should be answered by nearby RFID tags. It addresses the largest security problem in RFID technology: the tag's constant transmission of its identity to any reader that asks. This functionality is selectively locked down, and the tags will still function properly for valid uses but remain mute when queried by an untrustworthy RFID reader. The researchers suggest that the new device be integrated into an everyday object that is usually carried by an individual, such as a cell phone or PDA, to protect tags that may be sewn in to the owner's clothes or contained in his or her wallet. It improves existing security systems, which only considered a single tag, to create a holistic approach that protects the user's entire "constellation" of RFID devices. The Guardian will be able to selectively turn tags off, randomize identities, and vet unfamiliar RFID readers. Many privacy concerns focus on attacks against an individual's identity or data, but technical solutions have been restricted only a single tag. Because an RFID attack can take into account multiple tags on a person, the security approach must do the same. The RFID Guardian allows granular control to be given to the entirety of a user's RFID chips; for example the Guardian could tell your passport to only answer RFID requests if it is in range of an official Customs reader. This product would effectively neutralize the two previous passive attacks because the passport would only respond to requests for data if the user gives his or her consent, which should only happen at a Customs desk or other official checkpoint (pp. 1-10).

A more extreme approach to security employs a special RFID transmitter called a "blocker tag" that answers requests to all tags within its range, an idea similar to the RFID Guardian, but then answers with false data. Its implementation relies solely on tricking the algorithm that an RFID reader uses to differentiate two different tags. By changing the blocker tag's response to the reader, the tag can fool the reader into believing many thousands of chips are present. The real RFID tag is then lost in the flood of the numerous responses, and the eavesdropper cannot identify the individual. The effectiveness of the blocker tag hinges on its ability to flip between regular RFID operation and the spoofing mode. In an airport or other secure location, the blocker tag may set off alarms because of the large number of false passports detected, which renders it useless in the situation that most warrants its use. It may only take one irresponsible use of the blocker tag before it is outlawed, just as it is illegal to spoof a cell phone or pager. The blocker tag may be just a little too overpowered for the privacy hole it is meant to fix (Juels, Rivest, & Szydlo, 2003, pp. 103-110).

LEGISLATIVE SAFEGUARDS

Efforts to improve e-passport privacy safeguards and operational procedures should occur through the legislative process in tandem with the development of technical safeguards. Existing legislation only applies to the government's use of certain RFID data, but does not restrict the technology itself (Government Accountability Office, 2005, pp. 22-23). Consistent and responsible RFID use by the government set an exemplary model for private corporations to use when deploying their own RFID tags.

Garfinkel et al. (2005) have proposed the creation of an RFID bill of rights enforceable by federal law. Its broad scope encompasses all RFID use in the United States, including the e-passport system. The most essential right proposed is the ability to have an RFID tag removed, destroyed, or deactivated at any time if requested. Additionally, citizens should not lose other rights or incentives if they have asked to have any RFID chips removed. Although e-passports would most likely by exempted from the bill of rights because these features undermine the desire to have a universal RFID-enabled passport system, the expanded protections would significantly improve customer rights when buying retail items tagged with RFID chips (pp. 41-42).

Another proposal to improve privacy problems with RFID technology would require retailers to affix a special label to all items containing an RFID tag. Proposed legislation from the citizen watchdog group Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) would mandate that RFID-enabled products carry a special label and have provisions for the protection of user data. This label would indicate risks associated with the tag, similar to hazard labels prevalent on products today. Such a law would eliminate the threat of a stealthy adversary eavesdropping on RFID transmissions without the victim's knowledge, but it may not be sufficient because many new problems will arise as RFID readers become mobile in the future. The combined mobility of both the reader and tag will create new situations unforeseeable by lawmakers today. In the e-passport domain, the proposed law would also have a reduced impact because e-passports already contain an RFID emblem on the cover. This emblem does not convey any of the inherent risks, but this law may force that to change to help educate citizens about their new electronic passport (Lee & Kim, 2006, p. 3).

BEHAVIORAL BEST PRACTICES

Educating American citizens about the risks and benefits of RFID-enabled passports is the last of the three-pronged approach to safeguarding e-passport privacy. Simple preventative measures undertaken by everyday travelers may be effective enough to disrupt an attack regardless of a lack of technical or legislative defenses in place. Voters also have the power to elect politicians who make privacy legislation a priority.

Just as consumer spending patterns can sway retailers away from unsafe RFID practices in stores or products (Ohkubo, 2005, pp. 66-69), citizen voting patterns also hold sway over Congress and the President. Economic effects of the e-passport requirement are most likely to be felt by those in power, however it make take years for those effects to trickle through the economy. For example, RFID hassles may by the final straw that cancels a family vacation or convinces foreign visitors to avoid making a trip to America. These decisions have economic effects on all sectors of the economy, and citizens should be encouraged to vote explicitly in polls but also vote with their money to promote products or practices that safeguard their privacy.

Travelers who have an e-passport should following two simple rules to ensure their passport's security remains intact. First, the passport must always be stored in a protective case when not in use at Customs. Many travel accessory manufactures offer special e-passport cases, which incorporate a metal lining in both covers to prevent RFID signals from escaping when the passport is shut. Second, the e-passport must be stored in a way that ensures it will always remain completely closed. Mahaffey's (2005) attack shows that even an opening of only a fraction of an inch leaves the passport holder vulnerable (pp. 1-3). These two simple rules may seem trivial, but research has shown that they are enough to protect your data from many types of attacks.

Security expert Bruce Schneier (2006) recommends that everyone renew their passport before e-passports become mandatory in 2007. He notes that any demonstrated attacks are not deal-breakers by themselves, but indicate that more significant attacks may come with time. Passports are valid for 10 years, and in that timeframe technology may advance rapidly, allowing new attacks against the system. Long-term security is the most important goal. Because it is unclear how the government will react to a valid passport with a broken RFID chip, Schneier does not recommend that citizens should take action to disable the chip. Renewing before the e-passport implementation deadline buys citizens a decade to analyze the risks of RFID technology and to benefit from any advancement in RFID blocking technology during that time (pp. 1-2).

THE FUTURE FOR RISK AND DEVELOPMENT

RFID technology is widely deployed throughout the developed world in a variety of different applications, primarily for supply chain management and e-passports, to wirelessly identify objects. Individual products will include supply chain tags as the cost per tag drops, and RFID proponents have identified many exciting potential uses for these individual tags in the retail sector. The downside to this wireless capability is that an RFID tag always transmits its identity, which means that it has instantly become a very effective tracking device.

A variety of technical attacks exist to compromise RFID-enabled U.S. passports, but researchers have devised effective defense mechanisms as well. Passive attacks enable malicious users to eavesdrop anywhere passports are checked and reveal the holder's personal information in near real-time. Using this data, citizens of different nationalities could be specifically targeted for physical attack or just simply added to a tracking database. The most effective defense available to passport holders is a special RFID device that proxies requests to their tags and allows selective responses to data requests. Such a system facilitates legitimate uses of e-passports while effectively closing the gaps in privacy protection. Proposed legislation can protect the private data or shield the victim of the attack by informing them of RFID-associated risk with any objects they own. Once potentially risky tags have been found, the individual can make any necessary behavioral changes to protect his or her private data. Each separate recommendation on its own is not totally effective, but one hopes that a few approaches taken together will reduce the risk of the attack to an acceptably low level.

Although the e-passport program is still new, its effects will soon be felt by millions of travelers across the nation. The percentage of e-passports will only increase as older paper-only passports expire and must be renewed with RFID-enabled ones. Additionally, security research will continue to find new ways to attack the valuable private data contained within the RFID chips. The technology as implemented must hold up to rigorous real world attacks for its full 10-year lifespan, but that may be too long for this fast changing technology to remain secure.

BIBLIOGRAPHY

Baritaud, C. (2010, February 22). System in context model. Charlottesville, Virginia.

Brito, J. (2004). Relax don't do it: Why RFID privacy concerns are exaggerated and legislation is premature. *UCLA Journal of Law and Technology*, 8(2). Retrieved from http://www.lawtechjournal.com/articles/2004/05_041220_brito.pdf

Bundesdruckerei. (2005). Specimen ePassport, Retrieved April 1, 2010, from: http://www.bundesdruckerei.de/en/press/press_photoarchive/photoarchive_idDoc/index.html

Carluccio, D., Lemke-Rust, K., Paar, C., & Sadeghi, A. (2007). E-Passport: The global traceability or how to feel like a UPS package. *Proceedings of Workshop Information Security Applications 2006*, 391–404.

Garfinkel, S. L., Juels, A., & Pappu, R. (2005). RFID privacy: An overview of problems and proposed solutions. *IEEE Security and Privacy*, 3(3), 34-43. Retrieved from http://www.computer.org/portal/web/csdl/doi/10.1109/ MSP.2005.78

Government Accountability Office. (2005). Report to congressional requesters: Information security: Radio frequency identification technology in the federal government. Retrieved from http://www.gao.gov/new.items/ d05551.pdf

Juels, A., Rivest, R. L., & Szydlo, M. (2003). The blocker tag: Selective blocking of RFID tags for consumer privacy. *8th ACM Conference on Computer and Communications Security*, pp. 103-111. Retrieved from http://www.rsa.com /rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf

Kātz, B. (2006). Intelligent design. *Technology and Culture*, 47(2), 381-390. Retrieved from http://muse.jhu.edu/journals/technology_and_culture/v047/47.2katz.pdf

Lee, H. & Kim, J. (2006). Privacy threats and issues in mobile RFID. *Proceedings of the First International Conference on Availability, Reliability and Security*, 510 - 514. Retrieved from http://portal.acm.org/citation.cfm?id=1130967

Mahaffey, K. (2005). RFID passport implementation vulnerabilities: technical analysis. *Black Hat 2006*. Retrieved from http://www.flexilis.com/download/RFID PassportTechnicalAnalysis.pdf

Ohkubo, M., Suzuki, K., & Kinoshita, S. (2005). RFID privacy issues and technical challenges. *Communications of the ACM*, 48(9), 66-71. Retrieved from http://portal.acm.org/citation.cfm?id=1081992.1082022

Richtel, M. (2004, November 17). In Texas, 28,000 students test an electronic eye. *The New York Times*. Retrieved from http://www.nytimes.com/2004/11/17 /technology/17tag.html

Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2007). RFID guardian: A personal platform for RFID privacy management. *O'Reilly Emerging Tech Conference*. Retrieved from http://www.cs.vu.nl/~ast/publications/acisp-2005.pdf

Schneier, B. (2006, September 16). The ID chip you don't want in your passport. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2006/09/15/AR2006091500923_pf.html

Automatic Adaptation Of A Vehicle's Environment For Its Current Occupants By Mobile Phone Triangulation

Privacy Implications Of RFID-Enabled Documents

A Thesis Prospectus
In STS 4010

Presented to

The Faculty of the
School of Engineering and Applied Science
University of Virginia

In Partial Fulfillment
Of the Requirements for the Degree
Bachelor of Science in Computer Science

By

John Szumski

November 4, 2009

On my honor as a University of Virginia student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments in the Undergraduate Thesis Manual.

Signed ________________________________ Date ______________________
John Szumski

Approved ________________________________ Date ______________________
Edmund Russell
Department of Science, Technology and Society

Approved ________________________________ Date ______________________
Mark Sherriff
Department of Computer Science

TABLE OF CONTENTS

INTRODUCTION

In the technical project, we plan to develop a highly personalized car system that dynamically adapts a car's entertainment system to its current occupants. In the STS paper, I will present a loosely coupled analysis of widespread electronic tracking of American citizens. I will primarily identify situations where an individual's privacy is at risk and the preventative measures that can be taken to protect it.

BLUETOOTH-BASED CAR ENVIRONMENT CONTROL SYSTEM

(co-authored with Matt Beattie)

As the market penetration of smartphones, in-dash digital entertainment systems, and wireless communication devices increases in the next decade, a new market will develop for services that integrate these discrete components into a unified system. Many of the faults of the current United States automobile system could be improved or eliminated entirely by weaving a digital mesh between the myriad of devices present in the modern car. We envision using software to eliminate driver distraction, increase enjoyment of a car ride for the group of passengers as a whole, and raise survival rates of automobile crashes by improving a paramedic's knowledge of the crash victims.

The automobile is almost unique to the extent in which it has completely permeated the lives of a majority of Americans. Excluding a few of the largest cities in the country, mass transportation is not a viable option for travelers, which leads to a large reliance on cars to commute to work, run errands, and travel long distances. Because of the sheer amount of time spent behind the wheel or in the passengers seat, even small improvements to the overall car environment can lead to a large net positive outcome when spread across the whole population. In a similar fashion, the National Highway Traffic Safety Administration estimates over 40,000 car accidents occur in the U.S. each year, and improving survival rates by only five or ten percent would still save many lives and bring happiness to countless families.

Our integrated digital entertainment system would provide a personalized experience tailored to the car's current occupants and transmit essential medical data to first responders in the event of a collision. Each passenger will be identified by his or her Bluetooth-capable mobile phone and located within in the car by triangulation of the Bluetooth signal (Bluetooth SIG 2007). Every phone would be tied to a previously created profile in which the rider has specified preferences for all aspects of the car environment. The system is easily expanded to almost any user-configurable function, however we will begin with preferences for the air temperature, radio stations, and artists for a music playlist. The Linux-based car system will take into account the choices of all the current occupants and make a decision based on a fair selection algorithm (Krasnyansky & Holtmann, 2002). If the driver's phone comes in range of the car sensors, he or she will have the option to have the doors automatically unlock (OConnor & Reeves, 2009). To address the survivability goal, a rider's profile will also include any medical information that would be beneficial to a paramedic arriving at the scene of an accident involving the car. Because the system keeps track of each individual's current seat, the paramedic will be able to more effectively triage the passengers by knowing where the rider with the most urgent pre-existing condition is sitting. This information will be shown on the in-dash display when the car's collision sensors are triggered and could be transmitted to a 911 operator via the OnStar communications system (Chaudry et. al., 2008). During normal operation, the display will show an overview of each passenger's location, the currently playing music selection, the temperature, and other statistics about the system.

We anticipate that this innovative system will increase safety and improve the experience for the driver and passengers. The key benefit will be increasing driver independence from entertainment system configuration because many choices will be made automatically. The chances of an accident occurring are reduced because the driver can keep his or her eyes on the road instead of fiddling with the knobs on the entertainment console. The passengers also benefit from the fairness requirement of the selection algorithm; the system will not make decisions that do not benefit the largest number of riders. Appreciation for the system will spur the passengers to consider the inclusion of our software package in their next car purchase. As it becomes widespread, accident statistics should show a drop in the number of accidents and automobile fatalities because of the improved safety characteristics.

Two ethical issues must be addressed before our system can be deployed in the real world. United States law strongly protects the privacy of medical information, and we will have to ensure that we store and transmit our users' data in a secure manner. The location data we collect is also personally identifiable information that must be protected (Ye, 2005). Because our system is an opt-in tracking system, our users will not be surprised that we are tracking their locations, however they will want to know how that data will be used and stored. Appropriate privacy safeguards are important to reassure the users and convince them to continue using the software package.

John Szumski and Matt Beattie will undertake this collaborative project to develop the software and hardware for the system described above. Professor Mark Sherriff of the Computer Science department will give technical and design advice as the project progresses. We plan to implement the hardware sensors and display unit in Matt Beattie's Honda Civic as a prototype system for testing and demonstration purposes. High-level design and technical specifications will be written through winter 2009 and the software and hardware components will be implemented in spring 2010. At the completion of the project, we plan to deliver a web application that will be used for profile creation and editing, a Java application to control the display of the in-dash unit, a physical prototype of the sensors required for Bluetooth triangulation, and a technical report about the system in the Association of Computing Machinery journal format.

PRIVACY IMPLICATIONS OF RFID-ENABLED DOCUMENTS

The digital revolution has revolutionized the way Americans communicate, discover new music and television, buy plane tickets, withdraw money, and perform countless other everyday tasks that are simplified by the move to digital systems (Caprio, 2005). With this added convenience comes the threat that digital data can be easily copied, stolen, or deleted entirely. The revolution's next takeover target is the humble paper document. Everyday items like driver's licenses, passports, and groceries are being outfitted with radio frequency identification (RFID) chips, commonly referred to as “tags”, that can be used to wirelessly identify the object, an improvement on the optical bar codes used to identify most items on store shelves today (Juels, 2005). The downside to this wireless capability is that an RFID tags is always transmitting its identity, which means that it has instantly become a very effective tracking device. Proponents of the RFID initiative will point to the limited range of the wireless signal or the fact that the broadcast can be encrypted, however both of these limitations can be overcome by would-be trackers (Carluccio, 2007).

Compounding the easy availability of potential tracking data is the lack of government regulation or oversight regarding RFID emanations. Because the technology has advanced very quickly, it is already in real-world use before any thought has been given to the ramifications of its widespread deployment. Legislation should be drafted to set guidelines for the disclosure of tracking information of all kinds, not only limited to RFID chips. Social media services like Loopt or Google Latitude, both of which track their users’ locations and inform their friends periodically of their current activity, also collect highly personal data that should be protected from release or misuse. Other wireless technologies such as Bluetooth communication or wireless car tire sensors transmit signals that can be used to track an individual (Scorer 1998). Care needs to be taken when collecting, storing, using, or sharing location-based data to protect users from the service provider itself or other attackers who might subvert it for nefarious uses (Richtel, 2004).

While real-world attacks against RFID have not yet surfaced, the publication of academic attacks proves that protections need to be put in place to guard against their future development as RFID chips become more prominent. The potential for widespread tracking by a government agency is high because of relaxed privacy laws in the post-9/11 world. RFID chips are now mandatory in certain government documents, primarily the new U.S. passport, which ensures that most individuals will eventually have at least one RFID chip on their person. When mandatory chips are combined with recent academic research showing the feasibility of tracking an RFID chip, the threat becomes even more significant.

In this project I will present a case study of RFID-enabled U.S. passports and analyze areas where privacy or security are at risk. Once these weak spots have been identified, I will suggest technical barriers that may block the attack, legislation that will protect the private data or shield the victim of the attack, and behavioral changes that all passport owners can make to protect themselves. I hypothesize that each recommendation on its own will not be totally effective, but I hope that all of them taken together will reduce the risk of the attack from “significant” to “unlikely”. I will also forecast the probability of each solution being adopted by the appropriate individuals or groups and discuss the difficulties that each faces.

The main outcome from my project will be to vastly improve the educational materials available to the public that discuss the potential dangers of new RFID implementations. Even if an individual does not decide to follow any of my advice, at least he or she will have had the chance to make an informed decision about the danger instead of continuing in ignorance. I also plan to develop an easy list of steps that a citizen can take to protect his or her privacy regardless of any inaction on the part of legislators to develop regulatory protections. The availability of such steps is essential because the privacy and tracking issues have a very large impact. Mandatory RFID chips in documents ensure that most U.S. citizens will be concerned with my research, and any non-citizens will certainly be troubled because they own a car with wireless sensors or use a modern mobile phone.   We are almost approaching the point where a critical mass of deployed RFID tags enables effortless tracking of U.S. citizens, and it is imperative that technical and legislative roadblocks be put in place to prevent it.

RELATIONSHIP BETWEEN TECHNICAL AND STS PROJECTS

The two projects I have outlined are loosely coupled because they are both concerned with tracking someone using a wireless device. The STS project focuses on a wide range of technologies, capabilities, and risks at a higher level. The technical report simply chooses a specific technology, wireless Bluetooth communication, and implements the system for tracking it. We will develop a decidedly innocent system that requires you to opt-in to the tracking methodology, however it is easy to extrapolate how a more unscrupulous and stealthy implementation is possible.

Many of the core principles behind the Bluetooth tracking are easily generalized to almost all wireless tracking, including the U.S. passport case study discussed in the STS project. Legislative solutions discussed to protect the privacy of passport holders should also apply to protect users of the Bluetooth system. Specific technological barriers developed to defend U.S. passports from attack most likely won't apply to other wireless technology, however the intent behind them will. The broad applications of the solutions created in the STS paper give support for the choice of U.S. passports as an excellent case study for a discussion regarding wireless tracking of individuals.

TECHNICAL BIBLIOGRAPHY

(co-authored by Matt Beattie and John Szumski):

Bluetooth SIG, Inc. (July 26, 2007). *Core Specification v2.1 + EDR*. Retrieved on October 10, 2009, from http://www.bluetooth.com/NR/rdonlyres/F8E8276A-3898-4EC6-B7DA-E5535258B056/6545/Core_V21__EDR.zip.

Krasnyansky, Maxim, & Holtmann, Marcel. (November 12, 2002). *Manual Page for hcitool*. Retrieved October 10, 2009, from the Linux Operating System manual.

OConnor, MAJ Terrence & Reeves, Douglas. *Bluetooth Network-Based Misuse Detection.* Retrieved October 18, 2009, from http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04721574.

Chaudhry, Marium Jalal & Sadia Murawwat, Farhat Saleemi, Sadaf Tariq, Maria Saleemi, and Fatima Jalal Chaudhry. (December 23, 2008). *Power Optimized Secure Bluetooth Communication*. Retrieved on October 18, 2009, from http://ieeexplore.ieee.org/ stamp/stamp.jsp?arnumber= 04777733.

Ye, Jason Yipin. (2005). *Atlantis: Location Based Services with Bluetooth*. Retrieved September 20, 2009, from Brown University Department of Computer Science: http://www.cs.brown.edu/research/pubs/theses/ugrad/2005/jye.pdf.

STS BIBLIOGRAPHY

Caprio, Daniel W. (October 5, 2005*). Radio-Frequency Identification (RFID): Panorama of RFID Current Applications and Potential Economic Benefits*. Retrieved September 20, 2009, from U.S. Department of Commerce: http://www.oecd.org/dataoecd/60/8/ 35465566.pdf.

Carluccio, Dario. (September 7, 2007). *E-Passport: The Global Traceability Or How to Feel Like a UPS Package*. Retrieved September 20, 2009, from Ruhr University Bochum: http://www.cs.virginia.edu/~kc5dm/repository/rfid/distributed%20computing/E-Passport%20The%20Global%20Traceability%20Or%20How%20to.pdf.

Juels, Ari. (September 28, 2005). RFID security and privacy: a research survey. *IEEE Journal on Selected Areas in Communication*, 24(2), 381-394. Retrieved from

Richtel, Matt. (November 17, 2004). In Texas, 28,000 Students Test an Electronic Eye. *New York Times*. Retrieved from http://www.nytimes.com/2004/11/17/technology/

Scorer, A. G. (May 1998). Vehicle Tracking and Security. Journal of Navigation, 51, 170-179. Retrieved from http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=37857.