Shaikh Sultani

Gerald Scott

CST 373

20 May, 2017

CYBERSECURITY IN AUTONOMOUS VEHICLES

Since the introduction of personal computers and all the incredible technology that has followed out ever increasing reliance on computer systems and the internet has managed to make us more vulnerable to the nefarious hackers of the world. With this reliance on computers, and the internet our need for cybersecurity is at an all time high. Not just with computers themselves being at risk, but in every day items that requires a computer to run it (which now seems like everything around us) cars, phones, watches, tv's, planes, and more.

With automobiles needing computers to drive, and now having technology give vehicles the ability to drive almost autonomously, using computers almost exclusively to do so, they become more and more vulnerable to a cyber attack. As the focus of the tech world leans more towards a more autonomous vehicle in the coming future, vehicle has been made stronger, and along with the security more ethical concerns to go with it. Such being the case with the farmers in the midwest and their autonomous John Deere tractors.

In America's heartland, where the main business is agriculture, farmers are growing more and more frustrated as they are unable to properly access the autonomous tractors that they have purchased from John Deere in order to increase productivity, only to find out how unproductive the machine can get. These machines have the capability to steer themselves while doing the work that would normally require a human to do, using three technologies: GPS, automation, and sensing. By having someone map out the path the tractor needs to take on a separate computer, the human does not need to be fully a part of the automation process. Allowing them to be nearby, to keep an eye out for the tractor, working one some other needs that require attention, making farming, a bit more productive and streamlined.

But when a component of the tractor breaks down, needs repair or replacement, thats where the vehicles cybersecurity, and the John Deere license agreement, which farmers are forced to sign, frustrates the farmers. This license agreement not allowing these farmers to make any "unauthorized" repairs. The license agreement saying that almost all repairs and modification are not allowed to be done, all the while the farmers are not allowed to sue John Deere for any loss in crops, profits, or use of equipment due in any part to the software. Any break in the licensing agreement, and these farmers open themselves up to be sued by the company (Koebler, 2017). This agreement doesn't allow these farmers any freedom with their purchased tractors. If it breaks down, they cannot fix the problem themselves or go to a repair shop down the street. And even if they were to do any repairs or modifications, the software on the tractor would need an authorization key, one that requires a service technician to come out to the tractor to plug into the onboard computer, and authorize it, all the while the farmer is paying per the hour. With this being the case, the farmer is not only losing out on time, time that is essential in farming certain crops, but also losing tons of money since technicians aren't always available right away. This all leading to a fear from many of the farmers, that John Deere can shut down the tractor whenever they wanted, without the farmer being able to do anything about it.

This has prompted the farmers to turn to an unlikely source, eastern European hackers. These hackers have been able to crack the software, allowing anyone to have authorization whenever without having to wait for a service technicians. All that is required is to pay a one time fee to this hackers, and they have the key for the rest of their the tractors lifespan.

There are two clear parties that are involved in this ethical case; John Deere, a big corporation, and the farmers that own John Deere autonomous tractors.

We live in a country where capitalism is at the heart of the very nation itself. So with a nation that is big on capitalism, it the right of John Deere to do whatever it can, and wants, within legal reason, to make the most money it can. In the capitalist system, the best and quite frankly the at times most selfish will make the most money. It is the responsibility of everyone at that company in order to make the company money. In this case, they have the right to have a monopoly on the autonomous vehicle repair, to make money by making it impossible for anyone other than their company to fix the tractors, and to make the farmers sign an agreement to not allow them to fix the tractor themselves. In order to pay all of the workers who are a part of making the machines, design them, advertise them, sell them and so forth, but also have a responsibility to all of the shareholders and investors that have a stake in the company. Their values are as follows, integrity, quality, commitment, and innovations (John Deere, n.d.).

On the other side of the issue are the farmers of America who have purchased the autonomous vehicles for use on their farms. Such with the big businesses like John Deere, these farmers also thrive on the capitalism system. They have the right to run their businesses how they please, make money however they can. It is also their right as consumers to be able to do whatever they please with the products they have purchased and have proof of ownership. Everyone who has paid in full for a product has a right to do with that product what they will. Their responsibilities include farming, producing products in a timely manner, and having products that the American consumer will enjoy. Their values include that of pricing quality, usually family, and commitment. So both these parties both have very similar goals, values, and responsibilities the only difference is the size and amount of money each company makes.

When looking at the ethical issues going on with these two parties involved there is a breach of ethics from both sides. The easiest breach of ethics comes from the farmers side of thing. By turning to hackers who reside thousands of miles away in order to help them to break the license agreement by illegally hacking into the software in order to get around having to wait for service technicians every time a problem arises. Not only is this illegal, since the license agreement is a legal document, but the farmers are using a ethical approach to deciding to pursue this action. When analyzing this decision to turn to illegal hacking, we know this decision to do this does not come lightly. Because of the license agreement they were made to sign, they can open themselves up to being sued by John Deere if they break it, and they clearly break the agreement by cracking the software. But if this decision were to be broke down through a ethical viewpoint, we can see that the farmers are thinking about this through a “Rights Approach”. The rights approach defined as “This approach stipulates that the best ethical action is that which protects the ethical rights of those who are affected by the action” by Brown University Ethical department. This definition shows that the farmers believe that their ethical rights are being taken for granted, that because they do not have the ability to fix their own tractors when they break own, since they have the ownership of the tractor it is their right to fix if themselves if they so please.

On the other side of the issue is the ethical breach done by John Deere. This breach being, John Deere is not allowing the consumer full rights when it comes to its products it sells. Although, like it was mentioned before, they have the right to charge for services that they deem necessary in order to make some money. But looking at this decisions through a ethical framework, we see that John Deere clearly has a “Self-interest” ethics, or the “Egoistic approach”. This framework defined as “…an individual often uses utilitarian calculation to produce the greatest amount of good for him or herself” by the same Brown University Ethics department. This company is clearly looking out for themselves when they implement this sort of monopoly on the tractor when it comes to fixing it. Does making the farmers pay for a technician to authorize certain repairs and parts before the tractor is functional help the farmers in any way? No, it does not. Is there any reason for them to be charging extra? No, it doesn't either. So this clearly is all done for the monetary gain that the company will get by implementing such agreements and repair restrictions.

Resorting to hackers is the course of action that is being taken by the farmers, but there is two other options that could potentially help ease some of the issues going on. The first option being to work hard to get bills passed in legislature to prevent companies such as John Deere from having so much monopoly over these services. By implementing this course of action, the farmers would be able to take back control over their purchased equipment. Another positive effect of this course of action would be that not only John Deere would have to stop the monopoly over the services, but it would stop any other company later on from trying to do the same. But with the good, comes bad, and this course of action brings some bad with it. If John Deere were to stop these services, they will most undoubtedly lose money. If they lose money, then that has a potential to dip into the type of products they have to offer. Maybe this money they make from the services goes into research and development, that allows products such as the autonomous tractor to come to be.

A second option that could be implemented is having John Deere still offer these services, but instead of selling them for every time they offer a type of key for the software for a one time fee. This allowing farmers to get more control over their tractors, while still making money. This option would allow both sides of the issue to get something out of this. The company of John Deere would still make money off of the service, albeit not as much, and the farmers would not have to pay for a service technician to come to their farm every time a piece needs to be fixed to authorize it. This gives the power back to the farmer, allowing them to fix their tractors themselves, and then authorize the fix to get right back to work.

If the decision to choose a course of action were up to me, it would be clear to me that the best opinion to take is the first one, work to find a way to get a bill that prevents big companies from making these type of services required, and making it illegal to make fixes on your own tractor. I believe that the consumer has the right to do what he will to his own purchased product. I know that if people were told that they cannot work on their own cars, personal vehicles, or do any type of modifications unless its all done by the manufacture themselves, then it would not go over well with anyone. Everyone has the right to do with their own products what they will. Not many people like to go to a manufacturer garage to get their car fixed, it is always much more expensive for something that you could either do yourself, if you have the knowledge, or have your trusted mechanic do. So by taking this course of action you give the power back to the farmer in this case. By giving them full power, you give them full access to their machine. To get past the security software in place. This gives them the right to do anything they want without the risk of being sued, or loosing out on the crops that would be destroyed due to lack of farming in time.

With autonomous vehicles becoming more of a norm in everyday life, the idea of a autonomous tractor is strange to the everyday man. Perhaps this is why John Deere has such strong cybersecurity that does not allow farmers to get the full access to their purchased vehicle. I believe that the consumer has the right to have full control over his or her own vehicle, to allow them to do with it what they will. Not to have to ask permission to make repairs every time something happen. It is the right of the farmers, sometimes stronger cybersecurity isn't the best approach. When it comes to hurting what is the backbone of the economy, no one really benefits.

REFERENCES

1. **Autonomous vs connected vehicles – what's the difference? (n.d.). Retrieved March 29, 2017, from http://www.atkinsglobal.com/en-gb/angles/all-angles/autonomous-vs-connected- vehicles-whats-the-difference**
2. **Brown University. (n.d.). Retrieved from https://www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions**
3. **Byrne, J. (2016, December 19). Security & Ethics: Two key considerations in automotive. Retrieved April 15, 2017, from https://www.blackpepper.co.uk/viewpoints/security-ethics- two-key-considerations-for-the-automotive-industry**
4. **Core Values. (n.d.). Retrieved from https://www.deere.com/en_US/corporate/our_company/about_us/core_values/core_values.page**
5. **Fox-Brewster, T. (2015, March 25). Former Tesla Intern Releases $60 Full Open Source Car Hacking Kit For The Masses. Retrieved April 1, 2017, from https://www.forbes.com/sites/ thomasbrewster/2015/03/25/hack-a-car-for-60-dollars/#**
6. **Greenberg, A. (2016, August 04). Hackers Fool Tesla S's Autopilot to Hide and Spoof Obstacles. Retrieved April 1, 2017, from https://www.wired.com/2016/08/hackers-fool-tesla- ss-autopilot-hide-spoof-obstacles/**
7. **Hsu, T. (2017, February 15). Cybersecurity in Autonomous Vehicles Sparks Consumer Anxiety. Retrieved March 29, 2017, from https://www.trucks.com/2017/02/08/cybersecurity-autonomous-vehicles-concerns/**
8. **Interesting Asides: Connected Cars: From Hacking to Bullying. (n.d.). Retrieved April 1, 2017, from http://www.infocore.com/insights/interesting-asides-connected-cars-from-hacking-to-bullying.htm**
9. **Koebler, Jason. "Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware." Motherboard. N.p., 21 Mar. 2017. Web. 05 Apr. 2017.**
10. **Lin, P. (2016). Why Ethics Matters for Autonomous Cars. *Autonomous Driving,* 69-85. doi: 10.1007/978-3-662-48847-8_4**
11. **Pogue, D. (2015, October 13). Why Car Hacking Is Nearly Impossible. Retrieved April 12, 2017, from https://www.scientificamerican.com/article/why-car-hacking-is-nearly-impossible/**
12. **Price, R. (2017, March 16). Why GM invites ethical hackers to try and hack its cars. Retrieved March 28, 2017, from http://www.businessinsider.com/interview-gm-jeff-massimilla-chief-cybersecurity-officer-car-hacking-2017-3**
13. **Self-driving cars and cybersecurity: What are the risks of car hacking? (2016, June 09). Retrieved April 1, 2017, from https://betanews.com/2016/06/09/self-driving-cars-and-cybersecurity-what-are-the-risks-of-car-hacking/**
14. **Simonite, T. (2016, March 16). Self-Driving Cars and Autonomous Driving Features Will Introduce New Security Weaknesses to Our Vehicles. Retrieved April 3, 2017, from https:// www.technologyreview.com/s/546086/your-future-self-driving-car-will-be-way-more- hackable/**

15. **Sorrel, C. (2017, February 22). Are You Scared Your Future Self-Driving Car Will Get Hacked? Retrieved March 27, 2017, from https://www.fastcompany.com/3068051/are-you- scared-your-future-self-driving-car-will-get-hacked**
16. **Toews, R. (2016, August 25). The biggest threat facing connected autonomous vehicles is cybersecurity. Retrieved March 27, 2017, from https://techcrunch.com/2016/08/25/the- biggest-threat-facing-connected-autonomous-vehicles-is-cybersecurity/**
17. **World, A. (2015, September 18). Is the auto industry sleeping through the cyber security nightmare? Retrieved April 15, 2017, from http://www.automotiveworld.com/analysis/auto- industry-sleeping-cyber-security-nightmare/**