Computer Ethics And Democracy
Essay#1, Using An Analogy

DUE: Monday, September 23, 2013

Your purpose in this first writing assignment is to research self-driving cars and/or hacking into a car's computer system (or find another case with an ethical dimension, somehow dealing with computer technology in the popular press), think about a computer ethics issue presented, explain it concisely, and then analyze it according to the criteria given below. (I have attached two web articles to this assignment about the issues.) For example, one issue concerns who is responsible for accidents that occur involving a self-driving car or a hacked-car. What types of regulation would your analysis suggest? This is to be a short paper, approximately two to three pages long, double spaced (1000 words or less). You must email the paper to `croyden@cs.holycross.edu` by 3:00 p.m., September 23, 2013 **and** turn in a printed version in class the same day. If you choose to write about another issue for this paper, have your instructor okay it on or before 3:00 p.m. Wednesday, September 18, 2013.

The electronic version of your paper should be in rich text format (rtf) or pdf.

Your paper should be written in six sections. Give each of these sections the title shown below in bold face. Skip a line between each section. Here are the sections:

Section I. Names.: The first thing in this section should be your own name. On the next line, name the course (CSCI 328), the assignment (Essay #1. Computer Ethics and Society -Analogy), and the title of your essay. These four items should appear on separate lines, single spaced.

Section II. Reference(s): You should research the topic for your essay and find at least 2 addtional articles on the topic. Describe carefully where your reader could find the references you used in preparing to write the essay. For each website you cite, include the URL, the title of the site (if available) article, the title of the magazine or program, the date of publication, page numbers, the date you accessed it, and the date it was last updated (if available), and (if available) the author. If no author is listed, but an organization is listed, then list that organization. In addition to identifying your primary source(s), if you use someone else's words or ideas anywhere in your paper, you should indicate that use with quotes or with a paragraph set off with indentations and blank lines. Always advertise your sources and use complete endnotes. To not do so risks the serious charge of plagiarism. (One good source for citations is The Little, Brown, Handbook, 2nd Edition, by H. Ramsey Fowler. Endnotes are discussed on pages 480-489.)

Section III. The Technology Issues: Everyone taking this course has experience and some technical expertise about computers. Explain to your reader the most important points in your article/topic pertaining to the technical issues. Assume the reader is a reasonably intelligent undergraduate liberal arts student. Be concise, but don't leave out any details important to the ethical issue. (You only have 1000 words, don 't waste any of them.)

Section IV. Stakeholders/The Human Values at Stake:
In this section, explain to your reader why the technical issues in this article/issue are important to humans. List **all** the "players" and tell what is at stake for them in the ethical issue. What people, groups of people, and/or organizations either care or should care about this issue/decision? How are they affected, directly or indirectly, by the issue/decision? What are the costs and benefits, the risks and opportunities, involved? The questions should not be answered one after another in your section. Instead, think about all these questions and then write a concise answer to the following broad question: "Who are the stakeholders in this situation, and what human values do they have at stake?"

Section V. An Analogy: Use an analogy (or several) to explain your reasoning about this issue. (Remember: Using an analogy effectively requires more than just a statement. You must explain why the situation/activity is the same, and how it is comparable or different. When you make an ethical argument based on an analogy, you should illustrate the ethical differences and similarities between two situations. If the difference(s) is(are) are too significant, the analogy may not be applicable.) You might choose two analogies and explain why you think one is more appropriate than the other. Whatever analogy or analogies you decide to focus on should illuminate the ethical issue. Don't argue about what is right in this section; that's for your last section. In this section, discuss the analogy or analogies, and their similarities and differences to the situation.

Section VI. Conclusion: Based on your analogy or analogies, explain what you think is the right thing to do/right action to take. E.g. what is an appropriate policy or regulation to deal with accidents involving these cars? You are required to take and defend a position on this issue. "I'm not sure what to do" is not an acceptable conclusion. You don't have to be certain, but you do have to make a decision. Your essay should talk about what is right to do.

I'm looking for clear thinking in this (and subsequent) papers. Clear thinking is revealed in clear writing. Spelling, grammar, and style all count. Follow the instructions above carefully.

One of the aims in this course is to become more aware of the technical decisions being made in our society, and how they change our society and our lives. This paper gives you a chance to look for one such decision, to consider it in detail, and then to explain it to the rest of us by using an analogy.

http://www.nytimes.com/2013/05/31/technology/self-driving-cars-for-testing-are-supported-by-us.html?pagewanted=all

Self-Driving Cars for Testing Are Supported by U.S.

By CLAIRE CAIN MILLER and MATTHEW L. WALD

Published: May 30, 2013
New York Times

SAN FRANCISCO — Companies from Silicon Valley to Detroit to Germany are developing cars that park, steer and even drive themselves. Now the federal agency for traffic safety has said it wants to come along for the ride.

On Thursday, the Transportation Department made its first formal policy statement on autonomous vehicles. In a nonbinding recommendation to the states, it said that driverless cars should not yet be allowed, except for testing. But it said that semiautonomous features, like cars that keep themselves centered in lanes and adjust their speed based on the location of the car ahead, could save lives.

The statement, from the department's highway safety agency, comes as companies, led by Google, have made significant technological strides in making cars that drive themselves, but still face daunting legal, regulatory and cultural hurdles before the cars are widely available to drivers. It is the latest example of the tension between technological innovation and regulation, which move at very different speeds.

It is also a time of rapid change, and some anxiety, about autonomous systems in general. The transportation department is struggling, for instance, to determine how to regulate drone aircraft.

The statement detailed the benefits of self-driving and semiautonomous cars, which analysts said was a recognition by government officials that it had no choice but to keep up with the advancing technology in this area, which falls on a continuum from cruise control to full automation.

"It's not that they're trying to put the brakes on it," said Richard Wallace, director of transportation systems analysis at the Center for Automotive Research in Ann Arbor, Mich. "They're trying to get out in front of it."

Still, the highway safety agency was careful to address the tension between technology and regulation.

"Any potential regulatory action must appropriately balance the need to ensure motor vehicle safety with the flexibility to innovate," it said.

Even though technology companies like Google generally fear that innovation far outpaces regulation and risks being stifled by it, it has a different approach with cars than with software or cellphones because cars have been heavily regulated for decades, said Ryan Calo, a law professor at the University of Washington who co-founded the Legal Aspects of Autonomous Driving center at Stanford.

"We want to have some experimentation in the states to see what works, but it's nice to have federal experts helping out, as long as they don't take it too far," he said.

Autonomous cars could increase safety because they are not subject to human error like disobeying traffic laws and falling asleep at the wheel, according to analysts, car companies and the transportation department. They could also offer mobility to people who cannot drive, like the disabled or the aging.

Driverless cars could "change our lives, give us more green space, mobility, fewer hours wasted," Larry Page, Google's chief executive, said this month. "The average American spends 50 minutes commuting. Imagine if you got that back."

Still, many Americans are dubious about automated driving, according to a poll by the Auto Alliance, a Washington trade group that represents 12 of the largest carmakers selling vehicles in the United States. For instance, 81 percent said they were concerned that computer hackers could take control of an automated vehicle.

Even if automated cars were safer, people would worry about the lack of human judgment, Mr. Calo said.

"The first time that a driverless vehicle swerves to avoid a shopping cart and hits a stroller, someone's going to write, 'robot car kills baby to save groceries,' " he said. "It's those kinds of reasons you want to make sure this stuff is fully tested."

Yet most people will have the option of buying a car that is part robot in some sense next time they visit a dealership. Vehicles ranging from German luxury cars to mass-market American sedans are now equipped with automated safety systems, which rely on computer processors, software and sensors.

Future models from Mercedes-Benz have radar systems that brake a car in the event of an impending collision, stay in its proper lane around curves and sense when a driver is fatigued. Ford Motor Company's midsize Fusion sedan has a lane-assist system that alerts drivers when they stray on the roadway. Many cars come with adaptive cruise control that automatically cuts the speed when the distance between vehicles gets too close.

Greg Martin, a spokesman for General Motors, the largest American automaker, said, "G.M. has been working hard on autonomous vehicle technologies because we believe in its safety potential."

Google has gone the furthest, equipping Lexuses and Toyota Priuses with technology that drives the car without human intervention. Though Google still requires people to sit in the driver's seat, employees use the cars to commute the 40 miles between San Francisco and Mountain View, Calif., its headquarters, and have driven the curves of California State Route 1, a treacherous road overhanging the Pacific Ocean. The cars have driven more than a half million miles, according to the company.

The government's statement would likely not slow development of automated safety systems, but regulators expressed discomfort with driverless cars like Google's, which some people predict will be commercially available in less than a decade.

"Self-driving vehicle technology is not yet at the stage of sophistication or demonstrated safety capability that it should be authorized for use by members of the public for general driving purposes," the document said.

Leslie Miller, a Google spokeswoman, did not respond directly to the statement. She said Thursday, “We are introducing autonomous vehicle technology to improve people’s lives by making driving safer, more enjoyable and more efficient.”

People in the driverless technology industry said the agency’s caution about self-driving cars was reasonable.

“You can’t write regulations for something that is just getting into the prototype stage,” said Richard Bishop, who represents the Association of Unmanned Vehicle Systems International, a Washington trade association.

It is up to state and local governments to decide whether autonomous or semiautonomous cars are allowed on public roads. States including California, Nevada and Florida have already legalized driverless cars. They are not explicitly illegal in other states, because there is no law that says cars must have drivers.

The National Highway Traffic Safety Administration, which issued the policy statement Thursday, has jurisdiction over the vehicles themselves.

Driverless car technology is not advanced enough to develop safety standards, according to the statement, which defined four levels of autonomous vehicles. It said it was beginning a four-year research project on how to safely use automation, including studies of how humans interact with the cars, the reliability of the technology and risks like cyberattacks.

The agency offered recommendations for the states, including requiring drivers to get special licenses to operate autonomous vehicles, cars to have a button within easy reach that returns control to the driver and companies to report detailed data on accidents.

Claire Cain Miller reported from San Francisco and Matthew L. Wald from Washington. John M. Broder contributed reporting from Washington and Bill Vlasic from Detroit.

http://www.nytimes.com/2011/03/10/business/10hack.html

Researchers Show How a Car's Electronics Can Be Taken Over Remotely

By JOHN MARKOFF

Published: March 9, 2011
The New York Times

With a modest amount of expertise, computer hackers could gain remote access to someone's car — just as they do to people's personal computers — and take over the vehicle's basic functions, including control of its engine, according to a report by computer scientists from the University of California, San Diego and the University of Washington.

Although no such takeovers have been reported in the real world, the scientists were able to do exactly this in an experiment conducted on a car they bought for the purpose of trying to hack it. Their report, delivered last Friday to the National Academy of Sciences' Transportation Research Board, described how such unauthorized intrusions could theoretically take place.

Because many of today's cars contain cellular connections and Bluetooth wireless technology, it is possible for a hacker, working from a remote location, to take control of various features — like the car locks and brakes — as well as to track the vehicle's location, eavesdrop on its cabin and steal vehicle data, the researchers said. They described a range of potential compromises of car security and safety.

"This report explores how hard it is to compromise a car's computers without having any direct physical access to the car," said Stefan Savage of the University of California, San Diego, who is one of the leaders of the research effort.

Given that the researchers were able to do it, they are now trying to pinpoint just how hard it might be for others, he said.

The car security study is one of a growing array of safety concerns that are emerging as the Internet comes in contact with almost every aspect of daily life, be it through financial systems or industrial controls. Computer security researchers have long argued that wholesale computerization and Internet connectivity of complex systems present new risks that are frequently exploited first by vandals with malicious intent.

The new report is a follow-on to similar research these experts conducted last year, which showed that cars were increasingly indistinguishable from Internet-connected computers in terms of vulnerability to outside intrusion and control. That project tried to show that the internal networks used to control systems in today's cars are not secure in the face of a potential attacker who has physical access to the vehicle.

Their latest study was the first time that independent computer security researchers have tried to show how potential attackers could hack into a car from a remote location.

As in their first experiment, the research teams bought a car they described as a representative example of a moderately priced sedan. (They declined to identify the brand, saying that advanced telematics are rapidly becoming commonplace within the automotive industry.)

“In the case of every major manufacturer, if they do not have this capacity in their mainstream products, they’re about to,” said Tadayoshi Kohno, an assistant professor in the department of computer science and engineering at the University of Washington.

For example, services like General Motors’ OnStar system, Toyota’s Safety Connect, Lexus’s Enform, Ford’s Sync, BMW’s Assist and Mercedes Benz’s Mbrace all use a cellular connection embedded in the vehicle to provide a variety of automated and call center support services to a driver. These subscription services make it possible to track a car’s location, unlock doors remotely and control other functions.

In their remote experiment, the researchers were able to undermine the security protecting the cellular phone in the vehicle they bought and then insert malicious software. This allowed them to send commands to the car’s electronic control unit — the nerve center of a vehicle’s electronics system — which in turn made it possible to override various vehicle controls.

“These cellular channels offer many advantages for attackers,” the report said. “They can be accessed over arbitrary distance (due to the wide coverage of cellular data infrastructure) in a largely anonymous fashion, typically have relatively high bandwidth, are two-way channels (supporting interactive control and data exfiltration), and are individually addressable.”

The researchers declined to speculate about the worse situations, such as interfering with a vehicle’s control system to make it crash. However, they noted that their research showed how a next-generation car thief might operate: instead of using today’s so-called smash and grab tactics, the thief might be able to simply dial up a parked car, unlock its doors and turn on the engine, then arrive on the scene and drive off.

In addition to the cellular telephone vulnerability, the report details similar weaknesses in other systems that allow remote access, including short range wireless networks like Bluetooth, network ports used for car maintenance and even internal CD players.

The researchers noted that their report was about potential vulnerabilities and said there was no evidence that the safety loopholes they discovered had been used by criminals. They also said they believed that the automotive industry was treating the threats responsibly and working to improve the security of modern automobiles.

“Everyone has taken this extremely seriously,” said Dr. Savage.