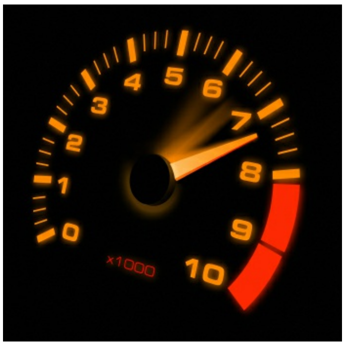
Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

Securing the Autonomous Connected Car

By: Mark Cummings, Ph.D.



As the transportation industry continues its transformation, security concerns about connected cars will prove major priorities for consumers. How customers perceive their security will shape consumption decisions, spelling success and failure for transportation, communication, and information service providers as well as those companies selling hardware and software to the service providers.

While many companies are staking money on the benefits of autonomous connected vehicles, security concerns will play a key role in adoption decisions and product choices. Customers will choose a service or product that makes them feel that they are in a bubble of physical and cybersecurity, with strong privacy. The Symposium on the Future Networked Car, organized by ITU and UNECE within the March 2018 Geneva International Motor Show, made it clear that some industry players currently recognize the need for security while others are resisting it based on cost concerns. Unfortunately, there is as of yet no general recognition of the role that security plays in customer adoption or competitive decisions. Companies that get security right will have a much higher likelihood of achieving the returns on their investments they are hoping for. Others – not so much.

Recent Examples Illustrating Security Concerns

Some recent examples help illustrate the problem today and point to what we are likely to see in the future. Security perceptions' ability to influence transportation decisions was dramatically demonstrated in Beijing during the SARS virus outbreak. During that time, the number of cars registered in Beijing tripled in two months. People were afraid to use public transportation because they felt it would expose them to the SARS virus, and they turned to private transport instead.

gotransverse
Go nimble
Agile billing for Smart Business
An Executive Guide to Intelligent Billing Platforms
An Executive Guide to
Intelligent Billing Platforms
Let's go
Click this ad for more information

Ride-hailing services already concern customers with well-publicized physical security problems. There are currently a series of lawsuits and criminal cases pending involving both passengers' and drivers' physical security in a variety of locations around the world. These cases involve physical attacks by drivers on passengers, as well as passengers on drivers. We are likely to soon see lawsuits involving attacks by passengers on other passengers. The recent case where an Uber in autonomous mode killed a pedestrian adds the potential for injuring people outside the car, which may be one of the greatest consumer fears when it comes to self-driving vehicles.

The state of California reported that in the first two months of 2018, there were six accidents involving autonomous vehicles. In two of those cases, the autonomous car with a test driver in place was attacked by a person outside the car. One instance involved a pedestrian, and the other a taxi driver who got out of his car at a light when the autonomous vehicle was stopped and attacked the autonomous vehicle.

This month, the state of Pennsylvania brought suit against Uber for failing to notify passengers and drivers personal information had been obtained by hackers. This breach affected thousands of people. It seems likely that Uber didn't notify them because Uber feared a negative impact on its business if drivers and passengers felt that their personal privacy might be compromised if they used Uber.

Recently, there was a widely reported vulnerability in Fiat Chrysler cars that allowed hackers to gain remote control of cars that were not designed to operate except under the control of a resident driver. An attacker outside of the car was able to gain control despite the efforts of the resident driver. The company responded by publicly acknowledging the vulnerability and making it clear that the cause of the vulnerability had been eliminated. Fiat Chrysler has also announced that it will have a fleet of autonomous taxis carrying paying customers in the second half of 2018.

Audi has announced an A8, to be made available this year, that will have the ability to drive autonomously on divided highways in traffic jams up to a speed of 37 miles per hour. Audi has announced that the company will assume all liability for accidents while the car is in autonomous mode. This likely means that Audi will be monitoring the vehicle in real time and also interfacing with a re-insurance company that will want data. These additional layers potentially pose additional security concerns.

Concerns about autonomous cars have also appeared in popular culture. Recently in the widely syndicated newspaper comic strip "Dilbert" there were two strips featuring autonomous cars. In the first cartoon, Dilbert is asked by some of his colleagues to program the car carrying another colleague go off a cliff and kill the colleague. Dilbert refuses and those same colleagues attack Dilbert because he refuses. In the second cartoon, the car goes off the cliff, killing the disliked colleague and Dilbert is asked if that was a bug in the program or if he made it happen. He answers that it was a bug. He is then asked if it was a known bug and he answers, "Now we are getting into a grey area."

Physical Security

People in cars, whether drivers or passengers, want to feel that the car will go where they want it to go and that they will arrive there safely. They also want to feel that others outside the car will be safe, unlike the unfortunate pedestrian who was killed by an autonomous car. Consumers are aware of potential physical security threats in vehicles driven by other people and autonomous vehicles. Given a choice, with all else being the same, consumers will choose a more physically secure product over a less physically secure product.

Experience with autopilots in commercial aviation is instructive. In the past, in commercial aviation 95 percent of all accidents resulted from pilot error. 2017 marked the first year ever without any fatal commercial airplane accidents. Compare this milestone to 1957 or even 1967, when most leading airlines suffered at least one major tragedy per year. In 2014, 1.2 million humans died globally in road traffic. However, commercial airplanes have not been subject to the kinds of cyber attacks that autonomous vehicles are likely to face. Consumers need reassurance on this score. That is why the Audi acceptance of liability for accidents cited above is so important.

Occupants of vehicles (passengers, and drivers if not autonomous) also want to know that they are safe from attack by other occupants in the vehicle or other people or things around the vehicle.

If the vehicle appears to be operating in an unwanted fashion, or if some person or thing appears to be threatening occupants, they want to be able to call for help and have effective intervention happen almost immediately. The *Pipeline* article *Connecting the Connected Car* describes some of the challenges inherent in communicating a call for help. In addition, there needs to be support systems that can respond quickly and intelligently to the call for help. While many types of responses may be needed, one type is a digital response through an orchestration and/or a security system that intervenes through digitally controlled resources in the vehicle. This requires delivering a digital stream back to the vehicle with low latency and this faces the same limitations as the call for help.

The second Dilbert cartoon illustrates a vulnerable group other than the occupants of the vehicle – the programming and operations staff. Disgruntled staff have new ways to wreck damage and controls are needed for that. But there may be a more important vulnerability. Periodically, groups of thieves attack bank branches by kidnapping an employee’s family member and holding him or her hostage to force the employee to provide access to bank assets. A similar approach is now possible with connected car operations and programming staff. Steps must be taken to protect programming and operations staffs.

Passenger Cybersecurity

As cars become autonomous, interiors are going to look more like offices or living rooms. This can be seen in the concept cars shown at the March 2108 Geneva Auto Show. It means a very high rate of usage of information tools from inside the vehicle. Occupants are going to want reassurance that their cybersecurity is at least as good as in their offices or homes. What they really want is to feel that they are in a bubble of both physical and cybersecurity.

Privacy

The cellular industry has been pretty good about keeping location information associated with cell phones private. Now with the connected autonomous car, there will be added emphasis and new players to contend with.

With vehicle orchestration systems overlaid on navigation, toll collection, ecommerce, insurance, physical security, engine control, personal calendars, and other information, there will be many more ways to expose personal information. Not only do customers want their credit card, personal identifiers and more protected, they want information about their travel protected as well.

Some think of the desire to protect location information as only related to immoral or illegal acts. However, a recent incident indicates that lawful activity also needs to be protected. Recently there was a possibility that Sprint and DT might merge. To signal that it was a real possibility, the CEO of DT tweeted that he was in the headquarters city of Sprint. Eventually, the deal did not happen. This was an authorized attempt to use location information to signal a business outcome. However, it is easy to imagine how unauthorized access to location information could have many serious business consequences.

In Summary

It is good news that both the information and transportation industries are beginning to recognize the importance of securing the connected autonomous car and discussing it venues like the Symposium on the Future Networked Car organized by ITU and UNECE within the March 2018 Geneva International Motor Show.

Success in these ventures, however, hinges on making decisions and provisions for consumers' security and privacy. Those companies who get this right will have a higher likelihood of achieving the returns on their investments they're hoping for, and society in general will benefit from better outcomes.