Connected and Autonomous Vehicles: Navigating the Future of Cybersecurity

by S. Candanedo - University of Warwick

I was walking back home with a friend one late afternoon, when she pointed out to me these small wheeled containers traversing a maze of fences. They were two autonomous vehicles or pods as the supervisor running the tests told us. The Warwick Manufacturing Group (WMG) was doing a run-through of a track before some public demonstrations the next day. Although our offer to help test by riding in the pods was declined, it was amazing to see the technology up-close, something that is usually reserved for videos online or the odd segment on TV. Automated vehicles were, quite literally, just around the corner.

The pods being tested that winter evening are known as Swarm pods.[1] Inspired by nature's swarms, they behave as a connected system, helping each other route shortest paths to their destination and efficiently transit areas. It is the type of model that could replace future public buses and similar transport systems. The days of long waits at the bus stop could be over but connected systems have always been susceptible to attacks as it only takes one weak link to break the chain.

As we look ahead to the future of autonomous and automated vehicles, a useful exercise is to study lessons of the past. The Morris worm famously caught the world by surprise being one of the first attacks that was so widespread and costly; traversing and infecting computers through the internet.[2] It bred a generation of malware known as worms; malware focused on spreading through connected systems. Imagine a city that has fully embraced connected and autonomous transportations. These vehicles should be able to communicate among themselves and a headquarters. How easily could a worm traverse through these networks? Imagine the worm was able to carry malware that makes the cars unusable and the repercussions of shutting down a public system even if only for a few hours.

Part of the reason the Morris worm was originally so successful in its attack was its novelty. It is quite difficult for current cybersecurity to stop completely new threats, especially if they exploit vulnerabilities only known to the attackers. You could revert to human interaction in these cases and have a person monitoring the systems, but the sheer size and complexity a city-wide network of connected vehicles would make this a difficult and costly choice. Traditional cybersecurity is ill-fitted for these types of scales and problems, due to its rigid and reactive nature. With the very safety of the user's life at play, it is not enough to implement pre-emptive measures after security incidents occur. Cybersecurity in automated and connected vehicles must be proactive.

Artificial Intelligence (AI) is one way to transform cybersecurity from reactive to proactive. Normally systems are given parameters in which to identify a threat. We tell a system that malicious behaviour has characteristics A, B, and C, and then it reports when it sees some or all these as a possible attack. If we could tell a system that a threat has certain characteristics and then train it to identify traits it has never seen before as possible issues too, we could have systems that actively become more secure. The presence of systems which actively learn to detect threats instead of passively going through a checklist will be an important step to keeping users safe.

We could take this train of thought a step further and say that the embedded hardware in a vehicle should consider having a specialized AI accelerator, specialized hardware to make sure that the time between the landing and detection of any malware is as small as possible and constantly running.

Yet, we cannot expect autonomous cars, especially personal use ones, to be secure no matter the technology available if their users are not aware of cybersecurity threats. Any basic lesson on cybersecurity will start stating the most significant vulnerability of all: people. Just as we learn to buckle our seatbelts as we step into cars, we should also learn to keep the software and hardware of the vehicles safe. The future of cybersecurity not only depends on technological enhancements but also in the increased cybersecurity literacy of its users. People need to be aware of simple strategies, like recognizing insecure connections to our cars or being aware that software needs to be updated.

Another consideration is "legacy" cars, how long will these vehicles be in use? There are still cars released 15 years ago on the road. Will automated cars have a similar life expectancy? If so, what could this implicate for cybersecurity? Infamously, the NHS was attacked in 2017 by the WannaCry malware.[3] Their computers were running on Windows XP, software released in 2001. The age of the system's software meant that it was well explored and dissected for vulnerabilities. This made the system susceptible to more current attacks. Backward compatibility and older software maintenance would become an essential step in keeping "legacy" cars safe, ensuring that older hardware can run newer software safety features. An alternative is to make the hardware "brain" of automated vehicles an interchangeable component, like how an old car can be improved with a brand-new engine, an older automated vehicle could be updated with a current "brain". This would allow for the modernization of outdated automated vehicles but would come with the design cost consideration of applying such a strategy.

Even if it is a few years before these products become more prevalent in our everyday lives, it is important to look ahead at the challenges connected and autonomous vehicles will face, especially when it comes to cybersecurity. The transformation of cybersecurity in a more proactive and automated surveillance, increasing average user's savviness, and designing vehicles not only for the present but future cybersecurity needs; will help keep users safe.

Resources

[1] Warwick Manufacturing Group. Autonomous pods born in Coventry swarm together in a world first. Available at: https://warwick.ac.uk/fac/sci/wmg/research/cav/

[2] FBI. The Morris Worm: 30 Years Since First Major Attack on the Internet. Available at: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

[3] The Telegraph. NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history. Available at: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/