Automotive Electronics Competition

To raise awareness about cyber security and automotive electronics among students, AESIN and the UKESF teamed up to run an Automotive Electronics writing competition, kindly sponsored by UltraSoC.

Entrants were required to produce a 'think piece' about the future of cyber security for connected and autonomous vehicles (no more than 1,000 words) in the style of a blog post.

Alan Banks, CEO of TechWorks and former AESIN Chairman

"AESIN are delighted to be able to support the Automotive Electronics Competition. The Automotive Electronics industry is going through unprecedented change, and the security challenges we face both now and in the future with Connected and Autonomous vehicles will be solved by the next generation of engineers and scientists who truly understand the challenges of Digital Resilience and Cyber Security in the new Automotive space."

The winner will receive £1,000, with a runner-up receiving £500. Both winning entries will be published online and finalists are invited to the 2019 AESIN Conference to receive their awards.

Aileen Ryan, Chief Strategy Officer

"At UltraSoC we believe that strong links with the academic world provide multi-faceted benefits to everyone involved – an opportunity for students to learn about and use state-of-the-art commercial products, an opportunity for UltraSoC to stay abreast of the latest academic developments in many related relevant fields, and the ability for us all to advance our industry together. We are delighted to sponsor this UKESF project."

We were delighted to receive a substantial number of entries, especially in this inaugural year of the competition. The standard was impressively high and the students produced some fascinating pieces, demonstrating their engagement and interest in the subject. The two finalists' entries are included in the following pages.

Cyberattacks: Invisible Threats to the Eyes of Autonomous Vehicles

THE UNIVERSITY of EDINBURGH

by David Kong

You're on your way to work and your car suddenly starts to drive in an infinite loop around a roundabout. "Another One Bites the Dust" by Queen starts blasting out of the infotainment system. You've been hacked!

When I think about automotive cybersecurity, one of the first things that springs to mind is the movie scene from "Fast and Furious 8: The Fate of the Furious" where a hacker wreaks havoc in New York City by turning over 1000 cars into a swarm of "zombies". With many companies already trialling self-driving vehicles, how close are we to a safe and secure driverless future?

Before we dive into cybersecurity, let's take a quick look at how connected and autonomous vehicles (CAVs) work. For driverless cars to "see" the road, they *currently* rely on a combination of image sensors, LiDAR, radar and ultrasonic sensors. Using vehicle-to-everything communication (V2X), CAVs will be also able to make decisions using data from other vehicles, the infrastructure and the cloud. As vehicles become connected to smart cities, they will even be able to know what's happening three blocks away!

The Society of Automotive Engineers (SAE) has defined six levels of autonomy. At level 0, full human control is required; and at level 5, no human interaction would be needed in any situation. Over the past few years, companies like Waymo have released level 4 vehicles which are fully autonomous in geofenced areas.

Today, electronics accounts for around 40% of the value of a typical car. Each vehicle can usually have 100 to 150 electronic control units (ECUs). These controllers are interconnected via the CAN (controller area network) bus which can be easily accessed from the OBD-II (on-board diagnostics) port. Although advanced driver assistance systems (ADAS) can make driving safer, the addition of every new feature brings more attack surfaces for hackers to play with.

In 2015, two researchers exploited a "zero-day vulnerability" (an unknown weakness) in the entertainment system of a Jeep to take full control of the vehicle from a remote location. By spoofing level 1 and level 2 ADAS features such as cruise control and self-parking, they were able to control both the speed and the steering of the vehicle on the motorway. Then, they carried out an even more sophisticated attack from inside the vehicle using the OBD-II port. Fortunately, most successful automotive cyberattacks to date have been ethical "white hat" attacks rather than malicious "black hat" attacks.

A lot of work in cybersecurity revolves around protecting the processor. However, researchers have shown that automotive sensors can easily be spoofed using fake data. As a UKESF scholar sponsored by ON Semiconductor, I spent a lot of my summer investigating different ways to mitigate the cyber threat against automotive sensors. I learned that forgetting to protect sensors on a driverless vehicle is like locking all the doors but leaving the windows open for hackers to crawl through.

You know that hackers can do a lot with the data in your mobile phone. Now imagine what they could do with your car – a mobile data centre with you in it! In comparison to mobile phones, autonomous vehicles have additional safety risks; a myriad of ECUs and sensors that are not localised; and a longer lifecycle. Most importantly, they will be connected to everything around you.

With so many companies developing solutions for autonomous vehicles, a chain of trust must be created across the whole supply network. From the semiconductor and software companies to the Tier 1 suppliers

and the OEMs (Original Equipment Manufacturers), everyone must work together to make the whole ecosystem cyber-resistant.

In the future, it is likely that cybersecurity will underpin functional safety. The ISO 26262 functional safety standard is very important for the design of electronic and electrical systems in the automotive industry. This ensures that vehicles remain safe if any faults or failures occur. Up to this point, there has not been a formal standard for automotive cybersecurity and the upcoming ISO/SAE 21434 standard is a chance to get things right.

Although the recent explosions in technologies such as the Internet of Things (IOT), 5G, artificial intelligence (AI), cloud computing, edge computing and data science have brought autonomous vehicles closer to reality, they have also made cybersecurity more challenging. For example, if hackers begin to use adversarial machine learning algorithms to attack CAVs, the battle against cybercrime could become a war between defensive AI and offensive AI – like the fight between Jarvis and Ultron in “Avengers: Age of Ultron”.

After so much talk about hacking, you’re probably wondering how realistic the scene in Fast and Furious is. The good news is that it would be impossible for such a complicated attack to be carried out by one hacker in such a short amount of time. However, researchers at Georgia Institute of Technology have shown that hackers would only need to control a small number of autonomous vehicles to cause chaos. By simulating an attack on the streets of Manhattan, they found that if only 40% of cars were CAVs, only half of them would need to be hacked to cause gridlock. At rush hour, hacking only 1 in 10 of all cars would completely block the emergency services.

As engineers and scientists, we often find ways to turn science fiction into reality. However, from a cybersecurity perspective, it is our role to ensure that the scene from Fast and Furious can never happen in real life. Before driverless vehicles become mainstream, we must work together to ensure that countermeasures are in place to detect hackers, prevent cyberattacks and keep people safe. Just as sensors have allowed us to see things that human eyes would not; it is our responsibility to protect autonomous vehicles from invisible threats to their eyes.

It is estimated that CAVs could bring the UK economy an annual boost of £62 billion by 2030. What an exciting time to be working in the automotive electronics industry!

Safety Net: Working to Protect Passengers

by James Leyland

THE UNIVERSITY of York

In modern vehicles there is an unrivalled amount of data being collected about them as they run all the time. From the millage being clocked up on an engine, to the degree to which a panel flexes and the GPS location, sensors are everywhere collected and storing. In the future there will be more of this, to the point that vehicles will be able to reliably and safely pilot themselves. Cars will be able to collect more data on themselves to prevent hardware causing incidents as well as their surroundings – working as a collective to better maintain flows of traffic for example. As for automated vehicles, the more sensors that there are around, the more eyes they have to respond to their surroundings. Smarter algorithms, developed through modern research into data mining, along with more sensors will lead to safer vehicles all round.

Where will the next vehicle take you? Ellesmere Port train station. Photo taken by James Leyland.

More data does however mean more to protect…

The magnitude of the data collected means that everything from storage to transmission needs to be secure. In the future there will be a network of all vehicles, each contributing their local data. The integrity of the data as well as the integrity of each sensor in the system is very important. On the other side of the coin is the user – a huge security issue. Primarily there's accessing the car, where the user has a key or password which can be obtained by someone else. I was lucky enough to be in shown new technology for facial recognition and analysis while working over this summer from OMRON which is capable of telling the age, sex, where the user is looking and the approximate emotional state of the person in front of it – something that could be perfect for this kind of use.

However, there is also the fact that the user can access the vehicles system through various means; in cars the centre console allows access to all kinds of settings and data, something that can easily be exploited. These security holes will become more and more prevalent as the amount of data collected and processed increases.

Firstly, data generation/collection must be secured to ensure that the data being transmitted into the system, or network, is reliable and trustworthy. If false or corrupt data is used in analysis by a vehicle or network of vehicles, there could be very dangerous outcomes. I feel that the only real way to address this is by having sensors that are certified by the government by meeting a certain standard.

Next there is the transmission of the data, especially should roads become huge networks to allow self-driving and smart vehicles to use them. I think that the best solution that could be put forward here is a new protocol specifically for vehicles that is heavily encrypted and has unique identification stamps for each sensor and vehicle that data comes from – allowing maximum traceability. Its very important to have traceability for something like this and identification of each device included in the network means that false devices for stealing data or even cheaply made counterfeit devices that could cause hazards on the road, can be detected, ignored and traced.

Finally, there is storage of data. The data that is collected needs storing somewhere physically away from people tampering with it and safe from hackers etc. Eliminating access, for example in cars currently, through centre consoles will prevent accessing data being simple. But also hiding the memory devices means that the chips can't be pulled, cloned or wired to do other, potentially malicious, things. Now, having the data on a device that wipes itself and sends an alert when its being tampered with would be a good start. However, all data could easily be lost for a vehicle and it would then have to go about rebuilding itself. Like a large system, periodic backups would be a good idea – and easy to do since the data is constantly broadcast to create an image of the road to other vehicles.

In my opinion, smart vehicles and self-driving vehicles being on the same roads will require moderation – just as a network is moderated by IT staff in any sizeable company. Having a department that monitors the dataflow between vehicles, similar to the role of ATC in airports however will much less interaction with the system, means that there is always a person in control of what is going on and should something be predicted to be about to happen, there is someone watching who can override what is going on. This idea stems from the fact that people are sceptical of giving up control of a vehicle entirely to a computer – hence train drivers and having manual controls in self driving cars so that a human user can override and take back control of the vehicle. I feel that having this body that watches over the network and can stop accidents that might occur from multiple analysis points will happen. Due to the multiple vehicles each giving their perspective, even if not all of them predict an incident, someone can look over it and make decisions to prevent incidents. They can also maintain a store of the data, so that it can be reviewed after incidents but also, should a vehicle need its history restoring from previous backup, they can identify it from the very specific identification stamps in the universal protocol and feed data back to that device through the network.

No Matter what type of vehicle, I think that they'll all just be network nodes with different properties – all collecting data for the same reasons. Photo taken by James Leyland.

Obviously, there is some data that will need to be accessible by the user, such as speed and general diagnostic information. There are things implemented to only allow garages to access certain data, such as having expensive diagnostic computers and uniquely shaped connectors, which work for now, but the data will have to be secured to more extremes because all data is valuable and there will be much more of it.

AESIN

Our mission is to be the catalyst that enables rapid innovation in Automotive Electronic Systems in a collaborative and non-competitive environment.

AESIN is a collaborative, non-profit, response to the Automotive Sector Revolution in complex Electronic Systems enabling technology for the more Electric Connected and Automoted vehicles of tomorrow.

With roots in the Electronics Deep Tech sector AESIN aims to be the home for OEMs, Tier 1 Systems integrators, Component and Software companies, infrastructure providers, insurers, local authorities, government agencies and anyone seeking to embrace next generation Automotive Electronics innovation.

Our aim is to help create an environment where the best innovators in the world can meet to develop and deliver world class Automotive Electronic enabling technologies of the vehicles of the future.

AESIN facilitates collaborative innovation, expert knowledge and best practice sharing with endorsement of the Automotive Council UK and Government. In addition to supporting the Automotive Council UK consensus roadmapping we drive collaborative activity through our core Workstreams.

UKESF

Our mission is to encourage more young people to study Electronics and to pursue careers in the sector.

In the UK, the Electronics sector is big, valuable and growing; however, the demand for capable, employable graduates is currently outstripping supply. We are an educational charity, launched in 2010, with both public and private seed-corn funding. We operate collaboratively with major companies, leading universities and other organisations to tackle the skills shortage in the Electronics sector.

The UKESF ensures that more schoolchildren are aware of Electronics and the opportunities available, helping them to develop their interest through to university study. At university, we support undergraduates and prepare them for the workplace.

UltraSoC

UltraSoC is a pioneering technology start-up based in Cambridge, UK.

Our products put intelligent self-analytic capabilities in the systems-on-chip (SoCs) at the heart of today's consumer electronic, computing and communications products.

Our embedded analytics technology helps solve the most pressing problems faced by the high-tech industries today – including cybersecurity, functional safety, and the management of complexity. Our solutions also allow designers to develop SoCs – the driving force behind both performance improvement and cost reduction in the electronics business – more quickly and cost-effectively.

UltraSoC's flagship product line is a suite of semiconductor IP that puts an intelligent analytics infrastructure into the core hardware of an SoC. This provides intimate visibility of the real-world behaviour of entire systems. The ultimate benefits include robustness against malicious intrusions; enhanced product safety; reduced system power consumption; and overall better performance – with fine-tuning of end products even after they are deployed in the field. These capabilities address applications in a broad range of market sectors, from automotive and IoT products, to at-scale computing and communications infrastructure.