Computers and Stuff.

Sam Houliston.

Report scams to the ACCC via www.scamwatch.gov.au or by calling 1300 795 995.

How can we stop Driverless Cars from being Hacked?

Once hackers get into your internet-connected car, they could disable the air bags, brakes, door locks and even steal the vehicle. That's the finding of researchers who recently uncovered a flaw in the way the different components of a connected car talk to each other. Their work follows several demonstrations of researchers remotely hacking into and taking control of cars, including one that led to a worldwide recall of one connected model of Jeep.

None of these hacks have yet been demonstrated with regular vehicles on the road, but they show how cyber security is becoming a big challenge to the car industry, especially as vehicles incorporate more and more driverless technology. It has even worried the UK government enough to release a set of guidelines for the sector. These emphasise the need for companies to work together to build resilient vehicles whose security can be managed throughout their lifetime. But what can actually be done to ensure that as cars effectively become computers on wheels they are kept safe from hackers?

There are three main reasons why cars are becoming vulnerable to cyber attacks, and these trends have also made security more challenging to design and test.

First: The different systems that make up a car are increasingly designed to work together to improve their efficiency and so they all need to be able to communicate, as well as being connected to a central control. Adding autonomous systems that make cars partly or fully self-driving means the vehicles also have to connect to other cars and infrastructure on the road. But this opens up what was traditionally a closed system to outside, possibly malicious influences. For example, there has been demonstrations of attacks using a cars' Bluetooth, WiFi and radio frequency (RF) on passive key entry systems, which all create possible entry points for hackers.

Second: More features and functionality in cars means more software and more complexity. A single vehicle can now use millions of lines of code, put together in different ways in different components from different manufacturers. This makes it hard for security testers to know where to look, and hard for auditors to check a car complies with the rules. If the software recently used by Volkswagen to circumvent emissions limits had been a malicious virus, it may have taken months or years to find the problem.

Finally: The volume and variety of the data and content stored and used in a vehicle is ever increasing. For example, a car's multimedia GPS system could contain contact addresses, information about the driver's usual routes and, in the future, even financial data. Such a hoard of information would be very attractive to cyber criminals.

One of the best ways to protect connected cars from this growing threat is by building security into the design of the vehicles. This means, for example, ensuring that there are no conflicts, errors or misconfigurations in individual components. Fully assembled cars should be tested more rigorously to ensure the final product lives up against security hacks, using methods such as penetration testing, whereby systems are purposefully attacked to expose flaws. This in turn would mean better tools and standards that would force everyone in the industry to factor in security right from the start.

The next big challenge is likely to be designing vehicles that match security with safety. As self-driving technology evolves to use more artificial intelligence and deep learning techniques, we will be relying on yet more software to control our cars and make decisions on safety grounds

like human drivers would. This will make it even more important that the cars are secure so that they also protect drivers' safety.

The industry is slowly but steadily responding to the growing threat of cyber attacks. Aside from government regulations, the US Society of Automotive Engineers (SAE), has introduced its own set of guidelines that show how cyber security can be treated like other safety threats when designing a car. There are also efforts to make drivers more able to protect their vehicles, for example by warning them in car manuals against plugging in unknown devices. In the longer run, the biggest challenge is simply getting the car industry to coordinate more. The sector is very competitive at every level, and companies rely on the latest autonomous and connected technologies to set themselves apart and win new customers.

This rivalry means that companies are reluctant to share intelligence about cyber threats and vulnerabilities or work together to develop more secure designs. To make cars truly secure we'll need to see the industry change gear.

Self-drive vehicles will shake up industry.

Autonomous vehicles are standing at the foot of a path for seemingly limitless potential. From a practical standpoint, automotive autonomy doesn't seem like much beyond the ability of a vehicle to navigate roads without being directly controlled by a human driver. While this feat is certainly impressive on its own, this only scratches the surface of the resonating effect vehicular autonomy will have not just on the automotive, but countless other industries.

The best way to realize how big of an influence autonomous vehicles will have on different industries is to determine (or remind oneself) how heavily-utilized vehicles are in different fields of work. We rely on semis for shipping food and other goods, spend hundreds of millions in insurance on vehicles every year, utilize transportation services (like Uber and taxis), along with other noteworthy municipal needs that incorporate vehicular transportation.

It's estimated that by 2025, driverless cars will be the norm. Some industries that will need to adapt include:

Parking:
Driverless cars will drop passengers off at their destination and go find a free park elsewhere (or remain on the road if they are part of a ride-sharing program). Every major city has huge chunks of land tied up in parking spots and some reports estimate that driverless cars will reduce the need for parking space by 50%. This will release this land for more beneficial social and economic purposes but will also reduce the income for car park operators.

Law Enforcement:

Each State issues hundreds of tickets from cameras used to identify cars speeding, running red lights, returning millions of dollars' worth of fines. Self-driving cars will significantly reduce the number of speeding tickets and there will be fewer drunk driving and other traffic violations which may lead to a decrease in the size of police forces and resources to more important areas of serving and protecting the public.

Insurance:

About 90 percent of car accidents are caused by human error. In a world of autonomous vehicles, we can expect to see a major reduction in the number of accidents, which will significantly change the insurance revenue model. As the risk of accidents drops, demand for insurance will take a sharp dive as well. In anticipation of this shift, some insurers are rolling out usage-based insurance policies (UBIs), which charge consumers based on how many kilometres they drive and the safety of their driving habits.

Legal Professionals:

Personal injury lawyers will see a significant decrease in demand for their services. Vehicle collisions, which account for a large chunk of all civil trials will be all but eliminated with automated vehicles.

Hotels:

The need for lodging will drop as people sleep in their cars during overnight road trips. Just think, if you're driving from Melbourne to Perth, you could hop in the back seat and snooze

while the car headed across the Nullarbor all by itself. Audi's vice president of brand strategy and digital business, has predicted that car interiors will eventually be able to morph between driving mode and sleeping mode, presenting a major obstacle for the hotel industry.

Media, Entertainment and Online Retail:
Experts predict there will be more media consumption as autonomous cars transform into rolling living rooms.

Package and Food Delivery:
For delivery services, there will be enormous economic gains, most of which will come from the elimination of truck drivers and their wages. We're already witnessing the digitization of package delivery systems with drones and UberEats, but the effects will become more devastating for drivers when autonomous cars are the norm.

Motor Mechanics/Panel Beaters:
With multiple sensors, no distractions and no drunk driving, self-driving cars will largely eliminate car crashes so body shops will lose a huge portion of their business and with no burn

outs, street racing or flat out cornering, tyres, engines and gear boxes will last a lot longer. Indirectly, the decreased demand for new auto parts will hurt steel producers and part manufacturers.

Car Manufacturing:

By 2030, PwC predicts electronics will account for 50 percent of automobile manufacturing costs, up from one-third today. With Intel buying Mobileye for $15.3 billion, we're already seeing a shift in value from traditional auto manufacturers to software and electronics companies, which will form the core of all automotive systems. Traditional parts manufacturers will face competition from more technology-focused companies like Nvidia, which has already been tapped by automakers to help build the computers needed for driverless cars.

The disruption has started; autonomous cars will run the roads sooner than we expect. Business leaders in *all industries* can no longer take a "wait and see" approach. Companies must start being hyperaware by monitoring changes in their environment (which extends beyond what their competitors are doing); they must start making informed decisions and execute those decisions quickly to respond to the threat of autonomous vehicles. Further, company and government leaders must immediately address the impact on jobs and get serious about retraining efforts.

The infographic below (click it for a bigger view) provides a detailed visual that breaks down the industries where automotive transportation is a major operational factor, along with the potential effects the incorporation of driverless vehicles could have in each line of work.

In flight internet/phone.

Once upon a time, inflight connectivity used to be a dream, air travel always offered a brief digital detox, a precious few hours away from the squall of emails, messages and app notifications. But no more, now it's common-place on a lot of overseas airlines and at last is being introduced to Australian airlines. Qantas plans to have it available on 80 of its aircraft by the end of 2018. Most of us carry around at least one connected device which we check reflexively and friends, colleagues and business partners expect us to be accessible no matter where the day takes us - often instantly. Sometimes, even a 30-second hiccup in service is enough to create anxiety. The fact that technology has met these business needs is remarkable. Behind the scenes, inflight connectivity requires impressive feats of engineering and planning - things that go unnoticed by most travellers simply because they work so well.

This isn't your average mobile phone service after all. When the devices to which you're connecting are moving near the speed of sound at an altitude of 35.000 feet, they require a whole new connectivity paradigm.

One of the most basic differences between ground connectivity and inflight connectivity is motion. Airplanes don't stand still. Instead, they dart through airspace at hundreds of kilometres per hour requiring the data link to adjust quickly in real time. On the ground it's a different matter, even if you're texting in the car the speeds and distances involved are modest compared to those in the sky, in the air, a signal has to connect with an aircraft thousands of times an hour and navigate rapid shifts in orientation, speed, and direction - all while ensuring an always-on experience for pilots and passengers. Distance and latency are two of the factors that impact these connections the most. The vast distances involved in air travel can weaken connections and demand switching between many ground stations or satellites. Latency, often caused by making such a switch, can cause service gaps. Fortunately, today's Inflight systems are extraordinarily efficient and make all of this nearly invisible to end users.

So how does it work?

Two of the most important resources for in-flight communications are air-to-ground (ATG) and satellite technologies.

ATG isn't much different from your mobile phone connection. An aircraft communicates with a ground station, ideally within a target range and line-of-sight bearing. With ATG, the ground

station antennas serve aircraft that pass through their airspace, similar to the way your mobile phone connects while you're in a moving car.

As you travel into different sections of airspace, the plane automatically connects to signals from the nearest tower, so there is (in theory at least) no interruption to your browsing. But if you're passing over large bodies of water or particularly remote terrain, connectivity can be an issue.

Satellites are different, and there are additional steps involved in getting, say. an email to outer space and back:

- Your computer/phone sends the signal to the onboard modem, which transmits this signal (radio transmission) to the satellite from an antenna mounted on top of the aircraft.
- The satellite receives and routes the radio transmission, along with countess packets of data from other sources, back to ground stations. Communication satellites often have geosynchronous orbits (they stay above the same patch of ground), but aircraft can still transfer between several satellites as they move along their flight path.

Importantly, once a satellite is in orbit, it's untouchable. This is one of the limiting factors of satellite communication, you can't just reach up there and upgrade the hardware. So, ground- or air-based communication devices have to be configured to optimize available satellite resources until something else makes its way into orbit.

Fortunately, the hardware involved in inflight connectivity is minimal. Aside from the obligatory box which resembles the modem box you have at home, which your device connects to WiFi via the onboard router, most connectivity solutions include aerodynamic antennas that attach to the fuselage.

Is it a good thing?

- For business travellers – possibly,
- For those that cannot exist without the phone in their faces - yes,
- For some parents on a long flight with one or more kids - yes, they can amuse the kids with the lap top
- But for some of us who can live without the phone or the computer for several hours without suffering extreme withdrawal systems – NO!

Us oldies don't want to sit next to a bunch of people tap tap tapping away on a laptop or speaking loudly on a mobile phone, but the world is changing and we're just going to have to get used to it.

Excel Tricks.

- If you want to add up a column of numbers, hilite the numbers plus one cell below the row of numbers then press ALT and the **+=** key. This will put the sum in the spare cell.

- If you want to insert the correct time into a cell, press Ctrl, Shift and the **:;** key.

- If you want to insert the correct date into a cell, press Ctrl and the **:;** key.

- If you want to hilite a column, click anywhere in that column then press Ctrl and the space bar.

- If you want to hilite a row, click anywhere in that row then press Shift and the space bar.

- If you want to remove a column, click anywhere in that column and press Ctrl and the **)0** key.

- If you want to remove a row, click anywhere in that row and press Ctrl and the **(9** key.

- If you want to show the formulas in all cells, press Ctrl and the **~** key. Press them again to toggle back to normal view.

- If you wish to repeat a cell, click the cell below the cell you wish to repeat, and press Ctrl and the letter **D.**

Saving Images.

All Windows users know how to save an image that they're looking at on their computer screen. If you open a site and get the screen below and you want to save one of those images, you just double click the one you want, it will open up, you then right click it and select "Save As" and save it.

But sometimes you'll find the image will be a JPEG file or a GIF file or a PNG file (or some-other file type) when what you want is a JPG file. Well, Windows will allow you to change the file type, and will do it easily.

All you do is *right click* the pic, which will open a window allowing you to select where you want the file saved, select that folder, then at the bottom right of the window, in the "Save as type" bar, click the down chevron (V) and select *All Files (*.*)* then in the "File Name" bar, change the JPEG or GIF or PNG extension to JPG and click save – and it's done. .

Uber signs with NASA to develop Air Taxi routes.

Uber has signed a deal with NASA to develop software for the air taxi it plans to have in service within five years. At a web conference in Lisbon on Wednesday, Uber's Jeff Holden said the company is teaming with NASA to develop a range of technologies designed to track and de-conflict its human-carrying quadcopters from each other and from other manned aircraft.

Earlier this year, Uber announced plans to develop an on-demand air-taxi system that by 2020 they will test initially in Dallas followed soon after in Los Angeles. According to a report in USA Today, the company said it hopes to launch UberAir before the 2028 Olympics in Los Angeles which will allow LA residents to literally fly over the city's historically bad traffic, giving them time back to use in far more productive ways. UberAir will perform tens of thousands of flights each day across the city and has hired NASA veterans Mark Moore and Tom Prevot to run the program. Moore, an electric aircraft expert, will oversee aircraft vehicle design and Prevot will handle air traffic management.

I'd rather look back
at my life and say
"I can't believe I did that"
instead of saying,
"I wish I did that."