CYBER-SECURITY: A NEW CHALLENGE FOR THE AVIATION AND AUTOMOTIVE INDUSTRIES

Written By ***Dr. S. Krishnan***[1]

Abstracts

Today's vehicles are increasingly 'connected'; there is wireless data exchange with servers, infrastructure and other vehicles. Tomorrow's vehicles will be automated and autonomous, capable of sensing their environment and navigating through cities without human input. The ongoing move from traditional air traffic control systems such as radar and voice towards enhanced surveillance and communications systems using modern data networks causes a marked shift in the security of the aviation environment. These advances will increase comfort and convenience for customers, improve products and services, and contribute towards achieving societal goals such as improving road safety, reducing fuel consumption, and facilitating traffic management and parking. The digital world offers unprecedented opportunities. Nevertheless, opportunity comes with risks, and one of these is the threat of a direct cyber-attack on vehicles or a whole vehicle fleet. Keeping cyber-security risks for connected vehicles in check is therefore of crucial importance. The interfaces of connected vehicles present an opportunity for exploiting vulnerabilities if adequate cyber-security mechanisms are not implemented and cyber-security risks are not dealt with appropriately. Attackers may compromise the user's personal data, threaten the vehicle's systems or endanger passengers.

Keywords: Aviation Security, Cyber Power, Wireless Attacks, Communication Security, Automobile Security

[1] The writer is an Assistant Professor in History in Seedling School of Law and Governance, Jaipur National University, Jaipur. He had worked as an Assistant Professor in History in Apex Professional University, Pasighat, Arunachal Pradesh. He had worked as a Journalist in esteemed newspapers like Indian Express and Daily News Analysis, online newsportals and a magazine in Ahmedabad. He had worked as a Liaison Officer and Media Relations In-charge, Indian Society of International Law, New Delhi.

ISSN 2581 3382

Introduction

"Good night. Malaysian three seven zero". So went the last words from flight MH 370. Three minutes later, the aircraft disappeared from the radar screens with all 227 passengers and crew on board. With the aircraft still missing, this casualty remains one of the greatest mysteries in recent aviation disasters and gave way to many conspiracy theories about the flight's sudden disappearance, including hacking of the plane's autopilot systems (Tasch, 2014). Such theories were quickly dismissed; however, the topic of cybersecurity seems to be more crucial than ever in a context of globalized terrorism.

"Remember to lock your car" is no longer sufficient advice to protect your vehicle. United States Senator Edward Markey's Tracking & Hacking report on gaps in automotive security and privacy, as well as successful attacks on car computer systems from different manufacturers, are just two reminders of the increased threat to vehicle safety. Computer attacks are now a clear and present danger for car drivers, owners, dealers, manufacturers, and suppliers. Increased automation, vehicle-to-vehicle and vehicle to-infrastructure communications, and advances in autonomous driving add computer security and data privacy to reliability and safety as cornerstones for consumer confidence and continued success in the automotive industry.

This paper will focus on cybersecurity in the civil aviation industry, but will also present some of the threats that exist in a much more daily transportation mode: personal cars.

We will present the stakeholders involved in the aviation industry, point out the sources of the vulnerability of the industry to cyber-attacks, and then analyze the efforts put in place to deter cyber-attacks against commercial aircraft. The same order of reasoning will be applied to the automotive industry.

The Aviation Industry

The aviation industry is important to the global economy. In 2013, the air transportation network carried over 48 million tons of freight and over 2.6 billion passengers. Its global economic value was estimated at 2.2 trillion dollars (AIAA, 2013). Any (cyber)-attack in this industry would result in important social and economic consequences.

ISSN 2581 3382

With the development of new technologies such as internet, the global aviation industry is subject to a new and growing type of threat coming from cyberspace. As in the other industries, cyber threats purposes are for example the robbery of information, political actions, make profit, or simply weaken one stakeholder of the industry.

The global aviation industry has many layers overseeing the safety of all the stakeholders involved, from aircraft manufacturers to the passenger boarding a flight. Overall, these different actors can be classified into 4 categories:

> **One international organization:** the International Civil Aviation Organization (ICAO), part of the UN. It codifies the rules of investigation internationally and designs international civil aviation Standards and Recommended Practices in collaboration with its member states.
>
> **Governments:** National Investigation Organizations, virtually security agencies that investigate on behalf of countries involved in the accident. France's Bureau d'Enquêtes et d'Analyses (BEA) or the USA's National Transportation Safety Board (NTSB) are the main examples of such organizations. On top of ICAO's guidelines, they may develop additional safety standards (for example, the NTSB developed smoke detectors in aircraft toilets).
>
> **Trade organization of airlines:** International Air Transport Association (IATA) oversees standards at industry level and is directly in contact with most of the world's airlines.
>
> **Manufacturers of aircraft and security systems:** many large corporations such as Boeing, Dassault, Thalès, Honeywell… They constantly update their systems to face new threats with the advice of the different boards described above.

Because of its complexity and its weight in the economy, breaking the aviation industry's security constitutes a great challenge for hackers and terrorists. Moreover, this industry relies more and more on information and communication technology (ICT). As an industry that is well known for providing one of the safest types of transportation, it is mandatory for all its stakeholders to understand the risks and to prevent any malicious events for the good of the industry, the economy, the population and the environment.

ISSN 2581 3382

The Aviation Sector, Subject To Cyber Threats

The aviation sector is not immune to the cyber security risks that have been critical issues for all the other industries. Aircraft like the Boeing 777 are very complex systems that rely on many transponders to communicate their position to air traffic control. It's quite difficult to hack all systems at once, including the on-board radios and the Aircraft Communications Addressing and Reporting System (ACARS), used to send messages or information about the airplane rather than voice transmissions. Consequently, "an attacker with a deep knowledge of the plane's system could intentionally cause serious problems with its normal operation" (Paganini, 2014). Major cyber-security incidents in the aviation sector strengthen this observation, and the threat is not as recent as one might think.

In 2013, security researcher Hugo Teso demonstrated at a conference that he was able to manipulate the ACARS described above using… his Android smartphone (Greenberg, 2013).

In 2015, Chris Roberts, another security expert, was questioned by the CIA following a now infamous tweet in which he allegedly pirated his flight's EICAS (Engine Indicating and Crew Alerting System) : "Find myself on a 737/800, lets see Box-IFE-ICE-SATCOM, ? Shall we start playing with EICAS messages? "PASS OXYGEN ON" Anyone ?" (Wagstaff, 2015).

In her research paper, security specialist Ruben Santamarta exposed the backdoors and remote control of SATCOM aviation radios, reaching the rather alarming conclusion that "the current status of the products [we] analyzed makes it almost impossible to guarantee the integrity of thousands of SATCOM devices" (Santamarta, 2014).

It isn't just navigation systems that have been subject to cyber-attacks. An attack on the internet in 2006 forced the US Federal Aviation Administration to shut down some of its air traffic control systems in Alaska. In July 2013, an attack led to the shutdown of the passport control systems at the departure terminals at Istanbul airport, causing many flights to be delayed. Finally, an attack that possibly involved malicious hacking and phishing targeted 75 airports in the USA in 2013. These are just a few examples among many more but they justify the needs to prevent such threats that could lead to dramatic consequences.

Communication between people and devices, the rise of computing performance, price erosion and software developments are all ingredients shared by all the industries that enhance the necessity to consider seriously the cyber threats in the aviation sector. Indeed, aviation security

ISSN 2581 3382

remains a critical topic despite all the investments and measures that have been made, especially when the examples above point out that this threat is not a new trend at all.

One of the major explanations for this new type of threat in this sector is the greater use of computer-based systems: sophisticated air navigation systems, on-board aircraft control and communication systems, airport ground systems including flight information and security screening, day-to-day data management systems.

In the same time, cyber threats have been developed regardless of the industries but in relation with technologies: computer viruses, malicious attacks, etc. Because of an increasing number of travelers, the creation of new modern airports, the introduction of more complex aircraft, the use of IT and advanced computer-based systems, the risks will increase considerably with time. In addition to this, it is important to consider the digitalization of the sector with electronic ticketing for example or the goal of reducing costs by the reduction of manpower for example.

Like any other industry, it is possible to consider two types of cyber security breaches:

1. "opportunistic": the goal is to exploit mistakes made by internal users like employees using the IT systems with the purpose of causing inconvenience and nuisance to any entity involved in the aviation ecosystem
2. "calculated and premeditated": it concerns any malicious attacks to disrupt operations or threaten lives. This category is critical as terrorism are fully aware of the potential of technologies and cyber-attacks.

Then, like in the other industry, we can mention different factors that would influence the cyber security strategy:

- There are more and more interactions between people, devices and services. This increase and diversity in the interactions make the paths of attacks less and less predictable
- Innovation and cost reduction made by the ecosystem transform nonexistent or unavailable technologies into common goods. Moreover, software is more and more used to provide effective solutions and digital experience to the workers of this industry and passengers. Consequently, this evolution exposes more and more internal and external systems to potential threats.

ISSN 2581 3382

For example, a report from the NASA (2009) highlights the rise of software complexity in all industries:

- Flight software lines of code has increased 10 times in ten years
- From 1960 to 2000, functionality provided by software to pilots has grown from 8% to 80%.

Moreover, despite this new complexity, the aviation systems seem not to be prepared. Indeed, since the creation of the first aviation network, the systems ran isolated and were designed more for high availability than for security.

Efforts have been made but not enough

It is important to consider the rise of software complexity in the aviation sector. Indeed, software complexity is increasing and software security cannot be totally guaranteed. This is the reason why it is important to handle vulnerabilities in this sector, to deploy software updates to prevent any attacks and of course to test regularly the security of critical systems.

With the complexity and the high number of stakeholders in this industry, the number and the origins of breaches could be substantial. In the same way, establishing the stakeholder accountable for a breach or an attack could be difficult. Some previous cases in the aviation sector have led to some observations. For example:

- When a vulnerability or a breach is discovered, vendors do not always address or fix it
- No stakeholder would accept to be accountable for a breach or a vulnerability: the suppliers blame each other, the main manufacturers such as Airbus or Boeing blame the suppliers, the airplane operators blame the manufacturers and so on
- Critical systems and cabin systems on airplanes are not isolated properly from external threats
- The principal internal communication protocol, Avionics Full DupleX (AFXD), had poor security solutions implemented

As cyber-attacks against the aviation industry have increased considerably, setting the cyber security as a major concern, all 4 categories of industry stakeholders as pointed out earlier worked together to address these cyber threats.

ISSN 2581 3382

The major efforts made by these stakeholders are the following:

- With the increase of cyber-attacks in all the industries and the increase of computer-based solutions used, ICAO encourages better and stronger collaboration between all the stakeholders to identify as many threats and risks as possible (Lim, 2014)
- ICAO organized a discussion to define responsibilities on cyber security for the aviation industry
- ICAO would like to encourage countries to implement strong cyber security strategy and management. The goal is to implement more policies and measures to prevent any cyber-attacks that could lead to dramatics consequences. This recommendation by the ICAO includes crisis management and business resilience.
- More and more countries started to work on cyber security few years ago. More and more airports started to implement measures to secure any IT systems already exposed. They also started to consider upstream the cyber-security issues for the future projects.
- With safety as a top priority, IATA conducts yearly audits mandated by governments and provides airlines with a cyber-security toolkit that has a traditional risk assessment approach (IATA, 2015).
- Finally, manufacturers have made some efforts as well: Boeing implemented additional security measures on the 777 aircraft to prevent onboard hacking of critical computer systems (Federal Register, 2013)

A good example of cross-stakeholder collaboration is the National Transportation Safety Board, the US government agency that investigates and provides recommendations on accidents that occurred in all forms of transportation. The processes in place in this agency are "more focused on figuring out what went wrong than in laying blame or assigning liability", and takes into account the perspective of all stakeholders involved in the accident to make conclusions. Many experts in the US have been recommending that the government develops a similar agency with a focus on cyber-security in transportation, a quest that may have found its answer in the 2016 Cyber-security standards for aircraft to improve resilience act, or the Cyber AIR act (Wolff, 2016).

ISSN 2581 3382

Although a lot of efforts have been made, there still exist a lot of issues to be addressed.

Cyber Security Challenges For The Aviation Industry

As the aviation industry is known for providing one of the safest types of transportation, it is mandatory for the stakeholder to consider seriously the cyber threats if they want to preserve the efficiency, security and resilience of their systems. Moreover, underestimating this new types of threats would lead to a drop in the number of users as people would are looking for a safe transportation network. To deal with these threats and to maintain a high degree of confidence, stakeholders would need to continue the efforts made to date.

To strengthen its cyber security, the aviation industry could consider some of the propositions made by experts and agencies globally. The following suggestions seem to be the most appropriate:

- The aviation industry has to evolve and to introduce strong systematic tests against cyber threats in addition to the compliance testing already implemented. The latter does not imply security and is managed internally by experts in compliance and availability testing. Internal security testing is then disregarded because of internal constraints and a lack of expertise. It is more than important to test all the components independently and the complete systems by external experts. These experts would have the advantage to be independent, less constrained, unbiased, creative, and more than anything else expert in breaking systems.
- The aviation industry is made up of traditional isolated systems that are more and more connected and exposed (AIAA, 2013). Like in other industries, for any project it is important to:
- Assess the needs and the allowance for these external links to ensure that security processes are implemented
- Ensure that vulnerabilities can be addressed quickly
- Be aware that security updates might break current certification. The choice of expose and connect isolated systems implies to consider a new environment

ISSN 2581 3382

- Critical systems should be tested by external and independent companies that have a real expertise in cyber security.
- Provide high security for critical communication systems such as the radio. This security should ensure strong authentication, confidentiality, integrity and availability. Any other unprotected communication systems should be considered as potentially compromised. Finally, it is important to check that critical and non-critical systems are isolated.
- Any company in the aviation industry should raise awareness among all the employees on the importance of considering seriously cyber threats. It is important to set up a real cybersecurity culture in the critical entities of this industry.
- Every company in the aviation industry should assess its needs in term of cyber security. These companies should be aware of their vulnerabilities and implement some measures to reduce them. Like any other industry, the aviation sector should consider seriously cyber security like they do for HR, Finance, operations and so on. The companies of this industry should have a deep understanding of the threats and the risks. Who are the attackers? What are their motivations? How will they attack? What should be protected in priority?
- Implement stronger internal policies and plans within the company. Indeed, as companies rely more and more on computer-based systems, interact more and more with other companies or people such as passengers, it is mandatory to strengthen internal policies and plans.
- It would be important to implement also recovery plan and to increase resilience.
- Governments should set up some regulations and norms in term of cyber security

All these recommendations might be already implemented today but it is interesting to note that they are shared with the other industries. The aviation industry might be more cyber-secure nowadays, it should continue to strengthen its systems as technologies evolve constantly, so do the threats.

The Automotive Industry

ISSN 2581 3382

The automobile industry is the most common way to travel from point A to point B, since its inception in 1768. The first steam-powered automobile capable of human transportation was built by Nicolas-Joseph Cugnot (Eckermann, 2001) who built the first working self-propelled mechanical vehicle that could transport people. Since then, the industry saw many changes and developments. Speed, gas consumption, performances and equipment all changed from the 18th century to the 21st. The automotive industry comprises passenger cars, trucks, buses and vans.

Today, it is Europe's number one source of mobility and a key sector for the economy of every major country (car manufacturers) in the world. According to the "Organisation Internationale des Constructeurs d'Automobiles" (OICA), the world motor vehicle production surpassed the 68 million in 2015. OICA says:

> "Building 60 million vehicles requires the employment of about 9 million people directly in making the vehicles and the parts that go into them. This is over 5 percent of the world's total manufacturing employment. It is estimated that each direct auto job supports at least another 5 indirect jobs in the community, resulting in more than 50 million jobs owed to the auto industry. Many people are employed in related manufacturing and services. Autos are built using the goods of many industries, including steel, iron, aluminum, glass, plastics, glass, carpeting, textiles, computer chips, rubber and more."

The level of output is close to 1.9 trillion Euros in turnover, and if the vehicle manufacturing industry was a country it would be the 6th largest economy in the world! (OICA, 2016).

Just like in the aviation industry, the development of new technologies, the world automobile industry is subject to a new and growing type of threat: Hacking and Cyber threats. With the growing interest and the vision for connected and driverless cars, the impact of such threats grow ever and ever. The basics of cyber security stipulate that in order to hack a system, you need to exploit a vulnerability. In our vehicle study it can be the driver, a car system, an induced engine failure etc. The vulnerability and the threat level of a system grows with the number of possible entry points; the more entry points there are, the more the chances of hacking a system become higher. Considering the direction the automobile industry is heading to, we can but worry about the growing hacking threat of such an indispensable product.

ISSN 2581 3382

The safety and surroundings of the vehicle industry is regulated by different layers and organizations:

- International and/or continental associations: The United Nations Road Safety Collaboration (a collaboration under the WHO of the UN, see reference) for example. The General Safety Regulation by the European Union.
- National: Federal Motor Vehicle Safety Standards (FMVSS) for example is the standards issued by the US department of Transportation
- Car manufacturers: Vehicle manufacturers are keen to produce safe cars, not only because they care about the people driving their cars, but because if a manufacturer produces unsafe cars, he will be doomed to failure and bankruptcy. Therefore, one key issue and concern of vehicle manufacturer is the safety of the drivers and passengers. Manufacturers are also represented by the OICA described above, whose mission is "to defend the interests of the vehicle manufacturers, assemblers and importers grouped within their national federation" (OICA, 2016).

Car Safety And Car Safety Systems

According to the *Global Status Report on Road Safety 2015* (World Health Organization, 2016)

- The number of deaths per year has slowed and averages of 1.25 million thanks to laws, regulations, drug-alcohol-substance abuse regulations, road safety improvements and car driving assistance and safety measures.
- Despite this progress, road accidents "are the leading cause of death among young people aged between 15 and 29 years, and cost governments approximately 3% of GDP. […] Action to combat this global challenge has been insufficient"
- "Road traffic injuries are currently estimated to be the ninth leading cause of death across all age groups globally, and are predicted to become the seventh leading cause of death by 2030"

Even though the number of annual road related death has plateaued at around 1.25 million, the number is still huge with approx. 3 200 deaths per day! Moreover, "Policymakers must give more attention to making vehicles and roads safer". This is especially true since the WHO report underlines the fact that most countries do not apply all the minimum safety standard put

ISSN 2581 3382

in place by the UN to the new cars issued. For example, Electronic stability control (ESC) is effective at reducing crashes and saving lives. However, only 46 countries have put in place a mandatory rule of implementing such a control system in new manufactured cars. Those underlined subjects and worries of the WHO and the UN are troublesome findings: in an era where cars are getting more and more advanced, the new types of security and safety issues are rising. But the car regulations are still not reflecting nor addressing all the old security checks. If these "basic" issues are sometimes overlooked, cyber-threats certainly would not be reflected in regulations.

With technological improvements, the car industry saw various types of modifications and the driving experience has been geared toward assistance and safety system implementation. Some of these systems are listed below (VDA, 2015):

- **DADS**: *Driver Alertness Detection System* to prevent crashes caused by fatigue
- **Automatic Braking** systems to prevent or reduce the severity of collision.
- **Adaptive cruise control** which maintains a safe distance from the vehicle in front
- **Electronic Stability Control**, which intervenes to avert an impending loss of control
- **Collision avoidance system**: designed to reduce the severity of a collision by braking, steering or alerting the driver
- **Automated parking** system

It should be noted that all these systems are connected and networked with the main network system of the car called a CAN bus. All the pieces in the car can communicate and take commands from this CAN bus.

Technological Prowess And The Incoming Cyber Threats

The technological prowess and the urge to make customer's life easier have led the car industry to head toward a more pronounced driver assistance: autopilot and driverless cars as well as constant internet connectivity.

Toyota is currently partnering with MIT and Stanford University to develop a driverless car. The firm established a collaborative research center in late 2015 to accelerate Artificial Intelligence Research by investing approximately USD 50 million (Toyota, 2015)

ISSN 2581 3382

Tesla on the other hand has already implemented an autopilot feature on its Model S and Model 3. "Autopilot allows Model S to steer within a lane, change lanes with the simple tap of a turn signal, and manage speed by using active, traffic-aware cruise control" (Tesla, 2016).

Toyota, among other manufacturer like Mercedes' trucks division, has already implemented a "Lane Keeping Assist" system, whereas with the push of a button the car/truck would stay on the same lane (on highways) and would signal the driver if it's getting too close to the lane limits or exceeds it. One of our group member experienced it with a Mercedes Truck on a highway: once the system is switched on, the truck would stay in lane via cruise control assistance. However, by steering a little bit off-lane, a loud alarm sound would detonate to alert the driver or wake him (If he's feeling some drowsiness). Speaking of truckers, we found that some of them use this feature to get 10 to 40 seconds of shut-eye on long roads.

All of the cars system are interconnected to its main computer and even have an entry point which is called the OBD-II interface or other variant of it (E-OBD for Europe, and J-OBD for Japan). This entry point is similar to an Ethernet point for the car, where all the systems (braking, steering, driver assistance, sensors, gas etc.) are connected and is used by mechanics to detect any error in the entire car's system.

In conclusion, any successful attack on any system in the car can lead to a total or partial control of the car's functions and systems.

My car… Can it be hacked?

The automobile industry is subject to threats. There are two types of cyber security breaches:

1. "opportunistic"
2. "calculated and premeditated": think of an assassination scenario

Also, like in the aviation industry, we can mention different factors that would influence the cyber security strategy:

- There are more and more interactions between people, devices, services but also and more importantly between Cars and the Internet. This increase and diversity in the interactions make the paths of attacks less and less predictable and the number of entry points climbs even more

ISSN 2581 3382

- Software and "AI" is more and more used to provide effective solutions and digital experience to the workers of this industry and passengers making internal and external systems open to potential attacks

As we mentioned before, the OBD port, typically located below the dashboard on the driver's side (Vanian, 2016) interconnect all the car's main systems. The threat that arises is that if someone plugs a malicious device into this port, he can take control of all the car's systems - "hackers who directly connect their laptops to the port through an intermediary device can basically plug into car's control system and have access to everything".

The implementation of SIM chips to connect them 24/7 to the internet is no small feat, this also expands the possibilities and multiply the vulnerabilities of a car. By connecting a car to the internet, it becomes the same as a computer with a certain IP address and can be hacked into (though not just as easily as a computer, which is not that easy to begin with). There are different motivations behind hacking a car. In the video How To Hack A Car (Motherboard, 2016), the most interesting reasons and their problem were:

- Small theft: Hacking into a car need extreme knowledge of the car and hacking skills are not easy to gain in order to do such a feat
- Surveillance: Cost may be too high to monitor a car's position or hear what is happening inside. Hacking into a cellphone may prove easier and less costly, moreover Governments have already access to all communications!
- Death/Threats/injuries: by taking control of a car on the highway for example or in mountain roads can lead to disasters and potential deaths. The problem is the same as with other reasons: Hacking into a car is no small feat.

There have been proofs that cars can be hacked, and some researchers have successfully hacked into cars and took control of them.

The Jeep Cherokee:

In 2015, after more than a year of work, two researchers Charlie Miller and Chris Valasak developed a technique to hack a Jeep Cherokee and took full control of the car (driven by a Wired.com journalist), making it crash at the end. According to the Wired article (Wired, 2015) "the result of their work was a hacking technique [zero-day exploit] that can target Jeep Cherokees and give the attacker wireless control, via the Internet, to any of thousands of vehicles." What they were able to do was to create a software that can be introduced to the

ISSN 2581 3382

car's entertainment system and lets them send commands to the dashboard function. Effectively this meant that they would have control over transmission, braking, vents, honk, radio and other systems, all this from their laptop from far away.

This was possible thanks to the internet connectivity of the vehicle. Uconnect, an Internet-connected computer feature in cars and trucks, controls the vehicle's entertainment and navigation. It also enables phone calls. This internet connection give an IP address to the car which can then be used to hack into the entertainment system. Once there, the hackers could rewrite the chip's software in order to introduce their code in it. The new firmware would then be capable of sending commands through the CAN bus, to its physical components like the engine and wheels.

The CHT (CAN Hacking Tool) Device:

Made to penetrate the CAN Bus system and relies information to the internet: "The device is a CAN Hacking Tool that attaches via four wires to the Controller Area Network or CAN bus of a vehicle, drawing power from the car's electrical system and waiting to relay wireless commands sent remotely from an attacker's computer […] It can take five minutes or less to hook it up and then walk away (Greenberg, 2014). This perpetrator is untraceable, even if the device is found!

Corvette's brakes:

"Researchers from the University of California at San Diego were able to find a way to wirelessly hack into any of thousands of vehicles through a device that is mounted on cars: A 2-inch-square gadget that's designed to be plugged into cars' and trucks' dashboards and used by insurance firms and trucking fleets to monitor vehicles' location, speed and efficiency." (Wired, 2015). The hack consists of the hacker sending and SMS to these devices that are connected to the dashboard of a Corvette and were able to transmit a message/command to the car's CAN bus and therefore turning on the Corvette's windshield wipers and disabling its brakes.

ISSN 2581 3382

The more we advance, the more the car ecosystem will be transformed into a computer-like one. As Francis Govers of Unmanned Vehicle University says:

> "With these advances, security concerns will soon move to the forefront. At that point you'll need all the things you have on a home computer -- a firewall, virus protection and regular updating for that software […] because it will be much easier for a hacker to find out where you are and, for example, burglarize your home" (Norton Cybercrime News, 2015)

The Tesla model S works with a unique iOS application tied to the Apple account of the driver. This application can lock and unlock the car for example. Technically speaking, hacking the Tesla IOS app of a Tesla owner could result in locking/unlocking the car and therefore theft.

What is being done

The European Commission has formed a working group to consider new legislation to make cars more secure, while the Alliance of Automobile Manufacturers in the US has set up a hub for carmakers to share information about attacks (Financial Times, 2016).

Car manufacturer are recalling any hackable car model. For instance, after the Jeep Cherokee hack, Chrysler pulled 1.4 million vehicles from the US after the discovery (BBC, 2015).

Governments also got involved by way of public announcement to encourage reporting of any potentially hacked vehicle. In the US, the FBI and the US department of Transportation asked all citizens to be careful with their connected cars and that they should report any suspicious issues. The government is trying to raise awareness on this topic (FBI announcement, 2016).

In the US, senators have already begun to put legislations in place in order to counter the cyber-attacks against vehicle, because vulnerabilities in this industry can lead to catastrophes.

Argus Cyber Security reported in a post from late 2015:

> "Senator Edward J. Markey (D-Mass.) and Richard Blumenthal (D-Conn.) announced legislation that would direct the National Highway Traffic Safety Administration (NHTSA) and the Federal Trade Commission (FTC) to to take action and federal standards to secure our cars from cyber-attacks. The proposal came right after Sen. Ed

ISSN 2581 3382

> Markey's office released a report stating that millions of cars and trucks are vulnerable to hacking through wireless, remote technologies that could jeopardize driver safety and privacy. This was followed by CBS News' "60 Minutes" story showing how a leading vehicle brand was subject to remote hacking."

However, what is worrisome is that we did not find any trace of regulations, laws or initiatives to move against those cyber threats in the WHO reports, OICA reports and announcements, the *Global Status Report on Road Safety 2015* or the *Annual Report* 2014 by the Global Safety Road Partnership.

Conclusion

Aircrafts and cars both evolve in complex, hierarchized environments where many stakeholders are involved. They are the by-products of many years of technological prowess and have greatly facilitated our daily lives. Unfortunately, this network of stakeholders and this advanced technology have failed to protect them from cyber-attacks in recent years. On June 30th 2016, a Tesla self-drive car user was killed when the system failed to detect a turning truck (Time, 2016). The investigation conducted so far may point at a technical failure and not intended crime, but this accident really does illustrate the threat on human lives in the case of a malicious attack on our connected planes and cars. We hope that all the actors in both industries will continue their efforts to make air and roads free from hackers.

Bibliography

AIAA. (2013). The connectivity challenge: protecting critical assets in a networked world - a framework for aviation cybersecurity. Retrieved from https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf

Argus Cyber Security. (2015). Senators to introduce legislation to protect drivers from auto cyber- attacks. Retrieved from https://argus-sec.com/senators-introduce-legislation-protect-drivers-auto-cyber-attacks/

ISSN 2581 3382

BBC. (2015). Fiat Chrysler recalls 1.4 million cars after Jeep hack. Retrieved from http://www.bbc.com/news/technology-33650491

Eckermann, E. (2001). World History of the Automobile.

FBI. (2016). Motor vehicles increasingly vulnerable to remote exploits announcement. Retrieved from https://www.ic3.gov/media/2016/160317.aspx

Federal Motor Vehicle Safety Standards. Retrieved from http://www.nhtsa.gov/cars/rules/import/FMVSS/

Federal Register. (2013). Special Conditions: Boeing Model 777-200, -300, and - 300ER Series Airplanes; Aircraft Electronic System Security Protection From Unauthorized Internal Access. Retrieved from https://www.federalregister.gov/articles/2013/11/18/2013-27343/special-conditions-boeing-model-777-200--300-and--300er-series-airplanes-aircraft-electronic-system

Financial Times. (2016). Internet-linked cars face hack threat, warns security expert. Retrieved from https://next.ft.com/content/515bc2c2-0360-11e6-9cc4-27926f2b110c

Greenberg, A. (2014). This iPhone-Sized Device Can Hack A Car, Researchers Plan To Demonstrate. Retrieved from http://www.forbes.com/sites/andygreenberg/2014/02/05/this-iphone-sized-device-can-hack-a-car-researchers-plan-to-demonstrate/#f58c9ab6b8c8

Greenberg, A. (2013). Researcher Says He's Found Hackable Flaws In Airplanes' Navigation Systems. Retrieved from http://www.forbes.com/sites/andygreenberg/2013/04/10/researcher-says-hes-found-hackable-flaws-in-airplanes-navigation-systems/#67f5622123b7

IATA. (2015). Aviation Cyber Security Toolkit 2nd Edition. Retrieved from http://www.iata.org/publications/Pages/cyber-security.aspx

Lim, B. (2014). Emerging Threats from Cyber Security in Aviation - Challenges and Mitigations. Retrieved from http://www.saa.com.sg/saaWeb2011/export/sites/saa/en/Publication/downloads/EmergingThreats_CyberSecurityinAviation_ChallengesandMitigations.pdf.

Motherboard. (2014). How to Hack a Car. Retrieved from https://www.youtube.com/watch?v=3jstaBeXgAs#t=18

ISSN 2581 3382

NASA. (2009). Study on flight software complexity. Retrieved from https://www.nasa.gov/pdf/418878main_FSWC_Final_Report.pdf

Norton Cybercrime News. (2015). Francis Govers on Connected cars. Retrieved From http://cybercrimenews.norton.com/eye_fi/feature/emerging_threats/internet_connected_cars_security/index.html#axzz4DB1MoY9A

OICA. (2016). About us. Retrieved from http://www.oica.net/category/about-us/

OICA. (2016). Passenger car production by country/region. Retrieved from http://www.oica.net/wp-content/uploads//Cars-2015-Q4-March-16.pdf

Paganini, P. (2014). Cyberthreats against the aviation industry. Retrieved from http://resources.infosecinstitute.com/cyber-threats-aviation-industry/

Santamarta, R. (2014). A wake-up call for SATCOM security. Retrieved from http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

Tasch, B. (2014). Former Malaysian Leader Accuses CIA of Cover-Up in Missing Jet. Retrieved from http://time.com/104480/malaysia-airliens-flight-370-mahathir-mohamad/

Tesla. (2016). Tesla Motor website, Model S features. Retrieved from https://www.teslamotors.com/models

Time. (2016). Tesla driver killed in crash while using car's self-driving system. Retrieved from http://time.com/4390853/tesla-self-drive-driver-killed-car-crash-auto-pilot/?xid=homepage

Toyota. (2015). Toyota to partner with Stanford University and MIT for driverless car development. Pressroom Release. Retrieved from http://pressroom.toyota.com/releases/toyota+establishes+ai+research+centers+mit+stanford.htm

Vanian, J. (2016). Security Expert Says That Hacking Cars Is Easy, Fortune 500.

Retrieved from

http://fortune.com/2016/01/26/security-experts-hack-cars/

ISSN 2581 3382

VDA. (2015). Automation report by the German Association of the Automotive

Industry. Retrieved from

https://www.vda.de/en/services/Publications.html

Wagstaff, J. (2015). Plane safe? Hacker case points to deeper cyber issues. Retrieved from http://www.reuters.com/article/us-tech-aviation-cybercrime-idUSKBN0OA1GK20150525

Wired. (2015). Hackers remotely kill a Jeep Cherokee on the Highway. Retrieved from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Wired. (2015). Hackers Cut a Corvette's Brakes Via a Common Car Gadget –Wired.com. Retrieved from https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/

Wolff, J. (2016). Hacking Airplanes**:** Cybersecurity is even more important when you're up in the air. Retrieved from http://www.slate.com/articles/technology/future_tense/2016/05/the_aviation_industry_is_starting_to_grapple_with_cybersecurity.html

World Health Organization. (2016). Global Status Report on Road Safety 2015. Retrieved from

http://www.who.int/violence_injury_prevention/road_safety_status/2015/en/

ISSN 2581 3382