【欧州】【Common，自動車】

Common - Policies in the use of IoT/Road - autonomous vehicles: European Union Agency for Cybersecurity ENISA report highlights importance of cyber security for connected and autonomous cars

Andrea Antolini　Former Researcher JTTRI

【概要：Summary】

Further automation of vehicles in all transport modes is expected to provide opportunities to improve traffic flows, increase safety for users and reduce environmental impacts of transport. While connected and autonomous cars are being introduced and expecting that fully autonomous vehicles will be commercially available by 2030, the importance of cybersecurity is also rising.

The cybersecurity within the transport sector is an increasingly important aspect as the digitalization of the transport system and the increased connectivity of vehicles makes them also more vulnerable to cyber threats or attacks.

All parts of the transport business including automated vehicles are increasingly exposed to cyber threats as the challenges for security of the Internet of things (IoT) and the digitally connected devices are constantly increasing. Since fully autonomous or driverless cars are connected to the Internet to perform various functions on the road, this connection also increases their vulnerability against cyber threats. In case of autonomous cars, there are many concerns regarding cybersecurity, data security, privacy and their impact on infrastructure. Attacks targeting smart cars including connected and automated cars could lead to vehicle immobilisation, road accidents, financial losses, disclosure of personal data and endanger road users' safety.

The European Union Agency for Network and Information Security (ENISA) as the EU's agency for cybersecurity with its cyber security expertise will have to play an important role in meeting the new challenges in the cybersecurity ecosystem. Numerous actions are undertaken based on the Communication on Cyber Resilience (COM (2016) 410 final) with the aim to mitigate the cyber security threats at different levels. The ENISA's study on good practices for security of smart cars highlights the importance of cybersecurity for connected cars. It mainly aims at promoting cybersecurity for connected and semi-automated cars and defines good practices for those vehicles and by highlighting emerging threats targeting the smart cars' ecosystem as well as the potential security measures to mitigate those threats.

【記事：Article】

1. Background of connected vehicles' cyber security

The increasing digitalization of the transport system makes it also more vulnerable to cyber risks and cyber attacks. So far, the aviation sector has been singled out as a sector with high vulnerability against cyber threats. However, cybersecurity is an important issue also for other transport modes, including rail, road, and maritime transport. Fully

autonomous or driverless cars do not need a driver's intervention to function. Connected cars use Internet connectivity to perform various functions, including measuring location, road conditions and car performance. Connected vehicles can exchange information wirelessly with the vehicle/vessel manufacturer, third-party service providers, users, infrastructure operators and/or other vehicles. The concepts of connected and automated transport (CAT) and especially automated driving is expected to contribute to increase the efficiency and safety of the transport system. However, concerns are increasing for the cyber security of the autonomous and connected vehicles, e.g. smart cars. They could become a potential target of cyber attacks. The EU as well as national authorities needs to introduce the necessary regulations regarding safety, liability, cyber security, data security and privacy.

2. Securing connected and autonomous vehicles

The automotive industry is undergoing an evolution towards connected and autonomous vehicles. Most of the latest automotive models have operating systems providing infotainment and other features to enhance car users' experience or improve car safety. In a fully autonomous world, cars will be connected to each other and also to a wider transport system regulating transportation of an entire city or region. However, by exploiting vulnerabilities in a connected or automated vehicle's internet-connected systems, the vehicle could be externally manipulated. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) interfaces needed for the deployment of intelligent transport systems and autonomous cars, further exacerbate security risks since they largely expand the potential of cyber attacks.

The importance of the vehicles' cyber security has further increased since 31 March 2018, as all vehicle models for which manufacturers want to obtain type approval in the EU must now be fitted with the eCall emergency assistance system. This means that the number of connected cars, and therefore the number of cars vulnerable to remote cyber attacks, will significantly increase.

Furthermore, in the case of fully or partially autonomous vehicles, IT security is vital for driving safety, and therefore for the lives and the physical protection of those in the vehicle and outside. If cybercriminals hack into the transport system, they can bring down entire transport networks, causing extensive damage and they could put the passengers' life at risk.

Therefore, autonomous vehicles will need unique security requirements, which will differ from the requirements for mobile devices or enterprise security, as a remote hijack or utilisation of an autonomous vehicle against other road users is also becoming a possible scenario. Due to the autonomous vehicles' vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, it is imperative that automobile manufacturing industry reacts on these new cybersecurity challenges. They will have to focus on measures that guarantee cybersecurity and they need to agree on and develop common cybersecurity standards to keep development and maintenance costs under control. The industry needs to establish a clear baseline involving the understanding requirements from relevant legislation in the original equipment manufacturer (OEM) markets and leveraging existing international standards around cybersecurity and software engineering. A management system for cybersecurity (CSMS) can help ensuring a relentless application of cyber practices across cars and the digital-mobility ecosystem. The automobile industry will also have to create a true digital-security-by-design culture in engineering, quality assurance, and other core value-chain functions and promote car-software architectures with security built-in. A security-by-design culture should focus on secure development practices, enhanced software-testing processes, and new supplier-audit processes that include cyber issues.

The European Commission's Communication on the road to automated mobility: An EU strategy for mobility of the future (COM (2018) 0283 final) of 17 May 2018

aims to ensure a smooth transition towards a safe, clean and connected & automated mobility system in the EU. The objective is to allow all Europeans to benefit from safer traffic, less polluting vehicles and more advanced technological solutions, while supporting the competitiveness of the EU industry. The Commission's Communication on connected and automated mobility strategy also intends to establish rules for self-driving cars in the entire EU under common legislation. The recommendation will look into the use of 5G large-scale testing, cybersecurity issues and into a data governance framework that enables data sharing, in line with the initiatives of the 2018 Data Package, and with data protection and privacy legislation. Furthermore, a new automotive cybersecurity standard, ISO/SAE 21434 is currently under development and could be published in 2020. The World Forum for Harmonization of Vehicle Regulations (WP 29) is also working on regulations for vehicles.

3. ENISA's new role to strengthen cyber security

Regarding the vulnerabilities of the transport sector's cyber security, the EU works on a number of measures to make the connected and autonomous vehicles more resilient to cyber risks. The EU has taken important steps including the adoption of the EU Cybersecurity Strategy in 2013. The European Commission's Communication on Cyber Resilience (COM (2016) 410 final) aims at mitigating the cyber threats at different levels, including road transport. In 2016, the EU adopted the first legislative act in the area of cybersecurity, the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive"). The NIS Directive puts in place requirements concerning national capabilities in the area of cybersecurity. It also introduced obligations concerning security measures and incident notifications across sectors, including the transport sector. In this context, a key role was attributed to ENISA in supporting the implementation of this NIS Directive. ENISA acts as a centre of expertise dedicated to enhancing network and information security in the EU. It also contributes to the overall goal of ensuring a high level of network and information security. In particular it addresses and responds to network and information security problems. Furthermore, it provides legal measures to boost the overall level of cybersecurity in the EU.

Since the adoption of the 2013 EU Cybersecurity Strategy the ENISA's mandate and role has been reviewed and re-defined, according to the significantly changed overall policy context. In September 2017, the European Commission presented a proposal on ENISA, the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") (COM (2017) 477 final). On 27 June 2019, this new European Cybersecurity Act, Regulation (EU) 2019/881, on ENISA and on information and communications technology cybersecurity certification became effective. It upgrades ENISA into a permanent EU agency for cybersecurity and strengthens ENISA's ability to help EU Member States to address cybersecurity threats. The new ENISA will also be empowered to contribute to stepping up both operational cooperation and crisis management across the EU. The two new key areas where the Agency will play an important role are cybersecurity crisis management and cybersecurity certification and standardization of ICT products and services. The Cybersecurity Act strengthens the mandate of the ENISA and establishes a EU-wide cybersecurity certification framework ("Framework") in which ENISA will play a key role. ENISA are given new tasks in supporting Member States, EU institutions and other stakeholders on cyber issues. It will organise regular EU-level cybersecurity exercises, and support and promote EU policy on cybersecurity certification.

4. ENISA's reports on the importance of cybersecurity for connected and automated vehicles

4.1. ENISA's 2016 study on cyber security and resilience of smart cars

As the EU Agency for Cybersecurity ENISA points out, cyber security attacks become increasingly sophisticated and this development does not spare vehicles, whose increasing connectivity provides a high-risk gateway for potential attacks by cybercriminals. With the emergence of semi-autonomous and autonomous cars, which make use of advanced machine learning and artificial intelligence techniques, the potential risks and cybersecurity challenges increase.

In 2016, ENISA published the study "Cyber Security and Resilience of smart cars", which aims at identifying good practices that ensure the security of smart cars against cyber threats, with the particularity that smart cars' security shall also guarantee safety. The study lists the sensitive assets present in smart cars and the corresponding threats, risks and mitigation factors. The ENISA study points out three categories of good practices, including policy and standards, organizational measures, and security functions. ENISA develops recommendations for smart car manufacturers, tiers and aftermarket vendors as well as insurance companies, industry groups, associations and security companies. According to ENISA, industry actors should improve cyber security in smart cars by establishing the good practices that effectively enhance the security of their products. They should improve information sharing amongst industry actors as it helps them to distribute information and challenge the relevance of their security mechanisms. ENISA also recommends exchanges with security researchers and third parties. Furthermore, the question of liability among industry actors needs to be clarified. Industry actors should define processes to clarify their respective liability in case that security issues arise. The good practices listed in this report are meant as an input for a standardization effort, rather than being directly applicable to a specific car design. The details of the security requirements should be defined in the context of standards. Since the existing safety standards for automotive systems only marginally address security, ENISA recommends to defining an independent evaluation scheme. Industry groups and associations and security companies should build tools for security analysis. Furthermore, industry actors can directly improve their security testing skills by building tools for security testing and security monitoring.

4.2. ENISA's report on good practices for security of IoT

Furthermore, in 2018, ENISA also released its "Good Practices for Security of IoT" report in order to promote security by design for IoT. This report particularly focuses on software development guidelines, which is one of the most important aspects for achieving security by design. Besides analysing security threats in all phases of the IoT software development lifecycle (SDLC) the key points to consider include concrete and feasible good practices to upgrade the cybersecurity. ENISA notes that there has been experimental remote attacks: "on autonomous cars' cameras and Light Detection and Ranging (LiDAR) systems showing effective camera blinding, making real objects appear further than their actual locations or even creating fake objects.", underlining the need to implement security measures to mitigate the potential risks for smart cars.

4.3. ENISA's 2019 study on good practices for security of smart cars

As smart cars are increasingly impacted by the growth of advanced machine learning and artificial intelligence, the number of risks posed by cyber-threats is expected to multiply. In order to deepen the analysis of the findings regarding cybersecurity and resilience of smart cars, ENISA published a new study on 25 November 2019. ENISA's new study

entitled "Good Practices For Security of Smart Cars" has the aim to serve as the reference for automotive cybersecurity and to identify the relevant assets and the rising concerns related to cyber threats that target smart cars, which include the connected and automated vehicles' ecosystem. With the increased connectivity that will be driven by the emergence of 5G, it is expected that new cybersecurity risks and threats will arise, which need to be managed.

While considering the relevant security threats, risks and attack scenarios, the ENISA study's main objectives are to collect good practices to ensure the security of smart cars. More specifically, the ENISA study sets the objectives including the analysis of smart cars architecture and defining a high-level reference model, to identify the smart cars' sensitive assets, as well as the potential and main cyber threats, risks and attack scenarios, which are targeting smart cars. Furthermore, the study aims at mapping identified threats to consider relevant security measures. The report also examines existing legislation, policy and standardisation protocols, which aim at integrating cybersecurity into the connected vehicle technology. Taking stock of all existing standardisation, legislative and policy initiatives, the report defines good practices for security of smart cars, including connected and (semi-) autonomous vehicles.

The ENISA study identifies the potential consequences of cyber attacks on connected vehicles, which can result in remote mobilisation of affected vehicles, road accidents, the loss or theft of sensitive user data, financial losses and potential danger to the safety of other drivers and road users. Therefore, appropriate security measures will have to be implemented to mitigate the potential risks, especially as these attacks threaten the security, safety and also the privacy of vehicle passengers and all other road users, including pedestrians. The report aims at serving as a reference point to promote cybersecurity for smart cars across Europe and to raise awareness on relevant threats with a focus on "cybersecurity for safety".

References:

Connected vehicle cybersecurity report identifies best practice. In: https://www.governmenteuropa.eu/connected-vehicle-cybersecurity/95581/, 26th November 2019

Cyber-attacks: Council is now able to impose sanctions. In: https://www.consilium.europa.eu/en/policies/cybersecurity/#, 17 May 2019, retrieved 29 November 2019

Dealing with cybersecurity threats in the age of autonomous vehicles. In: https://blogs.seqrite.com/cybersecurity-in-autonomous-cars/, 06 November 2019, retrieved 3 December 2019

Deichmann, Johannes, Klein, Benjamin, Scherf, Gundbert and Rupert Stuetzle: The race for cybersecurity: Protecting the connected car in the era of new regulation. October 2019. In: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-race-for-cybersecurity-protecting-the-connected-car-in-the-era-of-new-regulation, retrieved 29 November 2019

ENISA: Cyber Security and Resilience of smart cars. In: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars, December 2016, retrieved 27 November 2019

ENISA Good practices For Security of Smart Cars. In: https://www.enisa.europa.eu/publications/enisa-good-practices-for-security-of-smart-cars, 25 November 2019, retrieved 2 December 2019

ENISA puts Cybersecurity in the driver's seat. In: https://www.enisa.europa.eu/news/enisa-news/enisa-puts-cybersecurity-in-the-drivers-seat, November 25, 2019, retrieved 28 November 2019

ENISA good practices for security of Smart Cars. In: https://www.enisa.europa.eu/publications/enisa-good-practices-for-security-of-smart-cars, November 25, 2019, retrieved 28 November 2019

European Cybersecurity Agency Publishes Report on Smart Car Security. In: http://www.ciobulletin.com/cyber-security/europe-promotes-cybersecurity-for-automated-cars, November 29, 2019

European Union Cybersecurity Agency focuses on connected cars in latest research. In: https://www.iottechnews.com/news/2019/nov/27/european-union-cybersecurity-agency-focuses-connected-cars-latest-research/, 27 November 2019, retrieved 29 November 2019

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In: Official Journal of the European Union, L 119/1, 4.5.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC, retrieved 3 Dec. 2019

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). In: Official Journal of the European Union, L 151/15, 7.6.2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Reynolds, Conor: Connected Cars at Risk of Hijacking, Eavesdropping and DDoS Attacks, In: https://www.cbronline.com/news/vehicle-cybersecurity-enisa, 26th November 2019

Smart car security: Good practices to improve car safety. In: https://www.helpnetsecurity.com/2019/11/26/smart-car-security/, November 26, 2019

The Cybersecurity Act: For an enhanced cyber resilience. In: https://ec.europa.eu/digital-single-market/en/policies/cybersecurity, Last update: 19 November 2019, retrieved 28 November 2019

The EU Cybersecurity Act is Now Applicable. In: https://www.jonesday.com/en/insights/2019/06/the-eu-cybersecurity-act-is-now-applicable, June 2019, retrieved 3 Dec. 2019

Wessing, Taylor: Drive safe! – Cyber Security for connected and autonomous vehicles. In: https://www.lexology.com/library/detail.aspx?g=c5f2f0f7-0ea2-4cdd-84c3-0ae132c9efd2, November 3 2019, retrieved 29 November 2019