IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

A Review on Cyber Security

Manjunath H R[1], Prashanth N M[2], Prathiksha L Shetty[3], Preethi M Rao[4], Prenita Prinsal Saldanha[5]
Department of Information Science and Engineering
Alvas Institute of Engineering and Technology, Mijar, Karnataka, India
manjunathhrdvg@aiet.org.in, pr286354@gmail.com, pathugv12@gmail.com,
preethimylarirao1513@gmail.com, prenitasaldanha22@gmail.com

"Cybersecurity, within the context of road vehicles, is the protection of automotive electronic systems, communication networks, control algorithms, software, users, and underlying data from malicious attacks, damage, unauthorized access, or manipulation."

Abstract: *Virtual simulation experiment teaching is an important content of higher education information construction and experimental teaching demonstration centre construction, and is the product of the deep integration of discipline and information technology. At present, traditional crimes in China are gradually shifting to the Internet, and cybercrimes are frequently and frequently occurring, seriously endangering national security, social order and people's interests. The forging of a team of high-quality professionals in network security and law enforcement is the inevitable path to effectively crack down on network crimes and realise the comprehensive governance of network crimes, and also provides a new examination question for the teaching of network security law enforcement. In view of the network security law enforcement routine practice teaching cannot cover all types of the experiment, especially some reach or irreversible operations (such as electronic data on-site inspection, etc.), and need high cost, large comprehensive experiments training (such as a variety of types involved network crimes probing experiment, etc.), virtual simulation experiment teaching has become an important method in the teaching of network security law enforcement Therefore, combining with the characteristics of network security law enforcement major, exploring the establishment of virtual simulation experimental teaching platform for network security law enforcement plays a crucial role in the teaching of network security law enforcement experiment and practical training.*

Keywords: Cyber Security.

I. INTRODUCTION

With these first regulatory programs for cybersecurity and software updates in the automotive sector, the regulator will require automotive OEMs – the responsible parties for vehicle homologation – to demonstrate adequate cyber-risk management practises throughout development, production, and postproduction of their vehicles, including the ability to fix software security issues after the sale of vehicles and over the air. In this context and based on our extensive research and analyses, we offer a perspective on three key questions for the automotive industry:

- Engine power, fuel consumption, driving comfort, and the precision of a car's chassis and body are just a few dimensions that define the quality of a car. With more and more core vehicle functions enabled by software running on specialised hardware chips, the security of those components – cybersecurity – will become yet another dimension of quality in the automotive industry, in much the same way that physical safety is a major concern and quality parameter today.
- This measure of quality is underpinned by regulatory activities that impose minimum standards for managing cybersecurity risks and require OEMs to have the ability to fix security issues via software updates. Cybersecurity will become non-negotiable for the industry. In order to excel at cybersecurity, new processes, skills, and working practices along the automotive value chain will be required. This includes identifying cyber risks, designing secure software and hardware architectures, and developing and testing secure code and chips, ensuring that issues can be fixed – even years later – via software updates.
- The rising need for cybersecurity will trigger investments over the next few years. We expect to see the market

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

grow from USD 4.9 billion in 2020 to USD 9.7 billion in 2030, with software business representing half of the market by 2030. The strong growth of the market will create many new business opportunities for suppliers, established IT firms, specialist niche firms, start-ups, and many others, especially in the software development and services market. At the same time, the dynamics of the growing market will also challenge today's leaders in the market.

- Engine power, fuel consumption, driving comfort, and the precision of a car's chassis and body are just a few dimensions that define the quality of a car. With more and more core vehicle functions enabled by software running on specialised hardware chips, the security of those components – cybersecurity – will become yet another dimension of quality in the automotive industry, in much the same way that physical safety is a major concern and quality parameter today.

II. PROBLEM STATEMENT

Cyber security is becoming a new dimension of quality for automobiles:

1. **AUTONOMOUS:** Autonomous cars, which have been the subject of fantasy for a long time, are becoming reality. Leading companies have already driven millions of miles on public roads with them, but so far always under the watchful eye of a human behind the steering wheel. The disengagement rate in field tests, i.e., how often the human driver needs to take over control, is rapidly declining, putting fully autonomous cars in reach within mere years. While the autonomous car offers great advantages, it comes with the risk of hackers interfering with steering or braking. Such incidents would foster fear of autonomous cars and put the whole technology at risk.
2. **CONNECTED:** Cars are becoming more and more connected. The services enabled by connectivity today range from sending destination addresses to the vehicle, to receiving real-time traffic information, to parking the vehicle remotely via a smartphone app. However, the connectivity of cars is a potential attack vector for hackers to compromise a full fleet of cars, which is the worst nightmare of every OEM.
3. **ELECTRIC:** The rise of electric cars started several years ago and they are gaining more and more traction as their range increases and their price decreases. Challenged by many start-ups, almost all incumbent OEMs have embarked on the journey to including electric cars in their product portfolios. The electric car per se is not more susceptible to sabotage than a conventional car, but attacks on charging infrastructure can have severe effects, from power outages to fires.
4. **SHARED:** Enabled by connectivity, new business models for transportation have become viable, such as car sharing and ride hailing. The trend in mobility is moving away from car ownership and towards shared-car solutions, 2 Source: McKinsey, "Mapping the automotive software-and-electronics landscape through 2030," July 2019. 3 Source: McKinsey, "The race for cybersecurity: Protecting the connected car in the era of new regulation," October 2019. which is significantly increasing vehicle utilisation. This trend requires full protection of user data – a breach of sensitive data could foster massive distrust of the business model.

A deeper look into the connected car shows three types of software that will drive innovation in this area: — In-vehicle services: All software within the vehicle that runs on electronic control units (ECUs) or domain control units (DCUs) within the car — OEM back-end services: Cloud services for both the vehicle and user — Infrastructure and third-party services: Software links between the vehicle and infrastructure, e.g., gas/charging, parking, insurance. While the industry is investing in innovations across these types of software to enhance the customer experience and increase the value of modern cars, manufacturers must also build in cybersecurity from the beginning to avoid creating cyberattack-prone digital platforms and vehicles.

III. APPROACHES

Ultimately, OEMs are responsible for the homologation of their vehicles and demonstrating their adherence to regulations and mandatory legal requirements. However, since OEMs source a large share of their vehicle components from suppliers and semiconductor manufacturers, their upstream value chain partners will also be required to follow and implement state-of-the art practises to mitigate cybersecurity risks and produce vehicles that are secure by design. These partners must provide evidence of adhering to the regulations to support the type-approval process, which is the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

responsibility of the OEM. Looking at the current drafts of the UNECE WP.29 regulations on cybersecurity and software updates, it becomes evident that the value chain is affected across four areas.

Cyber-risk management. Automotive players must ensure end-to-end cyber-risk management and identify relevant cyber risks in their vehicle types (and in adjacent ecosystem components that might impact vehicle safety or security) and ensure that they implement measures to mitigate such risks. This includes reacting to evolving threats. — Security by design. OEMs must develop secure vehicles from step one by adopting state-of-the-art practises in hardware and software engineering, and ensuring that vehicle types (and adjacent ecosystem components that might impact vehicle safety or security) are designed, built, and tested for security issues and any cyber risks are mitigated properly. Although OEMs are ultimately responsible for cybersecurity, all participants in the value chain need to contribute. — Detection and response. Vehicle manufacturers must be able to detect technical vulnerabilities and security issues (e.g., cyberattacks) in their vehicles and adjacent ecosystem components (e.g., the back end or third-party services) that might impact vehicle safety or security. — Safe and secure updates. Automotive players must be able to respond to any detected security event and provide software updates to fix security issues. To do so, they must systematically identify target vehicles for updates and ensure that software updates will not harm certified safety-relevant systems and are compatible with the vehicles' configuration.

While certain practises are already in place today, the upcoming regulations, higher levels of enforcement, and potential liability implications will require a much more explicit agreement between parties along the automotive value chain on what exactly is expected of each other. To adhere to this higher level of rigour, we are expecting automotive players to: — Define clear roles and responsibilities for vehicle cybersecurity (not just enterprise cybersecurity) and establish interfaces and points of contact for vehicle cybersecurity between players — Agree on a minimum set of cyber-risk management and cybersecurity practises in contractual agreements and derive measurable service levels similar to what has been good practice in other dimensions of vehicle quality (e.g., safety) — Clarify organisational, technical, and legal (e.g., IP) prerequisites that allow security testing and attestation of vehicle software security of the entire E/E vehicle architecture or down to the individual ECU. However, security does not stop at the production of vehicles – it is important throughout the entire vehicle lifecycle, as security vulnerabilities can be discovered at any given time. It will require OEMs and suppliers to continually detect and react to security issues until vehicles have reached their end of life, just as we expect aircraft or engine manufacturers to continuously monitor their aircrafts and engines to detect and fix any operational, safety, or security issues for as long as that equipment is in use by any owner.

— Unit testing: Test the correct implementation of security requirements using software unit verification, software integration tests, and software qualification tests. — Integration testing: Perform system integration and system qualification tests to ensure the correct implementation of the cybersecurity requirements. — System testing: Perform acceptance testing of requirement fulfilment on the basis of a criteria catalogue (e.g., derived from UNECE). New capabilities and cybersecurity requirements along the development cycle will require significant reskilling and upskilling of the current workforce in many cases. The raising of skill requirements is also reflected in the market (see Section 4), where we see a variety of new products and services that all require new skills. But even beyond the activities mentioned above, many other areas require upskilling. For example: — The procurement of security components requires a more collaborative approach compared to the procurement of mechanical parts, e.g., chassis, powertrains, or batteries, where exact specifications can be detailed up front. Although specifications for security components can be laid out in the design phase, adjustments can be expected during the full development cycle. Due to the high complexity of cybersecurity, evaluating providers, especially for capabilities, will become much more challenging compared to sourcing physical parts or normal software. — Project management must take security-bydesign seriously and account for relevant cybersecurity-related activities and artefacts being part of the project, e.g., prioritising cybersecurity in the product backlog. — Dealerships, as the front line to automotive customers, will need to speak to cybersecurity matters (e.g., when reports of vulnerable cars or recent attacks are in the news) and must be able to assist in cybersecurity-related maintenance activities such as deploying software updates when over-the-air updates are not available. — Customer communication teams will need to convey and communicate cyber security related matters, like addressing public fears of cars being vulnerable to cyberattacks or navigating the challenging task of upholding external communication in case of a cybersecurity incident. In the aviation industry, for example, some players have already built-up new skills to address their cybersecurity needs. One leading aviation and defence

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

company developed all of the abovementioned skills internally. It has also built up SOCs to monitor its enterprise IT as well as its OT production. Going further, it's even offering these services to the market, strengthening its position and credibility on the cybersecurity front.

Build a Teaching Model of "Three-step Progression, Four Modernizations and Three Provincial Gauges

The three-step gradualism refers to the establishment of a step-by-step hierarchical system, with the primary stage oriented to general knowledge, the intermediate stage oriented to specialty, and the advanced stage oriented to practical practice. In the primary stage, general education will be carried out for undergraduates who are not majoring in cybersecurity and law enforcement, and immersive game experience mode will be adopted to master the standard awareness of electronic forensics. In the intermediate stage, we will carry out professional core education for undergraduates majoring in cybersecurity and law enforcement, using case analysis and experimental simulation mode, and focusing on mastering the on-site inspection process and electronic data analysis technology. The senior stage focuses on cultivating the practical ability of network security law enforcement for all students and trainees. The integration of the four modernizations refers to the organic integration of interaction and participation, practical cases, immersive experiments and ideological and political courses, and the construction of a high-quality experimental classroom education system. Interactive participation means to adhere to the student entered, use big data to carry out learning situation analysis, teach students in accordance with their aptitude, implement precise strategies, design participatory teaching strategies and methods in line with a variety of learning styles, and carry out all-round, effective and deep interaction. Case practice means that on the basis of the good mechanism of "school-bureau cooperation and school-enterprise cooperation", the "teaching-practical community" is jointly built, and the investigation activities of public security business are deeply carried out, and the classic cases and typical problems of law enforcement in the field of network security are collected, so as to accumulate first-hand case materials for teaching and scientific research work. Experimental immersion is based on the network security law enforcement actual combat teaching platform, the introduction of VR virtual reality technology, highlighting the immersive experimental experience, so that students can truly perceive the electronic inspection site, in order to pass the test, question and answer and immersive experience, learning electronic data extraction and fixed technology and norms, stimulate students' interest in learning; The ideological and political orientation of curriculum means to carry out the construction of professional ideological and political education deeply, to integrate the educational resources of condensed professional courses, to carry out ideological and political education silently and to improve the educational effect. The three provincial gauges mean that the experimental results and final results are no longer taken as the single assessment basis, but pay more attention to the process assessment, improve the formative assessment, and build a relatively fair and reasonable diversified course evaluation system and detailed gauges. Through online time, communication and interaction, platform log, intelligent evaluation and other ways to evaluate the process, result and effect feedback of the three aspects of comprehensive evaluation.

3.1 Approaches to solve the Problem

Build a "three-dimensional, open and multi-level" Experimental Space After the outbreak of COVID-19, the Ministry of Education put forward the work requirement of "no suspension of classes", and nationwide schools carried out large-scale and organized online education and teaching during the epidemic prevention and control period, which is of great significance to the promotion of education and teaching reform by using information means. Meanwhile, higher requirements are put forward for the systematization and functionality of the online experimental platform. In line with the resource sharing, "teaching, learning, practice," the design concept of integration, virtual simulation experiment teaching platform on network security law enforcement has carried on the structure optimization, improve the period of conventional and unconventional, "everyone can learn, to learn all the time, everywhere can learn" learning space construction, building of three-dimensional, open and multi-level experiment space [9]. Three-dimensional refers to the teaching content, based on the network security and law enforcement major teaching experiment outline framework, so that the basic theory of experimental training; In terms of teaching methods, online and offline teaching should be integrated to fully embody the principle of "combination of virtual and real" to carry out diversified simulation teaching experimental projects. Openness is open to students and teachers 24/7. It not only provides students with time and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, August 2022
Impact Factor: 6.252

space for cyber security law enforcement training, so that students can continue to deepen and improve in their spare time, but also builds a platform for teachers to grow in scientific research, so that scientific research feeds back teaching. Multi-level is education of record of formal schooling and go hand in hand, police training teaching experiment platform based on network security law enforcement, law enforcement can carry out network. Security skills contest, to practice promotion, whereas, in order to speed up network security theory knowledge and practice fusion, inspire the motivation for students majoring in network security and law enforcement, improve the students' active learning and expanding the ability to think. At the same time, police training should be carried out around hot topics, and professional training should be optimized in combination with the working situation of public security and cutting-edge technologies, so as to enhance the theoretical, targeted and practical aspects of police training.

REFERENCES

[1]. Administration, N.H.T.S., et al.: Cybersecurity best practices for modern vehicles. Report No. DOT HS 812, 333 (2016)

[2]. Automotive iQ: Automotive Cyber Security - Dedicated eBook for the Cyber Security professional. automotive-iq.com/events-automotive-cyber- security/downloads/complete-automotive-cyber-security- ebook (2017)

[3]. des ConstructersFranaisd'Automobiles, C.C.: Extended Vehicle (EXVE) and Standardisation. https://ccfa.fr/dossiers-thematiques/extended-vehicle-exve-and- standardisation (May 2019), [Online; accessed13. May 2019]

[4]. Ebert, C., Jones, C.: Embedded Software: Facts, Figures, and Future. IEEE Com- puter Society 0018-9162/09, 42–52 (2009)

[5]. Hunjan, H.: Iso/sae 21434 automotive cybersecurity engineering. http:// 2pe5rtjld2w41m0dy17n5an1-wpengine.netdna-ssl.com/wp-content/uploads/2018/07/8_Renesas_Automotive-Cyber-Security-Standardistation- v1.0.pdf (Jul 2018), [Online; accessed 12. May 2019]

[6]. IHS Automotive: Automotive Cybersecurity and Connected Car Report (2016)

[7]. International Electrotechnical Commission: IEC 62443: Industrial communicationnetworks network and system security

[8]. International Standardization Organization: ISO 27000 series, information tech-nology - security techniques

[9]. ISO: ISO 20828. https://www.iso.org/standard/41891.html?browse=tc (2006),[Online; accessed 13. May 2019]