Evolution of Automotive Networks:

One of the most important aspects of the automotive industry's continuous transformation has been the evolution of automotive networks, which have had to adapt to the demands and increasing complexity of modern automobiles. Back then, point-to-point wiring was the main way that vehicle electrical systems were implemented for features like lighting and ignition. Nevertheless, the necessity for a more complex system of controlling and coordinating amongst many electrical devices and modules emerged as cars gained additional features like air conditioning, motorized windows, and sophisticated safety systems.

Controller Area Network (CAN)

This necessity led to the introduction of the Controller Area Network (CAN) in the 1980s, developed by Bosch, which became a standard due to its robustness and efficiency in handling communication in the electrically noisy automotive environment. CAN is a robust vehicle bus standard designed to allow microcontrollers and devices to communicate with each other in applications without a host computer. The CAN protocol was designed to address the growing complexity of vehicle electronics, enabling various electronic control units (ECUs) within a vehicle to communicate with each other over a single or dual-wire network. This innovation drastically reduced the amount of wiring needed, leading to improvements in vehicle reliability, maintainability, and fuel efficiency due to decreased weight. The CAN protocol is known for its high resilience to interference, high-speed capability (up to 1 Mbps), and efficient handling of high-density network traffic, making it particularly well-suited for the demanding environments found in automotive applications. Over the years, CAN has become a standard in the automotive industry but has also been adopted in other areas such as industrial automation, medical equipment, and aviation, reflecting its versatility and reliability as a communication network.

On Data Privacy in Modern Personal Vehicles:

With a growing number of sensors, cameras, safety, and communication systems installed, automakers are incorporating Internet of Things technologies into their new models. As a result of this connectivity, cars collect and exchange enormous amounts of data. This prompts several crucial queries: Who has access to this information? Who is the owner of that? Can customers protect their data in any way? How might this information be used to assign blame in the case of an accident? Could it be used by car owners to prove to the manufacturer that something went wrong? Can emergency services or law enforcement access it? Despite the importance of these concerns in the context of developing automotive automation and telematics, definitive answers are still absent. [1]

Private Information Discovery:

A lack of data encryption emerged when Tesla enthusiasts GreenTheOnly and Theo found a ton of personal information, including contact information, navigation history, and accident recordings, from a salvaged Tesla Model 3. This incident highlights the critical need for laws protecting the privacy of vehicle data and giving owners control over their information in the event of an accident, loss, or sale. Although Tesla suggests that user data be erased upon car resale, there are cases where user data is preserved, indicating that manufacturers and users should share responsibility for data deletion. Privacy concerns are heightened by the changing world of automobile telematics, as seen by the way insurance firms use driving data to modify charges. A study also showed how driving behaviors could be used to identify drivers, highlighting the need for strong privacy measures, and revealing a wide range of privacy issues. [1]

Modern cars, equipped with advanced connectivity and computing capabilities, face significant cybersecurity risks, as evidenced by researchers remotely hijacking a Jeep Cherokee's functions in 2015. The potential for cyberattacks on connected vehicles could lead to scenarios ranging from widespread immobilization to uncontrolled movements during rush hour, posing serious safety and privacy threats. In response, Tesla has initiated a bug bounty program, offering substantial rewards for identifying vulnerabilities, highlighted by a successful attack on its infotainment system at the Pwn2Own event. This underscores the critical need for automotive manufacturers to enhance the security of vehicle systems to protect against emerging cyber threats. [1]

Classification of Attacks on In-Vehicle Network System:

There are four main types of vulnerabilities for possible entry points within in-vehicle systems: sensor-initiated, infotainment-initiated, telematics-initiated, and direct interface-initiated attacks, these draw attention to the two main attack vectors—wireless and physical access—that hackers use to compromise internal car networks. These entry points are used by external inputs to compromise Electronic Control Units (ECUs). Among other methods, hackers may use software bugs or remotely obtain the car's key over the internet to control ECUs. Many security issues pertaining to the in-vehicle network have led to continued study into developing stronger security frameworks. Vulnerabilities in wireless networks can be used to target the bus system of the car. Though many features are already available in smart cars due to the quick development of automotive technologies, no security system can completely prevent all possible attacks. Hackers are improving their techniques to take advantage of smart cars in the same way that technology is advancing.[4]

Security Solutions:

1. Machine Learning Algorithms: Machine learning (ML) techniques have become a prominent solution in the field of wireless networks for tackling security concerns in automobiles. The application of ML models in intrusion detection demonstrates how these methods have the advantage of precisely anticipating different sorts of attacks. Most notably, Song et al. [2] created a powerful machine learning (ML) system that uses time interval analysis of Controller Area Network (CAN) data to identify attacks without producing false positives. Subsequently, Kang and colleagues [3] presented a deep neural network (DNN) framework that improves security by using feature vectors from network packets to train a model that makes accurate distinctions between malicious and legitimate packets. This approach significantly outperforms traditional AI methods, benefitting from unsupervised learning initialization for improved detection accuracy.
2. Cryptography Techniques: The in-vehicle networks of automated vehicles are increasingly vulnerable to cyberattacks, necessitating advanced cryptographic defenses. To mitigate these risks, especially for the Controller Area Network (CAN) bus susceptible to data tampering, several cryptographic strategies have been developed. A notable advancement is the implementation of "delayed authentication" which is a technique that enhances security by generating a Message Authentication Code (MAC) from a sequence of messages, thus allowing for the verification of data integrity over time. Furthermore, an innovative authentication protocol employs symmetric primitives for security, utilizing key splitting and MAC mixing among node groups. This approach not only secures data transmission but also facilitates a more robust, progressive authentication process, significantly reducing vulnerabilities. Each of these solutions contributes to a layered security framework, enhancing the resilience of in-vehicle networks against sophisticated cyber threats.[4]

References:

1. Prevost, S., & Kettani, H. (2019). On Data Privacy in Modern Personal Vehicles. In Proceedings of the BDIoT’19, October 2019. ACM. <https://doi.org/10.1145/3372938.3372940>
2. Song, H.M.; Kim, H.R.; Kim, H.K. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In Proceedings of the 2016 International Conference on Information Networking (ICOIN), Kota Kinabalu, Malaysia, 13–15 January 2016; pp. 63–68.
3. Kang, M.J.; Kang, J.W. Intrusion detection system using deep neural network for in-vehicle network security. PLoS ONE 2016, 11, e0155781.
4. Rathore, R. S., Hewage, C., Kaiwartya, O., & Lloret, J. (2022). In-Vehicle Communication Cyber Security: Challenges and Solutions. Sensors, 22(17), 6679. <https://doi.org/10.3390/s22176679>