Vehicle System Forensics in the Digital World

Krutarth Ghuge - 0746015
COIS 2750: Computer Crime and Forensics

Transportation – one of the biggest needs that stand for the human race today, from bicycles to cruise liners, the advancements in architecture and technology in these have been massive. Of the group, road vehicles, especially the normal passenger cars, vans, pick-up trucks, stand tallest among the group with their daily usage requirements. People use these almost everyday, to commute for work, education, leisure, there are only a few reasons for use, but have plenty of repetitions. The human population as of today is nearly around 7.6 billion, and the number of cars on the road across the globe are approximately 1.4 billion. Although not practical and accurate, considering one person to have one car, nearly 18% of the world population owns a car (A. Chesterton, 2018).

Changes in Automobile Technologies

Ever since Henry Ford paved the way for the future of automobile industry in the 20th century, the progression has redefined how humans look at this industry – right from manufacture, operations and maintenance (Giles Kirkland, 2019). Henry Ford, even with his correct vision, could not have envisioned such a rapid growth of the industry.

One of the latest automobile technologies – autonomous driving, where the need for direct driving work from human is not required anymore, is making changes to the driving component of this industry, and making it optional. The presence of another being (a robot – artificial intelligence (AI)) that can monitor and control the entire vehicle helps humans to continue with their work, on the go, without having to worry about not reaching their destination and being unable to do work in-transit.

With these AI systems in place, data needs to be stored and evaluated. Now another being is in conscious to control the aspects of the vehicle – the speed, locks, temperature, etc, all numerical and statistical data that even a human tends to keep note of when driving.

Digital vehicle forensics deals with the collection of data (or evidence) accessible from the new age automobile servers available for individual automotive manufacturers. Much of the data is recovered to provide proof for criminal activities, find main reason behind accidents and other problems occurred with regard to an automobile.

Understanding how an automobile system collects and uses that data and provides a foundation for investigation purposes is an important exploration area. Without this knowledge, the advancements in general and automotive technology would prove to be useless.

Automotive Data Collection

Automotive data comprises of data from multiple aspects of car use - design, manufacturing, sale, use, operation or maintenance, this can include personal information and other highly confidential data (D'Andrea & Partners, 2021).

The ‘Black Box’ of a car holds any kind of information related to the car. Speed, acceleration, distance covered, location, braking data, etc, it’s like the memory of a car. This data is readily available for use by emergency services/ manufacturers in the event when the vehicle is a part of an accident. However, unlike the manufacturers, these emergency services do not have the same amount of ready access to the data. Data being collected and stored in the black box is constantly sent back to the manufacturer’s servers, and the biggest problem in this is – it includes location data. Hideous personnel in the company could misuse this privacy of the customer!

An AI interface like the General Motors’ OnStar or Mercedes Me Connect, has a very high access to your personal data. Credit card information, voice-command information, Wi-Fi data usage and images from the car’s cameras, all of these are in collection. As the industry develops further, the question need be asked is ‘Is our data safe?’. Automobile companies like Toyota and General Motors, have been avoiding questions related to user data usage, invoking a thought for consumers to look out for what part of their data is compromised (Matt Bubbers, 2020).

Information collected by a car’s sensors, cameras, other voice or touch equipment isn’t safe enough for the consumer and other people around the vehicle. With wireless connectivity, data transmission is synchronous, with live updates of a vehicle’s autonomy continuously being fed-back to the servers. There are approximately 140 data collection points in the average newer generation of cars – the amount of data collected and shared is vast, and finding out the need why as to exactly this data is collected is to be known. Although, this data provides mega benefits to a consumer’s ride, focusing on road safety measures with other vehicles, pedestrians, residents of the vehicles, safety during travel is enforced upon, however, the security of this data is still fairly weak, multiple identities can access and control this data collected.

Forensics in Data Collection

Any individual with access to the server or the vehicle itself can prove to be a source of data extraction, legally or illegally. Using the ideal software tools (like those from Berla Corporation), police services, companies, owners, or any other individual having access can have extract data stored in the black box or vehicle systems. A tool, iVe, created by Berla Corporation, gets information stored in digital systems in a car and presents them in a report structure similar to what is seen with computer or mobile forensics. This information includes, but is not limited to, vehicle serial number, device information, data accessed by Wi-Fi or Bluetooth, favourite travel data, etc (Nhien-AnLe-Khac et al., 2018).

Even so, iVe can also obtain information from synced devices to the vehicle infotainment systems, like a mobile phone. Given that newer vehicle systems give user the ability to make calls, view messages received on their phone on the system screen of their car, all record is present on both the devices, risking the privacy of the user and their contacts, as phone logs, SMS messages, etc, are viewed by personnel using this tool on the car (Nhien-AnLe-Khac et al., 2018).

Being able to obtain this load of information from sensors, event recorders (the black box), in-vehicle systems, provides great potential for vehicle forensics examiners (Dieter Steiner et al., 2019).

Some key methods and data sources like: EDR "Black Box" Data, Infotainment System Data, Diagnostic Trouble Codes (DTCs) and Vehicle Physical Examinations & Mechanical Assessments, all provide a way to figure out reasons behind vehicle system failures, accidents and other conspiracies linked with the car (Holistic

Evidence Preservation). All of this is possible with the right tools for the forensics investigator, however, with tools being available to any person with ease, data is not protected and it needs to be, else it may be used adversely.

Use of Data

Now that the data collected by a vehicle's systems can be extracted – to what extent can it be used? With the analysis of a person's driving attributes and habits, emergency services, insurance companies can understand, if in the event the person meets a car accident, whether or not it was the person's fault or someone else's. Some key figures here would be: braking system, speed, seatbelt being worn, etc. These factors can largely contribute for or against a victim of a car crash, and figure out the guilty (Michael Liedtke, 2018). Although this data can prove to be positively impacting towards society, to some it may not.

Data regarding how a person drives, should it be publicised? Every driver has their own style of driving, and it should not be entirely interfered with. For example, the speed at which a person drives (occasionally or regularly); a person might have to travel at high speeds when they are in a hurry or need to go someplace far in a short time, or it is a high-speed freeway – reasons can't be assumed to be potentially dangerous always.

Challenges Ahead

As manufacturers race to defend against security breaches and data hacks, whilst developing and adding improved automation systems, new vulnerabilities are keen to be inevitable. However, with these main two goals in mind, with any complex technology system today, security is never perfect. To make sure an autonomous vehicle does not become the source of weaponry, the handling of it should not be restricted to a single company – whereas the data should safely be (A. Mutschler, 2022).

Vehicle system architectures will keep getting all the more complex, both hardware and software will have multi-layered components processing at different data levels. With all of this security in each layer will become tedious, and may be overlooked, while we can make the best use of automated technology, if not cared for will become a weapon of destruction, either by itself or at the hands of someone else.

References List:

1. How many cars are there in the world? (Andrew Chesterton, 20 Sept 2018) https://www.carsguide.com.au/car-advice/how-many-cars-are-there-in-the-world-70629#:~:text=What%20percentage%20of%20people%20in,at%20around%2018%20per%20cent.

2. How new technologies have changed the automotive industry (Giles Kirkland, 11 July 2019) https://www.oponeo.co.uk/blog/how-new-technologies-have-changed-the-automotive-industry

3. What is Digital Vehicle Forensics? (SALVATIONDATA Technologies, 1 Oct 2021) https://www.salvationdata.com/tag/digital-vehicle-forensics/

4. New Rules on Data Security for Automobiles (D'Andrea & Partners, 30 Sept 2021) https://www.dandreapartners.com/new-rules-on-data-security-for-automobiles/

5. What kind of data is my new car collecting about me? Nearly everything it can, apparently (Matt Bubbers, 16 Jan 2020) https://www.theglobeandmail.com/drive/technology/article-what-kind-of-data-is-my-new-car-collecting-about-me-nearly-everything/

6. Who Owns the Data Your Car Collects? (Jeff Plungis, 2 May 2018) https://www.consumerreports.org/automotive-technology/who-owns-the-data-your-car-collects/

7. Smart vehicle forensics: Challenges and case study (Nhien-AnLe-Khac et al., 2018). https://www.sciencedirect.com/science/article/pii/S0167739X17322422

8. Vehicle Communication within Networks -Investigation and Analysis approach: A Case Study (Dieter Steiner et al., 2019). https://www.researchgate.net/publication/332819272_Vehicle_Communication_within_Networks_-Investigation_and_Analysis_approach_A_Case_Study

9. Holistic Evidence Preservation with Advanced Forensic Automotive Data Retrieval and Analysis, Kodsi Forensic Engineering https://kodsiengineering.com/holistic-evidence-preservation/

10. How is data being collected and used in my car? (Michael Liedtke, 25 Dec 2018). https://www.chicagotribune.com/autos/sc-auto-tips-0102-driving-data-collection-20181225-story.html

11. Data Security Challenges in Automotive (Ann Steffora Mutschler, 3 Feb 2022). https://semiengineering.com/data-security-challenges-in-automotive/