Годишник на Технически Университет – София, том 70, книга 4, 2020
Proceedings of the Technical University – Sofia, Volume 70, Issue 4, 2020

CYBERSECURITY IN SMART CARS

Maria Nenova, Vesselin Gueorguiev, Stoyan Madzhirov,
Desislava Georgieva, Ivan Evg. Ivanov

***Abstract**: This paper covers the main concepts of smart cars – threats, security, privacy, and a base overview of the technology.*

***Keywords:** autonomous; cars; IoT; security; smart*

1. INTRODUCTION

The term “computer system security” covers the processes and mechanisms by which important and sensitive information is protected from unauthorized access, alteration or destruction, which could be a consequence, both of the actions of persons of uncertain origin and of accidental events. Compared to other computer technologies, the strategies and methods used in the field of computer security are very different, mainly due to the special nature of the activity - prevention of unwanted computer action, instead of providing a specific, desired way of operating the system.

Due to their nature, few IoT devices contain large amounts of sensitive data, making traditional ransom attacks meaningless. As a result, cybercriminals are focusing on completely blocking users' access to devices. At first glance, this may seem more like an inconvenience than something else. But if, for example, this turns off the thermostat in a consumer's home in the middle of winter, the consequences can be significant. On a larger scale - such as compromising the thermostat controlling the refrigerators in a grocery store, or the air conditioning in a data center - the motive behind this new form of attack (and the threat they can be) becomes much clearer. [1][14].

2. AUTONOMOUS AUTOMOBILES – THE FUTURE OF TRANSPORT

An important development for the automotive industry is the awareness of the context that a vehicle is familiar with its neighborhood (including the presence and location of other vehicles). Modern cars now have a network of processors connected to a central computer platform that provides Ethernet, USB, Bluetooth and IEEE 802.11 interfaces. Newer cars also have such features as:

- Event Data Recorder (EDR), inspired by the "black boxes" in the aircraft (EDR records all basic data from the accident recovery vehicle);
- GPS receiver, the accuracy of which can be improved by knowing the road topology (GPS is currently used in many navigation systems);
- Obstacle detection radar at distances up to 200 meters (such radar is often used for adaptive cruise control) and a short-range radar or ultrasonic system normally used for parking.

ISSN 1311-0829
DOI 10.47978/TUS.2020.70.04.027

However, a major barrier to development is that for a long time only a small subset of vehicles will be intelligent, but security mechanisms, especially those involving wireless authentication, require most, if not all, vehicles to be "smart". As a result, the authentication mechanism becomes a business challenge. An additional obstacle is the negative perception that the population may have of such mechanisms - especially the feeling of being constantly monitored by any authority. [1]

3. THREATS

Most users today want more and more connectivity of their devices to the outside world from anywhere, which leads to potential system vulnerabilities and therefore to their privacy. This applies not only to smart cars that are able to connect to home security systems, smart TVs, smart refrigerators and other smart devices, but also to smart homes and apartments, as well as personal data stored on such devices. They are all connected through multiple networks, while their users are not necessarily aware of the vulnerabilities of these systems. Users are more familiar with the security and vulnerability issues of personal computers than those with mobile devices, which also include smart cars and other IoT devices. [2][11]

Unauthorized persons may perform the following activities:Control process is dived on three parts – pressure control loop (5 ms period), flow control loop (0.25 ms period), discrete events control (0.1 ms period). Real-time scheduler has to activate each of these parts according to its period and priority.

- Damage / loss (loss of information stored in the cloud, loss / leakage of sensitive information - for payment, routine rules and the like when selling the car, etc.);
- Eavesdropping / bugs / interception / abduction (repeated messages, when there are no adequate protection measures, attackers can easily control the stopping, control and other functions of the car);
- MITM - Man-in-the-middle or abduction of a session (potential financial losses, uploading malware, obtaining a legitimate key for vehicle theft, network data collection, etc.) ;
- Criminal offenses / abuse (denial of service (DoS, DDoS), which leads not only to damage to the network, but also to unexpected behavior of the vehicle; illegal access to the information system / network (attackers take control of the vehicle));
- Disclosure of confidential information;
- identity fraud (most often as a result of cloning the key, aimed at misrepresenting the vehicle within the road infrastructure systems (toll payments, etc.);
- Malware / malicious activity (using well-known routes for attacks against Linux, Android and Windows environments. Subsequently, such attacks are also carried out against smart cars). [2]

4. SECURITY AND PRIVACY IN SMART CARS

Surprisingly, most people ignore the security and privacy issues that the evolution of automotive technology raises. Currently, each vehicle is registered with its national or regional authority, which assigns it a unique identifier, but in some parts of the US and EU, registration authorities have made significant progress in electronic vehicle identification and similar progress has been made towards machinery. , readable driver's licenses. To allow wireless authentication of vehicles, these authorities must provide each vehicle with a private / public key pair, together with a shared symmetric key and a digital identity and public key. Such bodies are likely to be cross-certified, allowing each vehicle to verify the certificates of another vehicle.

To prevent abuse, the overall organization of the security architecture of such a system must be very carefully designed, especially if it is implemented worldwide and because of the information it will protect, so that registration authorities must create an appropriate infrastructure for public keys. By virtue of this challenge, it is equivalent to securing credit cards or mobile phones, but also involves newer, more difficult issues: it must incorporate security features into strict real-time protocols, such as those used to prevent accidents, securely physical location and distance, and support communication in highly sporadic groups of participants. [3]

Electronic vehicle tracking can be compared to Big Brother, depending on the point of view, but it is a fact that the level of traffic monitoring is increasing. Public acceptance of electronic tracking can be fueled by the prospect of improved safety and optimized passenger traffic and potential revenue for manufacturers. Ultimately, privacy concerns have not prevented the widespread adoption of the Internet, cellular networks or electronic payment systems. Therefore, the right question is not whether it should happen, but how to do it in the most desirable way. [1]

A. Electronic license plates

One of the main ideas is to call the certified identity that the vehicle provides via wireless connection an electronic registration plate. Protocols that use such license plates can be designed in different ways - for example, when the vehicle's engine is running, it can periodically emit a beacon containing its electronic license plate, road position, clock and current speed. In addition, it can store all related data in the EDR. Alternatively, the vehicle can constantly listen to the environment and record the signals it hears (ie it can hear beacons of other vehicles, whether the engine is running or off). This latest design solution helps maintain complex services, but must be designed carefully because it requires a lot of energy. [4][16]

A possible application of electronic license plates is dynamic pricing. The built-in navigation system (or alternatively the driver can check a website before leaving or while driving from a cellular terminal) can offer a choice of routes to the driver, with an estimate of current toll prices. The vehicle will then be charged when it enters the connected toll zones.

Another way to use electronic license plates is to find drivers visiting the scene of an accident: even if no vehicle is within radio range, the culprit is likely to soon pass a parked car that can record its identity (Fig. 1). By questioning the EDR of nearby parked cars, police can seize the identities of all vehicles that have passed a particular location at any given time.

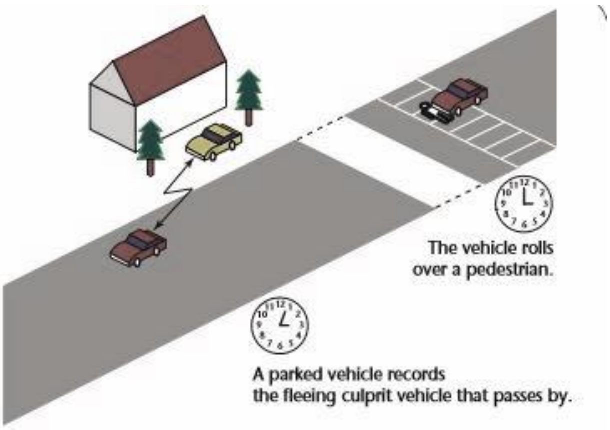

Fig. 1. *A parked vehicle recording a fleeting one. The recorded data can help the police identify the culprit. [1]*

Although complex as an idea, electronic license plates are vulnerable to attack. The first, obvious threat is the attempt by the owner (or thief) of the intelligent vehicle to at least partially deactivate its communication and storage capabilities (in particular EDR). Prevention is easier to automate electronic license plates than physical ones: we can try to protect the physical EDR or trigger an alarm or warn law enforcement. [4]

The second threat is the personification attack: the owner of a vehicle intentionally steals the identity of another vehicle and attributes it to his own car or vice versa. We can prevent this type of attack by storing the identity of the car in hardware resistant to illegal actions, its proper certification and the use of modern authentication protocols. Electronic license plates are much more resistant to this type of attack than physical ones.

A more dangerous attack is denial of service: an attacker systematically or selectively muffles the signals that vehicles exchange. There is no purely technical solution to such attacks, which is one of the reasons we do not see a car that will cancel its driver in the near future.

In order to use radio broadcast information to track the location of a car (and therefore its driver) in a socially acceptable way, it must protect the driver's privacy, at least until collisions occur. For this reason, the broadcast certified identity must be a pseudonym that changes over time; only regional or national authorities should be able to determine the relationship between a pseudonym and its real identity. (Since the car's public key is also broadcast, it must also be changed periodically.) This way, any personal information that the electronic license plate transmits will be insignificant compared to that provided by its physical counterpart. The quality of the scheme can be expressed through the degree of anonymity we defined earlier. [5]

B. Location verification

The location of each car can be determined using GPS or road infrastructure; IVC (Vehicle to vehicle communication) can also help. Existing positioning and distance estimation techniques assume that vehicles cooperate in determining or reporting their locations or distances, but some may try to report false distances or locations. The two solutions for checking the location of vehicles are: [5]

B.1. Tamper-proof GPS

Each vehicle must have a tamper-proof GPS receiver that registers its location at all times and provides this data to fixed stations or other vehicles in an authentic manner. Fortunately, this does not require additional infrastructure and can be implemented independently in any vehicle. One drawback, however, is its presence in urban environments: buildings, bridges or tunnels often block GPS signals. Another disadvantage is that this option relies on so-called tamper-resistant hardware, which has well-known weaknesses. [6]

The most serious problem with this approach is that GPS-based systems are vulnerable to several different types of attacks, including blocking, congestion, sponging, and physical attacks. In addition, relatively inexperienced opponents can successfully execute them. The most dangerous attack involves misleading the GPS receiver with a GPS satellite simulator that produces fake satellite radio signals that are stronger than legal ones. Such simulators are routinely used to test new GPS products and cost between $ 10,000 and $ 50,000. Some simple software changes to most GPS receivers would allow them to detect relatively unwarranted spoofing attacks, but more complex ones would still be difficult to detect. [6]

B.2. Verifiable multiateration

A second vehicle location check solution is based on road infrastructure and uses distance limitation and multilateration. (Distance limitation ensures that the distance is no greater than a certain value; multilateration is the same operation in several dimensions.) This approach eliminates the need for tamper-proof hardware, but requires the installation of a set of base stations controlled by a central power. The infrastructure covers specific roads or city blocks, and can check the location of vehicles in two or three dimensions. [7]

Verifiable multilateration works as follows: Four confirming base stations with known locations perform distance limitation to the vehicle, the results of which give them four upper limits on the distance from the vehicle. If the inspectors can unambiguously calculate the location of the vehicle using these distance limits, and if that location falls within the triangular pyramid formed between the inspections, then they conclude that the location of the vehicle is correct. Equivalently, only three checks are required to verify the location of the vehicle in two dimensions; the inspectors still consider the location of the car to be correct if they can be calculated in a unique way and if it falls into the triangle formed between them. [8][9]

This technology also intercepts remote attacks by external attackers: If an attacker tries to drown out the signal that the vehicle sends to the inspectors and delay its response, the inspectors detect this attack in the same way as if the vehicle itself extended the distance. The accuracy of distance measurements is very important. Today's technology, based on time and time, is extremely broadband, can achieve an accuracy of 15 cm for distances up to 2 km.

Figure 2 shows an example of verifiable multilateration. The intuition behind the technique is that a vehicle might try to cheat about its location. As we mentioned earlier, the vehicle can only pretend that it is further from the veri than er than it really is because of the distancebounding property. However, if it increases the measured distance to one of the veri rs ers, it would need to prove that at least one of these distances is shorter than it actually is, to keep its claimed location consistent with the increased distance. This property holds only if the claimed location is within the triangular pyramid formed by the verifiers: if an object is located within the pyramid and it moves to a different location within the pyramid, it will certainly reduce its distance to at least one of the pyramid vertices. The same holds in two dimensions. [10]

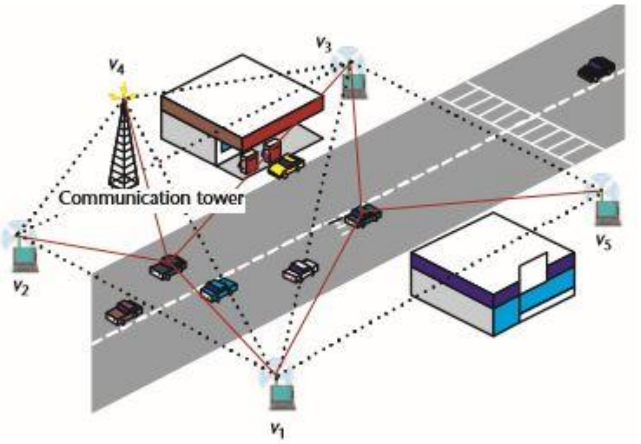

Fig. 2. *Two examples of verifiable multilateration. Base stations v1, v2, v3, and v4 can verify a vehicle's location in three dimensions if the vehicle is located in the triangular pyramid that v1, v2, v3, and v4 forms. Base stations v1, v3, and v5 can verify a vehicle's location in two dimensions if the vehicle is located in the triangle formed by v1, v3, and v5. [1]*

In a real deployment, the number of base stations would of course be much larger than what we see in Figure 5; as a result, a vehicle would always be within the geometric shape that three or four stations form.

5. MAIN PROBLEMS

The main problem that arises from all these technologies is related to the transmission of all this information. The continuous exchange of data between all autonomous vehicles (and there will be a lot, both information and vehicles) will predispose to the occurrence of many interferences and noises, which will interfere with good communication between vehicles and other IoT devices as well.

The solution to this problem lies in the networks of the future – ultra-dense networks, edge computing and fog computing. They will be able to transmit huge amounts of data in small and large spaces and will make the world of IoT possible.

6. CONCLUSION

Smart cars are one of the latest topics of discussion regarding IoT and smart devices and remain an under-explored area. Recently, experts are paying more and more attention to this problem, as the threats and risks affecting smart cars are growing in proportion to the introduction of these new technologies and their use. The domain or infotainment system used to display and connect to a variety of entertainment content that drivers don't really need but want to have in the car remains the biggest problem when it comes to protecting or securing a smart car. By attacking the infotainment domain with malicious code and / or exploiting the driver's own negligence, attackers are able to cause more damage than by hacking personal computers (instead of simply stealing personal data, which can lead to significant damage, as it can jeopardize our identity, misuse of a vehicle can also jeopardize the physical well-being and safety of both drivers and passengers). [12][13]

As smart cars become more accessible to all, the protection of drivers and passengers and the data they store on their mobile devices must not only be accompanied by the introduction of device and car protection features, but also by providing appropriate training and awareness raising for all users who use smart cars in their daily lives. Despite the abundance of security and protection mechanisms, people remain the weakest link in providing information security in general and smart cars in particular. It is also important that devices used by drivers and passengers, as well as cars (usually manufactured by several manufacturers), be certified to ensure a higher level of protection. At the same time, drivers should be informed of these problems when buying or selling such cars. Smart cars should be used with caution and safety, just like any other mobile device or computer. [2][15]

REFERENCES

[1] Srdjan Capkun, Jun Luo, The Security and Privacy of Smart Vehicles, IEEE Security and Privacy Magazine, May 2014.

[2] Gasper Skolc, Blaz Markelj, Smart Cars and Information Security, Journal of Criminal Justice and Security

[3] W. Jones, “Building Safer Cars,” IEEE Spectrum, vol. 39, no. 1, 2002, pp. 82–85.

[4] R. Moebus, A. Joos, and M. Morari, “Multi-Object Adaptive Cruise Control,” Proc. Hybrid Systems: Computation and Control, LNCS vol. 2623, Springer Verlag, 2003, pp. 359–376

[5] W. Franz, R. Eberhardt, and T. Luckenbach, “FleetNet: Internet on the Road,” Proc. 8th World Congress on Intelligent Transport Systems, 2001.

[6] L. Zhou and Z. Haas, “Securing Ad Hoc Networks,” IEEE Network, vol. 13, no. 6, 1999

[7] Anderson, M. J., Kalra, N., Stanley, D. K., Sorensen, P., Samaras, C., & Oluwatola, A. O. (2014). Autonomous vehicle technology: A guide for policymakers. Santa Monica: RAND Corporation

[8] Browne, W. (2016). Internet of things devices increases cyber vulnerability of vehicles (Master’s thesis). Utica: Faculty of Utica College.

[9] L. Klein, Sensor Technologies and Data Requirements for ITS, Artech House, 2001.

[10] A. Serjantov and G. Danezis, “Toward an Information Theoretic Metric for Anonymity,” Proc. Privacy Enhancing Technologies (PET), Springer-Verlag, 2002.

[11] J. Warner and R. Johnston, Think GPS Cargo Tracking = High Security? Think Again, tech. report, Los Alamos Nat’l Lab., 2003.

[12] G. Ateniese, M. Steiner, and G. Tsudik, “New MultiParty Authentication Services and Key Agreement Protocols,” IEEE J. Selected Areas in Comm.

[13] S. Brands and D. Chaum, “Distance-Bounding Protocols,” Theory and Application of Cryptographic Techniques, Springer-Verlag, 1993.

[14] J.-Y. Lee and R.A. Scholtz, “Ranging in a Dense Multipath Environment Using a UWB Radio Link,” IEEE J. Selected Areas in Comm., vol. 20, no. 9, 2002.

[15] Eskandarian, A. (2012). Introduction to smart vehicles. In A. Eskandarian (Ed.), Handbook of smart vehicles (pp. 2–13). Washington: Center for Smart Systems Research in the George Washington University.

[16] Hartfield, S. R. (2017). 21st century automobiles: Vulnerabilities, threats, cyber security and digital forensics (Master’s thesis). Utica: Faculty of Utica College.

Authors: *Assoc. prof. Dr. Maria Nenova*, Technical University of Sofia, Faculty of Telecommunications, dept. Communications Networks
email: mvn@tu-sofia.bg,

Assist.-prof. Dr. Vesselin Gueorguiev – Technical University of Sofia, Faculty of Computer Systems and Technologies, dept. Programming and Computer Technologies
email: veg@tu-sofia.bg,

Stoyan Madzhirov, mag. stud, Technical University of Sofia

Desislava Georgieva, assist.-prof. dr. NBU,
email: dvelcheva@nbu.bg,

Assoc.-prof. Dr. Ivan Ivanov, Technical University of Sofia, Faculty of Automatics,
dept. Systems and Control
email: iei@tu-sofia.bg