A Brief Survey on Cyber Security Attack Entrances and Protection Strategies of Intelligent Connected Vehicle

Zhao Wang[1], Yanqi Wang[2(✉)], Yanan Zhang[2], Yangyang Liu[2], Chao Ma[2], and Haijun Wang[2]

[1] Auto Standardization Research Institute, China Automotive Technology and Research Center Co., Ltd., Tianjin, China
[2] Automotive Data Center, China Automotive Technology and Research Center Co., Ltd., Tianjin, China
adc_wangyanqi@163.com

Abstract. The Intelligent Connected Vehicle (ICV) related to the communication of the stakeholders has become a large and open ecosystem. From the automobile ecosystem, it can be found that there are many attack entrances everywhere, which will bring a lot of risks and threats. In this work, we have summarized the seven major attack entrances of automobile cyber security, and proposed the corresponding six key protection strategies of intelligent and connected vehicle.

Keywords: Intelligent Connected Vehicle · Vehicle ecosystems · Automobile cyber security · Attack entrance · Protection strategy

1 Introduction

The automobile is a complex network communication system and it has a complex electronic information system, covering many information and communication technologies. So, the vehicle ecosystem is large and complex. But now, with the rise of Intelligent Connected Vehicles (ICVs) and mobile travel services, the vehicle ecosystem has been further expanded, including technology, services, infrastructure providers and smart cities. The four subversive technology trends – Electrification, Autonomous driving, Diverse mobility, and Connectivity – will transform a typical vertically integrated automotive value chain into a more complex, and more horizontally structured ecosystem. Everyone will be more dependent on the vehicle ecosystem in the future, especially when car companies use in-vehicle interconnection services to achieve personalized vehicle configuration. There are some similarities between the vehicle ecosystem and the cyber-physical system, which has three typical layers, namely the application layer, transmission layer, and perception layer [1].

While the rapid development of in-vehicle information systems is improving information technology, information security issues are becoming increasingly prominent. The way vehicles are subject to hacking is also being refurbished. The number of Trojans and virus variants continues to rise, threatening the driving safety of

M. Qiu (Ed.): SmartCom 2019, LNCS 11910, pp. 73–82, 2019.
https://doi.org/10.1007/978-3-030-34139-8_8

drivers' lives and property. It was first occurred in 2010 that attacking on the car information systems [2]. As the scope of application of the ICV continues to expand, cyber security also attacks continue to increase. Information tampering, virus intrusion and other means have been successfully applied by hackers in cyber-attacks on smart cars [3], which has aroused great concern from all walks of life.

This paper mainly focuses on automobile security based on the vehicle ecosystem. And we obtained the attack entrance of the ICV by means of testing the vehicle and other simulation investigation and research. Then, we summarize the key strategies of vehicle cyber security protection, which can be used as a reference in the design and manufacture of automobiles to improve the overall information security level of automobiles.

2 Vehicle Connectivity Ecosystem

In the digital age, the degree of global connectivity has increased, making people more connected, and the automotive industry has undergone the same transformation. With the rise of ICV and mobile travel services, the traditional ecosystem of vehicles has been further expanded to include technologies, services, infrastructure providers and smart cities to make vehicles an interconnected system. Vehicle ecosystems can be broadly classified into 4 broad categories that are terminal equipment, cloud platforms, third party service, and communication and network transmission as Fig. 1 shown.

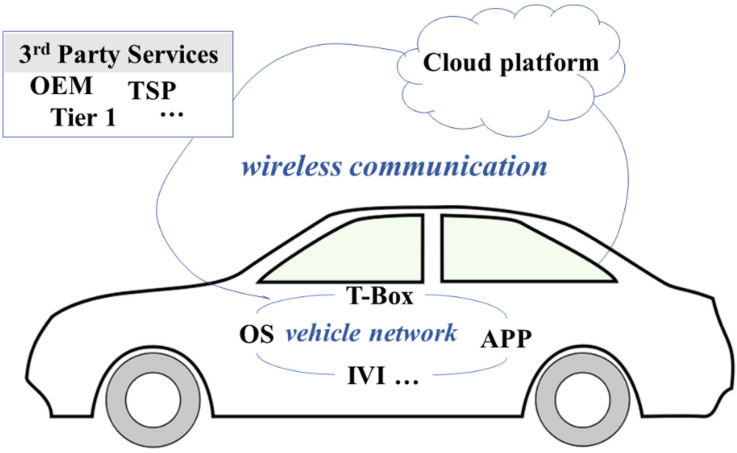

Fig. 1. The diagram of vehicle ecosystem. It contains terminal equipment, cloud platforms, third party service, and communication and network transmission.

The terminal equipment layer will always be used as a third-party interface that can be used to create services and applications. It contained inside car and outside car two parts. The equipment inside vehicle include the operating system (OS), semiconductor chip, T-Box, IVI, On Board Diagnostics (OBD), mobile application (APP), vehicle

APP, and so on. People has more directly interactions with the OS, mobile APP and vehicle APP in the vehicle ecosystem terminal equipment. In many use cases, other advanced technologies such as artificial intelligence and blockchain are also used in those equipment. The external infrastructure includes road test equipment, road conditions, sensor device, traffic conditions, weather conditions, and the others which may affect the vehicle.

The core of the cloud platforms is the connectivity platform, which consists of the vehicle and the 3rd part services. Cloud technology also provides a platform for users and vehicles to share information. It can get and share data and information through the vehicle includes precise positioning of the vehicle, vehicle health and climatic conditions. Such data sources will be connected to the cloud platforms, which requires technical support for cellular networks such as 4G, and will be implemented in the future using 5G communication networks. Users and vehicles can communicate in real time, and can obtain vehicle maintenance information in a timely manner. Vehicle service reservations are smarter and more convenient. In the future, the use of cloud storage will realize the sharing of information between vehicles and people, vehicles and vehicles, vehicles and infrastructure, laying the foundation for optimizing travel, improving efficiency and realizing smart life, and building a more complete intelligent ecosystem and intelligence.

In the development of new technologies in the automotive industry, more and more new players have emerged as the third-party service, such as internet and software companies, sensor manufacturers, and travel service providers. And data management and maintenance can also be outsourced to third-party organizations. These new players form a new automotive ecosystem with traditional vehicle manufacturers and component suppliers. They may represent business (e.g. legal, communications, purchasing) and technical organizations (e.g. engineering, IT) within original equipment manufacturers (OEMs), suppliers, and other automotive stakeholders. The OEM, telematics service provider (TSP), Tier1, suppliers, and other automotive industry stakeholders have played a role include product cybersecurity managers, support staff, crisis managers, executives, legal counsel, and product managers in vehicle cyber security. So, it is better to find and fix issues in vehicle ecosystems that with the help of a variety of internal and external stakeholders.

The communication in vehicle ecosystem includes in-vehicle communication and V2X communication such as vehicle to cloud communication, vehicle to infrastructure communication, and vehicle to human communication. The in-vehicle communication mostly contains CAN bus, LIN bus, FlexRay bus, and MOST bus. All data transactions in the vehicle are made through the gateway. A vehicle gateway that can communicate through various protocols is installed in the vehicle. The V2X communication contained 4G, LTE-V, WIFI, Bluetooth, USB, OTA, dedicated short range communications (DSRC), on board diagnostics (OBD), etc. DSRC is an efficient wireless communication technology that enables the identification and two-way communication of moving targets in high-speed motion in a small area (usually tens of meters), such as the “vehicle-road” and “vehicle-vehicle” of the vehicle two-way communication. It transmits image, voice and data information in real time, to connect vehicles and roads organically. ODB can monitor the working status of the engine electronic control

system and other functional modules of the vehicle in real time during the running of the vehicle.

From the vehicle ecosystem, we can find it is very widely, cantinas the numerous stakeholders, and has a lot of ways of communication. Therefore, the risks and threats faced by the vehicle are numerous and ubiquitous, so the information security of cars has a long way to go.

3 Attack Entrances of Vehicle Cyber Security

Any device connected to the Internet may be vulnerable to hackers. While enjoying the convenience of the network, we must also face the "dark side" of the network—the information security threat, which is not immune to the automotive industry. To ensure the cybersecurity of the vehicle, based on the car's ecosystem, we simulated the attack entrances for vehicle cybersecurity and came up with the following common attack portals.

3.1 Smartphone APP

Smartphones are network communication tools that are often used by car users. APP on smartphones can be freely distributed, downloaded and installed, and there are many types of APP, including many automotive-oriented APP, which may have low reliability and poor security. Such characteristics, hackers through the loopholes, through the smart phone, making the vehicle information system, navigation system abnormal, or eavesdropping on the user's conversation record and the driver's personal privacy information [4]. When a user uses a smartphone, it means that the entire vehicle is connected to the outside network. Therefore, hackers crack the smart phone through the external network, the purpose is to interfere with the in-vehicle information system and launch a vicious attack on the vehicle under high speed.

3.2 Electronic Control Unit (ECU)

Inside the car, each ECU communicates with each other via a CAN bus in a multi-stage interconnection, which not only significantly improves processing efficiency and stability, but also means that control of the entire car can be obtained from any interface. More importantly, the ECUs of the high-end models on the market have the learning function of recording data during driving. In addition, this learning function is also widely used in engines, ABS anti-lock braking systems, four-wheel drive systems, transmission systems, active suspension systems, hydraulic control systems and other systems controlled by ECUs, which makes the ECU get more and more information. The attacker uses the distributed ECU to control multiple systems of the vehicle, precisely because each ECU is connected to the CAN bus, and from the engine ECU to the airbag ECU, these ECU control systems are in the same level relationship. Once the attacker cracks the CAN bus system, and all the control system ECUs face a large security risk.

3.3 Vehicle Network

The controller in the vehicle mainly relies on the vehicle network to transmit messages, including the MOST bus responsible for multimedia communication, the CAN bus responsible for transmitting control information, and the LIN bus responsible for the central locking system. In theory, any controller on the CAN, MOST, and LIN buses can send commands to any other controller. Therefore, any controller that suffers from a bus attack poses a substantial threat to the vehicle communication network. Especially the security for T-BOX, ECU and other important parts, the vehicle network is the last line of defense.

3.4 T-BOX

T-BOX is the communication gateway of intelligent networked vehicles, that almost all communication like 4G, Wi-Fi, OTA and vehicle remote communication are all completed by T-BOX. So, it has played an important role in intelligent and connected vehicle. The main threat of the T-BOX is the attack of middlemen. The attacker hijacks the T-BOX session and listens to the communication data through pseudo base stations and DNS hijacking. For example, in an embedded system, the T-BOX-hardware layer UART debug interface can be used to enter the uboot for firmware upgrade, as the Fig. 2 shows.

```
=> md.b 14008000 10000
14008000: 00 00 a0 e1 00 00 a0 e1 00 00 a0 e1 00 00 a0 e1    ................
14008010: 00 00 a0 e1 00 00 a0 e1 00 00 a0 e1 00 00 a0 e1    ................
14008020: 02 00 00 ea 18 28 6f 01 00 00 00 00 c8 95 4e 00    .....(o.......N.
14008030: 00 90 0f e1 99 04 00 eb 01 70 a0 e1 02 80 a0 e1    .........p......
14008040: 00 20 0f e1 03 00 12 e3 01 00 00 1a 17 00 a0 e3    . ..............
14008050: 56 34 12 ef 00 00 0f e1 1a 00 20 e2 1f 00 10 e3    V4........ .....
14008060: 1f 00 c0 e3 d3 00 80 e3 04 00 00 1a 01 0c 80 e3    ................
14008070: 0c e0 8f e2 00 f0 6f e1 0e f3 2e e1 6e 00 60 e1    ......o.....n.`.
14008080: 00 f0 21 e1 09 f0 6f e1 00 00 00 00 00 00 00 00    ..!...o.........
14008090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
140080a0: 0f 40 a0 e1 3e 43 04 e2 02 49 84 e2 6b 00 00 eb    .@..>C...I..k...
140080b0: 5b 0f 8f e2 4e 1c 90 e8 1c d0 90 e5 01 00 40 e0    [...N.........@.
140080c0: 00 60 86 e0 00 a0 8a e0 00 90 da e5 01 e0 da e5    .`..............
140080d0: 0e 94 89 e1 02 e0 da e5 03 a0 da e5 0e 98 89 e1    ................
140080e0: 0a 9c 89 e1 00 d0 8d e0 01 a8 8d e2 00 50 a0 e3    ............P...
140080f0: 01 a9 8a e2 0a 00 54 e1 1e 00 00 2a 09 a0 84 e0    ......T....*....
14008100: 70 90 8f e2 09 00 5a e1 1a 00 00 9a 09 ac 8a e2    p.....Z.........
14008110: ff a0 ca e3 6c 50 4f e2 1f 50 c5 e3 00 00 4f e1    ....lPO..P....O.
```

Fig. 2. Extract the kernel from uboot.

3.5 In-Vehicle Infotainment (IVI)

IVI is an in-vehicle integrated information processing system based on a vehicle-mounted bus system and Internet service. It can be divided into four hierarchical categories, hardware layer, application layer, system layer and communication layer. Each layer may be subject to information security attacks, such as interfaces, chips and

USB of hardware layer, and system applications, third-party applications as well as some sensitive information in the application layer. IVI enables a wide range of applications including 3D navigation, real-time traffic, IPTV, assisted driving, fault detection, vehicle information, body control, mobile office, wireless communications, online-based entertainment and TSP services, which greatly enhances the level of vehicle electronics, networking and intelligence.

3.6 Cloud Platform

The cloud platform serves as a bridge between the vehicle and the owner for remote control communication. Vehicle-cloud communication plays an important role in the safety of vehicle networking, and it has become the main entrance of vehicle network attack. The vehicle networking service platform is generally based on cloud computing technology, so it is also easy to introduce the security problems of the cloud computing itself into the platform, such as operating system vulnerability threats, virtual resource scheduling problems, SQL injection, password security, and more. Figure 3 shown the attackers used the cloud platform HeartBleed vulnerability to attack the vehicle.

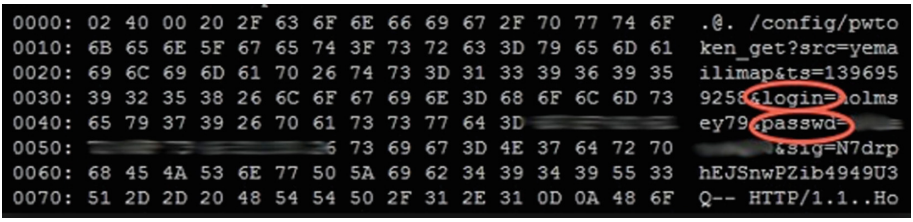

Fig. 3. Attackers can use the HeartBleed vulnerability of the cloud platform to directly read server data, including user's cookies and even plaintext accounts and pass-words.

3.7 Wireless Communication

To prevent physical attacks, vehicles have many functions that are completed through wireless networks. For example, smart key, tire pressure detection system, road shop communication and other devices use short-range wireless communication, which opens the door for hackers to intercept information content.

4 Protection Strategies of Vehicle Cyber Security

The complex application scenarios and technologies of the intelligent and connected of vehicles make it have more security risks. So, the comprehensive measures are needed to protect them [5, 6]. Based on above security attack entrances, we put forward several relevant and common protection strategies, which are OBD firewall, encrypted transmission, system protection, firmware hardening, application hardening, and code obfuscation [7, 8].

4.1 OBD Firewall

The OBD firewall is used to isolate message and information injected into the bus through the OBD port and isolate the internal network information. If abnormal conditions are found, the specific fault is determined according to a specific algorithm, and it is stored on the memory in the system in the form of diagnostic trouble codes (DTC). The useful information obtained after the system self-diagnosis can help the repair and maintenance of the vehicle. The maintenance personnel can use the original instrument of the original vehicle to read the fault code, so that the fault can be quickly located to facilitate the repair of the vehicle and reduce the manual diagnosis time.

4.2 Encrypted Transmission

Encrypted transmission is a technical means used to transmit data on the internet to prevent data from being stolen, falsified and forged, etc., and to ensure that data is transmitted securely over the Internet.

The method of encrypted transmission mainly uses encryption technology, digital signature technology, time stamp, digital voucher technology, and so on. The most commonly used technology is secure layer protocol like SSL and TLS. The SSL/TLS protocol provides client and server authentication, data integrity, and information confidentiality to client-server applications over the Internet based on transport protocol (TCP/IP), both at the server and client. Implementation support. The goal is to provide users with secure communication services for the Internet and corporate intranets.

Currently, for SSL/TLS, an attacker can perform a man-in-the-middle attack by forging a certificate. In order to prevent the generation of man-in-the-middle attacks and encrypt the transmitted data, the certificate must be authenticated in both directions. Two-way authentication which requires another certificate to be sent to the client for verification, is the client verification server certificate, and the server also needs to verify the client's certificate.

4.3 System Protection

Customized installation of professional protection software can effectively protect the normal and safe operation of the intelligent system used by the car's IVI and T-Box. For some common IVI, T-Box and system intrusion methods, the protection software can be divided into four major modules: Virus killing, Equity detection, Vulnerability detection, and Communication flow detection.

The virus killing module most rely on cloud virus databases. The cloud virus database is used to analyze and scan the suspicious program and the behavior is checked and killed, and the sensitive operation of the application is monitored in real time. And using the cloud virus database we can establish the virus signature database, which can scan the application by the signature code.

Equity detection module establish a blacklist of privilege software to detect the installed application, dynamically detect the behavior of the application to temporarily raise the right, and stop it in time.

Vulnerability detection module can regularly obtain vulnerability information of system kernel and system application, and update it in time.

Communication flow detection module establish a communication whitelist, monitor all traffic data communicated with the system, and filter all suspicious data outside the whitelist.

4.4 Firmware Hardening

Firmware is the software that is the most basic and bottom-level work of a system. In hardware devices, firmware is the soul of hardware devices, and it determines the function and performance of hardware devices. To harden the firmware, we can encrypt the chip, and increase the difficulty of firmware extraction.

4.5 Application Hardening

Application hardening allows adding programs that require hardened protection. In the way of detecting the application running state, it intercepts the behavior of the program and prevents malicious programs from exploiting the vulnerability of the application to damage the computer.

Reinforcement can protect its core code algorithm to a certain extent, improve the difficulty of cracking, piracy, and secondary packaging, and alleviate attacks such as code injection, dynamic debugging, and memory injection.

4.6 Obfuscated Code

Obfuscated code, also known as flower instruction, converts the code of a computer program into a functionally equivalent, but difficult to read and understand form of behavior. Identifier confusion is to rename the package name, class name, method name and variable name in the source program, replace it with a meaningless identifier, making the decompiled code more difficult to analyze.

Code obfuscation can be used for program source code or for intermediate code compiled by the program. There are three common ways to confuse code, rewriting various elements in the code, disrupt the format of the code, and using the code obfuscation tool. Rewriting various elements in the code, such as variables, functions, and class names, into meaningless names makes it impossible for the person reading the book to guess its purpose. Rewrite some of the logic in the code to make it functionally equivalent, but more difficult to understand. Disrupting the format of the code means first converting some of the more critical string variables into hexadecimal arrays or Unicode encodings, and then restoring them to strings when used. This can avoid the disassembled code is easy to be analyzed and understood by the cracker, so that the cracker analysis cost increases.

Use the code obfuscation tool to enhance the difficulty of the reverse. It provides 3 protection modes: control flow flattening, spurious control flow, and instruction replacement. Control flow flattening is to convert control statements such as if, while, for, and do in C, C++, or Java code into switch branch statements without changing the function of the source code. The spurious control flow confuses each basic code block,

creating a new conditional jump code block that jumps to the real basic block or another code block containing the garbage instruction, the original basic code block. Will also be cloned and populated with randomly selected spam commands. Instruction substitution does not change the original control flow of the function, but replaces ordinary arithmetic and Boolean operations with more complex operations. When several equivalent sequences of instructions are available, it will randomly select one to replace (Fig. 4).

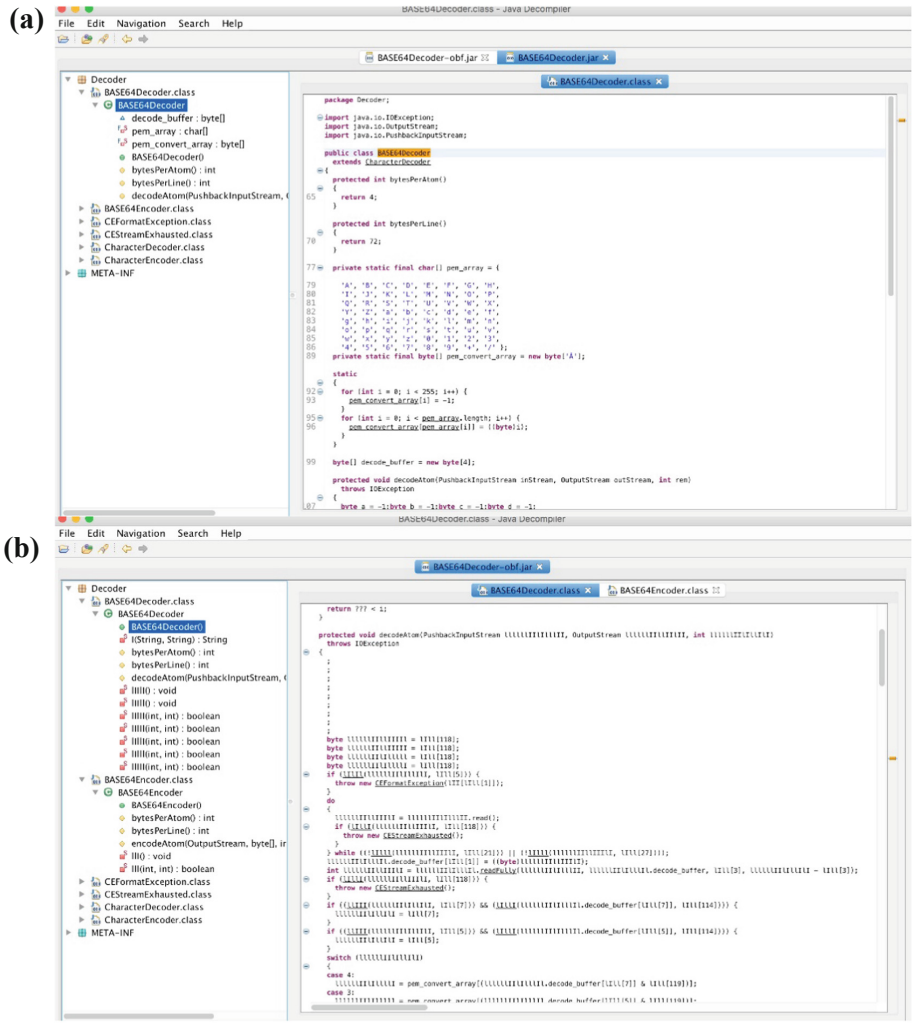

Fig. 4. Identifier confusing instantiation in code obfuscation. The (a) is before the confusion, and the (b) is after confusing, the confusion can increase the analysis difficulty of the decompiled code.

5 Conclusion

In general, the protection measures for ICVs cyber security are not only reflected in the hardware and software requirements of the vehicle, but also reflected in the requirements of communication and cloud. Only by doing cybersecurity protection measures in the entire automobile ecosystem, can we cope with various possible cyber security issues and ensure the cyber security of ICVs as much as possible

This paper outlines the vehicle attack entrance and protection strategies, analyzes the common attack methods and potential security threats for automobiles, and summarizes the corresponding vehicle protection measures for each security threat.

References

1. Ashibani, Y., Mahmoud, Q.H.: Cyber physical systems security: analysis, challenges and solutions. Comput. Secur. **68**, 81–97 (2017)
2. Chen, L.W., Syue, K.Z., Tseng, Y.C.: A vehicular surveillance and sensing system for car security and tracking applications. In: Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN 2010), pp. 426–427 (2010)
3. Okul, Ş., Aydin, M.A., Keleş, F.: Security problems and attacks on smart cars. In: Boyaci, A., Ekti, A.R., Aydin, M.A., Yarkan, S. (eds.) International Telecommunications Conference. LNEE, vol. 504, pp. 203–213. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-0408-8_17
4. Wolf, M., Weimerskirch, A., Wollinger, T.: State of the art: embedding security in vehicles. EURSIP J. Embed. Syst. **16**(1) (2007)
5. Lee, C.H., Kim, K.H.: Implementation of IoT system using block chain with authentication and data protection. In: 2018 International Conference on Information Networking (ICOIN), pp. 936–940. IEEE (2018)
6. Alfred, J.R., Sidorov, S., Tsang, M.C., et al.: In-vehicle networking. U.S. Patent Application 15/270,957, 22 March 2018
7. Wroblewski, G.: General method of program code obfuscation (2002)
8. Pizzolotto, D., Fellin, R., Ceccato, M.: OBLIVE: seamless code obfuscation for Java programs and Android apps. In: 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER), pp. 629–633. IEEE (2019)