The Analysis of Cybersecurity Problems in Distributed Infocommunication Networks Based on the Active Data Conception

Sergey V. Kuleshov[1(✉)], Alexey Y. Aksenov[1], Iliya I. Viksnin[2], Eugeny O. Laskus[2], and Vladislav V. Belyaev

[1] St. Petersburg Institute for Informatics and Automation of RAS, St. Petersburg, Russia
kuleshov@iias.spb.su
[2] ITMO University, St. Petersburg, Russia

Abstract. The paper considers the problems of cybersecurity for distributed infocommunication networks, related to the violation of the access rights of the executable code of active data to network node resources (shared memory, radio channel reconfiguration, motion control functions, onboard node sensor).

Keywords: Cybersequrity · Distributed networks · Active data

1 Introduction

In order to ensure the platform-independence of active data (AD) technology, as well as to increase its security, it is proposed to apply the technology of virtual machines. A virtual machine can use both the principles of para-virtualization and full virtualization [1–5] because the executable active data code should not receive direct access to hardware resources for security reasons. The role of the software layer is performed by the hypervisor. This software layer controls the provision of resources to virtual machines and decides which instructions must execute directly, and which ones must emulate. In the case of the paravirtualization, the embedding of the code responsible for the virtualization of hardware re-sources in the code of AD is implied. This eliminates the need to determine which instructions are safe and are allowed to run directly on the processor, and which ones are unsafe and require emulation. In the code prepared in this way, the AD will not contain unsafe instructions; instead, they may be called hypervisor application programming interface (API) [6–8].

2 Formalization of Active Data Virtual Machine

The principle of digital content separation to the transport (initializing) stream and the generating program [9, 10] enables flexible adaptation of the content to the existing features and limitations of the physical transmission channels. Within the active data conception, the decoding program can be generated on the transmitter side for every data type to be sent and be transmitted before initializing stream. If predetermined

D. G. Arseniev et al. (Eds.): CPS&C 2019, LNNS 95, pp. 491–499, 2020.
https://doi.org/10.1007/978-3-030-34983-7_48

standard data types are to be used (in this case, on the receiving side, there is a set of standard data recovery programs needed) it is possible to transfer only the index of the program required for recovery of the digital information object. The approach of software-defined systems being configured in accordance to demands and specifics of the transmitted active data enables to create flexible virtual communication environment. The single packet of active data can be described as a bit structure containing three components: signature S, program P and initializing stream D. The only mandatory component is the signature which is needed for the active data packet (ADP) identification and the program to be executed on the receiver side. Initializing stream (based on terminology in [9]) is an input data for the program P and is being transmitted to ADP only if it is needed.

To organize data transmission in mobile networks, there are a number of approaches described in [11–13], each of which has its own limitations. The AD concept is the expansion of such approaches, which allows solving the problem of limited controllability [14]. As an example of the scenario, we will give an example of the organization of relaying AD through a network of mobile nodes controlled by AD, by the analogy with [14].

In this paper, we use a formalization of the Active Data Virtual Machine (ADVM). As most of the modern computer systems are based on Turing Machine [15], we can define a computer system as:

$$M = \left(S,\ I,\ \delta,\ s_0,\ S_f\right)$$

where S denotes the set of all the states a machine (computer system) may have; I denotes the set of all the instructions a machine can provide; δ: $S \times I \rightarrow S \times I$ is the execution operator of an instruction of I; s_0 denotes the initial state of a machine; S_f denotes the set of all the possible final states of a machine.

Furthermore, we define a series of Execution Operator as $\delta(m)$, so we can get:

$$\delta^{(m)}(s_n, i_n) = \underbrace{\delta^{\circ} \ldots \delta^{\circ}}_{m}(s_n, i_n) = \delta(\ldots\delta(s_n, i_n)) = (s_{n+m}, i_{n+m}).$$

Accordingly, the active data is defined as:

$$A = \left(\delta^{(m)}, D\right)$$

where $\delta^{(m)}$ is a series of Execution Operator, D denotes the data stream.

Using the principle of homoiconicality (unity of the presentation of instructions and data) allows you to build a combined alphabet T:

$$T = I \cup D$$

Comparing to the classic Turing Machine model, we do the following changes to our model: redefine the Input Symbol as the set T (instructions and data), which are actually all the symbols a virtual machine can accept.

Depending on the permissions on the actions of the active data executable code, there are 2 possible variants of the virtual machine implementation, on the choice of which the analysis of potential system vulnerabilities depends:

- Active data are forbidden to modify the processor:

$$\forall \delta \quad \delta : M \to M.$$

- Active data allowed to modify the processor:

$$\forall \delta \quad \delta : M \to M^{*}.$$

3 Information Security of AD

Information security threats in info-communication systems can be divided into two broad classes - internal and external. In this work, attention will be paid to the elimination of internal threats arising from the use of active data, since external threats can be mainly eliminated using the classical methods of ensuring information security.

In data networks built using active data, internal threats can be caused by vulnerabilities in both hardware and software, including those associated with disruptions in the execution of an active data program, since active data can access control of network device components. These threats include [16–20]:

- The threat of unauthorized access to the host network memory. Realization of this threat may entail a violation of the confidentiality of information stored and transmitted on the network, or a violation of its integrity, which, if necessary for the correct functioning of a network device or network, may lead to problems in the operation of the system.
- The threat of access to the network functions of the device, in particular, to the possibility of reconfiguring the communication channel. The implementation of this threat makes it possible to change the properties of a communication channel organized by a compromised network device and the subsequent disruption of communication with it due to the discrepancy between the communication channel parameters of the nodes using it. A by-effect of this threat is a violation of the availability of information on the network.
- The threat of access to the functionality of the components of the node: on-board sensors, mechanical drives, etc. The implementation of this threat may lead to a violation of the correct operation of the node itself and, in consequence, of the network itself. For example, if an intruder gets access to the functionality of the onboard sensors, it can disrupt their work, which in turn will disrupt the node receiving information about the state of the environment. This may lead to the impossibility for the node to implement a number of functions depending on the information received from the sensors.

The threats listed above are related to the possibility of an access violation by the executable code of active data. To eliminate them, a clear distinction is required between the access rights of different types of active data programs to the node functionality depending on the purpose of their execution.

- The threat of selfishness. This threat is peculiar to mobile networks, nodes of which have limited resources, both battery and computing power. When reducing the number of available resources, the node that trying to save them may limit the provision of its own routing services to other nodes, which will lead to a violation of the availability of information in the network.
- Considering these threats, the following attacks on information-communication networks of active data are possible [16–20]:
- Man-in-the-middle attack. An attack in which the intruder changes the connection between the nodes, which in this case continue to assume that they communicate directly with each other. This attack leads to a breach of confidentiality of information, since information transmitted between nodes passes through the node compromised by the intruder. Also, depending on the violator's goals, it may also result in a violation of the integrity or availability of information: the intruder may replace the transmitted data with his own or not transmit partially or completely received data to the receiving node, while the sending node will consider them delivered.
- Insomnia test. An attack on mobile wireless networks that poses a threat of selfishness, in which the intruder increases the power of the target node, which is why the node, trying to save battery power, limits its work, resulting in a violation of information availability in the network.

4 Empirical Part

An experiment on the implementation of active data technology will be conducted based on a network of unmanned ground vehicles. The purpose of this experiment is to analyze the vulnerabilities and threats in these networks when using active data and to find ways to eliminate them.

The experimental stand consists of models of unmanned vehicles (MUVs) and an external information center (EIC), which is an intermediary in the exchange of information between the MUVs and is responsible for its storage. Each MUV is a system of physical elements, the interaction of which allows for the analysis of the environment, movement in it, communication within a group of models, as well as various algorithms necessary for the functioning of the system.

The MUV system includes two subsystems - computational and executive. The computational subsystem is responsible for building the route and analyzing deviations from it, developing a list of commands for execution and making communications. The executive subsystem, in turn, implements the commands developed by the computing subsystem and provides for the detection of obstacles to movement. The structure of the IBA system is presented in Fig. 1.

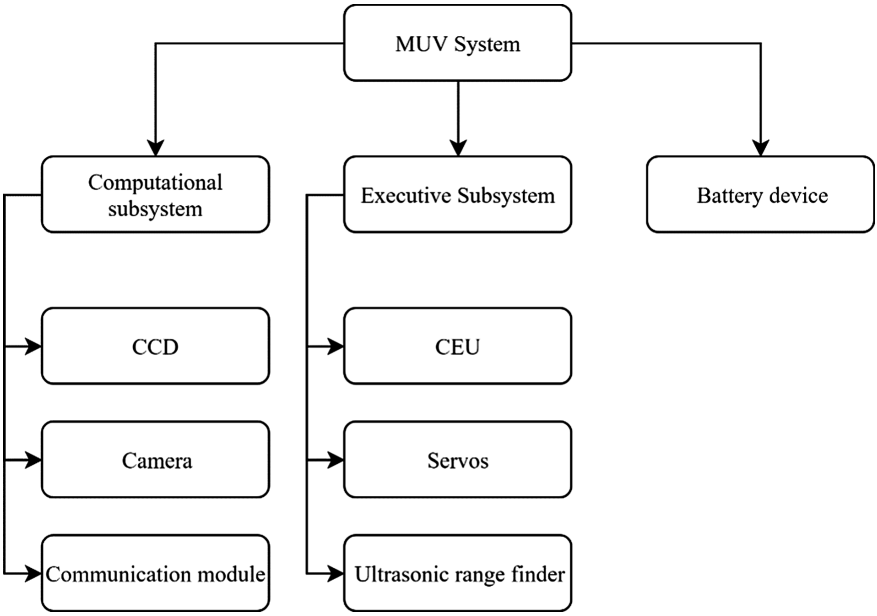


Fig. 1. The structure of the MUV system

The computational subsystem consists of three elements - the central computing device (CCD) of the Raspberry Pi, the Raspberry Pi Camera Board camera and the Xbee communication module. The main device of this subsystem is the CCD, which is responsible for processing information from other devices, developing the route and command lists.

The camera is responsible for the computer vision of the MUV - it accepts frames with road markings, thanks to which the CCD is able to determine the distance traveled and the need for route correction.

The communication module exchanges data between the MUV and the EIC, based on which the CCD determines the identification number of the MUV in the group and the priority of movement in disputable situations.

The executive subsystem consists of four elements - the central executive unit (CEU) Arduino Nano, two servo drives and an ultrasonic range finder. CEU is the main device of the subsystem, which analyzes the commands coming from the CCD necessary for execution, the processing of obstacle data from a rangefinder and the control of servo drives. The main task of the CEU is to supply pulses to servos, the change in the magnitude of which allows you to adjust the speed and direction of rotation of the servos. The ultrasonic range finder, based on the time elapsed from the moment of radiation to the moment of returning the signal, determines the distance to the obstacles and, in case of detection of an obstacle in dangerous proximity to the MUV, sends the command of the CEU to stop the servo drives.

The generalized model of information interaction is presented in Fig. 2: the information center includes CCD and CEU - elements of information processing and control of other elements, and elements with limited functionality (i.e., capable of performing only individual actions) are related to the physical level.

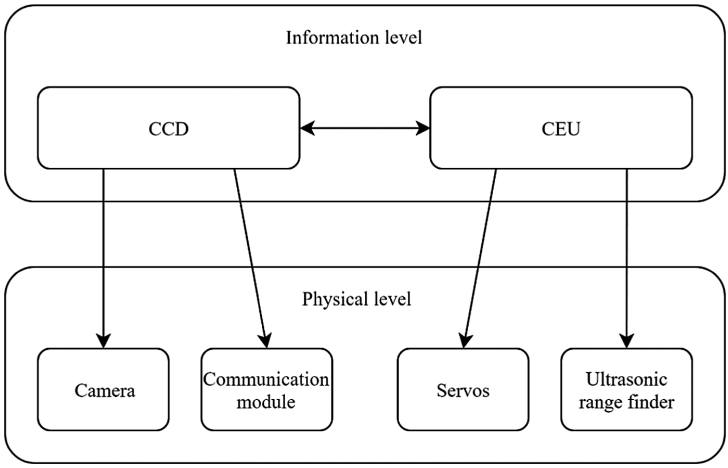


Fig. 2. The interaction of the MUV system elements

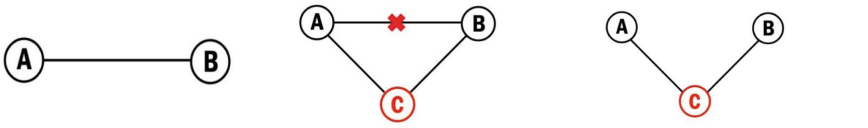
In this network, active data is a set of commands generated by the CCD of one MUV to execute the CEU of another, with which several system security problems are associated: the possibility of violating the confidentiality of the transmitted data, i.e., execution of the transmitted active data packet by the transit node, and the possibility of unauthorized access of the executable code of the active data to the elements of the physical layer MUV. To eliminate the first MUV threat, node authentication is required when attempting to execute an active data code; for the second - the implementation of the system of differentiation of access rights at the information level MUV.

Scenarios for the implementation of attacks on the MUV network [18, 19]:

- Man-in-the-middle attack. The implementation of this attack is as follows:

1. The offending node C sends a request to establish a connection to node A, pretending to be node B.
2. Node A establishes communication with Node C.
3. Node C sends a request to establish a connection to Node B, appearing as Node A.
4. Node B establishes communication with Node C.
5. In the process of transferring data from A to B and back, node C, when received, performs the necessary manipulations with them and then passes them on.

However, when a connection is already configured between nodes A and B, in order to launch an attack, it is necessary to break the current connection before performing these actions. To do this, you can send a request on behalf of the second one to stop the connection to one of the nodes, or make the channel ineffective for high-quality data transmission (for example, increase the noise level in it), as a result of which the connection through this communication channel is interrupted. In addition, this attack can be implemented in case of violation of the access rights of the executable code of active data to the functions of the communication module, as a result of which it is possible to reconfigure communications in the network in a manner necessary for the intruder.

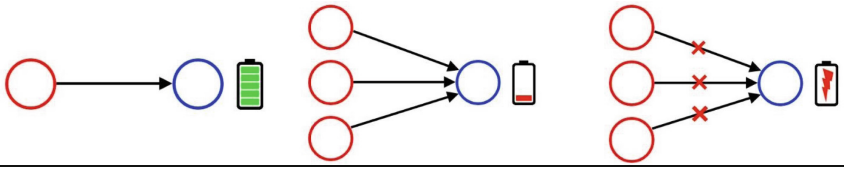


Initial connection of nodes A-B

Break of A -B connection and establish of A -C-B connection

Established A -C and C -B connections

- Insomnia test. The implementation of this attack is possible in several ways. The first is sending more traffic through the target node, as a result of which the node will need to direct additional resources to the processing of input data. The second – if there is access to the communication module functionality obtained as a result of an access violation of the active data programs being executed – the intentional non-optimal use of the device components from the point of view of energy consumption.



1. Normal operation of system

2. Increase the load on the node with increasing traffic

3. Denial of Service for Battery Depletion

5 Conclusion

In this paper, an approach to ensure security in active data networks, based on the use of virtual processing, is proposed. The main advantage of this approach is the independence of the solution implementation from the system hardware and network decentralization.

The threats and possible attacks on the active data networks were considered. Experimental stand for the implementation of active data technology was presented.

At the moment it is planned to consider described experiments on a simulator. After testing on a virtual network, to complete the study, this technology will be implemented on an unmanned drones network.

References

1. Carvalho, A., Silva, V., Afonso, F., Cardoso, P., Cabral, J., Ekpanyapong, M., Montenegro, S., Tavares, A.: Full virtualization on low-end hardware: a case study. In: IECON Proceedings of Industrial Electronics Conference, 21 December 2016, pp. 4784–4789 (2016)
2. Understanding Full Virtualization, Paravirtualization, and Hardware Assist. VMware technical documentation. Accessed 18 Apr 2019. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/ techpaper/VMware_paravirtualization.pdf
3. Chen, W., Xu, W., Wang, Zh., Dou, Q., Zhao, B.: A formalization of an emulation based co-designed virtual machine. In: 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 164–168 (2011). https://doi.org/10.1109/imis.2011.144
4. Craig Iain, D.: Virtual Machines. Springer, London (2006). 269 p. https://doi.org/10.1007/978-1-84628-246-1
5. Shi, Y., Gregg, D., Beatty, A., Ertl, M.A.: Virtual machine showdown: stack versus registers. https://www.usenix.org/legacy/events/vee05/full_papers/p153-yunhe.pdf. Accessed 18 Apr 2019
6. Polenov, M., Guzik, V., Lukyanov, V.: Hypervisors comparison and their performance testing. In: Advances in Intelligent Systems and Computing, vol. 763, pp. 148–157. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-91186-1_16
7. Cheng, Y., Chen, W., Wang, Z., Yu, X.: Performance-monitoring-based traffic-aware virtual machine deployment on NUMA systems. IEEE Syst. J. **11**(2), 973–982 (2017). https://doi.org/10.1109/JSYST.2015.2469652
8. Rao, J., Wang, K., Zhou, X., Xu, C.: Optimizing virtual machine scheduling in NUMA multicore systems. In: 2013 IEEE 19th International Symposium on High Performance Computer Architecture (HPCA), Shenzhen, pp. 306–317 (2013). https://doi.org/10.1109/hpca.2013.6522328
9. Kuleshov, S.V., Tsvetkov, O.V.: Active data in digital software-defined systems. Informatsionno-izmeritelnye i upravlyayushchie sistemy **6**, 12–19 (2014). (in Russia)
10. Alexandrov, V.V., Kuleshov, S.V., Zaytseva, A.A.: Active data in digital software defined systems based on SEMS structures. In: Gorodetskiy, A. (ed.) Smart Electromechanical Systems. Studies in Systems, Decision and Control, vol. 49, pp. 61–69. Springer, Cham (2016)
11. Samad, T., Bay, J.S., Godbole, D.: Network-centric systems for military operations in urban terra. The role of UAVs. J. Proc. IEEE. **95**(1), 4118473, 92–107 (2007). https://doi.org/10.1109/jproc.2006.887327
12. Lysenko, O.I., Valuiskyi, S.V., Tachinina, O.M., Danylyuk, S.L.: A method of control by telecommunication airsystems for wireless AD HOC networks optimization. In: IEEE 3rd International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD) Proceedings, Kyiv, Ukraine, pp. 182–185, October 2015

13. Ono, F., Ochiai, H., Miura, R.: A wireless relay network based on unmanned aircraft system with rate optimization. IEEE Trans. Wirel. Commun. **PP(99)**, 7562472 (2016). https://doi.org/10.1109/twc.2016.2606388
14. Kuleshov, S.V., Zaytseva, A., Aksenov, A.Y.: The conceptual view of unmanned aerial vehicle implementation as a mobile communication node of active data transmission network. Int. J. Intell. Unmanned Syst. **6**(4), 174–183 (2018). https://doi.org/10.1108/IJIUS-04-2018-0010
15. Turing, A.M.: Correction to: on computable numbers, with an application to the entscheidungs problem. Proc. London Math. Soc. Ser. **2**(43), 544–546 (1938)
16. Afanasyev, A.L., Garmonov, A.V., Kashchenko, G.A.: Analysis of security threats and secure routing protocols in MANET networks. In: Radiolocation, Radio Navigation, Communication: Materials of the XX International Scientific and Technical Conference (RLNC-2014), vol. 2. Voronezh: Publishing house SPC «CAKBOEE» OOO, pp. 846–857 (2014). (in Russia)
17. Anjum, F., Mouchtaris, P.: Security for Wireless Ad-hoc Networks. Wiley, Hoboken (2007)
18. Irshad, S., Halabi, B.H., Jamalul-Lail, A.M., Iftikhar, A., Daniyal, A.: Classification of attacks in vehicular ad hoc network (VANET). INFORMATION Int. Interdisc. J. **16** (5), 2995–3004 (2013)
19. Gohale, V., Gosh, S.K., Gupta, A.: Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks, 196–217. CRC Press (2011)
20. Zegzhda, D., Ivanov, P.V., Moskvin, D.A., Kubrin, D.S.: Actual security threats for vehicular and mobile ad hoc networks. Autom. Control Comput. Sci. **52**, 993–999 (2018). https://doi.org/10.3103/S0146411618080308