Mechanics Transport Communications

Academic journal http://www.mtc-aj.com

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
volume 21, issue 3/1, 2023
article № 2409

MODEL OF SECURITY OF DIGITAL PROCESSES IN ELECTRONIC RAILWAY BUSINESS

Zoran G. Pavlović
zoran.pavlovic@vzs.edu.rs

Belgrade Academy of Technical and Art Applied Studies,
College of Railway Engineering,
Starine Novaka 24, 11000 Belgrade
REPUBLIC OF SERBIA

Key words: *network attacks, network security, block chain, railway company*

Abstract: *Networking of computers and devices, the emergence of the Internet create new changes in the way of doing business. It can be said that the current electronic business in relation to traditional ways of direct communication has its advantages and disadvantages. Unwanted flaws include attacks from malicious individuals who may have different interests. This paper analyzes the types of attacks that can affect all digital processes in railway traffic. The model presented in this paper is based on the activities of IKOM (input, control, output, mechanism) components. The activity of the innovative model process includes Input, i.e. input data provided by all networked devices. Based on the input data, a large number of other predetermined related processes are launched. The conversion mechanism determines and at the same time enables the access and delivery of the service in the process of exchanging incoming and outgoing messages. Control as part of the activity determines the flow of the process with variables related to conditions, capacity and service availability, security requirements. The end result of the activity process includes Output through the delivery of the requested protected activity without any unwanted events. The service capability is defined by the core through which the digital data provided by the networked devices in the electronic business system of the railway company, mechanisms for accessing and delivering a specific process, devices responsible for delivery enter , security requirements and other parameters. All processes and service parameters are directly connected to block chain technology. Application of block chain technology is the most secure protection model today. The innovative safety model includes a description of the need to apply safety mechanisms for the implementation of all processes in the railway company.*

INTRODUCTION

The application of innovative electronic business technologies provides new ways of exchanging information between interested parties in everyday activities [1][2]. It is basically the application of computers and telecommunication channels for the exchange of information. The main purpose of computer systems is the collection, processing, storage of data, as well as safe storage. The development of computer systems leads to the need for networking and mutual sharing of data and information. In the world of science, new technical-technological improvements in computer systems are being developed every day

(e.g. electronic business, 5G and the announcement of 6G networks, artificial intelligence, the Internet of intelligent devices, expert systems, machine learning, etc.). The interested state and private sector, in order to improve daily activities, sees a chance to improve the current operational work through the application of existing and innovative solutions. In essence, the basis is the interconnection and exchange of data and information between interested parties in a protected and secure manner [3][4][5][6]. Any failure or delay in the implementation of the above solutions can interrupt the started activities and delay further work. In order to avoid work failures, protection measures must be applied in computer systems, as well as the improvement of existing mechanisms.

POTENTIAL ATTACK

The basic role of computer systems includes providing information for viewing, processing, storage and transmission. It implies the usual flow of information between interconnected devices in one computer system (eg computer memory with a camera or printer) or between multiple computers that are physically and spatially distant [7][8]. Normal flow of information when the protection system of computer systems is not compromised and resource sharing is enabled.

In addition to the mentioned usual flow of information, there may be an attack on the availability of the system where there is an interruption in communication. The easiest form of attack can be the interruption of a communication line, damage to a hardware component, obsolescence of a software program, etc.

Attacks related to integrity (content) involve modifying the message. Then there is a change in the content of the message, which can be a notification, information or even an order. In any case, the recipient of the message does not receive the original message, but a modified one, where the essence of the message and its meaning are changed. Changing information in the form of a message (e-mail, electronic invoice, electronic bill of lading in traffic, electronic purchase order, etc.) can be one of the attacks.

The next type of attack involves learning about the content of the information being transmitted, its secrecy and confidentiality. In this way, an unauthorized person who does not have the right of access, intercepted, gets access to the content of the information. With the help of appropriate software and programs, a third party in the attack can illegally copy the transmitted information. In this case, the requester or the final destination receives the information unchanged, but also without knowing that the attacker also received the same information. Based on the information obtained through interception, an unauthorized person can use it for his own needs.

The next type of attack refers to information fabrication, where an unauthorized person creates fake messages within a possible information stream. An example can be identity theft of a specific person and impersonation by sending messages containing wrong information or modifying some messages in the communication of interested parties.

Security measures for the protection of computer systems consist of a set of rules that define a general protection policy. A preventive countermeasure is the application of all available protection mechanisms that can be part of the operating system, to work independently of the user and to provide timely notifications about the state of the computer system itself. Then providing control of access to the computer system, applications and data related to any user who can be a potential initiator of infecting the computer or damaging certain files. The next step involves user training, which includes analyzing potential attacks (redirecting, intercepting, fabricating or modifying messages) and taking certain security measures to protect and remove malicious programs. In addition to preventive measures, technical mechanisms can also be used for [9].

- Detection: it is necessary to detect and determine the existence of a malicious program in the computer system;
- Identification: after detection, it is necessary to identify the specific malicious program that infected the computer system and
- Removal: detection and identification of a malicious program creates a prerequisite for its removal from infected computer systems and prevention of further spread.

RELATED RESEARCH

The Internet plays an increasingly important role in personal and business activities. In addition, with the advent of real-time applications, sensitive to potential malicious attacks [10].

In this paper, we present a defined network architecture as a new approach that enables key features such as communication in networks. RDNA explores the programmability of the residue number system as a fundamental concept for defining a minimalistic forwarding model for core nodes. Instead of forwarding packets based on classic table lookup operations, core nodes are tableless switches that forward packets using only the rest of the division operations [11].

This paper investigates system integrity protections and proposes a constrained communication delay model. To be precise, it can be divided into wide area protection and substation protection. In the first case, data buffering of phasor data concentrators and automatic protection switching of synchronous optical network/synchronous digital hierarchy are used to limit the delay of regional and backbone networks, respectively; then the communication delay is modeled as bounded, instead of average or stochastic in the literature. For the latter, network calculus theory is used to limit the delay in switched Ethernet networks, and the communication delay is modeled as bounded. In practice, one should preprogram the time delay of the protective relays and expect the communication delay to be predictable or predetermined [12].

In an unreliable Internet environment, there is a large amount of data that is vulnerable to various attacks, and for users, an important security problem is how to protect their privacy and additionally ensure anonymity. Each user has different privacy requirements for anonymous communication. However, anonymous communication methods cannot meet the diverse needs of anonymous users. This is why anonymous user communication on demand is proposed, which can dynamically adjust the level of anonymity according to the user's anonymity needs. However, the defense capabilities against the attack are insufficient in the existing anonymous on-demand user communication. Some malicious users in the network use anonymous communication to hide their identity and attack the Internet [13].

Today's power utilities around the world own multiple substations that are connected together to form a complex power grid. This automation results in efficient operation and improved protection of the power grid with the help of the communication system. The implementation of protection schemes modeled using standardized communication configurations for information exchange will lead to a digital power grid [14].

The communication network plays a key role in next-generation micro grid protection schemes. Therefore, communication costs and reliability are some of the key factors to consider before implementing a micro grid protection scheme. The concept of a hybrid micro-grid protection system is presented, which implements a traditional differential protection scheme together with an adaptive micro-grid protection scheme. The joint application of these two schemes has the potential to increase the accuracy and precision of the overall protection scheme, while simultaneously reducing the overall communication cost [15].

SECURITY MODEL

An innovative security model of all digital processes based on hardware and software components and the Internet is presented in figure 1. The service contains an interaction field and a core where all transactions from any process are registered. The activities that occur in the system include A=<p,a,m,t> where (***A)*** represents the request for service information, (***p)*** represents and determines the type of information, (***a)*** determines the identification of the activity, (**m)** represents the protocol that refers to the blockchain and (**t)** represents time periods that can be: a moment before a certain time, as soon as possible, at a certain time or a moment in time that repeats periodically.

The subset As represents a cooperation transaction patterns as interaction field ability, subset C represents the participants in the interaction (service resources) (As ={c_s,r_s,P_s}), Ps represents a component that explicitly bounds to the role of R and uses a set of interactions e-processes P*.

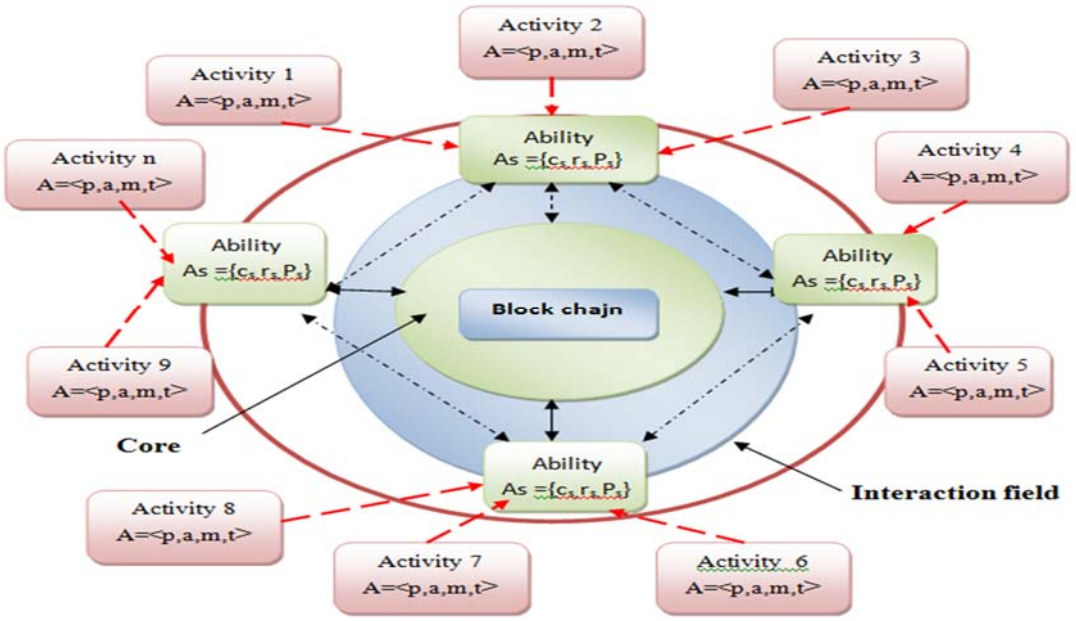

Figure 1: Ability of innovative security service

CONCLUSION

A special need for protection was observed through the networking of computers, a large number of devices in the railway company. The application of technologies and protection mechanisms so far has shown that there is no absolute security in computer systems, but all interested parties (designers, manufacturers, administrators) make efforts to raise safety and security to the highest possible level. This approach to increasing security in computer systems implies the constant development of new mechanisms and the improvement of existing ones in solving current and potential problems. Basically, due to the malicious attacks of an unknown user, the protection of the operating system can be realized in the following way by applying block chain technology. The ability of the service regulates all processes, their flow exclusively through the core of the service where maximum security is ensured.

REFERENCES:

[1] Pavlović Z, Banjanin M, Vukmirović J, Vukmirović D., (2020,05,04): *Contactless ICT Transaction Model Of The Urban Transport Service*; Research journal TRANSPORT, ISSN: 1648-4142 / eISSN: 1648-3480, Vol 35 No 5, pp 500-510. https://doi.org/10.3846/transport.2020.12529

[2] Pavlović, Zoran, Radičević Veljko: *Application Of Intelligent Agents On High Speed Lines In Railway Traffic*, XX International Scientific-expert Conference on Railway RAILCON'22, October 13-14.2022, Niš, Serbia, pp 101-104, ISBN 978-86-6055-160-5 https://railcon.rs/Proceedings/Railcon_22_Conference_Proceedings.pdf
[3] Pavlović Z. G., "Technologies of electronic business in traffic," *2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH)*, 2022, pp. 1-4, doi: 10.1109/INFOTEH53737.2022.9751297. https://ieeexplore.ieee.org/document/9751297
[4] Z. G. Pavlović, "Development Of Models Of Smart Intersections In Urban Areas Based On IoT Technologies," *2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH)*, 2022, pp. 1-4, doi: 10.1109/INFOTEH53737.2022.9751263. https://ieeexplore.ieee.org/document/9751263
[5] Z. Pavlović, *User'S Ability To Use Internet Tecnologies In Transport*, 7th International Conference ''Towards A Humane City''Environmentally Friendly Mobility, Serbia, Novi Sad 6th and 7th December 2019, pp 207-213, https://www.dropbox.com/s/95zjnjm3npxzzfr/Conference%20proceedings%20TAHC_2019.pdf?dl=0
[6] Radičević, V., Pavlović, Z. G., & Nikolić, D. (2021, 10 15). *Analiza mobilnih tehnologija i aplikacija.* (Z. Čekerevac, Ur.) FBIM Transactions, 9(2), 94-101. doi:10.12709/fbim.09.09.02.10 ; https://www.meste.org/fbim/FBIM_2_2021/18_10.pdf
[7] Pavlović, Z. G., Radičević, V., & Nikolić, D. (2021, 10 15). *Tehnologije za zaštitu podataka u digitalnim poslovnim procesima*. (Z. Čekerevac, Ur.) FBIM Transactions, 9(2), 63-70. doi:10.12709/fbim.09.09.02.07 https://www.meste.org/ojs/index.php/fbim/article/view/1202/1311
[8] Nikolić, D., Radičević, V., & Pavlović, Z. G. (2021, 10 15). *Modeliranje arhitekture i infrastrukture inovativnog modela e-poslovanja.* (Z. Čekerevac, Ur.) FBIM Transactions, 9(2), 55-62. doi:10.12709/fbim.09.09.02.06 https://www.meste.org/ojs/index.php/fbim/article/view/1201/1310
[9] W. Stallings, Osnove bezbednosti mreža, ISBN 987-86-7991-376-0, CET Computer Equipment *and Trade, 2014.*
[10] H. Geng *et al.*, "A hybrid link protection scheme for ensuring network service availability in link-state routing networks," in *Journal of Communications and Networks*, vol. 22, no. 1, pp. 46-60, Feb. 2020, https://doi:10.1109/JCN.2019.000056.
[11] A. Liberato *et al.*, "RDNA: Residue-Defined Networking Architecture Enabling Ultra-Reliable Low-Latency Datacenters," in *IEEE Transactions on Network and Service Management*, vol. 15, no. 4, pp. 1473-1487, Dec. 2018, https://doi:10.1109/TNSM.2018.2876845.
[12] C. Huang, F. Li, T. Ding, Y. Jiang, J. Guo and Y. Liu, "A Bounded Model of the Communication Delay for System Integrity Protection Schemes," in *IEEE Transactions on Power Delivery*, vol. 31, no. 4, pp. 1921-1933, Aug. 2016, https://doi:10.1109/TPWRD.2016.2528281.
[13] Y. He, M. Zhang, X. Yang, J. Luo and Y. Chen, "A Survey of Privacy Protection and Network Security in User On-Demand Anonymous Communication," in *IEEE Access*, vol. 8, pp. 54856-54871, 2020, https://doi:10.1109/ACCESS.2020.2981517.
[14] I. Ali, S. M. S. Hussain, A. Tak and T. S. Ustun, "Communication Modeling for Differential Protection in IEC-61850-Based Substations," in *IEEE Transactions on Industry Applications*, vol. 54, no. 1, pp. 135-142, Jan.-Feb. 2018, https://doi:10.1109/TIA.2017.2740301 .
[15] T. S. Ustun and R. H. Khan, "Multiterminal Hybrid Protection of Microgrids Over Wireless Communications Network," in *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2493-2500, Sept. 2015, https://doi:10.1109/TSG.2015.2406886.