THE CONCEPT OF BUILDING SECURITY OF THE NETWORK WITH ELEMENTS OF THE SEMIOTIC APPROACH

Serhii Yevseiev[1], Maksym Tolkachov[2], Darshan Shetty[3], Vladyslav Khvostenko[4], Anna Strelnikova[5], Stanislav Milevskyi[6], Sergii Golovashych[7]

[1]Department of Cybersecurity, National Technical University "Kharkiv Poltechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-1647-6444

[2]Department of Information System named after V. O. Kravets, National Technical University "Kharkiv Poltechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-7853-5855

[3]Department of Photonics, Technical University of Graz, Graz, Austria
ORCID: https://orcid.org/0000-0001-5096-1465

[4]Department of Cybersecurity, National Technical University "Kharkiv Poltechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-6436-4159

[5]Department of Cybersecurity, National Technical University "Kharkiv Poltechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-7964-7330

[6]Department of Cybersecurity, National Technical University "Kharkiv Poltechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-5087-7036

[7]Department of Software Engineering and Management Intelligent Technologies
National Technical University "Kharkiv Poltechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0009-0004-2468-1952
✉Corresponding author: Serhii Yevseiev, e-mail: serhii.yevseiev@gmail.com

ARTICLE INFO

Article history:
Received date 03.01.2023
Accepted date 16.02.2023
Published date 28.02.2023

Section:
Communications system

DOI

10.21303/2313-8416.2023.002828

KEYWORDS

artificial intelligence
semiotic
zero trust security
information technologies

ABSTRACT

The object of research: first, to identify and discuss the security problems of cyber-physical systems associated with the emergence of qualitatively new technologies and qualitatively new affordable artificial intelligence software. Secondly, building the concept of the security structure of a cyber-physical system based on the Zero Trust Security approach. Creation of a new secure load transfer structure based on the semiotic approach.

Investigated problem: information system security problems continue to cause significant costs and damage to organizations. Sustainability requires comprehensive and integrated security platforms that reach customers, whether they work at headquarters, in a branch office, or individually from random touchpoints.

The main scientific results: the concept of a structured protection system with the Zero Trust Security approach has been developed. The structure of the semiotic analysis of the segmentation of the transmitted load on the blocks is proposed. Blocks by signs are subjected to individual analysis. According to the features, the blocks are transformed by the selected representation into an object/groups of objects. Groups for transmission in the load are tagged, have different coding severity (depth), depending on the risk assessment. Groups are transmitted through the network in different ways (paths) – VPN (different ESP), unencrypted tunnel, open access, etc. This solution improves the throughput of malicious load analysis prior to transmission. The performance overhead for encoding/decoding the load and encapsulating/de-encapsulating during transmission is reduced. The transmission bandwidth is increased.

The area of practical use of the research results: businesses requiring secure access to on-premise resources and mission-critical cloud environments. Organizations using employees in distributed networks. Specialists in the deployment and analysis of the protection of cyber-physical systems.

Innovative technological product: The semiotic security concept extends the zero-trust security model, which focuses on protecting network traffic within and between organizations. This concept uses load traffic segmentation, which combines an advanced analysis and transfer load transformation framework.

This concept provides for integration with other cybersecurity technologies such as endpoint discovery and response (EDR) and security information and event management (SIEM) to provide a more comprehensive security solution.

This solution improves the throughput of malicious load analysis prior to transmission. Reduced performance resources for encode/decode load and encapsulate/deencapsulate in transit.

Scope of the innovative technological product: this concept can be applied to enterprises that already have some elements of zero trust in their corporate infrastructure, but cannot strictly control the state of the requested assets, are limited in implementing security policies for certain classes of users. This deployment model can also be applied to enterprises that use cloud services for individual business processes.

It can be useful for researchers and administrators in the development of corporate cybersecurity plans, which uses the concepts of zero-trust and covers relationships between components, workflow planning, and access policies.

Yevseiev, S., Tolkachov, M., Shetty, D., Khvostenko, V., Strelnikova, A., Milevskyi, S., Golovashych, S. (2023). The concept of building security of the network with elements of the semiotic approach. ScienceRise, 1, 24–34. doi: http://doi.org/10.21303/2313-8416.2023.002828

1. Introduction

1. 1. The object of research

The purpose of the work is to develop the conceptual foundations for building a multicontour network security system. The Zero Trust Security approach is proposed as the basis for interaction in such a system. This approach will allow the formation of a network security system that covers the entire network security stack. This approach will provide security services in both the internal and external security loop based on the application of a semiotic approach to transfer load transformation.

To achieve the goal of the work, it is necessary to solve the following tasks:

– apply the concept of network security based on the Zero Trust Security (ZTS) approach;

– analyze and propose principles for the design and deployment of Zero Trust Architecture (ZTA);

– propose a network structure model for the implementation of ZTA, which shows the basic relationship between components and their interaction. This model defines components operating in the control plane and in the data plane;

– taking into account the interaction of the software, the cyber-physical system (CPS) to develop a transmission load transformation structure based on the semiotic approach.

1. 2. Problem description

Computing resources and infrastructure of enterprises are becoming more and more complicated. Computation resources are growing in accordance with the Law of Moore, that is, since 2015, rapid growth has been undergoing, almost twice every 18 months [1].

In December 20, NIST (National Institute of Standards and Technology) published a report [2], which states that a full-scale quantum computer will hack 7,000 symmetrical and asymmetric cryptosystems. Systems that use cryptography on elliptical curves will be hacked in the next decade [3]. Existing quantum computers are still not powerful enough to implement the Shor (or Grover) algorithm [4, 5] and they threaten the safety of cryptographic algorithms currently used in the near future. It is not known exactly when such a quantum computer can be built, although experts suggest that this may be possible in the next two decades [3].

Although the question may arise: why this is a problem and if there is a potential threat to users today, although there is no large-scale quantum computer yet? That if at least one solution is found, which will ensure the drop in crypto resistance of asymmetric cryptosystems in total, then all others will be subject to the "domino" effect, that is, we will have an avalanche of hacks. Therefore, already since 2000–2005, options for new approaches to building security systems are already looking being look for.

On the other hand, in recent years, artificial intelligence (AI) systems have been significantly improved, and their capabilities have expanded.

OpenAI, Google AI and DeepMind are improving modern artificial intelligence technologies. To date, it is possible to see modern developments OpenAI, Bard, Dall E, Imagenet, etc. based on the Generative Pre-Trained Transformer 3 [6]. These developments actively use a database set. They convert and generate text, images, speech. Act as a filter for content. But the most important thing is that it is necessary to take into account the development trends of the security of systems, the fact that these developments have open commercial and non-profit API AI.

According to Georgetown University's Center for Security and Emering Technology (CSET), OpenAI and Stanford Internet Observatory (SIO) as artificial intelligence systems continue to improve, there is concern that malicious actors will have more reason to use them for nefarious goals. Today it is possible to see the influence of artificial intelligence on the stability of protecting various systems. Systems of artificial intelligence also carry a number of risks that are not fully taken into account with the help of existing structures and approaches to risk management. On the other hand, with proper control, artificial intelligence systems can soften threats of security, their consequences and control them [7].

Today, local or so called target attacks, which are realized with a probability of 95% pose the main threat. Because they are complex and aimed at the result. These threats have several channels of influence.

They can influence certain security services, and they can also receive the effect of synergy [8]. Not just the addition of threats, obtaining access or damage, but this is several times an

increased effect and influence on all components of security services. This is confidentiality, integrity, authenticity, availability of traffic management, involvement.

It becomes difficult to manage internal networks, remote offices with its local infrastructure, deleted and/or mobile users and cloud services.

1. 3. Suggested solution to the problem

Thus, in the new reality, where unprecedented hybrid work intersects, the threat of ineffective use of existing algorithms, deployment structures, and the incessant implementation of artificial intelligence and new attacks, a new approach to the direct formation of security systems is needed. An approach is needed using multicontour security systems [9] with an approach based on Zero Trust Security [10], which covers the entire stack of network safety. With effective use, this will open an incredible level of performance, providing each user with safe access to any application from any place.

The structure of the functional model of construction is needed, combining the improved structure of the analysis and transformation of the transmission load. It should combine the strength of existing vulnerabilities databases, for example, US National Vulnerability Database (NVD) [11], API AI, the semiotics paradigm and transformation of divided information using dynamic sets of representations.

The cyberphysical system is a system that is based on the synthesis of mobile technologies and classic computer networks and systems. Therefore, between the information resources of traditional IT systems and the resources of cyberphysical systems, there are significant differences, which makes it impossible to use the methodological foundations oriented towards traditional IT systems in the sphere of cyberphysical systems [12].

A comprehensive approach is needed, based on the analysis of existing technical solutions and the use of artificial intelligence based on semiotic transformation.

Publications devoted to the analysis and development of methodological foundations of building such a complex system can be divided into several groups. The first group combines the publications describing semiotics in the context of information transformation. The second group includes publications devoted to various applications of artificial intelligence, in relation to cyberphysical systems. Publications of the third group describe the principles of the Zero Trust Security approach.

In [13] Andersen, the main developer of computer semiotics determines that “semiotics can be useful to improve the interpretation of computer signs and create understandable interaction”.

The development of semiotic interfaces is described, which is true for the entire area of computer semiotics, including the semiotics of the transformed load and transformations in the protection of traffic: “Semiotics is an abstraction of individual disciplines, such as linguistics, art theory, drama theory and cinema theory. Therefore, it can serve as a general language for a systematic transfer of information from one area to another. This is useful when developing computer interfaces, since computers are inherently multimedia, where codes from these different areas are found and united in practice” [13]. It is noted that semiotics can also contribute to the correct design of program texts and give predictions about the interaction between computer systems and the context of their use. The work gives a characteristic by computer systems and describes interaction based on signs.

In [14] it is noted that in the “so called cyberspace” it is possible to find “the use of several concepts of space (attached to different symbolic forms). On the one hand, there is a concept of geometric space, but there are elements of the concept of space in the symbolic form of myth/religion”. It is noted here that in the artificial space of computer memory it becomes possible to simulate surrogate reality, synthetic hyperreality, which is difficult to distinguish from our conditional reality. Modeling surrogate reality can be used for various representations of symbolic forms.

In [15], a characteristic of cyberphysical systems (CPS) is given that they combine calculations and communication, using and/or controlling entities in the physical world. Models and description of perception and manipulation of the physical world are offered. System behavior and its interaction with other forms based on events are described. Such components as the physical world, software, traffic monitoring based on interactive agents are described. Interactive agents are formalized as actor-like objects with the rules of interaction through messages, interaction

through interface points and politicians of joint activities. The ways of interaction between them and the Semantic of interaction both vertically and horizontally are described. This is useful for understanding the interaction of cyberphysical systems in one perimeter.

To complete the coverage of the theme of multicontour protection and its use on the basis of the Zero Trust Security approach, the following work should be noted [16]. The article is relevant because the technologies of interaction with the participation of users, devices, interactions with the cloud go beyond the traditional network, the perimeter has expanded significantly and created gaps in appearance, which makes the organization more susceptible to attacks. After the attackers violate the perimeter, further horizontal movement becomes unhindered. The concept of attack with areas of application, such as software security, cloud computing security, security of mobile devices, moving targets defense (MTD), is well compared in it. In this article, the concept of the attack surface is transferred to the network level as a security indicator to assess the stability of networks to potential zero-day attacks. The levels of abstraction for software are analyzed. Compatibility is described with the surface and resources inside the network. Heuristic algorithms are offered for this compatibility.

It is worth considering also artificial intelligence systems (AI), which in recent years have significantly improved, and their capabilities have expanded.

First of all, it is worth mentioning the report of the National Institute for Standards and Technologies (NIST) entitled "The structure of risk management of artificial intelligence" (AI RMF 1.0) dated January 2023 [17]. It notes that for the Sustainability of artificial intelligence technology has great potential. However, there are also potential risks associated with AI, which can have negative consequences for individuals and society both in the short and long term. The risks associated with AI systems are unique, so their reduction can be a serious problem for organizations. However, at the same time, if they are not solved effectively, they can lead to adverse results. It is noted that the complexity of the systems of AI and the environment in which they are used and performed make it difficult to detect and eliminate failures. Achievements in the field of AI can change the current state of cybersecurity and, conversely, as cybersecurity of AI systems affects their safe and reliable development, deployment and operation. Therefore, it is important to manage the risks of AI, adhering to the responsible methods of AI. Part 2 describes four specific functions and division into categories that help organizations eliminate the risks associated with AI systems. Since the structure was developed within the framework of a consensus based on a consensus, an open, transparent and joint process, it reflects the opinion of all interested parties involved in the process. Thus, the resulting structure is more practical, flexible and easy to use for enterprises.

The publication [18] is also important, which systematizes the existing knowledge about the quantitative analysis of CPS and the CPS connection with intellectual systems. The article proposes dynamic, the structure of stability assessment for CPS, which consists of three stages: (1) description of the system, (2) scenario of violation and (3) intellectual stability strategy. Each step describes the objects of analysis regarding the description of CPS, the script of destruction and the intellectual stability strategy, respectively. Then the main quantitative methods used to evaluate them are analyzed. After the analysis, four criteria are given that analysts are guided when choosing a method for use in specific thematic conditions.

2. Materials and Methods

The concept of a structured protection system with the Zero Trust Security approach was chosen as the basis. The structure of the functional model for constructing the cyber protection of an enterprise network is proposed, which combines an improved structure for analyzing and transforming the transmission load. The implementation of such a construction is proposed using a five-stage methodology for employees, workloads and workplaces, which is based on a unified secure interaction of devices in the cyber-physical system of enterprises. A concept has been developed that takes into account an approach that uses multi-contour security systems and is based on an analysis of existing technical solutions and the use of artificial intelligence based on semiotic transformation.

It is proposed to segment the transmitted load into blocks using the methods of semionic analysis (policies, evaluation by criteria in the standardization bases (CVE® Program, etc.), signatures, etc.). Blocks by signs are subjected to individual analysis. According to the features, the

blocks are transformed by the selected representation into an object/groups of objects. Groups for transmission in the load are tagged, have different coding severity (depth), depending on the risk assessment. Groups are transmitted through the network in different ways (paths) – VPN (different ESP), unencrypted tunnel, open access, etc.

Implementation using a five-step methodology for employees, workloads, and jobs is proposed. The Trust Algorithm (TA) is the process used by the Policy and Internal Representation mechanism to finally mark the fragments of the transmission load. The policy engine receives input from multiple policy database sources with observable information about subjects, subject attributes and roles, historical patterns of subject behavior, sources of threat intelligence, a set of internal concept representations, a dynamic information feature hierarchy, and other sources of metadata.

3. Results and discussion

3. 1. Implementation of a cyberphysical system based on program-defined perimeters

Since the technologies of interaction in cyberphysical systems with the participation of users, devices, various software, interaction with the cloud go beyond the traditional network, the perimeter has expanded significantly and created gaps in appearance, which makes the organization more susceptible to attacks. This trend allows cybercriminals to use cyberphysical systems to obtain a synergistic effect, violating the perimeter and further horizontal movement becomes unhindered.

Early works to strengthen the security of the network usually rely on standard quality models with increasing network security [19–21]. Thus, to prevent, or ensure the security circuit in cyberphysical processes, it is necessary to solve a unified approach to building protection against threats, taking into account their synergism and hybridity for all security components: information security (IS), cybersecurity (CS) and security of information (SI), In the context of their complexing with methods of social engineering and a lack of funds to ensure the required level of security [12].

To reduce the vulnerabilities of organizations, comprehensive and integrated security platforms are currently being created, which cover customers, regardless of whether they work at the headquarters, in the branch or individually from the random points of the connect (**Fig. 1**).

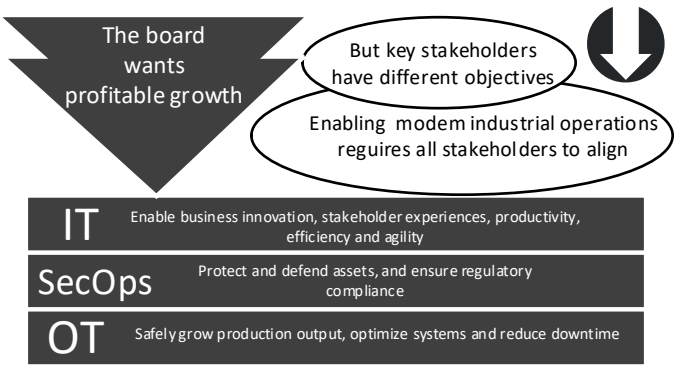

Fig. 1. Integrated security platform

In the new reality, where unprecedented hybrid work intersect, the ongoing introduction of cloud technologies and new attacks, an approach with zero trust, which covers the entire stack of network security, is used.

Using this model, a conceptual transition from permission is carried out from permission to all users, devices and workloads by default to the paradigm where organizations do not trust anything inside or outside their perimeter of the network. Access is provided only by authorized users, devices and workloads after establishing confidence and preventing threats and all this without reducing interaction with the user.

Several interconnected principles of design and deployment of a network based on Zero Trust Architecture (ZTA):

1. All data and computing services are considered as resources. For example, an enterprise can classify personal devices as resources if it is allowed to access corporate resources.

2. All communication is safe regardless of the network location.

3. Access to individual corporate resources is provided for each connection.

4. Access to resources is determined by politics, including the state of user identification and the requesting system, and may include other behavioral attributes. The "requesting system" refers to the characteristics of the device (software version, network location, etc.). "Behavioral attributes" include analytics of users and devices, any deviations of behavior from basic models.

5. The company monitors the state of systems and applies corrections as necessary.

6. There is a "permanent access cycle" of threat assessment and continuous authentication, as well as continuous monitoring throughout the interaction in the system [10].

A huge number of components of the cyberphysical system are associated with each other. Suppliers often rely on proprietary API interfaces. This requires a close partnership between suppliers' communities to ensure an early notice of changes in the API, which may affect the compatibility between products. In the interaction of software, transmission control, more adaptive protection of the transmitted load of the load to various role -playing devices on the network is required. Dependence on changes in the API is required to minimize.

Since zero trust as a strategy for the design and deployment of corporate infrastructure is still in the formation stage, a unified secure interaction of the device in the cyberphysical system of enterprises is required.

For the external circuit of the security system, access to services, resources that do not require account data (for example, a generally accessible webstrap) can be distinguished. In this case, ZTA principles do not apply directly. The company cannot strictly control the state of the requested assets that do not belong to it. Information about incoming requests may be useful for determining the state of public service and detecting possible attacks masking to legal users. This can be analyzed using additional segmentation and intellectual analysis of traffic load.

If to take into account these security calls comprehensively for the internal and external contour, it is necessary to start with the development of the interaction scheme of the components of the infrastructure and separately components of the network perimeter. And this infrastructure must be program-defined [10].

Taking into account the listed calls, an approach is proposed that uses a network infrastructure based on ZTA.

The model on **Fig. 2** shows the basic relationship between the components and their interactions. In **Fig. 2**, the decision on the decision on politics (PDP) is divided into two logical components: politics mechanism and policy administrator (PA). The logical components of ZTA use a separate control plane for communication, while the data of the applications are transmitted in the data plane.

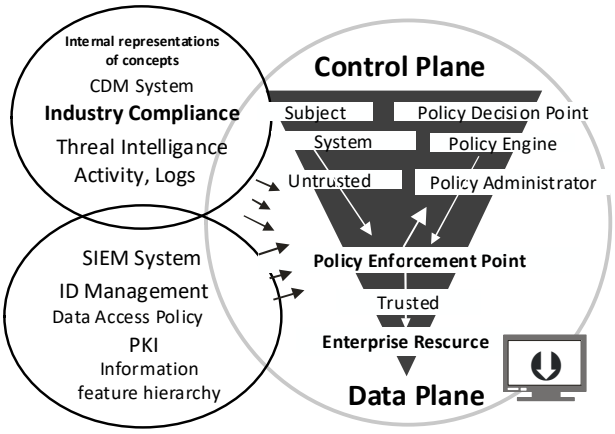

Fig. 2. Basic relations between the components of the network infrastructure and their interaction

The Policy mechanism (PE) uses the policy of the enterprise, the input data from external sources (for example, CDM systems, threat analysis services), as well as the hierarchy of signs of information as input data for the trust algorithm.

PE is associated with the component of the administrator politics.

Politics Administrator (PA): This component is responsible for the establishment, labeling and separation of the load on the signs. It is closely connected with the PE and depends on its solution what idea to apply to the load fragment. Some implementations can consider PE and PA as one service; Here it is divided into two logical components. PA is associated with PEP when creating a communication channel. This connection is carried out through the control plane.

To implement ZTA based on software-defined perimeters, the following gateway-based model is proposed (**Fig. 3**).

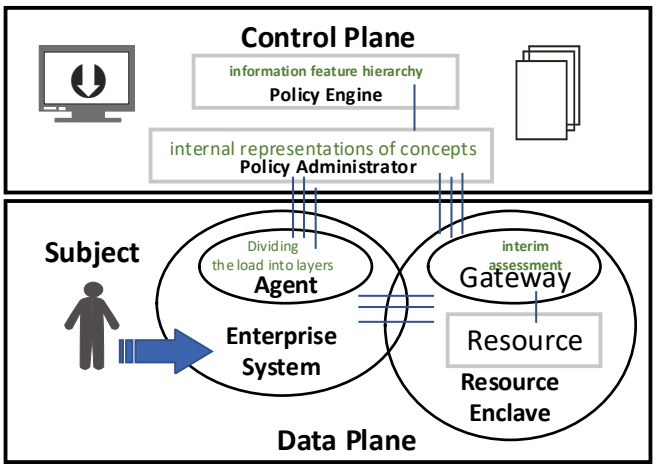

Fig. 3. Software defined perimeter gateway model

Gateway components are located at the edge of a software-defined resource perimeter (for example, a local data center), as shown in **Fig. 3**.

Typically, these resources perform a single business function or may not be able to interact directly with the gateway. This deployment model can also be applied to enterprises that use cloud services for individual business processes.

To segment and label the load by signs, end devices must have a software agent that is used to connect to software-defined perimeter gateways. The gateway protects a set of resources, each resource individually, and determines further behavior for the operation of the outer loop. It can also allow subjects to see resources to which they do not have privileges. Assuming that an enterprise knows the applications/services and workflows it wants to use for its operations, it can create a zero-trust architecture for those workflows.

The proposed approach does not imply trust in the entire load intended for transmission, but establishes trust for each fragment of the load obtained as a result of segmentation based on the trust algorithm.

Implementation is proposed using a five-step methodology for employees, workloads, and jobs through:

1. Establish trust in a user, device, application, etc. before granting access or allowing connections or communications.

2. Determination of signs of the transferred load.

3. Device/application user identification, device/application vulnerability status, typical load, application/service trust, any signs of compromise.

4. Load segmentation based on policies and algorithms developed on the basis of semiotic analysis.

5. The policy engine receives input from multiple sources: policy databases with observable information about subjects, subject attributes and roles, historical patterns of subject behavior, sources of threat intelligence, and other sources of metadata.

6. Enforce trust-based access policies with granular controls based on changing context, such as device security status and application behavior.

7. Continuous verification of trust by monitoring for dangerous devices, non-compliance with policies, behavioral anomalies and software vulnerabilities.

3. 2. Trust algorithm

For an enterprise deploying ZTA, the policy mechanism can be considered as a brain, and the PE trust algorithm as its main thought process. The Trust Algorithm (TA) is a process used by the policy engine and presented internally to finalize the transmission payload fragments. The policy mechanism receives input data from several sources of the policy database with observable information about subjects, attributes and roles of subjects, historical patterns of subject behavior, sources of information about threats, a set of internally presented understood, dynamically changing hierarchy of information attributes and other sources of metadata. The process can be grouped into broad categories and presented in **Fig. 4**.

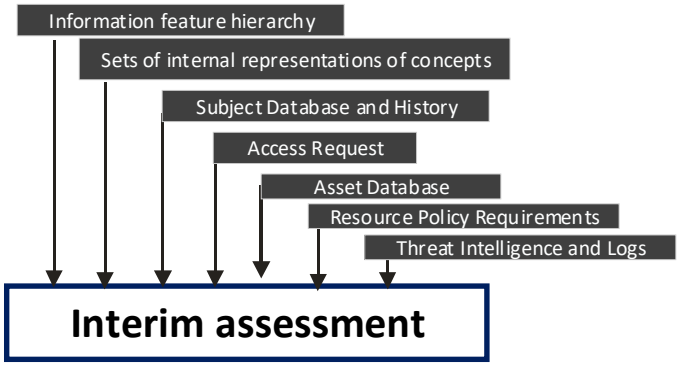

Fig. 4. Input data of the trust algorithm

In the figure, the input data can be divided into categories depending on what they provide to the trust algorithm.

– Database of subjects: this is "who" who requests access to the resource [22].

– Database of assets (and observable state): this is a database that contains the known state of each corporate asset. This is compared to the observable status of the requesting asset and may include OS version, installed software, and integrity.

– The database of internal data is represented by a concept based on a set of information features. It is formed on the basis of policies and can be based on the results of the work of artificial intelligence.

The weight of importance for each data source is determined by an algorithm that connects the source – representation – object and can be adjusted by artificial intelligence. These weight values can be used to reflect the importance of a data segment to an enterprise.

The final decision is then forwarded to the PA for execution. The task of the PA is to configure the necessary PEPs to ensure authorized communication. Depending on how ZTA is deployed, this may include sending authentication results and connection configuration information to gateways and agents or resource portals, and determining the choice of security technology for transmission beyond the enterprise's area of responsibility.

3. 3. Segmentation of transmission load

The process of segmenting the transmission load, determining the weight of importance and, as a result, marking the fragment can be represented as follows in **Fig. 5**.

Initially, the agent software on the transfer side analyzes the contents of the ready payload for transfer. Based on the policies and the hierarchy of features of the complexity of the future representation, the load objects are divided into layers (maybe convolutional layers). For division into layers S_n, the volume of interacting data can be represented by a multidimensional model with flows of influence, analysis

$$S_n = f\left(y, P\right), \tag{1}$$

where y – payload data to transmit, P – policy engine.

$$P = f_n\left(D, v, m\right). \tag{2}$$

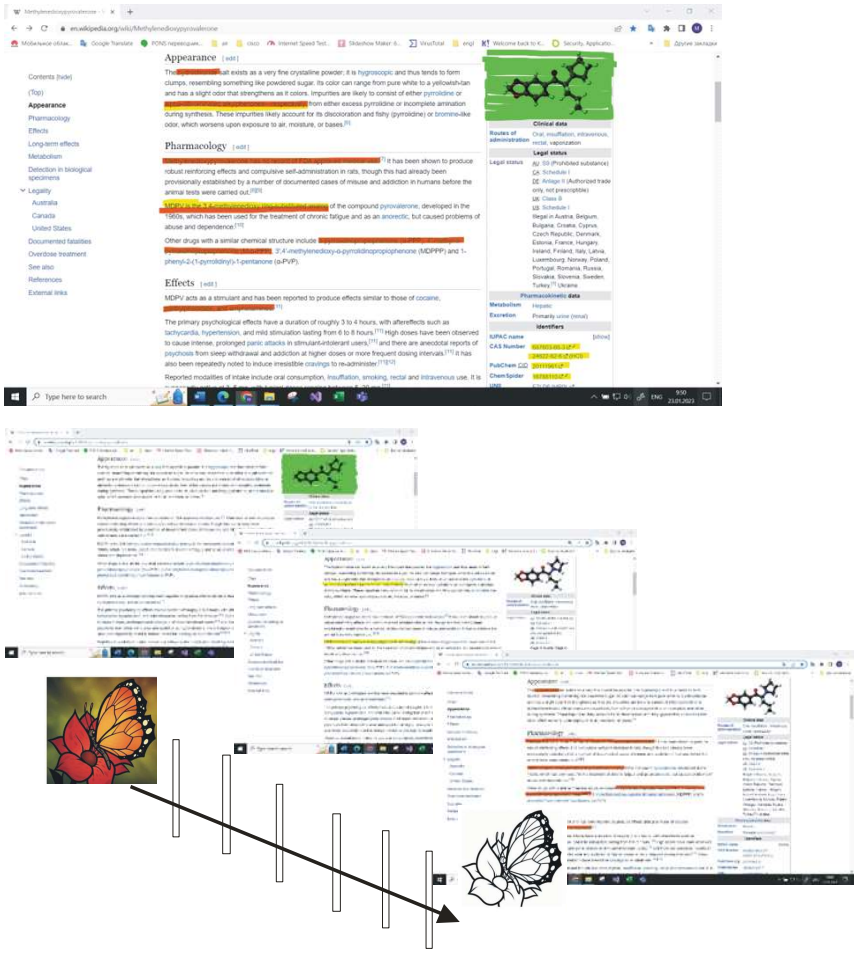

Fig. 5. Transmission load segmentation

The policy engine *P* obtains data from several sources: a policy database *D* with observable information about subjects *h*, attributes *a* and roles of subjects *r*, historical patterns of behavior of subjects *b*, sources of information about threats *v* and other sources of metadata *m*.

$$D = f_d\left(h, a, r\right). \tag{3}$$

According to the algorithms, on the basis of semiotic analysis, there is a choice of an internal representation for an object/group of objects.

Formation of the selection of the relationship between the internal representation and the object/group of objects is proposed to be performed as an optimization problem. The goal is to find the optimal response *E* to the contents of the load *y* given the multimodal context *c*. Depending on the context, the optimal response may be a statement of fact or a follow-up question to remove ambiguity. Statistically, *E* is estimated as

$$E = \frac{\arg\max p\left(r \mid c, m\right)}{r}, \tag{4}$$

where *m* – the whole message, *c* – the context block, *r* – the probability of an arbitrary response. The probability of an arbitrary response can be expressed as the product of the response probabilities

$$\left\{r_i\right\}_{i=1}^{T} \tag{5}$$

for *T* iterations of the analysis [23].

AI when choosing a view can also react in several ways.

The representation is verbalized in the form of objects, the object is projected into a digital image. Overhead information is added to each load block for transmission. The intermediate estimator (gateway) analyzes the service information and applies the current template and determines which way to transmit the load block.

The general concept is shown in **Fig. 6**.

When developing, it was taken into account that the system has a certain structure and a limited list of interaction resources. Each subject has an agent that interacts with a strict set of resources. An enterprise is assumed to know the applications/services and workflows it needs to use for its operations. The agent is used to connect to software-defined perimeter gateways.

For further development of the concept, it is required to expand the structure and list of interaction resources. This applies primarily to the resources that determine the transformation of the load. In the future, it is required to develop algorithms for semiotic analysis, to choose the implementation of using the API associated with generative language models and automated influence operations.

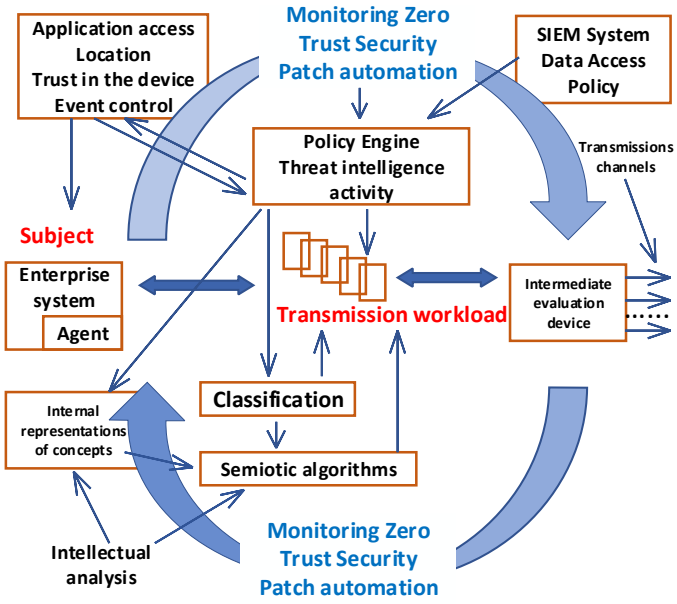

Fig. 6. The concept of building network security using a semiotic approach

4. Conclusions

The concept of Zero Trust Security [10] was chosen as a basis, in part, its implementation as tagging (characteristics or signs) of the load in Cisco's approach to this. It is proposed, using methods of semiotic analysis, to segment the transmitted load into blocks (policies, evaluation by criteria in standardization bases (CVE® Program, etc.), signatures, etc.). Blocks by signs are subjected to individual analysis. According to the features, the blocks are transformed by the selected representation into an object/groups of objects. Groups for transmission in the load are tagged, have different coding severity (depth), depending on the risk assessment. Groups are transmitted through the network in different ways (paths) – VPN (different ESP), unencrypted tunnel, open access, etc.

This approach increases the throughput of pre-transmission malware analysis. The performance overhead for encoding/decoding the load and encapsulating/de-encapsulating during transmission is reduced. The transmission bandwidth is increased.

Conflict of interest

The authors declare that there is no conflict of interest in relation to this paper, as well as the published research results, including the financial aspects of conducting the research, obtaining and using its results, as well as any non-financial personal relationships.

Funding

The study was performed without financial support.

Data availability

Manuscript has no associated data.

References

[1] Riordan, A. O., Fagas, G., O'Flynn, B., Rohan Galvin, J. P., Mathúna, C. Ó. (2022). More Than Moore. International Roadmap for Devices and Systems (IRDS) white paper.

[2] NISTIR 8413 – Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process (2022). Available at: https://csrc.nist.gov/publications/detail/nistir/8413/final

[3] Mosca, M., Piani, M. (2022). Quantum threat timeline report 2021. Available at: https://globalriskinstitute.org/publication/2021-quantum-threat-timeline-report-global-risk-institute-global-risk-institute/

[4] Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134. doi: https://doi.org/10.1109/sfcs.1994.365700

[5] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing – STOC '96, 212–219. doi: https://doi.org/10.1145/237814.237866

[6] Hao, K. (2020). OpenAI is giving Microsoft exclusive access to its GPT-3 language model. MIT Technology Review. Available at: https://www.technologyreview.com/2020/09/23/1008729/openai-is-giving-microsoft-exclusive-access-to-its-gpt-3-language-model/

[7] Tabassi, E. (2023). AI Risk Management Framework. doi: https://doi.org/10.6028/nist.ai.100-1

[8] Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. doi: http://doi.org/10.15587/978-617-7319-31-2

[9] Nevliudov, I., Yevsieiev, V., Maksymova, S., Filippenko, I. (2020). Development of an architectural-logical model to automate the management of the process of creating complex cyber-physical industrial systems. Eastern-European Journal of Enterprise Technologies, 4 (3 (106)), 44–52. doi: https://doi.org/10.15587/1729-4061.2020.210761

[10] Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020). Zero Trust Architecture. National Institute of Standards and Technology (NIST) Special Publication 800-207. Gaithersburg. doi: https://doi.org/10.6028/nist.sp.800-207

[11] National Vulnerability Database. Available at: http://nvd.nist.gov

[12] Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et al. (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (105)), 6–19. doi: https://doi.org/10.15587/1729-4061.2020.205702

[13] Andersen, P. B. (2000). What Semiotics Can and Cannot Do for HCI. Position paper for the CHI'2000 Workshop on Semiotic Approaches to User Interface Design.

[14] Marx, P. W. (1999). The Paradise of Immediacy is closed. Some Remarks Concerning a Semiotics of Culture Rooting in Cassirerean Philosophy and Greimassian Semiotics. S. European Journal for Semiotic Studies, 11 (1-3), 327–352.

[15] Talcott, C.; Wirsing, M., Banâtre, J. P., Hölzl, M., Rauschmayer, A. (Eds.) (2008). Cyber-Physical Systems and Events. Software-Intensive Systems and New Computing Paradigms. Lecture Notes in Computer Science. Vol. 5380. Berlin, Heidelberg: Springer, 101–115. doi: https://doi.org/10.1007/978-3-540-89437-7_6

[16] Zhang, M., Wang, L., Jajodia, S., Singhal, A. (2021). Network Attack Surface: Lifting the Concept of Attack Surface to the Network Level for Evaluating Networks' Resilience Against Zero-Day Attacks. IEEE Transactions on Dependable and Secure Computing, 18 (1), 310–324. doi: https://doi.org/10.1109/tdsc.2018.2889086

[17] Tabassi, E. (2023). AI Risk Management Framework. doi: https://doi.org/10.6028/nist.ai.100-1

[18] Cassottana, B., Roomi, M. M., Mashima, D., Sansavini, G. (2023). Resilience analysis of cyber-physical systems: A review of models and methods. IET Cyber-Physical Systems: Theory & Applications, 6 (3), 139–150. doi: https://doi.org/10.1111/risa.14089

[19] Sheyner, O., Haines, J., Jha, S., Lippmann, R., Wing, J. M. (2002). Automated generation and analysis of attack graphs. Proceedings 2002 IEEE Symposium on Security and Privacy, 273–284. doi: https://doi.org/10.1109/secpri.2002.1004377

[20] Wang, L., Noel, S., Jajodia, S. (2006). Minimum-cost network hardening using attack graphs. Computer Communications, 29 (18), 3812–3824. doi: https://doi.org/10.1016/j.comcom.2006.06.018

[21] Wang, L., Albanese, M., Jajodia, S. (2014). Network Hardening: An Automated Approach to Improving Network Security. Springer Publishing Company, Incorporated, 60. doi: https://doi.org/10.1007/978-3-319-04612-9

[22] Grassi, P. A., Garcia, M. E., Fenton, J. L. (2017). Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3. doi: https://doi.org/10.6028/NIST.SP.800-63-3

[23] Shang, L., Lu, Z., Li H. (2015). Neural Responding Machine for Short-Text Conversation. Proceedings of the 53rd Annual Meeting of the Association for Computational Linguistics and the 7th International Joint Conference on Natural Language Processing (Vol. 1: Long Papers). Beijing: Association for Computational Linguistics, 1577–1586. doi: https://doi.org/10.3115/v1/p15-1152