Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network

Pavlo Anakhov[1], Viktoriia Zhebka[2], Svitlana Popereshnyak[2], Pavlo Skladannyi[3], and Volodymyr Sokolov[3]

[1] National power company "Ukrenergo", 25 S. Petliuri str., Kyiv, 01032, Ukraine
[2] State University of Information and Communication Technologies, 7 Solomenskaya str., Kyiv, 03110, Ukraine
[3] Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine

Abstract

The environment is changed by people, both unconsciously and consciously. The engineering and economic development of the environment is complemented by actions that involve deliberate destruction. Since 2014, units of the Russian army have been carrying out illegal military and terrorist actions on the territory of Ukraine, in particular, against critical infrastructure objects. The purpose of the article is to find ways to protect critical information infrastructure objects from cyber attacks. A universal way to counter cyber attacks is to decentralize the telecommunications network. A universal way to ensure the "decentralization" of a network is its hybridization, which ensures proper scalability. The values of signal parameters in a hybrid network depend on the physical nature of the signal and the transmission medium. Based on this, it may be logical to use a hybrid telecommunications network to protect against cyber attacks, which allows the selection of a channel with parameters that do not correspond to the harmful signal for the transmission of a useful signal.

Keywords

Hybrid network, communication channel, signal, signal transmission medium, useful signal, malicious signal.

1. Introduction

The environment is changed by humans mainly unconsciously.

At the same time, the environment is changed consciously by humans—engineering and economic development of the natural and geological system leads to its qualitatively new natural and anthropogenic state.

But some actions imply deliberate destruction, both of infrastructure and the environment itself [1]. In late February and early March 2014, Russian army units occupied the Crimean peninsula. In mid-April 2014, a conflict broke out in Donetsk and Luhansk regions between the armed groups of the Donetsk and Luhansk "people's republics" on the one hand, and Ukrainian law enforcement officers with the involvement of the Armed Forces of Ukraine on the other. On February 24, 2022, Russian President vladimir putin announced a military operation on the territory of Ukraine; a few minutes later, missile attacks began. Russian troops invaded Ukraine, entering from Russia, Belarus, and the temporarily occupied Crimea. There is an obvious threat of an increase in the number of emergencies related to illegal acts of terrorism, as well as military emergencies related to the consequences of the use of weapons.

At the end of 2022, Russian troops launched attacks on critical electricity infrastructure. Drones and missiles hit 40% of Ukraine's

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: anakhov@i.ua (P. Anakhov); viktoria_zhebka@ukr.net (V. Zhebka); spopereshnyak@gmail.com (S. Popereshnyak); p.skladannyi@kubg.edu.ua (P. Skladannyi); v.sokolov@kubg.edu.ua (V. Sokolov)
ORCID: 0000-0001-9169-8560 (P. Anakhov); 0000-0003-4051-1190 (V. Zhebka); 0000-0002-0531-9809 (S. Popereshnyak); 0000-0002-7775-6039 (P. Skladannyi); 0000-0002-9349-7946 (V. Sokolov)

energy facilities [2]. All thermal and hydroelectric power plants suffered varying degrees of damage [3]. The total damage in the energy and extractive sector is estimated at approximately $10.6 billion; aggregate economic, social, and other monetary losses totaled almost $27.2 billion [4]. On 6 June, Russian occupation forces blew up the dam of the Kakhovka hydroelectric power station.

As a result of military-terrorist actions, the total loss in the telecommunications and digital sector is estimated at approximately 1.6 billion US dollars; combined economic, social, and other monetary losses amount to almost 1.6 billion US dollars.

The sustainable functioning of the system of interconnected critical infrastructure facilities is ensured by the critical information infrastructure of these facilities. The critical information infrastructure of Ukraine's energy sector has become the second springboard of warfare, and cyber-attacks are a full-fledged component of this aggression. Ukraine's energy sector had been subject to Russian cyberattacks before 24 February 2022, but with the start of the full-scale invasion, the number of attacks increased significantly. Last year, the Operational Security Centre of the transmission system operator recorded more than 1.5 million corresponding blockages of attempts to attack the industry [5].

The purpose is to find ways to protect critical information infrastructure facilities from cyber threats of military and terrorist origin.

2. Universal Application of Identifiers and Secrets

According to the classic scheme, authentication data is separated for each service separately. The result of the L_i login will be a value determined by a separate function for each service:

$$L_i = F_{S_i}(ID_i, AU_i),$$

where ID_i is the user ID in a specific service; AU_i is a secret; $F()$ is a service-side authentication data verification function; S_i is the corresponding service.

To ensure the hidden secret, you can add its hashing:

$$L_i = F_{S_i}(ID_i, \mathcal{H}(AU_i)).$$

The type of hashing function $\mathcal{H}()$ can be any, the main thing is that it matches both on the user side and on the server side.

This approach creates a burden on the user to store authentication pairs for all services. Each service can have its own open session time, which obliges the user to transfer their data each time. On the other hand, each service must maintain a base of trusted users. With the increase in storage locations, the number of vulnerable repositories increases. And since users simplify their lives and create the same authentication pairs for different services, the hacking of one of the services indirectly compromises others.

It should be noted that some users use password managers, but in this case, if an attacker gains unauthorized access to the password manager [6] not only one authentication pair but also a reliable list of services with all authentication pairs becomes available to him.

One of the ways to ensure the uniformity of passwords is to transfer the function of the password manager to a separate service that is located in the middle of the infrastructure of one organization, for example, identity provider, or in the role of a third party, for example, according to the OAuth 2.0 [7].

If the services are combined into one information system, then the need to save separate authentication pairs for access to different services $\mathbf{S}$ of the same information system recedes into the background. It remains sufficient to perform one login through the security gateway:

$$L|_{\forall \mathbf{S}} = F\big(ID, \mathcal{H}(AU)\big),$$
$$\mathbf{S} = [S_1, S_2, \dots, S_n],$$
$$n \in Z.$$

The zero trust security model postulates the separation of access not only at the login level for the security loop of the information system but also defines the levels of access to each service:

$$L|_{\forall \mathbf{S}} = F\big(ID, \mathcal{H}(AU)\big),$$
$$\mathbf{S} = [(S_1, R_1), (S_2, R_2), \dots, (S_n, R_n)],$$
$$n \in Z,$$

where R_i is the role of the user in the service S_i.

If a user can have several levels of access/roles in different services, then to

switch between roles it is necessary to go through the re-login procedure or use several access media, for example, for web systems it can be different browsers or different instances of the same browser.

On the other hand, a single service may accept more than one identifier from a single user, such as an email address or phone number. In this case, instead of a single identifier, an **ID** array of identifiers should be used:

$$L|_{\forall \mathbf{S}} = F\big(\mathbf{ID}, \mathcal{H}(AU)\big),$$
$$\mathbf{S} = [(S_1, R_1), (S_2, R_2), \dots, (S_n, R_n)],$$
$$\mathbf{ID} = [ID_1, ID_2, \dots, ID_m],$$
$$\{n, m\} \in Z.$$

Different **AU** secrets can be applied to multiple IDs at the same time, such as password, fingerprint scan, face or retina image, etc. This method allows you to use multiple secrets of the same type, for example, multiple fingerprints. Therefore, the general formula has the form:

$$L|_{\forall \mathbf{S}} = F\big(\mathbf{ID}, \mathcal{H}(\mathbf{AU})\big),$$
$$\mathbf{S} = [(S_1, R_1), (S_2, R_2), \dots, (S_n, R_n)],$$
$$\mathbf{ID} = [ID_1, ID_2, \dots, ID_m],$$
$$\mathbf{AU} = [AU_1, AU_2, \dots, AU_k],$$
$$\{n, m, k\} \in Z.$$

The novelty of this method is that it is not important for the authentication service which identifier and which secret were sent. Thus, any communication by any communication channel is allowed. As a result, the authentication system becomes more universal, and the influence of temporarily unavailable methods of transmitting identifiers and secrets is reduced.

3. Results

According to the definition, information security objectives are confidentiality, data integrity, authentication (entity and data origin), and non-repudiation (for example, [8–9]).

Thus, the probability of violation of the functional properties of Critical Information Infrastructure (CII) takes into account the classes of threats to its security:

$$P = 1 - \sum_{i=1}^{4} (1 - q_i), \qquad (1)$$

where q_1 is the probability of a breach of confidentiality (protection of data from unauthorized reading by unauthorized persons, entities, or processes); q_2 is the probability of a breach of data integrity (the ability to detect any modifications, insertions, or deletions that affect the correctness of the data stored in the information resource); q_3 is the probability of breach of authentication security (protection against unauthorized use of the resource); q_4 is the probability of breach of non-failure security (security when a participant in the interaction cannot successfully deny the performance of certain actions) [10–11].

According to practice, the analysis of possible threats is carried out during the design, modernization, and reconstruction of CII. The synthesis of measures aimed at reducing damage is usually carried out for individual threats [8–9, 12].

A universal way to counter cyber threats is to decentralize the telecommunications network [13–15].

A universal way to ensure the "decentralization" of the network is its hybridization, which ensures proper scalability.

Fig. 1 shows a diagram of a hybrid telecommunications network consisting of a hierarchical sequence of multiplexers.

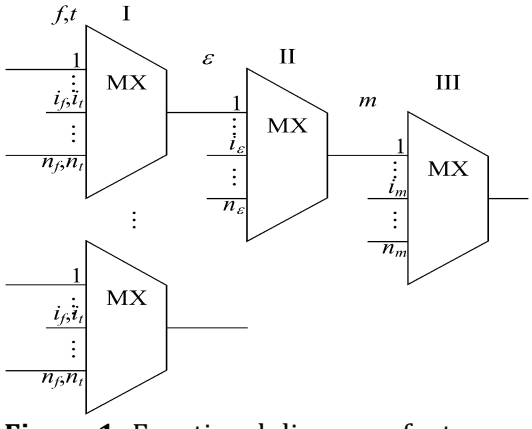

Figure 1: Functional diagram of a transmitter of a hybrid telecommunication network: (I) level of channel multiplexing with frequency and time division of signals; (II) level of channel multiplexing with division of signals by physical nature; (III) level of channel multiplexing with division of signals by transmission media [16].

According` to the functional diagram, communication channels are described by a dependency of the form [16]:

$$e_j = \left(i_f, i_t, i_\varepsilon, i_m\right),\ i_f = \overline{1, n_f},\ i_t = \overline{1, n_t},\ i_\varepsilon = \overline{1, n_\varepsilon},\ i_m = \overline{1, n_m},\ j = \overline{1, j}, \quad (2)$$

where e is the designation of a communication channel; j is the identifier of a communication channel in a multiplexed telecommunication network; i_f, i_t, i_ε, and i_m are channel identifiers of multiplexing systems with frequency f, time t channel separation, channel separation by the physical nature of signals ε, by transmission media m, respectively; n_f, n_t, n_ε, and n_m are numbers of channels n of multiplexing systems with frequency f, time t channel separation, with channel separation by physical nature of signals ε, and by transmission media m, respectively.

According to the scheme shown in Fig. 1, a hybrid telecommunications network, in addition to frequency (the same as spectral, with wavelength division) and time division multiplexing, supports multiplexing of communication channels with division by physical nature and transmission media. Table 1 shows the matrix of their correspondence.

Table 1

Matrix of correspondence of signals of different physical nature used for information transmission to transmission media

The physical nature of the signal	Transmission medium				
	Earth's atmosphere	Space	Underwater	Underground	Artificial guide rails
Acoustic [16]	+	–	+	+	+
Electromagnetic [16]	+	+	+	+	+
Optical [16]	+	+	+	–	+
Quantum [16]	+	+	–	–	+
Neutrino [16]	+	+	+	+	–
Geophysical [17]	–	–	Microseisms caused by standing water waves	Microseisms caused by standing water waves	–

The values of signal parameters in a hybrid network depend on the physical nature of the signal and the transmission medium [16]:

$$X\left[e_j = \left(i_f, i_t, i_\varepsilon, i_m\right)\right] \neq X\left[e_j = \left(i_f, i_t, i_{\varepsilon'}, i_m\right)\right], \quad (3)$$

or

$$X\left[e_j = \left(i_f, i_t, i_\varepsilon, i_m\right)\right] \neq X\left[e_j = \left(i_f, i_t, i_\varepsilon, i_{m'}\right)\right], \quad (4)$$

where X—is a certain signal parameter in a hybrid network (signal attenuation in the medium, range, and maximum signal transmission rate, etc.); ε, ε'—signals of different physical nature; m, m'—different transmission media.

Based on this, it may be logical to use a hybrid telecommunications network to protect against cyber attacks, which allows the selection of a channel for the transmission of a useful signal with indicators that do not correspond to the malicious signal through which the malicious code is distributed. Protection in the event of an attack is provided by changing the physical nature of the useful information signal and/or its transmission medium.

4. Discussion

Decentralized control systems provide an effective solution to many problems of managing large-scale industrial processes. They are more effective in terms of cyber attacks than distributed and centralized control systems [13, 18–19].

A decentralized authentication and access control protocol addresses broader data privacy and security needs [14]. In Fig. 2 shows a comparative characteristic of centralised and decentralized telecommunication networks.

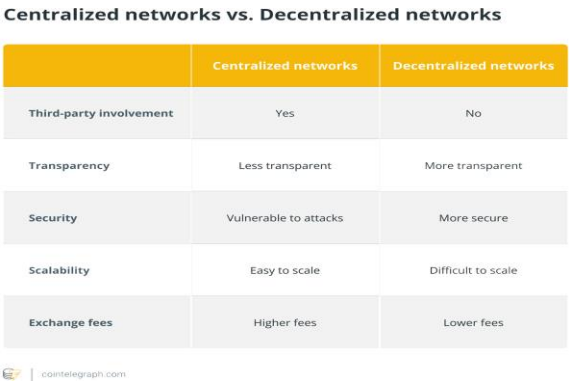

Figure 2: Centralized networks vs. decentralized networks [15]

5. Conclusions

Different values of signal parameters in a hybrid telecommunications network decentralized through the use of channels and channel sections (communication lines, telecommunications equipment) with signals of different physical nature is a feature of a hybrid telecommunications network. This determines the feasibility of choosing a channel from the available list of existing ones in the event of a cyber attack or cyber threat. Protection is achieved by changing the physical nature of the useful information signal and/or its transmission medium.

References

[1] F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021). doi: 10.1109/picst54195.2021.9772181.

[2] Center for Combating Disinformation, How Ukraine Survived Russia's Winter Terror (2023). URL: https://cpd.gov.ua/articles/yak-ukrayina-perezhyla-zymovyj-teror-rosiyi/

[3] V. Perun, The Russian Federation Launched more than 1,200 Missiles and Drones at Key Energy Facilities of Ukraine, Ukrenergo (2023). URL: https://lb.ua/society/2023/04/08/551391_rf_vipustila_klyuchovih.html

[4] UKRAINE. Rapid Damage and Needs Assessment. February 2022 – February 2023; Anne Himmelfarb (Ed.). The World Bank, the Government of Ukraine, the European Union, the United Nations.

[5] Ukrinform, Last Year, more than 1.5 Million Cyberattacks on the Ukrainian Energy Sector Were Beated Off (2023). URL: https://www.ukrinform.ua/rubric-technology/3729720-torik-vidbili-ponad-15-miljona-kiberatak-na-ukrainsku-energeticnu-galuz.html

[6] otto-js Research Team, Chrome & Edge Enhanced Spellcheck Features Expose PII, Even Your Passwords (2022). URL: https://www.otto-js.com/news/article/chrome-and-edge-enhanced-spellcheck-features-expose-pii-even-your-passwords

[7] D. Hardt, The OAuth 2.0 Authorization Framework (2012). URL: https://www.rfc-editor.org/rfc/rfc6749

[8] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography (5th printing), Boca Raton: CRC Press (2001).

[9] H.C.A. van Tilborg, S. Jajodia, Encyclopedia of Cryptography and Security, New York: Springer-Verlag (2005).

[10] I. Kuzminykh, et al., Investigation of the IoT Device Lifetime with Secure Data Transmission, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, vol. 11660 (2019) 16–27. doi: 10.1007/978-3-030-30859-9_2

[11] V. Buriachok, et al., Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2746 (2020) 23–32.

[12] P. Anakhov, et al., Increasing the Functional Network Stability in the Depression Zone of the Hydroelectric Power Station Reservoir, in: Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149. (2022) 169–176.

[13] S. Chen, Z. Wu, P.D. Christofides, Cyber-security of Centralized, Decentralized, and Distributed Control-detector Architectures for Nonlinear Processes, Chem. Eng. Res. Des. 165 (2021) 25–39. doi:10.1016/j.cherd.2020.10.014.

[14] X. Xiang, J. Cao, W. Fan, Decentralized Authentication and Access Control Protocol for Blockchain-based E-health

Systems, J. Netw. Comput. Appls. 207 (2022) 103512. doi:10.1016/j.jnca.2022.103512.
[15] COINTELEGRAPH, Centralized vs. Decentralized Digital Networks: Key Differences (2022). URL: https://cointelegraph.com/public/index.php/explained/centralized-vs-decentralized-digital-networks-key-differences/amp
[16] P. Anakhov, et al., Evaluation Method of the Physical Compatibility of Equipment in a Hybrid Information Transmission Network, J. Theor. Appl. Inform. Technol. 100(22) (2022) 6635–6644.
[17] P. Anakhov, Prospects for the Use of Microseisms, Caused by Standing Waves of Water Bodies, Geodynamics 2(33) (2022) 91–98. doi:10.23939/jgd2022.02.091.
[18] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.
[19] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.