Volume XXV, 48 – No.1, 2023, DOI: 10.35116/aa.2023.0006

THE CYBERSECURITY ASPECT OF REMOTE TOWER OPTICAL SYSTEMS

Gábor HORVÁTH
Faculty of Military Science and Officer Training, National University of Public Service, 1 Kilián utca, H-5008 Szolnok, Hhungaria
E-mail: horvath.gabor@uni-nke.hu

Abstract. In the aviation domain, the past decade has seen the rise of emergent and often disruptive technologies, including automation, digital transformation, and data analytics. The solutions derived from these technologies, like unmanned aircraft or remote tower operations, on one hand were created in order to generate some sort of a benefit, but on the other hand they led us to a previously uncharted territory, called cybersecurity vulnerabilities. If these vulnerabilities are exploited, they may lead to a massive damage to the Aviation Ecosystem that can contribute to catastrophic failures. With this in mind, protection to the remote tower optical systems is of paramount importance. Therefore, this study focuses on providing a framework for cybersecurity assessments of remote tower optical systems.

Keywords: remote tower, cybersecurity, cyber vulnerabilities, air traffic control

1. INTRODUCTION

The achievements of the Fourth Industrial Revolution affect our everyday lives in many ways, some of which are may not noticed by laymen. In relation to the hardly noticeable examples, the so called "virtual / digital tower", which make the provision of location-independent air traffic control services at and in the vicinity of an aerodrome (remote tower operations, rTWR) a reality, is the key aspect of this paper. Remote Tower represents the concept of replacing the conventional control tower on airports by remotely located tower control center that use – mostly optical – sensor platforms (cameras) in order to maintain situational awareness [1]. The need for adequate data communication capability to support rTWR between the airport and the remote tower location is probably the most challenging question. Alongside with data adequacy requirements, the cybersecurity aspect of rTWR optical system needs to be addressed as well. Under the auspices of the Future Communications Study (AP17) data link technologies for new communication infrastructures required to manage aeronautic communication traffic demand, and to provide an always connected infrastructure identified one or mix of the followings [2]:

- a ground-based, high capacity, wired surface data link system;
- a ground-based, high capacity, wireless surface data link system;
- a satellite-based data link system.

In addition, multi-hop / ad-hoc communications alternatives are also considered in studies of future air traffic management systems and accordingly, in the case of rTWR the suitable interpretation(s) of the mentioned technologies might be addressed in a beneficial way eventually. While these data link technologies are promising and efficient means to support remote tower operations, concerns have been raised in their vulnerability to malicious attacks that may lead to serious consequences. Several analyses and studies have been carried out by ICAO [3], EUROCONTROL [4], NASA [5] and NATO [6] that underline the graveness of the cybersecurity aspect of the Aviation Ecosystem. In this paper, cybersecurity techniques used for networks have been considered for securing the communications of remote tower optical systems.

2. BASELINE OF rTWR CYBERSECURITY ASPECT

Computer security can be defined as the protection obtained to an – automated – information system in order to preserve the confidentiality (C), integrity (I) and availability (A) of information system resources (incl. hardware, software, firmware, information-data-telecommunications). Confidentiality preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Integrity guards against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. Availability ensures timely and reliable access to and use of information. In addition to these three key objectives, additional ones have been introduced to present a more comprehensible picture of security concepts including the following two which are most commonly mentioned: authenticity and traceability. The former assures the confidence in validity of a transmission, a message or message originator, usually with Peer Entity Authenticity or Data-origin Authenticity. The latter ensures actions of an entity being uniquely traceable to that entity [7]. This implies that systems must keep records of their activities to permit later forensic analysis to trace security breaches.

From rTWR communications perspective, these security objectives need to be stringently fulfilled using cryptography and network security techniques to ensure that the system will not be hampered by any security breach into rTWR network and computing sphere. Based on The Standards for Security Categorization of Federal Information and Information Systems (FIPS 199) three level of security breaches are identified [8]:

- **low:** loss of CIA could be expected to have a limited adverse effect on operations, assets or individuals (e.g., minor degradation in mission capability to an extent and duration that the system is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced);
- **moderate:** loss of CIA could be expected to have a serious adverse effect on operations, assets or individuals (e.g., significant degradation in mission capability to an extent and duration that the system is limited to perform its primary functions, and the effectiveness of the functions is significantly reduced);
- **high:** loss of CIA could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals (e.g., severe degradation in mission capability to an extent and duration that the system is unable to perform one or more primary functions).

2.1 Security attacks

Primarily, security attacks can be categorized into active or passive sets. A passive attack tries to learn or make use of information from the system but does not affect system resources directly. An active attack attempts to alter system resources or affect their operation, therefore it has a direct effect on the targeted system [9].

2.1.1 Passive attacks

The goal of passive attacks is to obtain information that is being transmitted by eavesdropping or monitoring the transmission. Eavesdropping can result in the release of information or data whereby an opponent is able to obtain the content of information, which may be sensitive, during transmission and subsequently release the sensitive information to other parties. Conventionally, passive attacks are difficult to detect since they will not disrupt the system's data-stream or the connected resources. Thus, the emphasis is on the prevention of such attacks rather than detection. Encryptions, and shielding are normally used in order to prevent passive attacks.

2.1.2 Active attacks

Active attacks involve modifications of the data-stream or the creation of a false stream. In connection with these, the following four categories worth addressing:

- **masquerade:** an entity pretends to be a different, often privileged entity;
- **replay:** passive capture of information and its subsequent retransmission to produce an unauthorized effect;
- **modification of messages:** altering, delaying or reordering some or all parts of a legitimate transmission to produce an unauthorized effect;
- **denial of service:** suppression or disruption of all messages directed to a particular destination in order to disable, overload or degrade the network performance.

3. CYBERSECURITY OVERVIEW

Malicious cyber-actions have only been considered recently in air traffic management (ATM), since the standards ruling this field inherently are more focused on the safety aspect [10]. The dilemma regarding this approach lies in the discrepancy between safety-focused and security-focused angle in threat assessment. Minding the security threats has a separate and special impact on the system design which cannot be completely covered by a safety-oriented perspective. As a result, criterions of technology, threats and motivations categorized in a manner described below [11]:

- **threat actors (who?):** the identification of potential attackers against rTWR optical system enables task-appropriate adaptation of the prevention toolkit, a threat can be linked mens rea to an organization / a person that desires to breach security and accumulate ill-gotten gains;
- **assets (what?):** an accurate and detailed description of the rTWR system is required in order to identify the security context of desirable CIA, including perimeter of a piece of equipment and / or the (sub)systems that are exposed to attacks through network interfaces, logical data flow and other dependencies;
- **topology (where?):** assets with associated features must be mapped to be the subject of a given threat assessment, it is important to determine the optimum grouping of assets from a pragmatic viewpoint;
- **motivation (why?):** the weight of determination, therefore the scope of threats can be measured – and presented in a somewhat easily understandable way – by correctly identifying the motivation of potential attacker;
- **attack vectors (how?):** specific pathway and / or methods are used by attackers to exploit system vulnerabilities, therefore it is crucial to identify and eliminate as many attack vectors as possible.

From a technology standpoint, rTWR optical systems have many similarities with other IP-based surveillance systems; nevertheless, in order to develop secure architectures and implement efficient defense strategies, it is far more crucial to understand the attack vectors and the catalyst fueling the malicious intent. As a result, the attack vector is not the zenith of the various system vulnerabilities, but rather the motivation of the threat actors. Ergo, the key of creating a secure rTWR system and constructing a successful countermeasure is understanding the attack vectors and the motivation.

3.1 System overview

The purpose of rTWR optical system must be defined in order to discuss its security aspects. Primarily, the main objective of air traffic control is to ensure safe, orderly and expeditious flow of (air) traffic [12]. Accordingly, the purpose of rTWR optical system, which enables location-independent tower control, is to digitize and display in real time the area of responsibility of the tower controller, including the maneuvering area and the relevant airspace affiliated to an aerodrome [13].

To have a better understanding of this line of thought, Figure 1 presents a simple concept of rTWR optical systems.

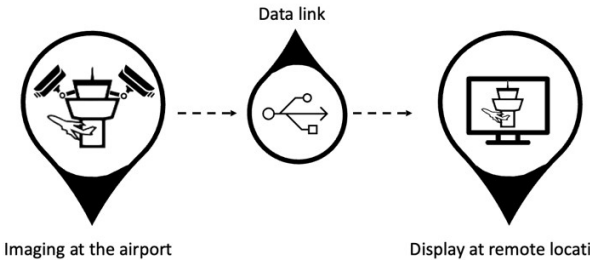

Figure 1 Basic diagram of rTWR optical systems

The principal difference between conventional aerodrome air traffic service and rTWR derived from the way visual observation is performed. In the former case observation is executed by eyes directly, in the latter case the area of responsibility is displayed on screens therefore the observation is indirect [14].

3.2 Taxonomy

Based on the principle that a system can generally be described in terms of its purpose, implementation, topology, and protection, a conceptualized taxonomy of the rTWR optical systems' security concept is introduced in Figure 2.

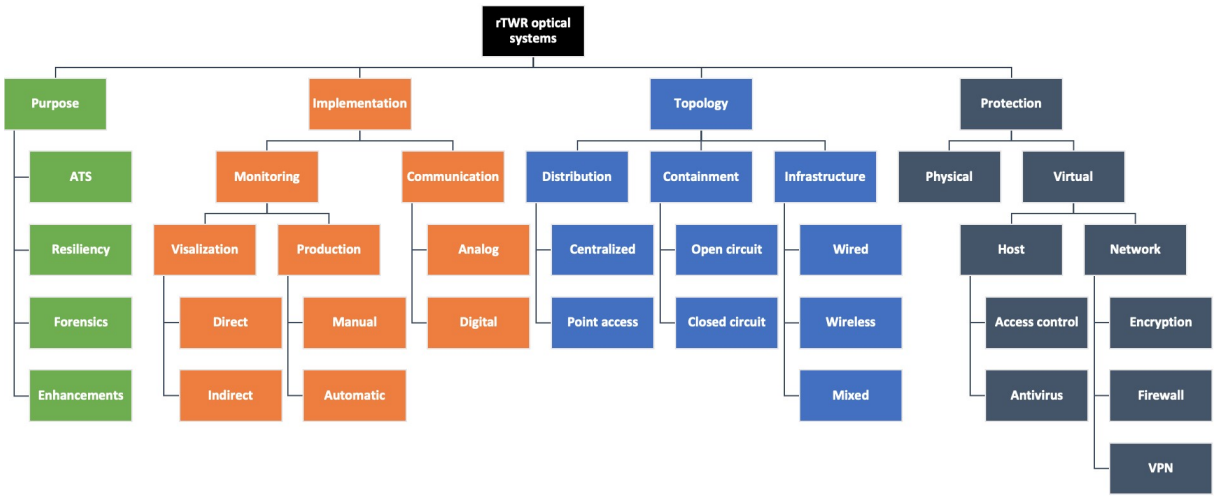

Figure 2 Conceptual taxonomy of rTWR

3.2.1 Purpose

As outlined above, the primary purpose of rTWR optical systems is to ensure safe, orderly, and expeditious air traffic services (ATS) for one (or more) airport from a remote location. In addition, this technology enables other useful features like resiliency to recover hastily from a malfunction or attack, forensics to gain verified evidence (e.g., time stamped video footage) in case of investigations, and other enhancements to help controllers perceiving air traffic (e.g., digitally labelled aircraft) [15].

3.2.2 Implementation

A specific hardware and software layout of a rTWR optical systems can be configured in a variety of ways to gather and display video data efficiently, although implementation wise two categories are distinguished principally: monitoring and communication. Monitoring regards how the controller

visualizes rTWR footage, and how the video content is produced. The visualization can be provided indirectly (file conversion) to a controller working position (CWP), or directly (raw video files) to a maintenance workstation. The production of the footage can be done automatically via cameras arranged fixed-panoramic way or manually with PTZ camera(s) [16].

The method by which rTWR system transmits video footage is referred to as communication. The be thorough, it is worth noting that video data can be transferred as an analog signal to a digital video recorder, but in case of rTWR application every known implementation is based on digital video signals. That means the video data is processed, compressed and then sent as a packet stream via existing (most likely IPv4 or IPv6) network protocols [17].

3.2.3 Topology

The distribution, containment, and infrastructure of a rTWR optical system can be utilized in order to describe its topology. Distribution refers to whether all the cameras are located a centralized place at or scattered around an airport. Depending on whether the rTWR optical system uses a stand-alone network (not connected to any intranet) or a shared one, containment determines if users without the proper credentials can gain access to. Noting infrastructure, it describes how the system's components are connected to each other, whether in a wired way, wirelessly or both.

3.2.4 Protection

The security of physical and virtual access to the rTWR optical systems' assets is referred to as protection. Physical protection is a must to prevent an attacker causing damage in the assets located at the airport, at the remote facility and the data link itself. In addition, it might be even more important to achieve and maintain virtual protection of assets, specifically focusing on the host (e.g., cameras, computers, servers) and the network aspects. By protecting the network with encryption, firewalls and end-to-end virtual private network connections (VPN), a user can safeguard the assets and the rTWR optical system as a well.

4. RANGE OF CYBERSECURITY RISKS

Based on Chapter 2, and other publicly available data [18], existing and novel threats from selected sources capable to disrupt rTWR optical systems are shortly reviewed below minding the criterions (threat actors, assets, topology, motivation, attack vectors) described in Chapter 3. Due to its scope, this study cannot cover all threats, but the insights gained from the reviews can subsequently be utilized to better comprehend and identify the range of cybersecurity risks connected to the design, implementation, and use of a specific rTWR optical system.

4.1 Malicious code injection

Code injection is an exploitation of improper parsing of an input which results in the input being executed as a malicious code. In case of rTWR optical systems, a threat actor may perform a code injection to gain control – with or without the awareness of operative users – over assets. Even when the data-stream is encrypted, the software may still be using an outdated protocol or be susceptible to downgrade attack attempts. Poodle, for instance, attacks that deceive the server into downgrading the encryption to a vulnerable or out-of-date version that may be exploited by intercepting the initial handshake [19].

4.2 Visual layer attacks

Remote Tower optical systems, like many other video surveillance systems, feature an additional level of abstraction, known as the visual layer. As a result, it is conceivable to (ab)use this layer to execute inventive attacks on rTWR assets that benefit from imaging semantics and image recognition.

First, the rTWR asset gets infected from a malicious source (e.g., firmware update over USB). Second, when a malicious imagery (e.g., QR code) is visualized by the optical sensors, the harmful code is triggered and then controlled that way [20]. This attack vector, in one example, enables the attacker to partially or fully blur the area monitored by the system. As a result, this type of malicious functionality could be used directly endangering passengers or hinder crucial (military) tasks.

4.3 Covert channels attacks

Recently, considerable research capacity was invested in covert channels, data exfiltration and modulation employing electromagnetic [21], acoustic [22], thermal [23], and optical channels [24], especially in air-gapped solutions that a military rTWR optical system can be. In this category, the attack vectors discussed includes Infra-Red (IR) LEDs and Audio Layer.

4.3.1 Infra-Red LEDs

Infrared spectrum is invisible to human eye therefore it can be adapted effectively for covert channel purposes. According to a particularly dangerous scenario, assets controlling IR lights could relay data and commands to each other using IR spectrum in order to form an autonomous collaborative network of malicious assets. Consequently, the rTWR optical system can be compromised in several malignant ways, including the previously described partial or full blur of the monitored area, but the range of possible malicious commands depend only on the attacker's resourcefulness. The essential prerequisite for this attack vector is that infected IR assets that placed and operated in one system are within visual sight of each other [25].

4.3.2 Audio Layer

The ability to record and process one or more audio channels from microphones incorporated into (rTWR) assets is a feature that many other video surveillance systems have. As a result, an infected rTWR asset may employ tactics like concealed voice instructions to use the audio layer as a command-and-control channel, which may present a threat described in case of IR LEDs. The essential prerequisite for this attack vector is that infected audio layer assets that placed and operated in one system are within audible range of each other, while most likely the signals are inaudible to the human ear [25].

4.4 Manipulating data-stream

The data-stream may be manipulated, redirected, or observed by a threat actor. In case of rTWR, one feasible example of this attack vector is launching a man-in-the-middle-attack (MitM) by Address Resolution Protocol poisoning via the local network, and then freezing the live video feed, or injecting a false one. Since video codecs (e.g., H.264) compress motion between frames, in case of data-stream observation – even if it is encrypted – the footage can be inferred by monitoring the bandwidth usage patterns of the stream. Furthermore, network topological information can also be obtained from data-stream observation [26], [27].

4.5 Adversarial Machine Learning

As Figure 2 shown, a Remote Tower solution requires either a manual or automated way of handling video footage. Therefore, the domain of video analytics has been applied in case of rTWR optical systems to optimize operational effort performing this task, including [1]:

- object detection, recognition and identification;
- PTZ tracking;
- aircraft labeling;

- area masking and;
- alerting.

To some extent, all the aforementioned solutions rely on machine learning, therefore they are susceptible to adversarial actions. A machine learning model can be abused in an adversarial action in one of three ways: (1) poisoning the model during training to make it behave as the threat actor desires, (2) creating an input that will yield an unexpected output, or (3) learning the training data or the model by looking at the input-output relationship. A successful threat actor may be able to fake object recognition, mask important areas or causing denial-of-service attack by raising the solution's false positive rate [28].

4.6 Social Engineering

Social Engineering (SE) is the term for the psychological manipulation of a person acting accordingly to the will of the threat actor. E-mail phising attempts and baiting are frequent SE attack vectors. Since phising techniques are focusing to obtain key personnel credentials, it is not as useful in case of rTWR optical systems as baiting. In baiting, a threat actor plants a malicious source code onto a device (e.g., USB drive, smartphone) and then the victim unwittingly – or forcingly – plugs it into an intranet-connected machine [29], [30].

4.7 Supply Chain

Attack on the supply chain occurs when a threat actor alters an asset (e.g., camera, IR emitter, router) during the production process by the attack vector of installing a rootkit or hardware-based malware. A successful supply chain attack against rTWR optical system can provide a threat actor total control over the infected-by-design asset and presumably ultimate access to the network. Moreover, implementing non-rTWR-specific technologies from the supply chain already available legacy considerations must be taken in order to avoid security bleeding like in case of MIL-STD-1553 Communication Bus design anomaly [31].

4. CONCLUSION AND FUTURE CONSIDERATIONS

In the past decade, rTWR optical systems have been continuously evolving and their applications are becoming more mature as their technological elements are getting sophisticated and cost-effective [32]. Worth noting that the civilian application of this technology is – and probably will be – dominant, but the military utilizations are already on the way, and the latter might expose the system to threats from satellite-communication angle [33]. In the meantime, technological progress should not be mistaken automatically with (cyber)secure-by-design solutions. Having that stated, the constantly evolving threats to the rTWR optical systems also appear on the horizon as, on one hand endangering lives, on the other hand engaging in information warfare. On both hands, due to the gravity of a potential adversarial machine learning actions glimpsed in Chapter 4.5, disruptive and emerging technologies must be taken of utmost importance.

The primary objective of this study was to outline the foundations of the cybersecurity framework associated with the rTWR optical systems. Accordingly, a brief summary of the rTWR optical systems was provided, then the baseline of its cybersecurity aspect was drawn, next a system overview with an essential conceptual taxonomy was given, and last but not least a spectrum of possible attack vectors was presented.

Assuming the growing prevalence of rTWR solutions, this study ultimately aimed to provide a valuable set of knowledge, to lay the foundations for upcoming theme-specific researches and applications that can implement security measures effectively preventing malicious attacks.

This paper
„*prepared with the professional support of the Doctoral Student Scholarship Program of the Co-operative Doctoral Program of the Ministry of Culture and Innovation financed from the National Research, Development and Innovation Fund.”*

NEMZETI KUTATÁSI, FEJLESZTÉSI
ÉS INNOVÁCIÓS HIVATAL

References

[1] Fürstenau, N.: Virtual and remote control tower: research, design, development and validation. New York, NY: Springer Berlin Heidelberg, 2016.

[2] *Communications Operating Concept and Requirements for the Future Radio* System (Future Communications Study), EUROCONTROL, Federal Aviation Authority, 2007, Available at: https://www.eurocontrol.int/publication/communications-operating-concept-and-requirements-future-radio-system

[3] *Cybersecurity Action Plan*, ICAO, 2022, Available at: https://www.icao.int/aviationcybersecurity/Documents/CYBERSECURITY%20ACTION%20PLAN%20-%20Second%20edition.EN.pdf

[4] *Air Traffic Management: A cybersecurity challange*, EUROCONTROL, 2021, Available at: https://www.eurocontrol.int/publication/air-traffic-management-cybersecurity-challenge

[5] Sandip, R.: Cyber- Threat Assessment for the Air Traffic Management System: A Network Controls Approach”, NASA, 2016, Available at: https://ntrs.nasa.gov/api/citations/20180000393/downloads/20180000393.pdf

[6] Verhoogt, T. & et al. Towards Dynamic Cyber Security Risk Assessment of Military Aircraft, NATO, 2018. Available at: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SCI-300/MP-SCI-300-13.pdf

[7] Stallings, W.: Network security essentials: applications and standards, Sixth edition. Boston: Pearson, 2017.

[8] *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199). National Institute of Standards and Technology, 2004, Available at: https://csrc.nist.gov/publications/detail/fips/199/final

[9] *Security architecture for Open Systems Interconnection for CCITT applications*. INTERNATIONAL TELECOMMUNICATION UNION, Available at: https://www.itu.int/rec/T-REC-X.800-199103-I/en

[10] Everdij, M. - Gijsen, B. - Smulders, A. - Verhoogt, T – Wiegers, R.: Cyber-security management of ATM services: are we ready for the future?, Aviat. Secur. Int., 2016, Available at: https://www.nlr.org/wp-content/uploads/2018/02/Cyber-security-management-of-ATM-services.pdf

[11] Zhen, L. - Kaizheng, L. – Yiling, X.: An End-to-End View of IoT Security and Privacy, in GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, dec. 2017, p. 1–7. doi: 10.1109/GLOCOM.2017.8254011.

[12] Palik, M. (editor): The fundamentals of air traffic control (published in Hungarian language, original title: A repülésirányítás alapjai). Budapest: Dialóg Campus, 2018.

[13] *Guidance Material for Remote and Digital Towers.* CANSO, 2021, Available at: https://canso.fra1.digitaloceanspaces.com/uploads/2020/12/CANSO-SDT-Remote-Tower-Guidance.pdf
[14] Zhang, Y. - Zhengning, Y. – Zeng, L.: Analysis of Remote Tower System, in 2020 IEEE 2nd International Conference on Civil Aviation Safety and Information Technology (ICCASIT, Weihai, China, 2020, p. 128–133. doi: 10.1109/ICCASIT50869.2020.9368521.
[15] *Whitepaper: Introduction to remote virtual towers.* Frequentis, 2016, Available at: https://www.frequentis.com/sites/default/files/support/2018-02/RVT_whitepaper.pdf
[16] *PJ05 - Remote Tower for Multiple Airports - Research and Innovation actions* SESAR.IR-VLD.Wave1. SESAR, 2019.
[17] Peterson, L. – Bruce, D.: Computer Networks - a systems approach, 6th edition, Elsevier, 2014, Available at: https://titania.eng.monash.edu/netperf/docs/computer-networks-peterson-davie-v6.0.pdf
[18] Sandeep, K.: Cyber Security of Cyber Physical Systems: Cyber Threats and Defense of Critical Infrastructures, in 29th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID), Kolkata, India, 2016, p. 30–31. doi: 10.1109/VLSID.2016.153.
[19] Möller, B.: This POODLE Bites: Exploiting The SSL 3.0 Fallback. Security Advisory, 2014, Available at: https://www.openssl.org/~bodo/ssl-poodle.pdf
[20] Amin, K. & et al.: Optical Delusions: A Study of Malicious QR Codes in the Wild, in 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Atlanta, GA, USA, p. 192–203. doi: 10.1109/DSN.2014.103.
[21] Guri, M. - Kedma, G., - Kachlon, A. – Elovici, Y.: AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies, in 2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE), Fajardo, PR, USA, p. 58–67. doi: 10.1109/MALWARE.2014.6999418.
[22] Guri, M. - Solewicz, Y. - Elovici, Y.: Fansmitter: Acoustic data exfiltration from air-Gapped computers via fans noise, Comput. Secur., 2020, doi: 10.1016/j.cose.2020.101721.
[23] Guri, M. - Monitz, M., - Mirski, Y. - Elovici, Y.: BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations, in 2015 IEEE 28th Computer Security Foundations Symposium, Verona, p. 276–289. doi: 10.1109/CSF.2015.26.
[24] Loughry, J. - Umphress, D.: Information leakage from optical emanations, ACM Trans. Inf. Syst. Secur., p. 262–289, 2002, doi: 10.1145/545186.545189.
[25] Costin, A.: Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations, in Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, Vienna Austria, 2016, p. 45–54. doi: 10.1145/2995289.2995290.
[26] Tekeoglu, A. - Tosun, A.: Investigating Security and Privacy of a Cloud-Based Wireless IP Camera: NetCam, in 2015 24th International Conference on Computer Communication and Networks (ICCCN), Las Vegas, NV, USA, p. 1–6. doi: 10.1109/ICCCN.2015.7288421.
[27] Schuster, R. - Shmatikov, V.: Beauty and the Burst: Remote Identification of Encrypted Video Streams. USENIX, 2017, Available at: https://www.semanticscholar.org/paper/Beauty-and-the-Burst%3A-Remote-Identification-of-Schuster-Shmatikov/7f3c3b4556795161de8e704c886ab8eab5c6ff74#citing-papers
[28] Chandni, M. - Puneet, G.: Machine Learning Adversarial Attacks: A Survey Beyond, in Machine Learning Techniques and Analytics for Cloud Security, 1st edition, Wiley, 2021, p. 271–291. doi: 10.1002/9781119764113.ch13.
[29] Grimes, R.: Hacking Multifactor Authentication, 1st edition, Wiley, 2020. doi: 10.1002/9781119672357.
[30] Kovács, L.: The defense of cyberspace (published in Hungarian language, original title: A kibertér védelme). Budapest: Dialóg Campus, 2018.
[31] Orly, S. & et al.: Protecting Military Avionics Platforms from Attacks on MIL-STD-1553 Communication Bus, ArXiv170705032 Cs, 2017, Available at: http://arxiv.org/abs/1707.05032

[32] *World's biggest digital tower centre opens in Norway*, atc-network.com, 2022, https://www.atc-network.com/atc-news/avinor-norway/worlds-biggest-digital-tower-centre-opens-in-norway

[33] Vas, T.: The establishment and usage options of the Hungarian Defence Forces' deployable air traffic management component (published in Hungarian language, original title: A Magyar Honvédség mobil légiforgalom szervezési komponens kialakításának and alkalmazási lehetőségeinek vizsgálata), National University of Public Service, Budapest, 2019, Available at: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12878/vas_timea_doktori_ertekezes_2019.pdf?sequence=11

Received 02, 2023, accepted 06, 2023