UDC 004.056.55

Bogdan Tomashevsky
Candidate of Technical Sciences, Associate Professor, Department of Cyber Security
Ternopil Ivan Puluj National Technical University, Ukraine

Serhii Yevseiev
Doctor of Technical Sciences, Professor,
Head of the Department of Cybersecurity and Information Technology,
Simon Kuznets Kharkiv National University of Economics, Ukraine

Andrii Tkachov
Candidate of Technical Sciences, Senior Researcher,
Associate Professor of the Department of Cybersecurity and Information Technology
Simon Kuznets Kharkiv National University of Economics, Ukraine

PERSPECTIVE NATIONAL COMMUNICATION SYSTEM FOR CYBER MANAGEMENT OF CRITICAL FACILITIES

Abstract. *In a promising confidential communication system, it is proposed to use special communication systems (networks), special dual-purpose systems, as well as systems of open public Internet systems and mobile communication systems. Secrecy of data transmission, cryptographic strength, authentication and authenticity is ensured by the use of a verbatim container, cryptoalgorithms of protection, hash functions, random switching of transmission channels and blockchain transaction technology.*

Keywords: *communication system, cyber control, cyber security*

The transition of society to mobile communications is irreversible, while the security implications of this phenomenon are not well understood. Moreover, the rise in popularity of social media is changing the pattern of interpersonal and global communication. Information about the activity of individuals and legal entities, distributed access control from personal devices without proper protection to security

systems, commercial carriers and the like, as well as new elements pose a risk to the integrity of classified data and systems. For example, the loss or theft of a laptop or mobile phone with electronic data, documents or links can be dangerous for individuals and legal entities, as well as for the state. This section discusses the security issues associated with these trends. “Use a personal mobile device” is a company policy that permits employees to use personal mobile devices (“laptops”, “tablets” and mobile phones) in their workplace and use these devices while performing official duties to gain access to classified information and programs. This policy creates a conflict of interest between an organization whose security policy is designed to ensure the confidentiality and integrity of information resources, as well as to protect employees who wish to retain ownership of the device and personal data and avoid monitoring. Organizations should establish rules and practices for situations where an employee quits, or if a device is lost, stolen, or sold, to avoid intruders using an unsecured device to gain network access to an enterprise system. Using the cloud to store information presents a similar challenge with access and configuration control. General security practice is to build a carefully zoned and layered security architecture to create controlled "cut-off points" for Internet access control. The policy of using your own Internet-enabled devices creates new access points that are likely to be outside the scope of enterprise security policies. This is a basic principle of computer security where the integrity of the lower layers is usually considered axiomatic with respect to the upper layers. This prevents users from changing the implementation of the security policy for corporate programs on personal mobile devices. In other words, corporate security systems (programs, etc.) cannot be installed on a personal device on an ongoing basis due to the user's possession of administrative control over the device, which (for example, a personal smartphone) cannot be secured just by installing programs or security tools. There are a number of techniques that can help keep personal mobile devices secure or limit the risk they pose. These techniques are based on a security framework that restricts access from a device to an enterprise network, as well as information that can be transferred to such a device. Zoning principles that

provide network segmentation and segregation can provide mobility at work and a relatively secure strategy for using personal devices for work purposes. However, solutions that offer a higher degree of security call into question the widespread use of personal devices. In addition, the move to cloud-delivered infrastructure as a service is potentially losing the underlying security architecture and security principles. Mobile devices themselves create data streams that may be of interest to foreign intelligence services and commercial enterprises. The use of social networks also leads to the possible use of personal information of users, which was posted on the social network by the users themselves or open for access / stored on their mobile devices, revealing a lot of information (personal status, opinions, location, habits) that can be used by attackers. Such social networks can also pose a potential threat, serving as a conduit to various IT systems, making them vulnerable to viruses or intrusions. Social media can also be an effective vehicle for spreading propaganda and misinformation, engaging the general public, sending multiple messages to mobilize the populace, and similar activities.

The ubiquity of modern interdependent information technology infrastructures, including the Internet, telecommunications networks, computer systems, embedded processors and controllers, and their ability to communicate or interact through a variety of means, from mobile devices to wearable computers, create a number of inherent vulnerabilities and potential vulnerabilities for government and non-government actors. attack vectors. Exploitation of these vulnerabilities can have widespread national security implications through deliberate actions such as espionage, degrading command and control facilities, stealing intellectual property and sensitive personal information, disrupting essential services and critical infrastructure, or damaging economies and industries. ... Accordingly, the need to support activities to ensure a process capable of realizing the possibility of ensuring a state in which information and communication systems, as well as the information contained in them, are protected and / or protected from harm, unauthorized use, modification or operation, is relevant.

The architecture of the Internet backbone includes key communication channels between major computer networks and backbone routers. These networks and routers are hosted in commercial, government, scientific, and other high-power network centers. These centers operate Internet exchange points and network access points, and exchange traffic between countries and continents. Typically, large Internet service providers (for example, Tier 1 providers) are involved in the exchange of traffic in the Internet backbone based on private agreements on the interaction of telecommunication networks. ISPs that control individual segments of the Internet are called Autonomous Systems (AS), which register and receive a unique Autonomous System Number (ASN). Routing between autonomous systems and their reachability is provided by backbone routers using Border Gateway Protocol (BGP). The relationship between domain names (for example: www.google.com) and routed addresses is managed by the Domain Name System (DNS) and its own registration authorities. National Internet Registrar (NIR) is an organization that distributes IP addresses (Internet protocols) and other Internet resources nationwide under the control of an international Internet registrar [1]. National governments can also regulate Internet service providers within their region.

To ensure the safety, reliability and efficiency of the transmission of information of state importance, a set of special dual-purpose communication systems (networks) is used, which, by means of cryptographic and / or technical means, ensure the exchange of confidential information in the interests of public authorities and local authorities and create appropriate conditions for them. interaction in peacetime and in the event of the introduction of a special and martial law.

The main feature of such systems is its hierarchical structure and the method of transmission based on direct error correction, which greatly simplifies the detection-suppression and / or complete blocking of communication channels for the enemy [2].

However, the rapid development of computing resources, both Internet technologies and mobile technologies, makes it possible to use such methods of information exchange, taking into account the capabilities of telecommunication

systems for transmitting or storing information, in which the uncertainty of the very fact of such an exchange remains, which makes it possible to use open communication channels with a commercial method of delivering information to the recipient. Using this approach in the framework of cyber management of critical resources to ensure the required level of cyber security does not require significant economic and human resources [3].

In a promising confidential communication system, it is proposed to use special communication systems (networks), special dual-purpose systems, as well as systems of open public Internet systems and mobile communication systems.

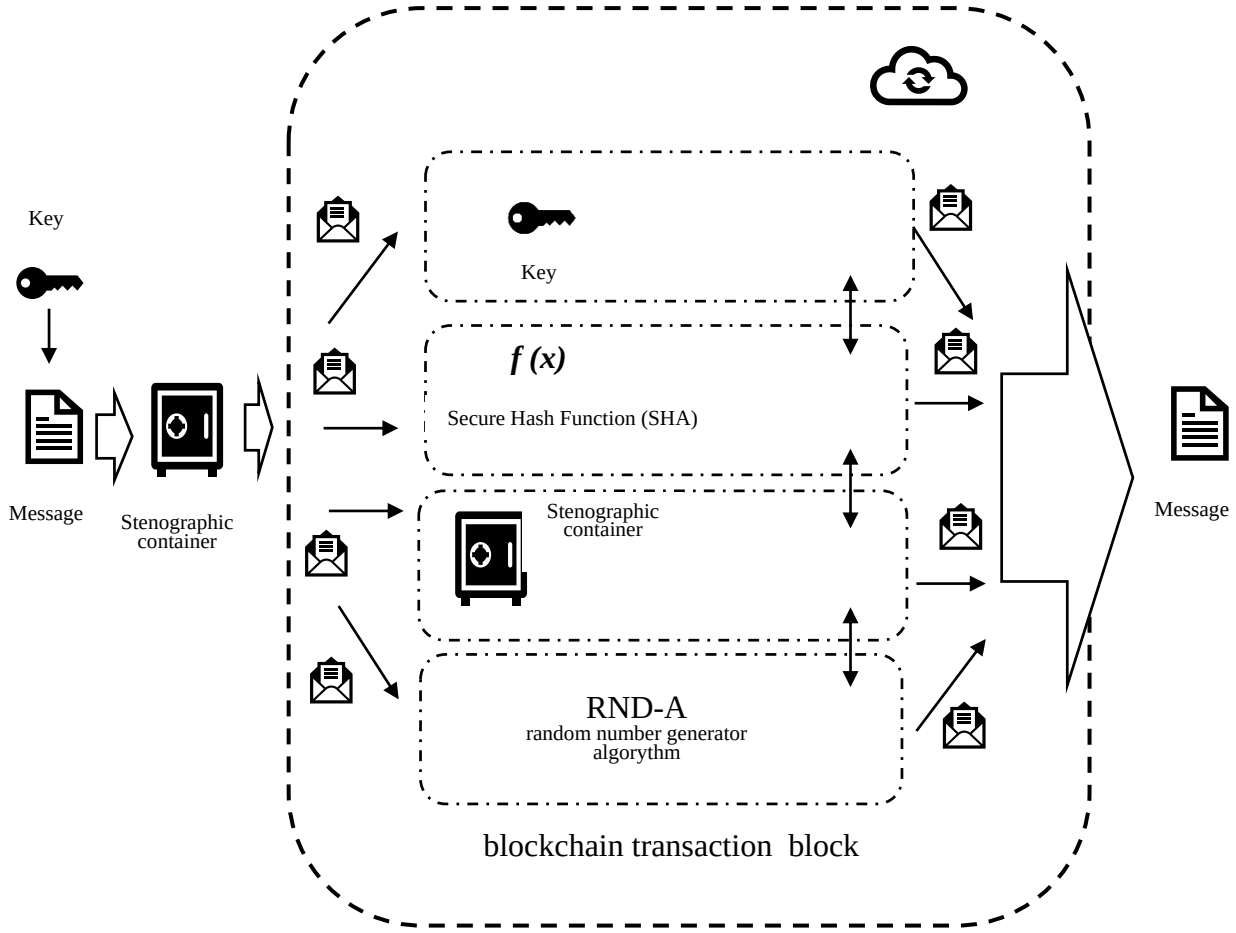

Fig. 1. The perspective system of confidential data exchange

In fig. 1 shows a structural and functional diagram of a confidential information exchange system that allows the use of open communication channels with a commercial method of delivering information to the recipient to ensure the necessary level of cybersecurity when managing critical important resources.

Incoming messages will be encrypted with a key and enclosed in a verbatim container to hide the fact of information transfer. The closed message will be transmitted over open data networks, which will be switched according to the pseudo-random number generator algorithm. The recipient of the message retrieves the message from the verbatim container, obtaining the parameters for the cryptographic key, the pseudo-random number generator algorithm, and the hash function to authenticate the information. The sequence of messages is divided into blocks using blockchain technology, which provides the required level of authentication for subsequent transactions.

Let the probability of command transmission without distortions and failures for a special communication system (network) – P^K, the Internet –P^f, in the mobile network – P^S, in a dual-purpose network – P^R, which can be caused by attacks of different classes.

The probability of transmission of a message through at least one of the networks could be calculated as follows:

$$P = P^K + P^f + P^S + P^R = (1 - P_m^K) \times \left(1 - P_m^f\right) \times (1 - P_m^S) \times (1 - P_m^R). \quad (1)$$

where P_m^K – probability of erroneous command reception in a special communication system (network); P_m^f – probability of erroneous command reception on the Internet; P_m^S – probability of erroneous command reception in the mobile network; P_m^R – probability of erroneous command reception in a dual-use network. Expression (1) can be interpreted as the value of the probability that all four systems will not fail simultaneously.

When building the system, the following provisions should be taken into account:

- the attacker has a complete understanding of the system and the details of its implementation. The only information that remains unknown to a potential adversary is the key and the parameters of the information exchange network, which makes it possible to establish the presence and content of a hidden message;

- if an attacker somehow learns about the existence of a hidden message, this should not allow him to extract similar messages in other data, or at least provide the required information security;

- a potential attacker should be deprived of any technical or other advantages in recognizing or disclosing the content of messages.

The need to create such a system is of an urgent nature. The rapid pace at which countries establish cyber governance and strengthen their military capabilities to combat cyber conflicts must be balanced by the existence of a system that provides a new level of "minimum necessary communications" protected from conflict. This provision of the necessary level of cybersecurity is vital to keep the benefits of the Internet out of reach of the destructive capabilities of new technologies.

References:

1. Hamadoun I. Touré, General Secretary of the International Telecommunication Union and the Standing Group on Information Security Monitoring of the World Federation of Scientists: In search of cyberworld. Available at: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-R.pdf
2. Martin Libicki, Senior Research Fellow, RAND Corporation Cybersecurity: Problems and Solutions. Available at: https:// www.pitsasinsurances.com/ ru/ article/cyber-risk-problems-solutions-insurance
3. Martin C. Libicki, Lillian Ablon, Timothy Webb, RAND Corporation Cybersecurity report: The Defender's Dilemma: Setting the Course Towards Cybersecurity. Available at: https://www.rand.org/pubs/ research_reports/ RR1024.html
4. Cybersecurity. A generic Reference Curriculum, October 2016. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10 / 20171004_1610-cybersecurity-curriculum-r.pdf