Technology for automated security assessment of information and communication systems

UDK 004.056.53

Oleksandra Shlapak[1], Nataliia Petliak[2]

Khmelnytskyi National University,
[1]sasaslapak839@gmail.com, [2]npetlyak@khmnu.edu.ua

In the context of digital transformation, information and communication systems (ICS) have become essential components for the functioning of government institutions, enterprises, and critical infrastructure facilities. The intensification of digitalization processes is accompanied by a rapid increase in the number of cyber threats, as well as their growing complexity and adaptability, which necessitates the improvement of approaches to assessing the security level of such systems. Traditional information security assessment methods, based on periodic audits, expert analysis, and the use of standalone scanning tools, do not ensure the required efficiency, integrity, and scalability. Moreover, they are characterized by a significant dependence on the human factor, which reduces the objectivity of the obtained results and complicates the decision-making process in the field of cybersecurity [1].

The relevance of the research is due to the need to develop an integrated technology for automated security assessment of ICS, which enables continuous monitoring of the network infrastructure, detection of unauthorized devices, vulnerability analysis, and the formation of a generalized risk indicator. Particular importance is given to the problem of identifying unknown or unauthorized network nodes that may act as potential sources of data leakage or entry points for cyberattacks.

The proposed technology for automated assessment of information and communication system security is based on the integration of network scanning, vulnerability analysis and risk-based threat ranking processes within a single software-analytical loop. Unlike existing solutions such as Nessus, OpenVAS or Qualys, which are mainly focused on detecting vulnerabilities without taking into account the context of business processes and network dynamics, the proposed approach involves a comprehensive integration of data about assets, their behavior and criticality. Also, unlike SIEM systems (for example, Splunk or IBM QRadar), which are focused on correlation of security events, but do not perform a full analysis of network topology and automatic detection of unauthorized devices, the proposed technology covers the full cycle of security assessment. This allows for a more substantiated and adaptive assessment of the level of security.

The initial stage is automated discovery of network assets through a combination of active and passive scanning methods. The integration of these approaches increases the completeness of device detection and reduces the likelihood of missing hidden or temporary nodes. The identified assets are matched against a reference database of authorized devices by comparing MAC and IP addresses, which allows for the identification of unauthorized connections. Additionally, behavioral characteristics of nodes are taken into account, in particular the frequency of connections, atypical protocols, and abnormal traffic volumes, which can be implemented through statistical analysis or simple anomaly models.

The next stage is automated vulnerability analysis, which involves identifying potential weaknesses in software, network services, and system configurations. From a technical perspective, this process includes banner grabbing, comparing obtained version information with databases of known vulnerabilities, as well as configuration checks using signature-based and heuristic rules. Information from known vulnerability databases such as CVE, NVD, and Exploit Database is used, which makes it possible to map detected services to known security issues. For example, if an outdated version of an Apache web server is detected, the system automatically finds the corresponding CVE records and assesses the level of risk.

Each detected vulnerability is characterized by a set of parameters, among which the level of criticality, exploitability probability, and potential system impact are of particular importance. Within the scope of the study, it is proposed to formalize the vulnerability assessment as a function:

$$V_i = C_i * P_i * I_i$$

where C_i - is the criticality coefficient of a vulnerability; P_i - is the probability of its exploitation, which can be determined based on the availability of exploits or external accessibility of the service; I_i represents the potential impact on the Information and Communication System (ICS), evaluated with regard to the type of processed data.

In order to obtain a generalized characterization of the system's security level, it is proposed to use an integral risk indicator that takes into account both the properties of vulnerabilities and the significance of the corresponding assets. The generalized assessment can be represented as follows:

$$R = \sum_{i=1}^{n} w_i * V_i$$

where w_i is a weighting coefficient that defines the importance of the asset or service associated with the corresponding vulnerability.

The use of such an integral indicator makes it possible to obtain a holistic assessment of the ICS security level and provides the ability to compare different system states over time.

The scientific novelty lies in the development of an automated security assessment technology that integrates methods of network asset discovery, vulnerability analysis, and risk-based evaluation within a unified formalized approach. The method of identifying unauthorized devices has been improved through the use of behavioral characteristics of network nodes, which allows increasing the accuracy of detecting anomalous connections. The risk assessment method has been further developed by taking into account the interdependencies between vulnerabilities and assets, as well as their impact on the overall security state of the system.

The practical significance of the obtained results lies in the possibility of creating a software tool that implements the proposed technology and can be used to automate information security audit processes, monitor the state of network infrastructure, and support decision-making in the field of cybersecurity. The application of this approach enables faster detection of threats, reduces the impact of the human factor, and ensures more effective cyber risk management in ICS of various purposes.

1. A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies / K. Bennouk et al. Journal of Cybersecurity and Privacy. 2024. Vol. 4, no. 4. P. 853–908. DOI: https://doi.org/10.3390/jcp4040040

Біометрична автентифікації для платформ дистанційного навчання на основі голосових відбитків

УДК 004.056

Олена Головачова[1], Лідія Тимошенко[2]

Національний університет «Одеська політехніка»,
4507629@stud.op.edu.ua[1], l.m.timoshenko@op.edu.ua[2]

Актуальність теми зумовлена стрімким переходом освіти у цифровий формат в умовах пандемії, вимушеної міграції або навчання із зон конфлікту та необхідністю гарантувати академічну доброчесність та безпеку даних. Дистанційне навчання створює значні виклики для контролю знань [1]. Традиційні методи не дають 100% впевненості, що виконує завдання або дає усну відповідь саме той учень. Голосова біометрія дозволяє підтвердити особу, що запобігає підміни особи. На відміну від паролів, які можна передати іншим, унікальні характеристики голосу (тембр, висота, ритм) підробити значно складніше.

Метою роботи є розробка захищеної архітектури системи голосової біометричної автентифікації для підвищення рівня безпеки та академічної доброчесності в дистанційній освіті.

Основною проблемою ідентифікації учнів при дистанційному навчанні є виявлення того, що відповідає саме учень, а не стороння особа, нейромережа, або використовується запис. При побудові архітектури для освітніх платформ безпека передачі даних є критично важливою. Оскільки будь-яке перехоплення даних може мати серйозні наслідки. Коли учень вимовляє фразу, дані проходять шлях від мікрофона до сервера. Аудіопотік має шифруватися, кожен пакет голосових даних має підписуватися унікальним токеном учня. Аудіопотік передається під час верифікації, його не можна зберігати довго, після виділення математичних ознак він має видалятися. Потім звук перетворюється у математичний вектор До голосового вектора додається «сіль» — випадкове унікальне число, прив'язане до унікального токену учня [2]. Додавання «солі» до біометричних даних робить систему стійкою до атак через витік бази даних. Навіть якщо зловмисник викрав голосові вектори, він не зможе порівняти їх між собою або використати в іншій системі, бо кожен вектор має унікальний ключ. «Сіль» завжди однакова для одного учня, це дозволяє проводити порівняння. Якщо учень видаляється із системи, сервер видаляє «сіль». Без цієї специфічної «солі» відновити оригінальний голосовий вектор із бази практично неможливо. Далі числовий код голосу (голосовий вектор) шифрується за допомогою алгоритму AES-256[2]. Події логуються, вони розділені на три типи: пройдена - успішна ідентифікація, попередження – низька схожість, критична – виявлена підробка або підозра на атаку. Для порівняння біометричних шаблонів використовується косинусна подібність[3].