Modeling the State of Information Security of a Smart Campus

Alexsander Sobol
Center of Information technologies
Belarussian State University
Minsk, Belarus
Email: sobolam@bsu.by

Viktor Kochyn
Vice-Rector for Academic Affairs and
Internationalization of Education
Belarussian State University
Minsk, Belarus
Email: kochyn@bsu.by

***Abstract*—The state of information security system in smart campuses is the main source of obtaining reliable events. This paper discusses the modeling of the state of information security system of smart campus. Special attention is paid to the smart campus infrastructure on which the state of the information security system depends, the interrelationships between the levels of the smart campus, and the subsystems of the information security system are highlighted.**

***Keywords*—smart campus, information security, state modelling**

I. Introduction

Technology has become ubiquitous in modern society, and education is no exception. A smart campus is an innovative educational institution that utilises advanced technologies to create a stimulating learning environment.

The goal of a smart campus is to provide an intelligent environment that supports active learning, encourages creative thinking, and provides access to advanced educational resources and technologies. A smart campus employs technologies such as the Internet of Things (IoT), artificial intelligence (AI), cloud computing, and data analytics to create an integrated and effective educational environment .

The objective of a smart campus is to create a learning environment that adapts to the needs of students and faculty, provides access to state-of-the-art educational resources and technologies, and supports a variety of learning and assessment methods. A smart campus provides innovative teaching methods, including online courses, virtual labs, and simulations, as well as various forms of feedback and learning assessment analysis based on machine learning [1], [2], [3].

However, the increasing number of interactive devices and networking technologies also brings about an increase in vulnerabilities and threats that pose information security issues for smart campuses. One example of such challenges is cyberattacks: Smart campuses may use Internet of Things (IoT) networks, which are vulnerable to cyberattacks such as DDoS attacks, IoT device hacking, or malware injection.

Additionally, there is a risk of sensitive or personal data leakage due to the large amount of data collected by smart campuses. Finally, physical security is also a concern. Unauthorized access to the physical infrastructure of a smart campus, such as surveillance cameras, sensors, and building management systems, can result in severe consequences, including vandalism, data theft, and privacy breaches.

Smart campus networks can also have vulnerabilities in their infrastructure that attackers can exploit for unauthorized data access or security breaches. Additionally, social engineering is a potential threat. Social engineering attacks may deceive smart campus personnel and allow unauthorized access to systems or information. Additionally, DDoS attacks can cause critical smart campus systems to experience denial of service, which can disrupt the learning process and campus operations. To address these issues, a comprehensive approach to security is required. This includes installing up-to-date information security tools, regularly updating software, providing staff training, ensuring physical security, and monitoring network activity to quickly detect and respond to threats. Initially, to build the information security of a smart campus, it is necessary to define the structure of both the smart campus itself and the components of the information security system [4], [5], [12], [13], [14] .

II. Components of a smart campus

A smart campus comprises several components, each of which plays a crucial role in creating an innovative educational environment. The following components can be identified for a smart campus.

A. Video surveillance systems

Video surveillance systems play an important role in providing physical security on campus. They provide constant surveillance of the campus and can be used to detect and prevent crime and ensure the safety of students and staff.

B. Access Control Systems

Access control systems provide access control to various areas of a smart campus. They can be used to control student and staff access to specific buildings, facilities, or resources.

C. Telecommunications Systems

Telecommunications systems facilitate communication and data exchange between different devices and systems on campus. They can provide Internet access, messaging, data sharing, online conferencing, and webinars [7].

D. Data processing systems

Data processing systems are utilised to analyse and process data collected by various systems in a smart campus. They can be used to analyse data on safety, student and staff activity, and to identify patterns and trends. Additionally, this system stores data on student and faculty performance [8].

E. Information Security Systems

Information security systems are employed to safeguard data and information in a smart campus. They are capable of detecting and preventing cyberattacks, protecting sensitive information, and securing the network.

"Fig. 1" presents the interconnection between the smart campus systems.

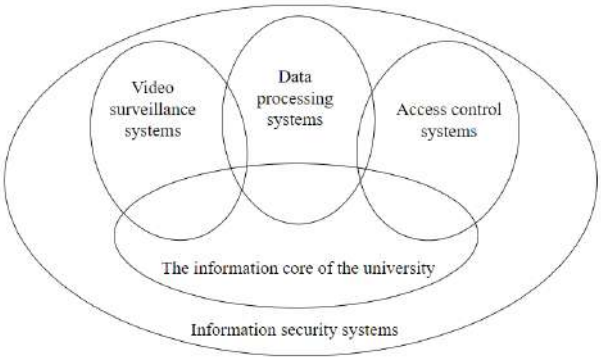

Figure 1. Relationship between smart campus systems.

The components of each of the systems are located at different interaction layers of the smart campus. Based on this, the smart campus can be visualised as a multi-layered architecture as shown in "Fig. 2".

The sensor layer provides event enrichment with additional information required for the intrusion detection and prevention system.

The access layer refers to the network resource access control layer and defines which users or devices are authorised to access certain network resources or functions.

The distribution layer provides connectivity between the various segments and subnets of the campus network.

The information core layer ensures the operability of business processes that exist in higher education

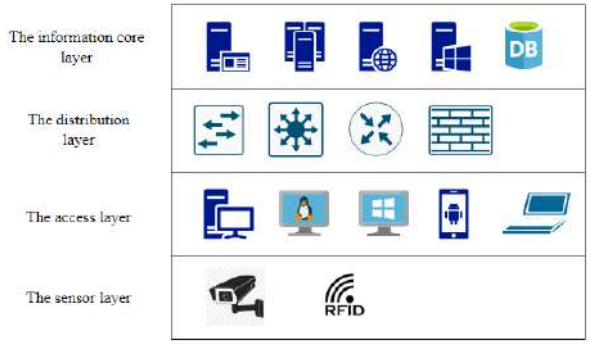

Figure 2. Multi-level structure of a smart campus

institutions such as: distance learning system, university management, etc.

Developing a state model for a smart campus is a pressing task.

Each smart campus system can be in different states at any given time and may depend on the state of other systems. Assuming that $V(t)$ represents the state of the video surveillance system over time. the following formula at any given time:

$$\frac{dV(t)}{dt} = f(V, T, D, S) \tag{1}$$

where f a function describing the relationship between the telecommunications system T, the data processing system D , the video surveillance system V and the information security system S .

The state of the access control system at any point in time can be described by the following formula:

$$\frac{dA(t)}{dt} = j(A, T, D, S) \tag{2}$$

where $A(t)$ a state of access control system, which depends on time t, j a function describing the relationship between telecommunication system T , access control system A , data processing system D and information security system S .

The state of the telecommunication system at any point in time can be described by the following formula:

$$\frac{dT(t)}{dt} = h(T, S) \tag{3}$$

where $T(t)$ a state of the telecommunication system, which depends on time t, h a function describing the relationship between telecommunication system T and information security system S.

The state of the data processing system at any point in time can be described by the following formula:

$$\frac{dD(t)}{dt} = g(D, T, S) \tag{4}$$

where $D(t)$ a state of data processing system, which depends on time t , g a function describing the relationship between telecommunication system T, data processing system D and information security system S.

The state of the information security system at any point in time can be described by the following formula:

$$\frac{dS(t)}{dt} = l(A, V, D, T, S) \tag{5}$$

where $S(t)$ a state of the information security system, which depends on time t, l a function describing the relationship between the telecommunication system T, access control system A , data processing system D , the video surveillance system V and information security system S .

Based on the above equations (1) to (6), the state of the smart campus infrastructure at any point in time can be expressed by the following expression:

$$\frac{dCam(t)}{dt} = q(A, V, D, T, S) \tag{6}$$

where $Cam(t)$ is the state of the smart campus infrastructure at time t .

III. Components of the information security system

Information security system [8] is one of the key systems in the smart campus infrastructure. This system should perform:

- Personal data protection: The smart campus collects and processes large amounts of data about students, faculty and staff. This data may include a variety of personal data such as names, addresses, financial data, academic performance, etc. The information security system must protect personal data from unauthorized access and use.
- Intellectual Property Protection: A smart campus may contain intellectual property in the form of research data, scientific articles, software, etc. The information security system should protect this intellectual property from leaks and theft.
- Protection against cyber attacks: Smart Campus may be susceptible to various types of cyber attacks such as viruses, malware, phishing, etc. The information security system should provide protection against these attacks and respond to them in real time.
- Ensuring Continuity of Operations: The smart campus must be available and operational at all times. The information security system must ensure continuity of system operations and quick recovery from failures or attacks.
- Regulatory Compliance: A smart campus may have to comply with various regulatory and legislative requirements for information security, depending on the country of implementation of that campus. The information security system must ensure compliance with these requirements and provide for auditing and reporting.
- Protection against internal source threats: A smart campus may be vulnerable to threats from internal sources such as students, faculty, and staff. The information security system must protect against these threats and control access to sensitive data.

An information security system according to international standards namely ISO/IEC 27000 and NIST-800 [9], [10] should contain the following subsystems:

- Administration subsystem: This subsystem is responsible for managing all security aspects of the system. This includes creating and deleting user accounts, configuring access rights, managing network settings, managing security certificates, and other administrative functions. The administration subsystem is also responsible for educating users about information security and ensuring their compliance with established rules and policies.
- Collection and Filtering Subsystem: This subsystem is responsible for collecting data on security events such as login attempts, attempts to access protected resources, changes to system settings, etc. The collected data is then filtered to remove unnecessary information and prepare the data for further analysis.
- Data Analysis Subsystem: This subsystem is responsible for analyzing the collected security event data to identify potential threats and anomalies. The analysis may include the use of machine learning algorithms, statistical methods, comparison with attack patterns, etc. The analysis generates reports on potential threats and anomalies that require further investigation.
- Response Subsystem: This subsystem is responsible for responding to detected threats and anomalies. This may include automatic actions such as blocking access to protected resources, alerting the system administrator, etc. The response subsystem can also offer recommendations for further action to the system administrator.
- Security Audit Subsystem: This subsystem is responsible for logging and analyzing user activity on the system to identify potential security violations and ensure compliance with security standards. Security auditing may include checking compliance with established security policies, analyzing event logs, etc.
- Secure Operation Subsystem: This subsystem is responsible for ensuring the continuous and secure operation of the system. This includes protecting against failures, providing redundancy, monitoring system status, etc.
- Backup Subsystem: This subsystem is responsible for backing up data and setting up recovery mech-

anisms in case of data loss or corruption. This includes regularly backing up data, verifying its integrity and recovery availability.
- Testing subsystem: This subsystem is responsible for conducting penetration tests, vulnerability analysis, and other testing to identify potential threats and anomalies. This includes the use of specialized tools and techniques to detect vulnerabilities and verify system security.

Interrelationships between subsystems of the information security system can be represented using graph formalism. Each subsystem can be represented as a vertex of the graph, and the interactions between subsystems can be represented as edges of the graph. For example, if subsystem A interacts with subsystem B, there will be a graph edge between the vertices A and B.

Then let the administration subsystem be vertex A , the collection and filtering subsystem be vertex B , the data analysis subsystem be vertex C , the response subsystem be vertex D, the security audit subsystem be vertex E , the secure operation subsystem be vertex F , the redundancy subsystem be vertex G , and the testing subsystem be vertex H .

Let $G = (V, I)$ be a graph where V is the set of vertices and I is the set of edges. Then the set of vertices representing the subsystems will be as follows

$$V = \{A, B, C, D, E, F, G, H\} \tag{7}$$

And the set of vertices will look like $I = \{(A, B), (A, C), (B, D), (C, D), (C, E), (D, F), (E, G), (F, G), (G, H)\}$.

The smart campus information security system will depend on the state of each subsystem depending on current conditions and events.

It is important to note that the states of subsystems can change depending on current conditions and events, and system administrators must monitor the state of each subsystem and take the necessary steps to restore normal operation when necessary.

In order to develop a hardware and software system of information security, it is necessary to mathematically describe the states of each subsystem. This can be done using the theory of automata and finite states. Each subsystem can be represented as an automaton with a finite number of states, where each state corresponds to a certain functional state of the subsystem. Transitions between states can be triggered by external events such as subsystem failures, administrative decisions, changes in the environment, etc.

The following states can be defined for each subsystem:

- Active state (Active): The subsystem is functioning as defined and performing its functions.
- Inactive: The subsystem is temporarily disabled or not functioning due to technical problems or administrative decisions.
- Recovery state: The subsystem is in the process of recovering from a failure or shutdown.

Similar states can be defined for an information security system. Based on this, represent the information security system as a tuple:

$$(S, \Sigma, \delta, s_0, F) \tag{8}$$

where S a the set of states of the subsystem, Σ a the set of input events (e.g., failure events, administrative decisions, changes in the environment), δ a the transition function, which defines which events lead to a transition from one state to another s_0, a the initial state of the subsystem and F a the set of final states, which denote the successful completion of the subsystem.

The set of states of the subsystems of the smart campus information security system can be described as follows:

$$S = \{Active, Inactive, Recovery\} \tag{9}$$

The set of input events of the smart campus information security system can be represented as follows:

$$\Sigma = \{Failure, Administrationdescision, Change\} \tag{10}$$

The transition functions between the states of the information security system based on formulas (9) and (10) will be as follows:

$$\delta(Active, Failure) = Inactive \tag{11}$$

$$\delta(Inactive, Recovery) = Recovery \tag{12}$$

$$\delta(Inactive, Succesfulrecovery) = Active \tag{13}$$

Initial status of subsystems of information security systems of the smart campus:

$$s_0 = Active \tag{14}$$

The set of final states of the smart campus information security system that denote the successful completion of the subsystem:

$$F = \{Active\} \tag{15}$$

On the basis of the given mathematical descriptions it is possible to model the information infrastructure of the smart campus and information security systems. These models may allow to initially develop the infrastructure of the smart campus and modify the above expressions, as well as allow to develop the software implementation of the information security system.

Taking into account the fact that expression (5) is presented as a differential equation, and the information

security system itself represents a graph with states described by expressions (7,8), the function describing the state of the information security system can be presented in the following form:

$$S(t) = \begin{cases} 1, \text{if the system in time } t \text{ Active} \\ 0, \text{if the system in time } t \text{ Inactive} \\ -1, \text{if the system in time } t \text{ Recovery} \end{cases} \quad (16)$$

However, this function is non-differentiable because it is not smooth and continuous. Therefore, using the Fourier transform, we present this formula in the following form.

IV. A model of an intruder in a smart campus

An intruder model is an abstract representation of potential threats that could be directed at an information system, network, application, or organization. It is a conceptual description of how attackers might attempt to penetrate a system or damage its operation or security.

The intruder model includes descriptions of the different types of attacks, intrusion techniques, vulnerabilities, and other factors that can be exploited by attackers. It can be used to assess the level of vulnerability of a system or network and to develop strategies to protect against potential threats.

The importance of an intruder model is that it helps in analyzing and understanding possible attack scenarios, which enables organizations to take measures to secure, prevent and respond to incidents when necessary. Such models are an important tool in cybersecurity and help improve the security of information systems and networks.

There are many types of intruders that may attempt to infiltrate a smart campus for different purposes. For smart campus infrastructure, the following intruders can be identified:

1) Hackers:
   - Ethical hackers: Information security professionals who use their skills to test systems for vulnerabilities and help organizations improve their defenses.
   - Unethical hackers: Attackers who attempt to infiltrate systems to cause damage, steal data, or engage in other illegal activities.
2) Scammers:
   - Phishing attacks: Attackers send false emails or create fake websites to trick users into accessing their sensitive information.
   - Social engineering: Attackers may use manipulation and deception to convince employees of an organization to grant them access to a system or sensitive information.
3) Internal Intruders:
   - Employees: Individuals with legitimate access to a system or data may abuse their privileges to gain unauthorized access or leak confidential information.
   - Compromised Accounts: Attackers can gain access to employee accounts through vulnerabilities or phishing attacks.
4) Spammers and Vulnerability Scanners:
   - Spammers: Attackers who use mass spamming to spread malware or phishing attacks.
   - Vulnerability scanners: Software tools that automatically scan networks for vulnerabilities for use in attacks.

Depending on the type of intruder, there may be the following popular attacks, which can correspond to several types of intruders at once:

1) Denial of Service (DoS/DDoS):
   - DoS (Denial of Service): An attacker may attempt to saturate the available resources of a smart campus network or servers by sending a large number of requests to a server, resulting in a denial of service for other users.
   - DDoS (Distributed Denial of Service): Multiple computers captured in a botnet simultaneously attack the smart campus network, causing it to become overloaded and unable to serve legitimate traffic.
2) Authentication and identification methods:
   - Login and password hijacking: Attackers may attempt to intercept smart campus user credentials through network traffic hijacking techniques or the use of malware such as spyware or keyloggers.
   - Cross-network spoofing (MITM): An attacker can use a MITM attack to interfere with communication between devices and intercept or alter transmitted data, including authentication data.
3) OS and application vulnerabilities: Attackers could exploit known or newly discovered vulnerabilities in operating systems or applications installed on smart campus devices to gain unauthorized access or perform malicious activities.

   These are only a fraction of the attacks that can be on a smart campus. Various modeling techniques can be used to design the information security system of a smart campus.

Various modeling techniques can be used to design the information security system of a smart campus.

V. Modeling information security systems

The expressions above, can allow modeling the information security system and building the virtual infrastructure of the smart campus. When modeling, it is necessary to consider the subsystems of the information security system as well as the relationship between the

components of the smart campus. For each subsystem of the information security system and components of the smart campus, the following tools and approaches can be identified:

1) Simulators and modeling tools: There are specific software tools such as NS-3 or OMNeT++ that can be used to model networks and communication protocols including information security aspects [15].
2) Risk and Vulnerability Analysis Programs: These software tools help to identify vulnerabilities in the system and assess the likelihood and consequences of various cyber attacks.
3) Modeling and specification languages: Some programming languages such as Alloy or Promela can be used to formalize system models and perform formal security analysis of the system.
4) Visualization tools: Visualization tools such as data flow diagrams or attack diagrams can help in analyzing vulnerabilities and developing remediation measures.
5) Configuration management and monitoring systems: Using configuration management and monitoring systems such as Splunk or ELK Stack can help detect anomalies and attacks in real time.
6) Attack modeling tools: Some software tools, such as the Metasploit Framework, provide tools to simulate different types of cyberattacks and assess the security level of a system.

References

Building a mathematical model of information security system state is a very complex task and can be solved by various methods: differential equations, Markov chains, automata theory, etc.

For comprehensive information security in a smart campus, it is necessary to use semantic technologies that allow integrating different types of knowledge and problem solving models, and the corresponding approaches are developed within the framework of OSTIS technology. Also with the help of OSTIS technology [16] it is possible to create a database of vulnerabilities and promptly react to cyber incidents in a smart campus.

To combine these systems it is necessary to use the theory of hybrid systems. In addition to using this theory, in order to combine the different mathematical models of the information security system, it is necessary to consider the information data flows that are generated by the smart campus itself. In order to successfully create a technical interpretation of the mathematical model of the information security system, the threat model and the intruder model of the smart campus must be considered.

References

[1] A. Smith and B. Johnson, "Implementing Smart Campus Security Systems: Challenges and Opportunities," Journal of Smart Cities, vol. 5, no. 2, pp. 123-135, 2020.

[2] C. Chen and D. Wang, "Design and Implementation of a Smart Campus Security Monitoring System Based on IoT Technology," IEEE Access, vol. 7, pp. 100342-100352, 2019.

[3] H. Lee and S. Park, "A Review of Smart Campus Security: A Case Study Approach," International Journal of Security and Networks, vol. 13, № 3, pp. 137-150, 2018.

[4] R. Gupta and M. Chandrasekaran, Smart Campus Security: Solutions for the 21st Century. Springer, 2020.

[5] Y. Zhang and K. Lee, Building Smart Campus Security Systems: A Comprehensive Guide. Wiley, 2019.

[6] Sobol A., Kochyn V., Grakova N. Mathematical Methods for Assessing Information Security Risks / Open Semantic Technologies for Intelligent Systems. – 2023. – Iss. 7. – pp. 317-322.

[7] Kochyn, V.P. Designing a secure fail-safe cloud repository of paperworks of students and employees of educational institutions / V.P. Kochyn, A.V. Zherelo // Journal of the Belarusian State University. Mathematics and Informatics. – 2021. – № 3. – P. 104-108.

[8] Ponemon Institute, "Smart Campus Security: Trends and Challenges," Research Report.

[9] ISO/IEC 27001:2022, "Information security, cybersecurity and privacy protection. Information security management systems."

[10] National Institute of Standards and Technology (NIST), "Guidelines for Smart Campus Security Systems," NIST Special Publication 800-123.G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (references)

[11] S. McClure, J. Scambray, and G. Kurtz, "Hacking Exposed". [Online]. Available: https://www.mheducation.com/highered/product/hacking-exposed-mcclure-scambray-kurtz/M0071780289.html. [Accessed: February 19, 2024].

[12] Y. Diogenes and E. Ozkaya, "Cybersecurity: Attack and Defense Strategies". [Online]. Available: https://www.oreilly.com/library/view/cybersecurity-attack-and/9781838827793/. [Accessed: February 21, 2024]..

[13] D. Kaafar, E. Panaousis, and G. Loukas, "Smart Cities Cybersecurity and Privacy". [Online]. Available: https://www.elsevier.com/books/smart-cities-cybersecurity-and-privacy/kaafar/978-0-12-815032-0. [Accessed: February 11, 2024].

[14] M. Brown and V. Sivaraman, "A survey of ns-3", in Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, 2011, pp. 1-14, doi: 10.1145/2068816.2068841.

[15] C. Fischione and F. Santucci, Modeling and Simulation of Computer Networks and Systems: Methodologies and Applications. Cambridge University Press, 2016.

[16] Technology of complex support of the life cycle of semantically Compatible intelligent computer systems of the new generation / edited by A. A. Kuznetsov. ed. B. V. Golenkov – Minsk : Bestprint, 2023. – 1064 p. – ISBN 978-985-7267-25-5.

МОДЕЛИРОВАНИЯ СОСТОЯНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УМНОГО КАМПУСА

Соболь А. М., Кочин В. П.

В статье рассматриваются компоненты умного кампуса и её многослойная архитектура. Описаны математические модели состояния системы информационной безопасности умного кампуса. Предложены программно-аппаратные средства для моделирования информационных потоков в умном кампусе, для проведения практических экспериментов.

Received 01.04.2023