Complex Control Systems
ISSN 1310-8255 **Proceedings of the International Scientific Conference "Robotics & Mechatronics 2023"**

Modern Aspects in Information Security in the Field of Robotics

Ivan Gaidarski, Pavlin Kutinchev

Bulgarian Academy of Science, Institute of robotics, Unmanned Robotic Systems Lab, Sofia, Bulgaria

***Abstract*:**
In the current article, an author's method for developing an information security system is considered. The method is based on defining a framework for describing the architecture of the system according to the standards IEEE 1471 and IEEE 42010. Essential to this framework is the formation of multiple stakeholder perspectives and ensuring that their requirements are included in system development. The next step is an analysis of the problem area from different points of view. The analysis presented in the article is from the Information Security point of view in robotics, which is presented with its main elements, concepts and implementation approaches - Vulnerabilities, Threats, Sources, Threat Vectors. They consider the main types of threats to the system - internal and external, as well as the main types of attacks and their countermeasures. As an example, a model for carrying out cyber-attacks proposed by the American company Lockheed Martin is considered.
As a result of the analysis, the main concepts and the connections between them are determined, vulnerabilities, threats, attacks and countermeasures are described for the purposes of designing an information security system in the given area.

***Keywords*: Information Security, Cybersecurity, Robotics Framework, Architecture, Stakeholders, Perspectives, View Points, Vulnerabilities, Threats, Vectors, Targets, Attacks, Model.**

I. NTRODUCTION

The robotization of various activities is gaining special importance and wide application in modern life. Robotic processes support various sectors - medicine, civil defence, meteorology, agriculture, as well as defense-related sectors. Some of these sectors are even unthinkable without the participation of robots - such as the industrial sector, ocean floor exploration, space exploration.

Along with the wide application of robots, however, there are certain concerns related to their safety from information security point of view - their control and regarding the information they collect, process and communicate. Like any system, they also have their weak points - vulnerabilities and, accordingly, susceptibility to threats of an informational nature. So are cyber-attacks and deliberate malicious use, which can pose a serious threat to both organizations and individuals. This leads to the extremely important issue of ensuring their safety from the point of view of information security.

In the current article, an author's method for developing an information security system is considered. Based on this method, an analysis of the domain Information security in robotics is carried out, giving the opportunity to define the main concepts and the connections between them, which allows to design the protection of the given system.

II. METHOD FOR DEVELOPMENT OF INFORMATION SECURITY SYSTEMS IN ORGANIZATIONS

In [1,2] we proposed a method for development of information security system (ISS) in organizations. The method consists of the following phases (Fig. 1):

1. A framework for describing the architecture of ISS, according to IEEE 1471 [3, 4, 5] and IEEE 42010 [3, 5] standards is defined. The framework takes in consideration multiple perspectives of stakeholders / observers (Fig.2) from their point of view of the ISS – requirements, goals and approaches.

2. To determine the requirements for the system from different points of view of the stakeholders, analysis of the problem area of the ISS is conducted.

3. The different viewpoints also are used to construct conceptual models of the problem area, which later are combined in multi-layered conceptual model of the ISS. Generalized and detailed conceptual models are being built, with all the essential for the goals of the ISS elements.

4. The conceptual modeling approach provides an opportunity for a unified presentation of the various elements and concepts forming the designed ISS from the different perspectives of the participants. With its help, both their understanding of the necessary elements and connections according to their requirements, specialization, professional experience and innovations in the relevant field can be presented, as well as the communication between the various stakeholders (observers) can be presented universally. Thus, conceptual models created from different perspectives can be integrated into a single model.

5. The problem area's conceptual model is being transformed into an object-oriented project model.

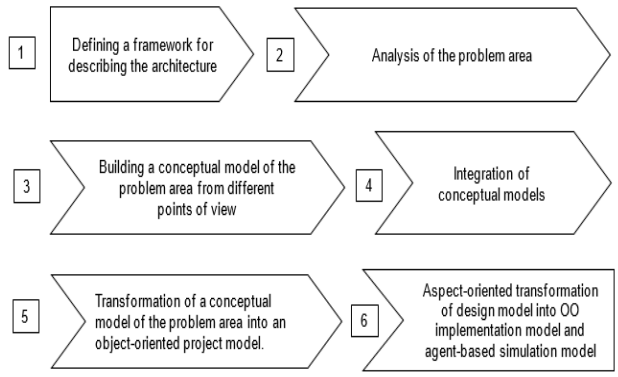

Fig. 1. Method for development of ISS

6. The last step is building a design model from the project model. Using Aspect-oriented transformation, the design model is being transformed in two different kinds of models - an object-oriented realization model and an agent-based simulation model. The purpose of the object-oriented realization model is to guide how the ISS can be realized with existing technologies and methods. The purpose of the agent-based simulation model is to give the opportunity to simulate the model, without spending unnecessary effort, resources and people and of course to be tested and optimized for the real implementation.

Fig. 2. ISS area of interest

The implementation of the first phase is based on the standards IEEE 1471 [4] and ISO/IEC/IEEE 42010 [5], specifying guidelines for creating a framework for the architectural description of systems. These standards allow the description of the architecture of a system [3], by introducing concepts such as: Environment, Stakeholder, Concern, View, Point of view, Architecture of the system (System Architecture), Architectural description, Architectural framework, Architectural View, Architectural Perspective point, Model Kind and etc.

These concepts are applicable to the analysis of the "Information Security System" domain and provide a context for defining a common conceptual framework allowing the construction of conceptual models of ISS. Fig. 2 shows sample areas of interest of the ISS, which is used as a framework for analyzing the domain of the information security system. This article examines some specifics in the field of "Information Security in the Field of Robotics", which complements the "Information Security System" viewpoint.

The development of complex systems is a complex process involving many participants, each of whom has his own point of view - these are the so-called "stakeholders". Each interested party has requirements for the goals of the developed system, as well as for the methods and technologies to be used for the realization of these goals, based on their respective skills, responsibilities, knowledge and experience. When designing complex systems, using a variety of technologies (software, hardware) and having different regulatory requirements, it is inevitable that the different perspectives of the participants intersect or overlap. A further complication factor is the fact that stakeholders may represent their knowledge differently. For example, a man of low has a radically different way of describing requirements or proposals than a mechanical engineer, let alone a programmer. Different requirements refer to different stages of system development and each of them can be subject to different strategies. Thus, one of the important tasks in the system design process is the coordination of the interested parties and the unified presentation of their requirements and contribution to the system.

The method takes into account and unifies the requirements of the different viewpoints and various elements from the field of interest of the ISS, which we consider:

- "Information Security" Viewpoint - includes the basic concepts in information security (Threats, Vulnerabilities, Sources, Motivation, etc.), as well as the main approaches to the implementation of information security;
- "Risk analysis" Viewpoint - through risk analysis the requirements to ISS are determined;
- Communication Viewpoint - determines the way of communication, predetermining the approach to information protection;
- Technological Viewpoint. This Viewpoint includes different approaches in information and communication technologies such as object-oriented approach, agent-based approach and others..
- "Processing of Information" Viewpoint - including the three main types of data defined according to information security - Data-in-Rest, Data-in-Motion and Data-in-Use.

III. ANALYSIS OF THE PROBLEM AREA OF INFORMATION SECURITY SYSTEMS

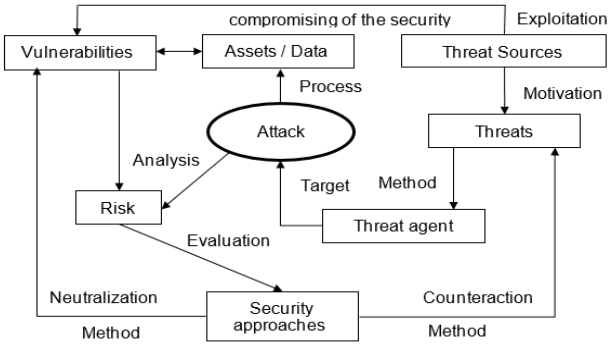

Fig. 3. Basic concepts in information security

Some of the basic concepts and their relations, which are the basis of the field of information security are shown on Fig. 3. It includes some concepts as "Event", "Signals / Alarms", "Incident", "Breach", "Vulnerability", "Threat", "Threat Agent" , "Attack", "Data Breaches", "Data Loss" [6, 7, 8, 9, 10]. In the same time they are realization goals during the development of an ISS.

VULNERABILITIES

Vulnerabilities are weaknesses used by the threat source to launch a successful attack (Fig. 3) [11]. Vulnerabilities inherent in robotic systems can greatly affect their performance, connectivity, control, and operational accuracy. In the Table 1 are shown some of the typical vulnerabilities, the causes of the threat and possible attacks on the system.

TABLE 1. VULNERABILITIES AND THREAT SOURCES

Vulnerability	Causes	Possible attacks
Network vulnerability: wired/wireless communication	Lack or the adoption of basic security measures	Replay, Man-in-the-middle, Eavesdropping, Sniffing, Spoofing,
Security vulnerability	Adoption of new security measures without thorough testing	All types of attacks, Zero-day attacks
Platform vulnerability. Can cause other vulnerabilities	Lack of updates of software and firmware patches	All types of attacks, Zero-day attacks, Unauthorized access,
Update vulnerability	Untested updates	Unauthorized access, Block of the system
Application vulnerability	Lack of proper testing of applications	Attacks to databases, leak of data, alteration of data
Bad practice vulnerability	Bad choice of security measures	Alteration of code or data, Data leak
Management vulnerability	Lack of security guidelines, procedures and policies	All types of attacks,

THREATS

In the event of a threat, the source of the threat intentionally or accidentally uses a given vulnerability of the system, which leads to a breach and danger to information assets. Threats to information security are specific and depend on the characteristics of the environment, source and agent of the threat. A characteristic feature of threats is their association with specific vulnerabilities, which can be used to launch an attack on the system. If the given vulnerability is neutralized, for example by updating the operating system, driver or firmware, the threat sources have no environment to exploit and, accordingly, carry out a successful attack [29].

Threats can vary in their nature, direction, source and outcome. For effective countermeasures, multiple factors must be taken into account [13,15]:

- Sources and agents of the threat and their motivation;
- Threat vector;
- Targets of the threat;
- Type of attack;
- Nature of the threat;
- Impact of the threat.

Threat assessment is an important part of risk analysis. By properly identifying them, the likelihood of their successful use for attacks on system elements that might otherwise remain unprotected is reduced.

SOURCES, THREAT AGENTS, MOTIVATION

A threat agent is any person, group, organization, or process that acts, causes, transmits, transmits, or sustains a threat. Threat agents exploit one or more vulnerabilities to launch an attack with the potential to cause harm, such as leaking or altering data, taking full control of the system, failing certain subsystems, and so on. [6, 11, 15, 16]. The motivation and resources to carry out attacks define humans as potentially dangerous sources of threat. Table 2 presents common threat agents, their motivation, and threat methods.

TABLE 2. SOURCES, MOTIVATION, AND THREAT METHODS

Threat agent	Motivation	Threat methods
Insiders	Unsatisfied employees, Profit, Unauthorized exchange of information, Destruction of data, Curiosity	Steal of confidential data Including passwords, Abuse of privileges, Physical damage, Physical destruction, Extortion
Outsiders	Malicious purposes, Curiosity, Profit, Destruction of data,	Usage of backdoors, system vulnerabilities, injection of malicious data, alteration of data, Social engineering, Extortion
Cyber-criminals	Destruction or Illegal Disclosure of sensitive data; Profit;	Computer crime, Identity theft, Data interception, Fraud,

	Unauthorized Exchange of information.	Misuse of information, Penetration into the system, Social engineering
Competitors	Displacing a rival	Industrial espionage
Incompetent developers	Incompetence	Bad manufactured parts, bad programing code.
Incompetent operators	Incompetence, Malicious purposes	Distraction, Incompetence,
State-sponsored hackers	Achieving political goals, diversion	Hijacking military robots, Steal of sensitive data, Diversion, Damage of critical infrastructure, Social engineering, Sabotage
Terrorists	Terrorism.	Terror, Destruction of infrastructure, including critical, Alteration of data, System attack (DDoS), Sabotage
Spies	Espionage	Stealing of confidential data, Social engineering, Sabotage

VECTORS, TARGETS AND NATURE OF THE THREAT

The source of the threat along with the path to reach the target is defined by the Threat Vector.
To identify potential threat vectors, a list of different threat types, threat sources, and potential threat targets can be compiled (Table 3).

TABLE 3. THREAT TYPES

Threat	Source	Target
Wireless jamming of communications	Outsiders, Terrorists Cyber- criminals.	Communications and control
Reconnaissance and scanning	Outsiders, Cyber-criminals.	Data, Control, Communicatons
Information disclosure	Local leaking of confidential data, Remote control	Data, Control, Technology Know-How
Abuse of privilege	Local or Remote unauthorized access	Data, Control
Information gathering	Insiders, Outsiders via phishing and social engineering	Data, Control, Technology Know-How, Intellectual Property
Information modification (alteration)	Local or Remote unauthorized access	Data, Control, AI aspects of control
Physical damage	Insiders, Outside intruders	Physical integrity
Denial of Service	Malicious Insiders, Outside attacks	Data, Control
Sabotage	Malicious insiders, Outside intruders	Physical integrity, Data, Control
Espionage	Cyber- criminals, Insiders, Outsiders	Data, Technology Know-How, Intellectual Property
Tracking and monitoring of personal	Cyber- criminals, Insiders, Outsiders	Data, Technology Know-How, Physical integrity, Intellectual Property
Interruption	Natural causes	Availability

ATTACKS AND COUNTERACTION

When the threat source performs a targeted action, exploiting a specific vulnerability, we have an Attack. The goal of the attack is to compromise the security of an asset through various methods. These include destruction, theft, alteration, gaining unauthorized access and disclosure. An attack is a process, a sequence of executable actions (Figure 3). To neutralize the attacks, a sequence of specific actions is also necessary - analysis of the conditions on which it depends, analysis of threats, sources of threats, vulnerabilities of assets in different working environments [15, 17]. To effectively counter the attacks, it is necessary to know the principle of operation of the different types of attacks, the risk that the attack poses to the assets, and the appropriate security approaches that we can use as a countermeasure for protection [18, 12, 17].
For this purpose, various frameworks and models for studying and modeling cyber-attacks can be used, such as the MITRE ATT&CK® [19], the NIST Cybersecurity Framework [20] or the cyber-attack model proposed by the Lockheed Martin company (Fig. 4) [21, 22, 23].

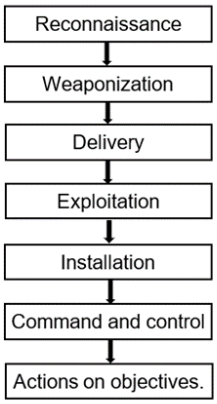

Fig. 4. Lockheed Martin Cyber Kill Chain® framework

Lockheed Martin's model consists of seven stages:

1. Reconnaissance,
2. Weaponization,
3. Delivery,
4. Exploitation,
5. Installation,
6. Command and control,
7. Actions on objectives.

The first stage "Reconnaissance" involves gathering of useful information about the target – IP addresses, operating systems, configurations, emails, names, etc. The second stage "Weaponization" involves the preparation of a malicious payload exploiting a given vulnerability and delivered to the target during the next stage of "Delivery". The malicious payload can be delivered, for example, via a misleading email or through social engineering methods. Once delivered, the "Exploitation" stage exploits vulnerabilities that allow malicious code to execute. During

the "Installation" stage, it is installed on the target's systems. The next stage is to take remote access to the target. The final stage is "Actions on objectives", where malicious individuals are in control of the target and can accomplish their goals.

IV. CONCLUSION

The considered author's method for developing an information security system, in addition to universality, also provides an opportunity to study and analyze specific features of information security in various areas and applications. One such area is robotics, which, from the point of view of information security and more specifically in cyber security, is characterized by both general well-known concepts such as vulnerabilities, threats, agents, methods and threat vector, attacks and corresponding defense methods, as well and with its own specificities arising from the complex nature of these systems. A systematization of the specific aspects of cyber security in the field of robotics would significantly support the effectiveness of the methods of protection, risk assessment (assessing which assets are worth protecting and the corresponding cost, effort and people), and the end result of the designed information system. security. The systematization and analysis of these aspects are planned in the future work of the authors.

ACKNOWLEDGEMENT

This work was supported by the NSP SD program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

REFERENCES

[1] Gaydarski, I., Minchev, Z., Andreev, R. Model Driven Architectural Design of Information Security System. Advances in Intelligent Systems and Computing, Madureira A., Abraham A., Gandhi N., Silva C., Antunes M. (eds) Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018)., 492, Springer, 2019, ISBN:978-3-030-17064-6, ISSN:2194-5357, DOI:10.1007/978-3-030-17065-3_35, 349-359. SJR (Scopus):0.17

[2] Gaidarski, I. K., Minchev, Z. B., Andreev, R. D. Model Driven Approach for Designing of Information Security System. Journal of Information Assurance and Security, 13, MIR Labs, 2019, ISSN:1554-1010, 149-158

[3] Hilliard R.,Emery D., Maier M., ANSI/IEEE 1471 and Systems Engineering, Systems Engineering 7(3):257 - 270, June 2004, DOI: 10.1002/sys.20008

[4] IEEE 1471, IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, https://standards.ieee.org/standard/1471-2000.html, last accessed 2023/04/13

[5] ISO/IEC/IEEE 42010:2011 – Systems and Software Engineering – Architecture Description, https://www.iso.org/standard/50508.html, last accessed 2023/04/13

[6] Whitman M, Mattord H., Principles of Information Security, Fourth Edition
Course Technology, Cengage Learning, 2012

[7] Gragido W., Pirc J.. Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats. Syngress, 2011.

[8] Keung Y., "Information Security Controls", Adv Robot Autom 2013, Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Hong Kong

[9] Bhaskar SM, Ahson SI (2008) Information Security: A practical Approach, Oxford: Alpha Science International Ltd.

[10] Schweitzer JA, Managing Information Security: Administrative, Electronics, and Legal measures to Protect Business Information. Boston: Butterworths. 1990

[11] Наредба за минималните изисквания за мрежова и информационна сигурност, https://www.mtitc.government.bg/sites/default/files/nar_minimalnite_iziskvaniq_mrejova_info_sigurnost-072019.pdf, last accessed 2023/04/13

[12] Andress J., The basics of information security : understanding the fundamentals of InfoSec in theory and practice, Elsevier Inc. 2011

[13] Suryateja P.S., "Threats and Vulnerabilities of Cloud Computing: A Review", International Journal of Computer Sciences and Engineering, Volume 6, Issue 3, published 30.03.2018

[14] Gragido W., Pirc J.. Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats. Syngress, 2011.

[15] Guide for Conducting Risk Assessments. NIST Special Publication 800-30 rev.1, NIST, September 2012, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, last accessed 2023/04/13

[16] Guidelines on assessing DSP and OES compliance to the NISD security Require- ments, ENISA, November 2018, https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements,last accessed 2023/04/13

[17] Taylor-Duncan L., Come in, We're Open – Keeping Your Company's IT Data Safe From Threats, Techni-Core productions, 2014

[18] ENISA Threat Landscape Report 2020 - 15 Top Cyberthreats and Trends, European Network and Information Security Agency (ENISA), 2019, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020, last accessed 2023/04/13

[19] MITRE ATT&CK® Framework, https://attack.mitre.org/, last accessed 2023/04/13

[20] NIST Cybersecurity Framework, https://www.nist.gov/cyberframework, last accessed 2023/04/13

[21] Bollinger J., Enright B., Valites M., Crafting the InfoSec Playbook, O'Reilly Media, Inc., 2015, ISBN: 978-1-491-94940-5

[22] Cyber Kill Chain, Lockheed Martin https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, last accessed 2023/04/13

[23] Hutchins, E. M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." Leading Issues in Information Warfare & Security Research Volume 1. 2011, pp. 80-106.