Security Model of IOT-based Systems

Oksana Mnushka
Computer technology and mechatronics department
Kharkiv National Automobile and Highway University
Kharkiv, Ukraine
mnushka.ov@gmail.com

Volodymyr Savchenko
GlobalLogic Ukraine
Kharkiv, Ukraine
savchenko.volod@gmail.com

***Abstract* – The increasing using of IoT technologies in the industrial sector creates new challenges for the information security of such systems. Using IoT-devices for building SCADA systems cause standard protocols and public networks for data transmitting. Commercial off-the-shelf devices and systems are a new base for industrial control systems, which have high-security risks. There are some useful models are exist for security analysis of information systems, but they do not take into account IoT architecture. The nested attributed metagraph model for the security of IoT-based solutions is proposed and discussed.**

Keywords – IoT; security; model; metagraph; SCADA; control

I. INTRODUCTION

The increasing using of IoT technologies in the industrial sector creates new challenges for the information security of such systems. Information systems based on IoT technologies are gradually replacing traditional solutions for SCADA (Supervisory Control and Data Acquisition) systems in various implementations from the control of remote equipment like oil pumpjack to logistics. The new systems are oriented for using WEB and modern information technologies like cloud computing, they based on mass IoT-products to collect and transmit data.

Using mass IoT-units leads to a decrease in the cost of solutions but causes new problems – lack of security for most of them due to constrained hardware resources. Each developer of such systems always has a choice – to provide high or at least reliable security of the system and to make it sufficiently valuable and uncompetitive on the market or by using inexpensive solutions to provide an acceptable level of security and cost of the system.

Unfortunately, most of the mass IoT-units have bad security and they do not have a sufficient level of protection against network attacks and hardware and software reverse engineering.

The lack of a formal security appraisal system for such systems, ready for engineering applications, is a deterrent and does not allow for an objective assessment of the impact of various threats on the final product.

II. THE STATEMENT OF THE PROBLEM STATEMENT AND ANALYSIS OF LITERATURE

The problem of security of IoT-solutions consists of three problems – availability, integrity, and confidentiality. Availability means the capability of customers to use system services online anywhere and anytime. In the case of system is down due to various reasons such as communication is broken the security is compromised. Data integrity means that all data are the same in the communication process between client and server, or between two or more nodes in the network. Only authorized persons can access all the data in a system, otherwise, the security is compromised. Confidentiality means data protection on both sides in communication during data transportation. Data protection by encryption used so only involved sides can read it. For better security, strong encryption used.

The typical architecture of SCADA-systems based on IoT technologies (Fig. 1) generally corresponds to the traditional automatic process control systems with some limitations as described in [1-4]:

- the data in such systems are not localized within the enterprise's technological computer network, but it is distributed in across a large area and transmitted throw various networks – WSN, LAN, mobile, etc;
- simpler and less secure constrained hardware is used that causes using of the lightweight software and protocols, less strict security network protocols used also;
- a server on the Internet is used for data collection with all the advantages and disadvantages of such use, in some cases for data acquisition, cloud solutions like Amazon Web Services are used;
- due to security reasons, the most appropriate form of use of such systems is the exclusion of the control function and only the visualization of the processes states, otherwise, the problems of security and availability must be solved;
- to provide a control function, one of the major problems is the safety and availability of equipment 24/7. The problem is primarily because data is often transmitted by standard 2G/3G/4G channels, which generally does not guarantee the availability of the channel in 24/7 mode, especially in remote areas.

As shown in Fig. 1 the system consists of four main parts – Web-based SCADA, data exchange channels, communication and computation unit, and sensors networks, which include standalone sensors and sensors subnetworks. For each level of

2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) 978-1-7281-5566-1/20/$31.00 ©2020 IEEE 10.1109/TCSET49122.2020.235462

the system various protocols and computational modules used, which leads to specific security issues. Let's look at these issues in more detail.

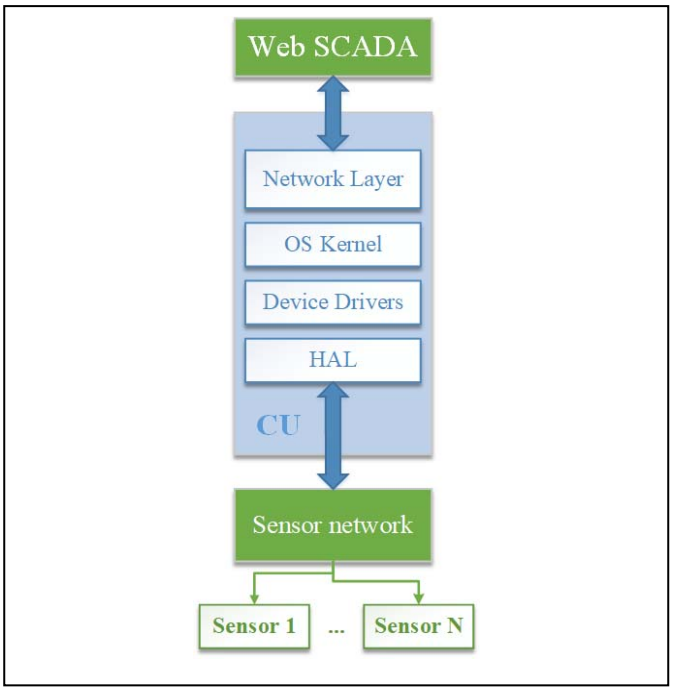

Fig. 1. Typical architecture of IoT-based SCADA: CU – computation and communiction unit.

Data transmission channels are one of popular targets for attacks. For data transmitting between CU and SCADA, CU and Sensors use protocols with various energy efficiency relate to transmission distance. For industrial applications not all protocols are royalty-free and part of them is closed and oriented to use only protocol provider network to data transmitting:

- Cellular (2G/3G), LTE(4G), WiFi, Ethernet – long distances and high power, high speed;
- LoRa, Sigfox, 6LowPAN – long distances, low power, low speed;
- ZigBee, NFC, Z-Wave, BLE – short distances, low power, low or high speed.

The data acquisition subsystem of SCADA consists of sensors, meters, and field devices, such as photosensors, pressure sensors, temperature sensors, and flow sensors. Any issues with sensors cause undefined behavior of system components or the whole system.

The conversion and control subsystem includes remote terminal units, intelligent electronic devices, and programmable logic controllers. All those devices used for obtaining data from sensors and actuators in the process and make control action based on data - states - analysis. Any issues in program logic or conditions cause an unpredictable state of control object.

These three subsystems and HMI (Human-Machine Interface) are an object of attacks. HMI based on web-technologies and as a result, web-related vulnerabilities could affect this component.

In [5-6], the issues of security of components of systems based on IoT technologies will be considered, problems of realization of the corresponding devices and protocols are analyzed, the basic tendencies of development of smart things and development of threats to the infrastructure of smart things related to privacy are shown. Due to vulnerabilities of embedded systems and basic communication and embedded technologies, it provides an overview of new IoT security technologies and current trends in IoT security research. In [5] using REST API to securely expose connected devices to applications on cloud and users are described. The model with middleware as an interface between user and sensor for expose device data through REST and to hide communication process details are proposed. In [6] the on-demand security configuration technique that we can easily set or change the security functionality of IoT-device are proposed. The proposed technics is based on security profiles and configuration map to generate and reconfigure a device image for just-in-time security configuration. Using security modules based on dependency analyzes make possible to determine all necessary modules to include on a device image.

Papers [7-8] provides an overview of mathematical models that describe the security of computer systems.

In [7] the historical development of various approaches to describing security, including. The Bell and LaPadula, The Clark Wilson Model, The Roscoe-Woodcock-Wulf Approach, Communicating Sequential Processes (CSP), etc., are shown. The advantages and disadvantages of individual approaches and models of computer security are described.

In [8] approaches to mathematical modeling of modern cyber threats are shown. It also demonstrates the use of simulation modeling to solve the problems of spreading viruses in computer networks.

III. Model of Information System Security Based on IoT Technologies

A metagraph as a kind of complex network model firstly proposed by A. Basu and R. Blanning [9] and then adapted for information systems and other systems in [10-12].

According to [11-12] the nested metagraph can be represented as an ordered pair:

$$\boldsymbol{G} = (\boldsymbol{X}, \boldsymbol{E}), \tag{1}$$

where $\boldsymbol{X} = \{x_1, x_2, \ldots, x_n\}$ is the set of all vertices of the graph; $\boldsymbol{E} = \{e_1, e_2, \ldots, e_m\}$ is the set of edges of a graph.

Each edge of the metagraph combines two subsets of vertices

$$\boldsymbol{e}_k=(\boldsymbol{V}_i, \boldsymbol{W}_i), \tag{2}$$

where $\boldsymbol{V}_i$, $\boldsymbol{W}_i$ belong to the set of vertices $\boldsymbol{X}$, and the union of the two sets is not an empty set.

Appearance functions (3) must exist for all vertices of the metagraph

$$f_1^a: g_1^a(x_1^a, e_1^a) \rightarrow x_2^b,$$
$$f_2^b: g_2^b(x_2^b, e_2^b) \rightarrow x_3^c, \ldots, \quad (3)$$
$$f^j{}_{n-1}: g^j_{n-1}\,(x^j_{n-1}, e^j_{n-1}) \rightarrow x_n^j.$$

The upper indices in (3) determine the number of vertices and edges at the corresponding level i=1, 2, …, n, which in (3) is indicated by the lower indices.

Each of the vertices and each of the edges in the metagraph has an unlimited number of attributes that are characteristics of real objects and represented as rows and numbers

$$x_i^j = \{a_1, a_2, \ldots, a_k\},\ i=1..n, j=1..m, \quad (4)$$
$$e_j^t = (x_i^S, x_i^F) = \{a_1, a_2, \ldots, a_q\}, \quad (5)$$

The metagraph (1)-(5) can be represented graphically as shown on Fig. 2. It should be noted that a metgraph can transform into a hypergraph or a simple oriented graph, depending on the presence of elementary vertices, that is, for which there are no appearance functions (3), at each level of the metagraph. Connections e^j_i are allowed between vertices of any level (e_7, e_8, e_9, e_{10}). If the vertices x^4_i and x^3_i, in turn, are also hyper edges of g^j_{n-1} (x^j_{n-1}, e^j_{n-1}), then we get a nested metagraph of 4, etc.

Also, the metagraph allows links between any components (levels) of a system instead of a traditional graph (dash lines). This allows us to identify more complex effects from the interaction of different subsystems.

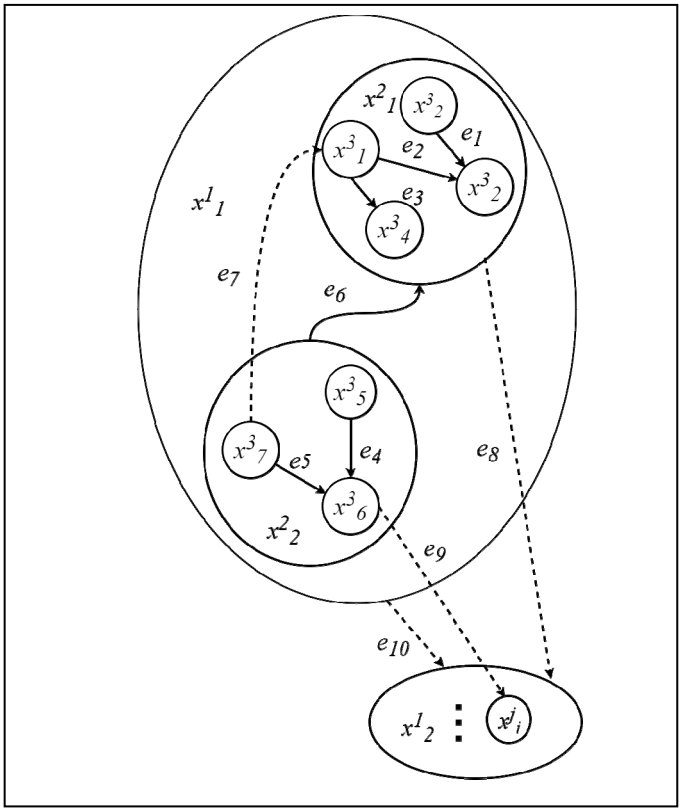

Fig. 2. Nested metagraph.

A multilevel model of an information system based on attributive metagraphs is known [11], but it does not take into account the features of the Internet of Things devices and the architecture of systems based on them (Fig. 1)

We proposed a model for describing the security of a web-based SCADA system based on IoT devices and technologies as the nested metagraph, which contains:

- a set of all devices and $\boldsymbol{X_1} = \{x_1, x_2, \ldots, x_k\}$ and their connections $\boldsymbol{E_1} = \{e_1^1, e_1^2, \ldots, e_1^K\}$;
- a set of system software $\boldsymbol{X_2} = \{x_1, x_2, \ldots, x_m\}$ and the links between the software components $\boldsymbol{E_2} = \{e_2^1, e_2^2, \ldots, e_2^M\}$;
- a set of application software $\boldsymbol{X_3} = \{x_1, x_2, \ldots, x_n\}$ and the links between the software components $\boldsymbol{E_3} = \{e_3^1, e_3^2, \ldots, e_3^N\}$;
- a set of communication protocols $\boldsymbol{X_4} = \{x_1, x_2, \ldots, x_p\}$ and the links between them $\boldsymbol{E_4} = \{e_4^1, e_4^2, \ldots, e_4^P\}$;
- a set of communication lines (networks) $\boldsymbol{X_5} = \{x_1, x_2, \ldots, x_r\}$ and the connections between them $\boldsymbol{E_5} = \{e_5^1, e_5^2, \ldots, e_5^R\}$;
- a set of clients of the system $\boldsymbol{X_6} = \{x_1, x_2, \ldots, x_s\}$ and the relationships between them $\boldsymbol{E_6} = \{e_6^1, e_6^2, \ldots, e_6^R\}$.

Thus, we have a nested metagraph, which consists of six levels and represents all the main components of the described system. The relationship between elements at some level exists only when there is a corresponding relationship between all elements of the upper levels. Given the specifics of the system and the basis of expert judgment, we determine the possible attributes for the system components:

- $\boldsymbol{A}_{X1}$ = {"identifier", "location coordinates", "operating mode", "physical address", "autonomy"};
- $\boldsymbol{A}_{X2}$ = {"name", "type", "logical network address"};
- $\boldsymbol{A}_{X3}$ = {"name", "exchange protocol", "host ID"};
- $\boldsymbol{A}_{X4}$ = {"name", "exchange protocol", "address / identifier"};
- $\boldsymbol{A}_{X5}$ = {"name", "line type", "exchange protocol", "address / identifier", "routing table"};
- $\boldsymbol{A}_{X6}$ = {"ID", "Permissions", "Attached Equipment"};

In our case, by exchange protocols we mean the TCP/IP stack model and its corresponding levels between SCADA and CU [14] and protocols for data-exchange between CU and various field devices (MODBUS, CAN, ProfiBUS, etc) [15].

During operation, the system is influenced by various factors that determine its safety. The main problem with IoT-based systems is the different computing capabilities of devices (constrained devices, smart dust, etc.), which, for example, does not allow for powerful and well-protected protocols or operating systems. The problem is the physical availability of devices that are often located outside security zones or directly used by the client in changing environments that may be compromised in terms of security. The presence of an operator (or any other operating personnel) or customer in the system is also an additional risk factor.

The main types of threats can be divided into three main groups:

- a substitution of an element of the system (metagraph) of the proposed model (6) is expressed by the substitution of the vertex or edge $(\boldsymbol{X}_1 \setminus x^j_1) \cup x_1^{k+1}$;
- an adding an element in a metagraph is about adding a new element $\boldsymbol{X}_1 \cup x_1^{k+1}$ and transforming the original graph by breaking relationships between edges or vertices;
- a deleting a metagraph element also breaks certain links between the elements of the metagraph $\boldsymbol{X}_1 \setminus x^j_1$;

We can write appropriate transformations for edges $\boldsymbol{E}$. Any edges transformations lead to various changes of data and control signals flows and break communications between system nodes. To control such a situation a safety subsystem must be a part of the system software set ($\boldsymbol{X_2}$). It mostly has relations with sets $\boldsymbol{X_1}$ and $\boldsymbol{X_2}$ and controls states of their elements; also, it has relations with elements from sets $\boldsymbol{X_3}$ and $\boldsymbol{X_6}$ as notifications and logging subsystems.

Due to the complexity of analyzing the whole system, we "simplify" metagraph with views or projections on interesting nodes according to [9] – $\boldsymbol{G'} = (\boldsymbol{X'}, \boldsymbol{E'})$ is a projection $\boldsymbol{G}$ on $\boldsymbol{X'}$ (for $\boldsymbol{X'}$ from $\boldsymbol{X}$) if:

- there is a dominant metapath $\boldsymbol{M}(\boldsymbol{V},\{\boldsymbol{x}'\})$ in $\boldsymbol{G}$ for any $e'=(\boldsymbol{V'}, \boldsymbol{W'})$ from set $\boldsymbol{E'}$ and for any x' from set $\boldsymbol{W'}$;
- for any dominant metapath $\boldsymbol{M}(\boldsymbol{V},\{x'\})$ in $\boldsymbol{G}$ for every x' from $\boldsymbol{X'}$ exists an edge $(\boldsymbol{V'}, \boldsymbol{W'})$ such that $\boldsymbol{V}=\boldsymbol{V'}$ and x is from set $\boldsymbol{W'}$;
- there are no two edges in set $\boldsymbol{E'}$ with the same invertex, that leads to minimizing the number of edges and make a projection to be unique..

An attribute replacement changes a system status information, does not affect metagraph characteristics but leads to misunderstanding of compromised data. On the other hand, attributes allow you to separate almost identical system components and similar to attributes of elements of a relational data model. As a root case, we use only one node that includes all components of a system without relations to an outer world.

For a typical node of IoT system, we have various rank for threats that depend on sets $\boldsymbol{X}_1$-$\boldsymbol{X}_6$ and their relationships $\boldsymbol{E}_1$-$\boldsymbol{E}_6$, that is, a "substitution" is more possible than the unauthorized "addition" of a new element to the system. We propose to use attributes for such cases.

CONCLUSION

A model of security for systems based on IoT technologies have been presented, which, unlike the known models, takes into account the architectural features of web-oriented SCADA systems and the hardware and software limitations of such systems.

The resulting model is form of a nested attribute metagraph, and provides a convenient tool for further analysis and optimizations, including visualization of data flows in the system, system states over time, etc.

A prospect of further research is to develop models for various subsystems and tools for their visualization and analysis based on matrix operations on metagraphs, and model for describing security vulnerabilities (CVSS) for each node and the whole system.

REFERENCES

[1] Unde, M.D. and Kurhe, P.S. "Web based control and data acquisition system for industrial application monitoring", 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, 2017, pp. 246-249.

[2] Liu, Y., Zhao, Y., Tao, L., Zhao, K. and K. Li "The Application of Digital Flexible Intelligent Manufacturing System in Machine Manufacturing Industry", IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Tianjin, China, 2018, pp. 664-668.

[3] Mnushka, O.V. "The architecture of a web-based SCADA system", Vistnyk National Technical University «Kharkiv Polytechnic Institute»: zb. nauk. pr. ser.: Informatika ta modeluvannia, Kharkiv, NTU "KPI", № 24 (1300), 2018, pp. 117-128. (in Ukrainian).

[4] Mnushka, O.V."SCADA based on the industrial Internet of Things: architecture of the system", Technical service of agriculture, forestry and transport systems, Kharkiv, №12, 2018, pp.117-124. (in Ukrainian).

[5] Garg, H. and Dave, M. "Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware", 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6.

[6] Chung, B., Kim, J., and Jeon, Y., "On-demand security configuration for IoT devices", International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2016, pp. 1082-1084.

[7] Ryan, P. Mathematical Models of Computer Security, LNCS 2171, 2000, 62 p.

[8] Dinesh, K.S. "Cyber Defense: Mathematical Modeling and Simulation", International Journal of Applied Physics and Mathematic, Vol. 2, No. 5, 2012, pp. 312-315.

[9] Basu, A., Blanning, R.W. Metagraphs and their applications, Springer, 2007, 174 p.

[10] Chernenkiy, V., Gapanyuk, Y., Revunkov, G., Kaganov, Y., Fedorenko, Y., and Minakova, S. "Using metagraph approach for complex domains description", Proceedings of the XIX International Conference "Data Analytics and Management in Data Intensive Domains" (DAMDID/RCDL'2017), Moscow, Russia, October 10–13, 2017, pp. 341-349.

[11] Astanin, S.V., Dragnysh, N.V., and Zhukovskaya, N.V. "Nested Metagraphs as Models of Complex Objects", Engineering Bulletin of the Don, Vol. 23, no. 4-2., 2012, pp. 74-78.

[12] Novokrestov, A.K., Konev, A.A, "A multilevel model of an information system based on attributive metagraphs", Electronic tools and control systems: Proceedings of the XI International Scientific and Practical Conference (November 25-27, 2015), Tomsk, V-Spectrum, 2015. - pp. 182-188.

[13] Shtogrina, Y., and Krivenkova, A., "Metagraph visualization method", Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 2014, No.3 (91), pp. 124-130, (in Russian)

[14] Forouzan, and Behrouz, A. (2003), TCP/IP Protocol Suite (2nd ed.), McGraw-Hill, 2003, 976 p

[15] Liptak, B. G, and Halit, E. Instrument Engineers' Handbook, Volume 3: Process Software and Digital Networks, Fourth Edition, 2016, 1142