B&H Electrical Engineering Volume 15 January/December 2021 31-39
sciendo DOI: 10.2478/bhee-2021-0015

Review scientific paper/Pregledni naučni rad

ANALYSIS OF THREATS FOR AMBIENT ASSISTED LIVING (AAL) WIRELESS SENSOR NETWORK (WSN)-BASED SYSTEM

ANALIZA PRIJETNJI ZA SISTEM POTPOMOGNUTOG ŽIVLJENJA BAZIRAN NA BEŽIČNOJ SENZORSKOJ MREŽI

Nejla Popaja[1], Sabina Baraković[1], Jasmina Baraković Husić[1]

Abstract: In the process of designing a system, it is necessary to identify potential threats to that system and to include appropriate countermeasures. The process that helps in finding problems in the initial phase of the system design is the threat modeling. Creating a threat model consists of several steps and there are many tools that can help in automating the procedure. This article deals with the threat analysis for an Ambient Assisted Living (AAL) system based on Wireless Sensor Network (WSN), whose main function is to provide information for carers in order to provide the best possible help to the elderly and disabled. We have identified and analysed 99 potential threats to the considered system, where Denial of Service (DoS) resulted in being the most represented class of threats. After conducting the threat assessment, the obtained results showed that the majority of threats are high-risk and justified the use of threat modeling in the design phase, since they can be utilized in further system development stages.

Keywords: assistance, living, model, network, sensor, threat, wireless

Sažetak: U procesu dizajniranja sistema, neophodno je identifikovati potencijalne prijetnje i uključiti odgovarajuće protumjere. Proces koji pomaže u pronalasku problema u početnoj fazi dizajna je modelovanje prijetnji. Izrada modela prijetnji se sastoji od nekoliko koraka, a postoje brojni alati koji mogu pomoći automatizaciji procedure. Ovaj rad se bavi analizom prijetnji za sistem potpomognutog življenja (eng. Ambient Assisted Living, AAL), zasnovanog na bežičnoj senzorskoj mreži (eng. Wireless Sensor Network, WSN), čija je osnova funkcija dati informacije pružaocima njege s ciljem davanja najbolje moguće pomoći onima u potrebi. Identifikovano je 99 potencijalnih prijetnji za razmatrani sistem, a odbijanje usluge (eng. Denial of Service, DoS) je najistaknutija klasa prijetnji. Nakon procjene prijetnji, rezultati pokazuju da ih većina spada u kategoriju visokog rizika, čime se opravdava upotreba modelovanja prijetnji u fazi dizajna budući da se mogu koristiti ove informacije u daljem razvoju.

Ključne riječi: asistencija, življenje, model, mreža, senzor, prijetnja, bežično

INTRODUCTION

In the last decade, Information and Communication Technologies (ICT) are subjected to the constant and rapid development and can contribute to the goal of an improved Quality of Life (QoL) [1]. The technological advances in sensors, wireless communications, and computing in terms of price, size, or power consumption have allowed the seamless integration of sensors into everyday objects, i.e., homes, offices, hospitals, etc. [2]. These ICT solutions, which are based on Wireless Sensor Network (WSN), are a part of our everyday life and can be used in various scenarios providing new intelligent functionalities. One of many possible utilizations of these solutions are the systems for older adults, since according to the statistics the population is ageing quicker than it used to [1]. These systems are commonly referred to as Ambient Assisted Living (AAL) systems, since they can provide assistance to disabled or older adults given that this group requires specific technological solutions. There are many challenges that development of these systems bring. One of them is the security aspect in the cyber security challenged world, given that it may lead to increased number of victims of illicit cyber-criminal activities which causes many loses, either in data, money, or lives [3].

Therefore, when designing and developing a system, knowing what threats can compromise a particular system is crucial to its whole lifecycle. Timely analysis and identification of threats to a particular system can help reduce the risk, effort, cost, etc. of the system in question. In order to prevent certain security vulnerabilities and problems when developing a system, potential threats need to be identified and appropriately addressed [4]. The process that can be used to conduct this analysis is the threat modelling. Threat modelling is an engineering technique that can be used to identify threats, attacks, vulnerabilities, and appropriate countermeasures in the context of a particular application or system [5], [6]. Its conduction is not a one-time process, but rather closely related to

[1] University of Sarajevo, Bosnia and Herzegovina
sabina.barakovic@fsk.unsa.ba
Paper submitted: Septembar 2021 Paper accepted: October 2021

the design and development stages of an application or a system. Threat modelling can help in finding problems in the design phase, and that is the greatest value of this approach.

Taking into account the contemporariness of AAL systems based on WSN concept, as well as rising security challenges in digital space together with the need to include the security in the system design, this paper analyses the security of a WSN-based AAL system [2] by using the threat modeling. The main aim of this work, therefore, is to identify potential threats to the subject system in order to be able to incorporate adequate protection mechanisms and apply measures in the system upgrade, thereby improving its security. Also, learned lessons may contribute to developers of other similar future systems.

The structure of the paper is as follows: After the brief introduction, Section 1 explains WSNs and gives a brief overview of the Ambient Intelligence for Caregivers (AmiCare) system. Section 2 explains the threat modelling process, while the step by step procedure for the considered system is given in Section 3. Results analysis and discussion are contained in Section 4, while Section 5 concludes the paper.

1. WIRELESS SENSOR NETWORK AND AMBIENT ASSISTED LIVING SYSTEM

WSN is a set of independent and spatially distributed nodes and their task is to collect data on changes in the environment, record them, and send them to the task manager who processes this data and performs further manipulation on them. The communication architecture of WSN is divided into a sensor network and a classical infrastructure. The following explains the parts of the network: sensor field, sensor nodes, gateway, and task manager [7], [8]. A sensor field is a set of sensor nodes with an environment from which nodes can collect information. The nodes are interconnected and with the help of wireless connections each node can communicate and cooperate with each other. The sensor node can perform tasks such as calculating data, storing data, communicating data, and reading/running data [9]. Gateways allow system managers to connect the sensor network to a personal computer, personal digital assistants, the Internet, and existing networks and protocols. The task manager connects to the gateway via an Internet or satellite network. All data (raw or processed) coming from sensor nodes is stored in task managers for further analysis. Users can use any interface to retrieve data locally or remotely.

The most important areas of application of wireless sensor networks are: industry, military, geo-location, public safety, agriculture, seismology, health, incident identification, facility monitoring, traffic, logistics, scientific, biological and environmental applications [10].

Advances in sensor, networking, and energy storage technologies have led to future WSN being combined to form the Internet of Things (IoT) nervous system. Combined with cloud computing and large data processing, the number of applications and the market size of the Internet of Things are almost limitless and will allow people and machines to interact in unprecedented and unpredictable ways [11].

The advent of WSN opens the way for many areas of research. WSN consists of small nodes with sensors and wireless communication capabilities, which are expected to play an important role in the coming age of more advanced technology such as AAL. Due to their limitations in computing, memory, power resources, and deployment in unattended environments, sensors are highly vulnerable and subject to a large number of security threats, while WSN has many security issues to be solved [12].

The need for security in WSN systems will grow even more as WSN continues to grow. Additionally, it is expected that current and future work in area of privacy and trust will make WSN a more attractive option in a variety of new areas. In a long way of WSN evolution, experts have encountered many problems. Now, in this cyber security challenged environment, they face the problem of security related to this technology. To address the challenge, security must first be an important factor to keep in mind when designing a WSN, especially in situation when it is used for AAL since it may lead to serious consequences such as life loss or injuries. One should strive to optimize network security by identifying targets and vulnerabilities, and then preventing or mitigating threats to the system. This is the idea of threat modelling, which is discussed in more detail in the following section.

Before describing the process of threat modelling of WSN-based AAL system, we will give a brief introduction of the system whose architecture served as an example for this analysis – the AmiCare, which has been developed by Bleda, et al. and presented in [2]. AmICare, is an AAL system whose main function is to provide information for carers in order to provide the best possible help to the elderly or infirm. This system is focused on providing support to caregivers through a very simple but useful solution. One of its main advantages lies in its simplicity, along with ease of installation, placement in a bed or any type of seat. This simplicity translates into low overall cost, including procurement, use, and maintenance. In particular, the auxiliary system is arranged in an intellectual residence with a disability, with 14 bedrooms arranged on two different floors. The total population can be up to 34. Beds are pieces of furniture on which sensor nodes are integrated in an inconspicuous way so that the user is not aware of them [2].

As authors state in Figure [2], the AmICare system is designed around a local server and database implemented in the Raspberry Pi 3 (model B +) that also acts as the central node of the WSN. Any burglary or unauthorized access to resident behaviour data should be prevented at all costs. The solution adopted during the first implementation and trial of this solution consisted of the implemen-

tation of a server and a database within the same local network, which restricts unauthorized access to data outside the network. The bed node includes a bed presence sensor connected to the main processing unit with a Wireless Fidelity (Wi-Fi) connection module. The node sensor consists of an electronic Printed Circuit Board (PCB) that includes a processor unit and some sensors.

The main functionalities of the interface, i.e., how the system helps with the day-to-day work tasks in the residence are: i. Tracking of residents within the facilities; ii. Absence detection from bed during a configured time period; iii. Occupancy detection in bed during a configured time period; iv. Impacts or shocks detection; v. Temperature room monitor; vi. Resting time monitor; vii. Configuration of personal alerts for each resident; viii. Monitor and track all alerts; ix. Sound signal when alert detected.

2. THREAT MODELING BASICS

Threat modelling is the process of optimizing network security by identifying targets and vulnerabilities, and then determining countermeasures to prevent or mitigate the effects of threats to the system. In order to improve this area, a lot of research has been done, so the threat modelling methodology has emerged as an independent and comprehensive [4], [6]. The most important thing about a threat model is that it is systematic and structured. Threat moderators need to go through a series of concrete steps to fully understand the environment they are trying to secure and identify vulnerabilities and potential attackers. In addition, threat modelling is still in some ways an art as much as a science, and there is no canonical threat modelling process. In fact, it is not a mathematical task. Threat modelling practices are drawn from a variety of earlier security practices [13]. In addition to the fact that it is an iterative process, it is important to stress that threat modelling can be conducted on different system architecture detail levels depending on the level of security the experts want to analyse.

There are many structured approaches to threat modelling [4] which are organized in various stages or steps. One of them suggests performance in 4 phases [6]:

- Diagram: what do we build?
- Identify threats: what can go wrong?
- Mitigation: what do we do to defend ourselves from threats?
- Validation: confirming the previous steps and following them.

On the other hand, Figure 1 presents a 6-step approach to threat modelling [5], [14]. This approach covers: i. identification of resources to be protected (data, confidential information, physical assets, etc.); ii. architecture documentation which includes identification of system's function, production of architecture diagram, and technology identification; iii. application break covering trust boundaries, data flows, entry points, privilege code recognition, and security profile documentation; iv. identification of threats; and v. their documentation; and finally, vi. assessment of identified threats.

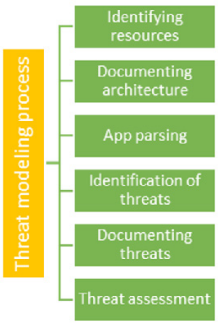

Figure 1. Threat modeling process

Approaches to threat modelling such as asset-centric approach, attacker-centric approach, software-centric approach, or defence-centric approach; methodologies such as STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privilege), PASTA (Process for Attack Simulation and Treat Analysis), etc.; or tools such as Microsoft Threat Modeling Tool (MTMT), Threat Dragon, etc. have been described and summarized in [4] and we will refrain from going into details.

3. THREAT MODELING OF AAL WSN-BASED SYSTEM

This section represents the process of threat modelling of the AmiCare system, i.e., AAL WSN-based system. Threat modelling is based on the idea that every system or organization has valuable resources that need to be protected. These resources have certain vulnerabilities that certain external and internal threats can exploit to harm those resources, but at the same time there are appropriate security countermeasures to mitigate the threats [14].

Therefore, in order to analyse the threats for the system in question, we have conducted the threat modelling covering the following procedure. **In order to facilitate understanding and identification of security objectives**, it is best to divide them into the following categories: identity, finance, reputation, privacy and regulation, and warranty availability. The subject system encompasses all of abovementioned categories of objectives.

In terms of **resource identification**, as any other system, this one as well has the resources that need to be protected. Resources cover a wide range, from confidential data to the availability of website. All resources that the system possesses are covered, and they need to be protected because any intrusion or damage to them would lead to system dysfunction or threats. Resources are: data in the database (tables: rules, warnings and users), sensors, Internet access, physical access to the server, device used by the user, electricity, and web application (user interface).

Further on, Figure 2 shows the architecture of the considered system, with which one can see the composition and structure of the application, as well as some of the features of the physical layout. The inputs to the system are: input and review of data by the caregiver who represents the right user and on the other hand the behaviour and environment of the patient, as data that the sensor receives and sends to the system. The caregiver accesses the system using a web browser that can be opened on any device that has a Wi-Fi antenna. Both, the sensor and the device, used by the caregiver are connected via a Wi-Fi network to a router that sends data to the Raspberry pi 3 device, also via Wi-Fi. The Raspberry pi 3 has a local web server and database. It is very important to note that on the right side of the router, the data only goes in one direction, from the patient onwards to the base. The sensor receives data about the patient and the environment and sends it to the router via a wireless network, which directs it to the database. While on the other side of the router, the caregiver can enter data, request a printout, change rules, and the like, which means that this is a two-way communication. These two entries are very different on the security side. The architecture is divided into several zones, which together form one whole. Those zones are: client, browser, router, frontend, server, and sensor zone.Once security objectives and resources have been defined, the application design is analysed to identify components, data flows, and trust boundaries. This step is performed by reviewing the **application architecture and documentation**, after which it is necessary to create a Data Flow Diagram (DFD) diagram that is given in Figure 3.

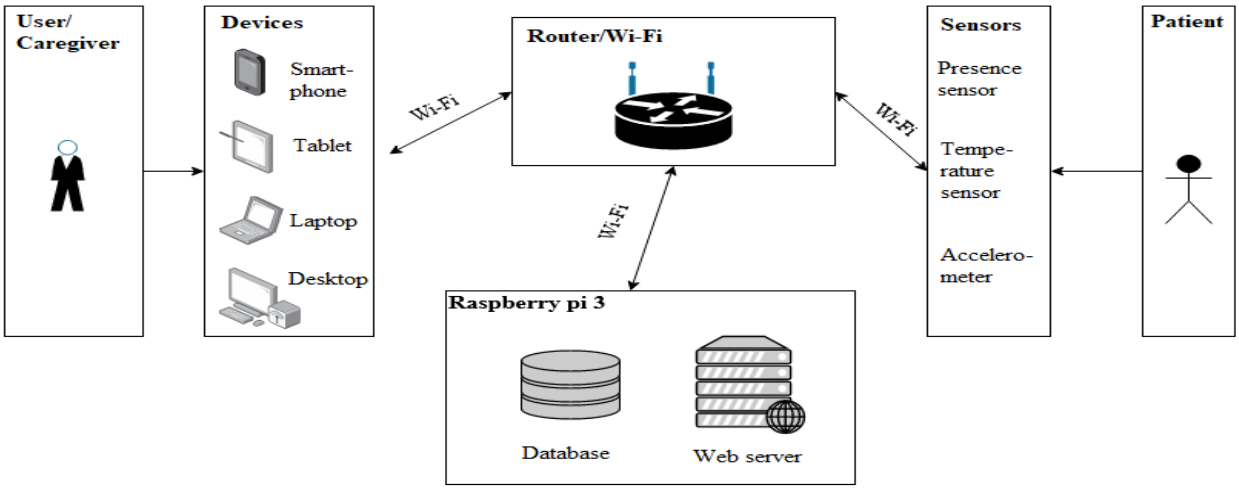

Figure 2. High-level architecture of the AAL WSN-based system

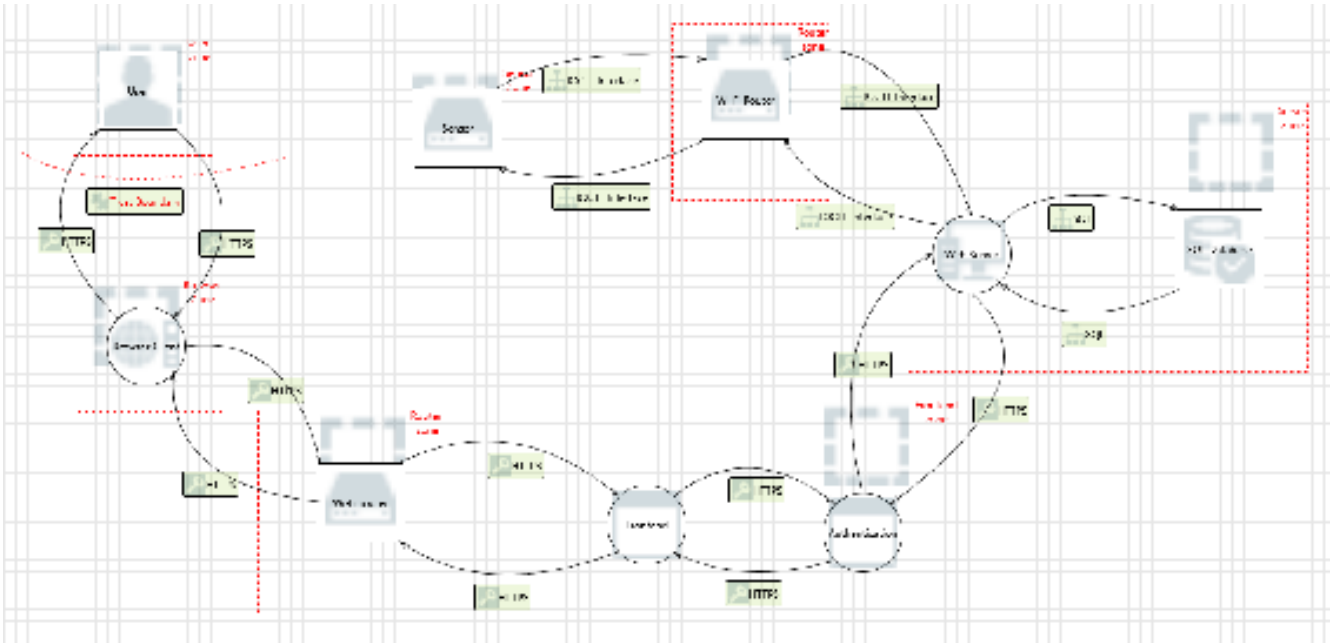

Figure 3. DFD for AAL WSN-based system in MTMT

Then follows **system parsing**. Parsing an application or a system involves breaking it and creating a security profile for the vulnerability-based application. It is necessary to know how the module checks and processes data, where the data flows are, how the data is stored and what basic decisions and assumptions are made when creating the module [14].

After having analysed the system, the following step includes **threat identification**. In this paper, we have used MTMT for identification of threats [15]. MTMT is a freeware tool that helps to identify threats in the software design phase. This tool is a key element of Microsoft Security Development LifeCycle (SDL). MTMT enables potential security issues to be identified and mitigated early, when it is relatively straightforward and cost-effective to address. MTMT uses STRIDE methodology. STRIDE is the acronym behind:

- **S**poofing (trying to access the system using a false identity),
- **T**ampering (tampering with data; here are possibilities for users to change the received data and thus change it back),
- **R**epudiation (the user can dispute transactions with no audits and activity repositories),
- **I**nformation Disclosure (unwanted reading of private information; the application must have strict monitoring to prevent user IDentity (ID) change and misuse, especially if it uses a single context to run the entire application),
- **D**enial of Service (action by disabling the service; to avoid this type of attack, it is necessary to use expensive resources, thus allowing only authenticated and authorized users to be accessed and disabled to anonymous users), and
- **E**levation of Privilege (the less privileged user assumes the identity of the privileged user), and is used for threat categorization [4], [16].

By considering threats of these different categories for each individual element in DFD, STRIDE greatly supports the identification of threats within the application. We refrain from analysing, describing, and discussing the MTMT's mechanisms of threat identification since it is a part of system functioning and it can be found in its documentation [15]. As it shall be explained in detail in the following section, MTMT output reported showed that it has identified 99 threats for AmiCare system.

In the final step of this process, **threats are assessed** based on the risk they cause using the DREAD method. DREAD [17] is part of a computer security risk assessment system. Provides mnemonics for security threats to risk using five categories:

- **D**amage: how bad could the attack be?
- **R**eproducibility: how easy is it to reproduce an attack?
- **E**xploitability: how much work is there to launch an attack?
- **A**ffected Users: how many people will be affected?
- **D**iscoverability: how easy is it to detect a threat?

The result of this step is a table with identified threats that are assessed by the amount of risk posed by each of the threats. When a particular threat is assessed using DREAD, each category receives a score of 1 to 10. The sum of all scores for a given release can be used to prioritize among different issues [18]. Possible outcomes include: low- (5-7), medium-(8-11), and high-risk (12-15) threats. In our case, as it will be further explained, 67 threats (68.33%) have been characterized as high-risk ones, while 32 (31.68%) medium-risk.

4. RESULT ANALYSIS

After the identification and assessment of threats, i.e., after finishing the threat model, statistical representation of the results and a brief overview of the remediation of each of the STRIDE threats is presented in this section.

As mentioned earlier, the MTMT tool has identified 99 threats. Threats are categorized by methodologies, methods, probabilities of occurrence in a method or methodology. Based on the STRIDE method, all threats are categorized and the numbers of threats are presented in Figure 4. This graph shows the amount of each threat individually without a filter, which means it refers to the total number of threats (includes all interactions: HyperText Transfer Protocol Secure (HTTPS), Input/Output Control (IOCTL), and Structured Query Language (SQL)). This shows that the most prominent threats come from Denial of Service (DoS) class of the STRIDE methodology (29.70%). This class of threats is followed by: Elevation of privilege (16.83%), repudiation (15.84%), spoofing (13.86%), tampering (11.88%), and information disclosure (9.90%). Figure 4 shows the ratio of STRIDE threats and therefore it is easier to determine which threats should be remedied first and pay the most attention.

Further on, the graphs in Figures 5, 6, and 7 are filtered by interactions from the architecture, in order to be seen in which places exactly threats pose the greatest threat to the system. The X-axis represents percentages, while the Y- axis represents threats according to the STRIDE methodology.

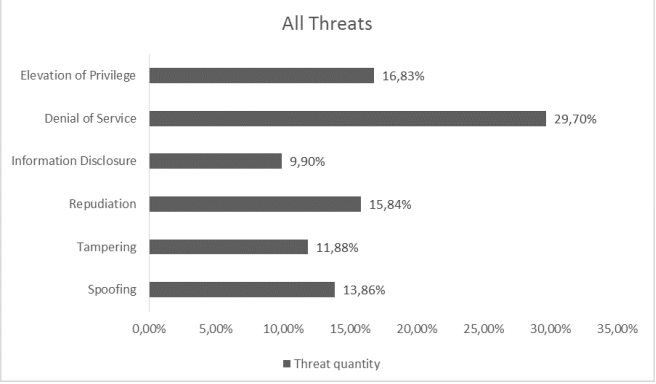

Figure 4. STRIDE categorized threats – Total

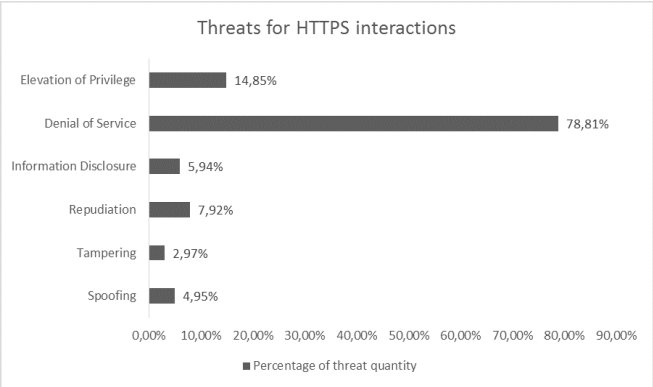

Figure 5. STRIDE threats – HTTPS

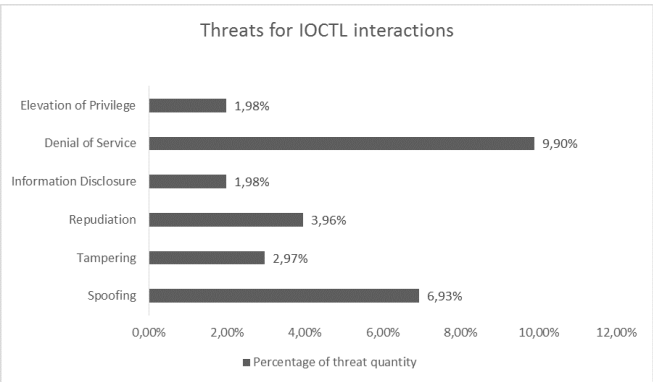

Figure 6. STRIDE threats – IOCTL

The graph in Figure 5 shows the amount of each threat individually, but this time filtered only for HTTPS interactions. A large number of threats from the category of threats of DoS of 78.81% can be seen in the graph. The graph in Figure 6 shows the amount of each threat individually with the IOCTL interaction filter. For the third time, threats from the category of DoS are the most prevalent, but with not as significant a difference from other threats as in the previous diagram. In Figure 7, the graph shows the representation of each threat individually in SQL interactions. It can be seen that most threats come from the categories of tampering, followed by the category of spoofing.

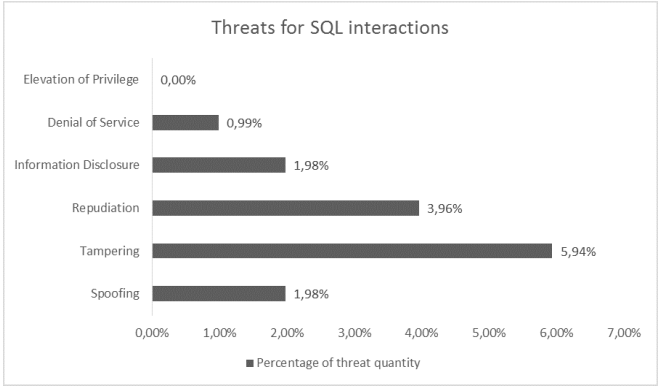

Figure 7. STRIDE threats – SQL

Having shown the graphs of threat representation for each interaction separately, it is very important to present the distribution of different threats in different zones of the observed system. The results show which zone is most endangered and, therefore, which needs to be upgraded first, i.e., for which to find a better solution than the existing one. In Figure 8, the X-axis represents the zones found in the system architecture, while the Y-axis represents the number of threats in percentages. Different colours, as presented in the legend of the graphics, show the threats per STRIDE, so that for each zone the percentage of each of the threat categories is presented. From the graphs, we conclude that the most endangered is the server zone, followed by the frontend zone.

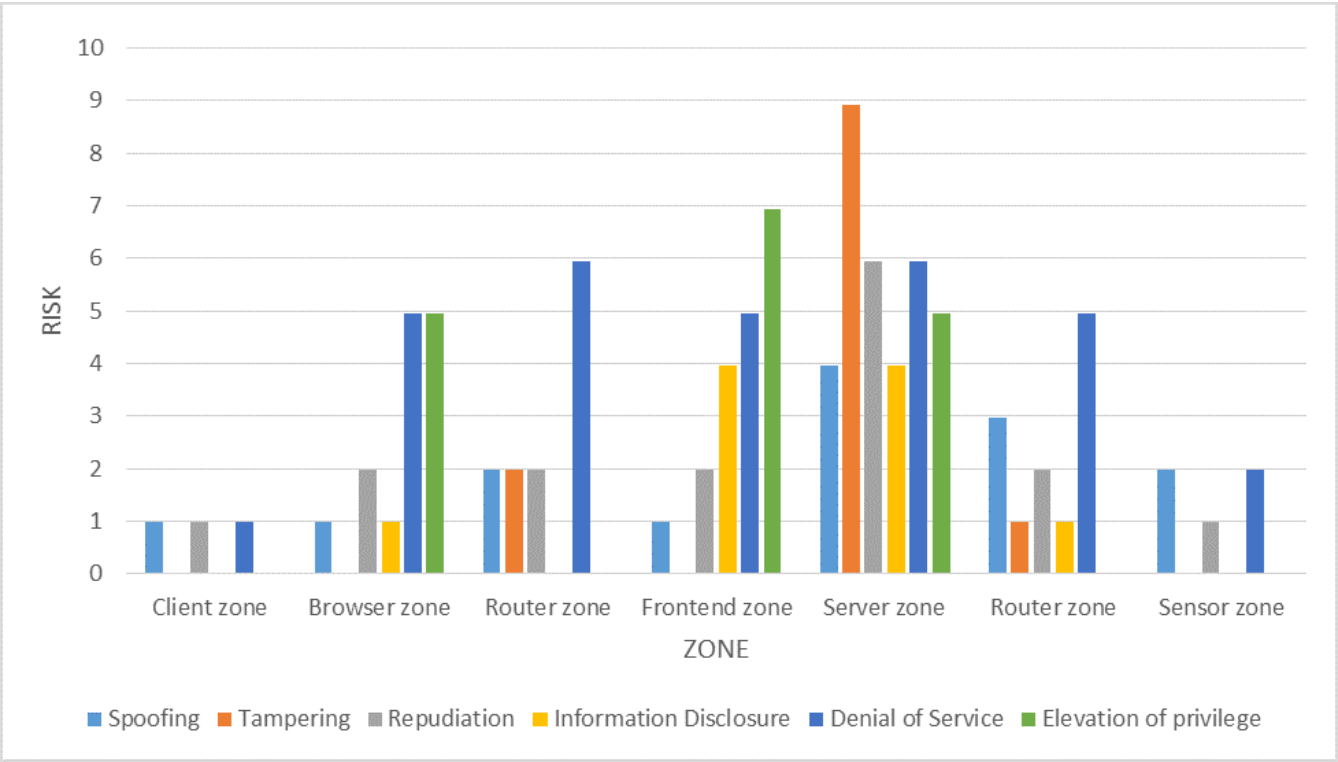

Figure 8. STRIDE threats by zones

After identifying the threats, they were evaluated. Threat assessment was performed using the DREAD method, as mentioned earlier, where each threat was evaluated individually and as a result the degree of risk for each threat was obtained. Table I presents the risk percentages for the relationships between the elements of the system and presents the sum of the risks for each identified zone of the system. Given that these data are combined with the data from the Figure 8, we can see that again the most vulnerable server zone is with as much as 28.71% of high-risk threats. The threats that are the most prevalent in this zone are from the category of interference, followed by rejection and DoS.

After presenting the statistics, we approached the best practices of addressing these threats. For each threat, there are countermeasures that have proven to be the most effective so far. The ones presented in Table II are motivated by the work given in [19].

5. CONCLUSION

This article identifies security threats and challenges for AAL WSN-based system. It is very important to include the security aspect in every stage of system development so that the system does not have many problems in the future. Throughout this paper, in addition to the process of the threat modelling, the statistical results are discussed. It is important to address these types of systems from security perspective, since due to rapid population ageing, which implies more health-related issues, the assistance will be needed in order to take good care of disabled and older adults. Taking into account the work force shortage in health sector, having systems like this for help is of great importance.

In order to successfully identify threats and analyse the security issues to this AAL system, we used the threat modelling process, STRIDE-based MTMT tool and

Table I: Risk level and percentage by zone

Zones	Relations	High risk		Medium risk	
		%	Sum	%	Sum
Client zone	Browser - Client	1.98	1.98	0.99	0.99
Browser zone	Client - Browser	2.97	6.9	2.97	6.93
	Router – Browser	3.96		3.96	
Router zone	Browser – Router	3.96	7.92	1.98	3.96
	Frontend – Router	3.96		1.98	
Frontend zone	Router – Frontend	2.97	10.89	4.95	7.92
	Within the zone	3.96		0	
	Server – Frontend	3.96		2.97	
Server zone	Frontend – Server	6.93	28.71	0.99	4.95
	Within the zone	12.87		1.98	
	Router – Server	8.91		1.98	
Router zone	Server – Router	3.96	6.93	2.97	4.95
	Sensor – Router	2.97		1.98	
Sensor zone	Router - Sensor	2.97	2.97	1.98	1.98

Table II: Countermeasures for STRIDE threats [19]

STRIDE	Countermeasures (Best Practices)
Spoofing	Strong authentication
Encryption	
Cryptographic protocols	
Tampering	Strong authorization
Hash and data signing	
Secure communication links	
Repudiation	Secure audit pathways
Information Disclosure	Strong authorization
Encryption	
Secure communication connections	
Denial of Service	Input condition check and filtering, use damping techniques
Elevation of Privilege	Least Privilege Principle

DREAD method for assessment of threats. The process identified 99 threats for the considered system. The most represented class of threats is DoS (30). This class of threats characterized the HTTPS relations the most, although the zones with these relations do not belong to the zones with the highest risk. The zone with the highest percentage of risk is the server zone, where SQL interactions are most represented. In SQL interactions, the most common threat category is interference (6). After the server zone, it is very important to pay attention to the frontend zone in which HTTPS interactions are exclusively present.

Threats are found to be high-risk (68.33%) and medium-risk (31.68%). This is understandable due to the fact that in this system if the security threats are exploited it may lead to loss of data and lives, as well as injuries. Following the results presented in this paper, countermeasures for threats should be defined and then the appropriate countermeasures should be applied. The results will contribute to protecting the security of the system as a final product and will reduce the possibility of exploiting system vulnerabilities.

It is important to note that we did not work on the concrete system, but used the architecture and functionalities of AmiCare system as a basis and an example for conducting the threat modelling process. The results obtained from this analysis may be used for the upgrade of the concrete system, but also in the context of improved development of other similar systems as well.

For future research, it is possible to analyse the architecture in more detail (using more detailed diagrams). Also, for the planned system improvements related to the Cloud platform, it is necessary to analyse all the advantages that this improvement brings in order to strive for the realization of improvements.

REFERENCES

[1] S. Baraković, et al.: Quality of Life Framework for Personalised Ageing: A Systematic Review of ICT Solutions, Electronics, 17, 2940, 2020

[2] A.L. Bleda, et al.: AmiCare: Ambient Intelligent and Assistive System for Caregivers Support, 16th International Conference on Embedded and Ubiquitous Computing, 2018

[3] J. Kulović, S. Baraković, J. Baraković Husić: Analysis of Threats for Web of Things (WoT) System, Bosanskohercegovačka elektrotehnika, 14:19-26, 2020

[4] A. Hajrić, T. Smaka, S. Baraković, J. Baraković Husić: Methods, Methodologies, and Tools for Threat Modeling with Case Study, Telfor Journal, 12(1): 56-61, 2020

[5] J.D. Meier, A. Mackman, B. Wastell: Threat Modeling Web Applications, Microsoft Corporation, 2005, Available at: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648006(v=pandp.10)?redirectedfrom=MSDN .

[6] A. Shostack: Threat Modeling: Designing for Security, John Wiley & Sons, Inc., 2014

[7] T. Agarwal: Wireless Sensor Network Architecture and Its Applications, ELPROCUS, 2016, Available at: https://www.elprocus.com/architecture-of-wireless-sensor-network-and-applications/.

[8] L. Banjanović-Mehmedović: Bežične senzorske mreže, University in Tuzla, 2009

[9] M. Angel, E. Villegas, S. Y. Tang, Y. Qian: Wireless Sensor Network Communication Architecture for Wide-Area Large Scale Soil Moisture Estimation and Wetlands Monitoring, WALSAIP Research Project, Technical Report TR-NCIG-0501

[10] B. Radenković, et al.: Internet inteligentnih uređaja, University of Belgrade, 2017

[11] Silicon Laboratories: The Evolution of Wireless Sensor Networks, Report, 2013

[12] S. Baraković, et al.: Security Issues in Wireless Networks: An Overview, Proceedings of the 11th International Symposium on Telecommunications, (BIHTEL 2016), Sarajevo, Bosnia and Herzegovina, 2016

[13] J. Fruhlinger: Threat Modeling Explained: A Process for Anticipating Cyber Attacks, 2020. Available at: https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html.

[14] Centar informacijske sigurnosti (CIS): Modeliranje sigurnosnih prijetnji (Threat modeling), 2012, Available at: https://www.cis.hr/files/dokumenti/CIS-DOC-2012-05-049.pdf.

[15] Microsoft Corporation: Threat Modeling: Microsoft Threat Modeling Tool, Available at: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling.

[16] T. Dervišević, S. Baraković, J. Baraković Husić: Case Study: Security of System for Remote Management of Windows, Bosanskohercegovačka elektrotehnika, 14: 4-11, 2020

[17] H. Mahmood: Application Threat Modeling using DREAD and STRIDE, Infosec Blog, 2017, Available at: https://haiderm.com/application-threat-modeling-using-dread-and-stride/.

[18] N. Shevchenko: Threat Modeling: 12 Available Methods, 2018. Available at: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/.

[19] M. Abomhara, G.M. Goein, M. Gerdes: A STRIDE-Based Threat Model for Telehealth Systems, Norsk Informasjonssikkerhetskonferanse (NISK), 2015

BIOGRAPHY

Nejla Popaja has graduated at the Faculty of Traffic and Communication, University of Sarajevo, Computer and information technologies, and received a Bachelor's degree in 2018. In the same year, she enrolled in a Master's program at the same faculty. Along with the Master's program she graduated from the CISCO academy, and in the last semester she was a participant in the Erasmus + student exchange in Spain. She completed her studies in 2021 when she has received a Master's degree.

Sabina Baraković is an Associate Professor at the University of Sarajevo. She is a co-founder of a research laboratory Little Mama Labs and an expert adviser at the Ministry of Security of Bosnia and Herzegovina. She is/was principal investigator on many national and international projects (Horizon2020, NATO, ITU, Erasmus+, CoE, OSCE, etc.) and has co-operators throughout the world (e.g., EU member countries, SEE region countries, etc.). She participates in the following COST actions CA19136 and CA16226. Her research interests include multidimensional QoE modelling of multimedia, mobile Web-based applications, and unified communications, QoS/QoE/QoL management, cybersecurity, and threat modelling in smart environments.

Jasmina Baraković Husić is an Associate Professor at the Faculty of Electrical Engineering, University of Sarajevo. She is employed by BH Telecom, Joint Stock Company, Sarajevo as a specialist in the Department for Planning and Development of Technologies and Services. She is co-founder of a research laboratory Little Mama Labs. She is/was principal investigator on many national and international projects (NATO, Erasmus+, Ministry of Education, RAI, etc.) and has co-operators throughout the world (e.g., EU member countries, SEE region countries, etc.). She participates in the following COST actions CA19136 and CA16226. Her research interests include variety of topics in networked multimedia services, QoS/QoE/QoL management, 5G-IoT communications.