

Review scientific paper/Pregledni naučni rad

ANALYSIS OF THREATS FOR WEB OF THINGS (WoT) SYSTEM

ANALIZA PRIJETNJI ZA SISTEM WEB-A STVARI

Jasmina Kulović¹, Sabina Baraković^{1,2}, Jasmina Baraković Husić¹

Abstract: The Web of Things (WoT) emerges from applying Web technologies to the Internet of Things (IoT) to access information and services of physical objects. These systems are likely to characterize the future of digital environment and they put certain security issues in the story. In order to help detect potential threats to WoT-system that is being built and designed, it is advisory to implement a threat modelling process. 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 and is a process best implemented at the system design stage. In this paper, we will analyse the threats for WoT-based door management system by using Microsoft Threat Modeling Tool (MTMT) in order to identify potential threats for this system in design phase. Obtained results justified the use of threat modelling in the design phase given that we have identified in total 89 threats, with Elevation of privilege and Denial of Service (DoS) being the most prominent ones. Those threats are characterized as high and medium risk ones.

Keywords: attack, Internet of Things, MTMT, threat, vulnerability, Web of Things

Sažetak: Web stvari (eng. Web of Things, WoT) proizlazi iz primjene web tehnologija na Internet stvari (eng. Internet of Things, IoT) za pristup informacijama i uslugama fizičkih objekata. Ti sistemi karakteriziraju budućnost digitalnog okruženja i stavljaju u priču određene sigurnosne probleme. Da bi se pomoglo otkrivanju potencijalnih prijetnji WoT sistemu koji se gradi i dizajnira, savjetuje se provođenje postupka modeliranja prijetnji. Modeliranje prijetnji je inženjerska tehnika koja se može koristiti za prepoznavanje prijetnji, napada, ranjivosti i odgovarajućih mjera suprostavljanja u kontekstu određene aplikacije i predstavlja proces koji se najbolje implementira u fazi dizajniranja sistema. U ovom radu se analiziraju prijetnje za sistem upravljanja vratima zasnovanim na WoT-u pomoću Microsoftovog alata za modeliranje pretnji (MTMT) kako bi se identifikovale potencijalne prijetnje ovom sistemu u fazi dizajna. Dobijeni rezultati opravdali su upotrebu modeliranja prijetnji u fazi dizajniranja s obzirom na to da je identificirano ukupno 89 prijetnji, pri čemu je najistaknutija bila Povećanje privilegija i Odbijanje usluga (eng. Denial of Service, DoS). Te su prijetnje također okarakterizirane kao prijetnje visokog i srednjeg rizika.

Ključne riječi: napad, Internet stvari, MTMT, prijetnja, ranjivost, web stvari

INTRODUCTION

When designing a system, it is important to know possible threats to it and incorporate adequate measures to avoid them. In fact, taking care of security is one of the most prominent challenges nowadays [1]. The ability to protect a system also makes it safer to operate. If there is an attack on a system, this attack can lead to bigger consequences in a form of disclosure of confidential data, disclosure of information, crashing of a system itself, unauthorized use of the same, etc. Recent security research suggests that most companies have unprotected data and poor cyber security practices in place, making them vulnerable to data loss [2]. Also, the fact is that our data is being more frequently transmitted via wireless mobile

networks, which consequently leads to increased number of victims of illicit cyber-criminal activities which causes many losses, either in data, money, or lives [3].

To successfully fight the threats and malicious intents, it is important to identify, analyse and evaluate potential threats when designing a system. One of possible ways to perform this analysis is to create threat model for a system in design.

Therefore, this paper deals with the process of threat modelling for a door management system, a Web of Things (WoT) system in design. 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 [4]. It is a structured approach that is significantly more efficient and less costly than randomly applying security features, without really knowing which threat the feature describes. Applying such a bad random approach raises the problem of determining if the system or application is secure enough. For this reason, it is first and foremost to know and eval-

¹ University of Sarajevo, Bosnia and Herzegovina

² Ministry of Security of Bosnia and Herzegovina, Bosnia and Herzegovina

barakovic.sabina@gmail.com

Paper submitted: March 2020 Paper accepted: May 2020

uate the threats well in order to properly protect the system. Threat modelling is not a one-off process, it is closely linked and intertwined with the design and development stages of an application or system. Threat modelling helps finding problems in the initial design phase, that is, before any line of code is written. Therefore, the greatest value of threat modelling is when it is involved in the design phase, as the system is then most flexible to change in order to eliminate threats. Getting rid of threats in the beginning phase is much easier than adding countermeasures, testing them, and ensuring they stay up to date. It is more difficult to eliminate threats on a mature system since that requires more work and compromise compared to modelling in the initial phase.

The main aim of the paper is to analyse potential threats to WoT-based system in design in order to perform timely application of adequate measures. The structure of the paper is as follows: After the brief introduction, Section 1 explains the notions of Internet of Things (IoT) and WoT, and switch from the former to the latter. Section 2 provides details on basics of the security in WoT. Section 3 gives the description of the subject WoT door management system and analyses the threats to it by using the threat modelling process. Results analysis and discussion are contained in Section 4, while Section 5 concludes the paper.

1. FROM IOT TO WOT

The IoT represents a global network of devices and other items embedded with sensors, electronics, software and connectivity [5]. It may also be defined as an interconnected network of things/objects that are able to interact with each other and cooperate with other things/objects through wireless and wired connections in order to create new services/applications for the benefit of society [6]. It is closely related to smart devices that can connect to the Internet and be controlled using applications remotely. Smart things include smart devices, various sensors, computing resources, storage devices, customer communication devices, etc.

The term IoT is a concept that describes the idea of everyday physical objects which are connected to the Internet and can be identified with other devices. The term is closely identified with the Reduced Functional Device (RFD) as a method of communication, although it may include other sensor technologies, wireless technologies, or Quick Response (QR) codes. The IoT is significant because an object that can represent itself digitally becomes something greater than the object by itself. The object is no longer only related to the user, but is linked to the surrounding objects and database data [7].

Figure 1 shows the IoT architecture. Sensors together with actuators and appliances communicate with a gateway at the edge of the network. The gateway supports multiple communication protocols for interoperability with the end device and sends processed data

to the cloud. This device also adds a layer of security since it bridges the communication between the devices and outer world. The cloud essentially gives increase of availability, reliability and security, but at the same time it takes advantage of higher computation power and scalable architecture. The cloud then integrates with third party services, such as data visualization, smart home device management, user access or role management [5].

The IoT architecture is a system of many elements: sensors, protocols, movers, cloud services and layers. Given its complexity, there are 4 phases of IoT architecture. Such a number has been chosen to integrate these types of components permanently into a sophisticated and integrated network. In addition, layers of the IoT architecture are distinguished to determine system consistency:

- Client side;
- Server-side operators;
- The path of connecting customers and operators [8].

IoT helps people live and work smarter, as well as establish complete control over their lives. In addition to offering smart home automation devices, IoT is crucial to business. IoT enables companies to take a real-time look at how their companies' systems really work, providing insight into everything from machine performance to chain and logistics operations [9].

The benefits of IoT are reflected in the ability to access information from anywhere, anytime, and from different devices. The other benefits are the improvement of communication between connected devices and the faster transition of data packets over a connected network, which saves time and money.

Developing new platforms that enable communication between devices takes a lot of time. Time can be saved by using an existing platform, such as the World Wide Web (WWW), which introduced the WoT into the game.

The **WoT** emerges from applying Web technologies to the IoT to access information and services of physical objects. In WoT, each physical object possesses a digital counterpart, i.e., object or a thing [10]. It is a concept that describes a future where everyday objects are fully integrated with the web. A prerequisite for WoT is that abovementioned things have embedded computer systems that allow communication with the web. Such

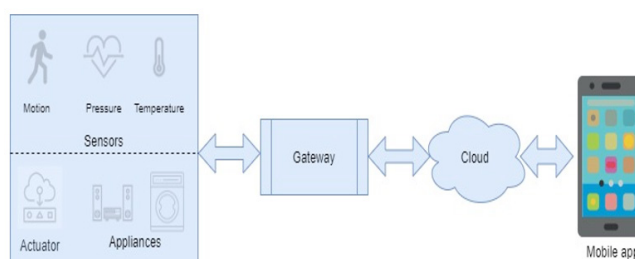


Figure 1: IoT mode

smart devices could communicate with each other using existing web standards. WoT is seen as a subset of the IoT and focuses on software standards and frameworks such as Representative State Transfer (REST) and Hyper Text Transfer Protocol (HTTP) to create applications and services that combine and communicate with various network devices.

In WoT, applications are integrated with physical objects with a known HTTP protocol and RESTful API (Application Programming Interface). This simplifies access to physical objects, allowing them to be used in web applications and merged with existing web resources [11].

WoT is created to enable interoperability across IoT platforms and application domains. WoT provides mechanisms to formally describe IoT interfaces so that IoT devices and services can communicate with each other, regardless of their underlying implementation, and across multiple network protocols. In addition, WoT offers a standardized way to define and program IoT behaviour [12].

WoT seeks to integrate itself into web networks of objects, things, systems and applications represented by IoT. Technically speaking, WoT can be seen as an application layer that is added over the network layer of the IoT. WoT provides access and control over IoT resources and applications using common web technologies [13].

The differences between IoT and WoT seem simple and easy to distinguish. However, the two concepts have far more complex differences, with each detail of IoT and WoT being made up of two very different entities, which have separate ideas, structure and usage. Despite their differences, IoT and WoT work together and will rely on each other to work seamlessly and efficiently.

2. SECURITY OF WoT

There are numerous (nearly a thousand) research studies and papers dealing with IoT security such as ones given in [14]-[22]. WoT does not introduce new security mechanisms over existing IoT security mechanisms. However, what matters is that it monitors functional requirements such as exposing, consuming and protocols. WoT security is defined by creating a threat model. A threat model is used to more easily identify the goals and vulnerabilities of the system, that is to say, it allows users to more easily identify and/or protect themselves against a threat. It is impossible to define a single threat model that will fit each threat scenario, but it is possible to define a framework by which it is possible to create a threat model that will make it easier to identify threats and help with WoT security. The frame is reflected through [23]:

- security stakeholders,
- security- relevant assets,
- possible attackers,
- attack surface,
- threats for WoT.

2.1. Security stakeholders

There are five primary WoT stakeholders, each with its own description and security goals. The first WoT stakeholder is device manufacturer. It is a producer of the hardware device and implements the WoT on the runtime device. The security goal is to meet the security requirements of system users and system providers. Second stakeholder is a system provider or system installer. It uses devices to build various WoT end solutions specific to particular WoT use cases. The security goals are to allow the system to be robust and resilient to DoS (Denial of Service) attacks, to hide proprietary scripts and other data from other parties.

The primary feature of system user as a third stakeholder is the need to use the WoT system to obtain some functionality. The security goal has the role of providing access to user data based on role, type of access and contrast. The fourth stakeholder is a system owner. A WoT system might have several independent system owners. Each system owner has their own set of provisioned certificates and credentials. The security goal is to provide full control over your own provisioned security credentials, including integrity and confidentiality. The last stakeholder is a system maintainer, who is an optional stakeholder and who administers a WoT system on behalf of a system provider or a system user. As a security goal it provides minimal access to the data of other stakeholders [23].

2.2. Security - relevant assets

Assets are a very important item in WoT, and their identification contributes to better protection. Assets are generally confidential information, such as customer information, databases, websites, etc. In terms of WoT security, the following assets are important [23]:

- Thing Description (TD) – the integrity of TDs is crucial for the correct operation of a WoT system. Some contents of TDs might be privacy sensitive and therefore should not be shared without a specific need;
- System User Data – includes all data that is produced or processed by elements of a WoT system. It can be highly privacy sensitive and confidential;
- System Provider Data – includes both WoT scripts and any WoT configuration data produced and owned by a system provider;
- WoT Thing Resources and WoT Infrastructure Resources – should only be used for legitimate purposes and be available when required;
- WoT Controlled Environment – WoT devices with actuator capabilities are able to affect the physical environment around them, and it can imply a possible safety risk;
- WoT Behaviour Metrics – indirectly transmitted information that represents measurements of a WoT system's behaviour from which other information can be inferred, such as user presence.

2.3. Possible attackers

Threats are dangers that lead to system malfunction. They also exploit system vulnerabilities to cause damage. The weak points of a system represent its vulnerability and make a system vulnerable to attack. The attacker exploits the vulnerability of the system and attacks the system itself. The basic steps in the attacker methodology are shown in Figure 2.

According to [23], attackers can be:

- Network attacker;
- Malicious Authorized User;
- Malicious Unauthorized User;
- Malware Developer.

Attack surfaces

In order to define WoT attack surfaces in a correct fashion we need to determine the system's trust model as well as execution context boundaries. Script Execution Boundary, WoT Runtime Instance Execution Boundary, WoT Execution Boundary are just some of the boundaries that are required in WoT security [23].

2.4. Threats for WoT

The threats that applications may face are different, but for the most part they can be categorized based on the attack purpose. Knowledge of threat categories helps organizing a security strategy that will help in response to threats.

Threats to WoT are categorized as the following [23]:

- WoT Protocol Binding Threat;
- WoT Interface Threat;
- WoT DoS Threat;
- WoT Communication Threat;
- WoT Script Management Interface Threat;
- WoT Untrusted Script Threat.

Security examples are constantly evolving. However, in order to successfully identify threats, it is necessary to determine the vulnerability of the system through a detailed threat model.

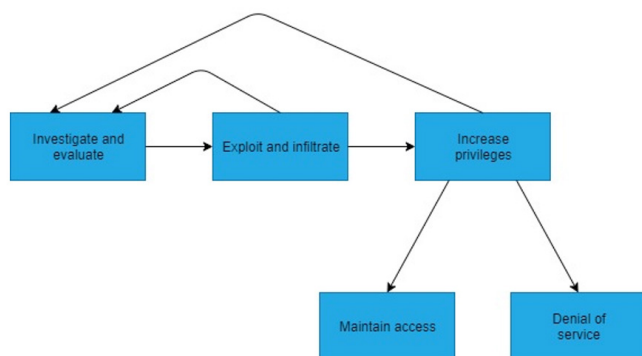


Figure 2: Steps in attacker methodology [24]

3. ANALYSIS OF THREATS FOR DOOR MANAGEMENT SYSTEM

3.1. Threat modelling basics

Threat models are helpful in identifying targets and vulnerabilities of the system. They are also used when users want to repair system vulnerabilities and improve system security. System modelling is used to better understand how certain systems work and how to improve them. Systematic threat modelling is used to systematically identify and assess the threats that affect the system. Different approaches are used for threat modelling, and the two most used approaches for threat modelling are the STRIDE methodology and DREAD rating method.

The acronym STRIDE stands for [25]:

- **S**poofing: The conversion attempts to access the system using a false identity;
- **T**ampering: Tampering is an unauthorized change of information;
- **R**epudiation: By refusing, the user may deny that the action or transaction performed was insufficient;
- **I**nformation disclosure: Information disclosure constitutes unwanted exposure of information that are private;
- **D**oS: Denial of service is an action on a system or application that makes it unavailable;
- **E**levation of privilege: Elevation of privilege means that a user with less privilege, takes the identity of a user who has higher privileges to gain more privileged access to the application.

The DREAD is an acronym created by the initial letter of each category, which are [26]:

- **D**amage potential;
- **R**eproducibility;
- **E**xploitability;
- **A**ffected users;
- **D**iscoverability.

Potential damage determines how much damage to the system can occur when vulnerability is exploited. Reproducibility defines ease of attack and repetition of attacks. Exploitability defines the ease of abandoning an attack and how much expertise it takes for an attacker to launch an attack. Affected users indicate the number of end users affected by exploitation. Discoverability determines the ease of attacking a system or detecting vulnerabilities.

For each assessed threat, a risk item is added that can be:

- High risk;
- Medium risk;
- Low risk.

In addition to these two approaches, there are many different approaches to modelling the threat, and they all depend on the type of application or system they are used for. The following terms are used to describe the different approaches [27]:

- Asset-focused threat modelling;
- Attacker-focused threat modelling;
- Software-focused threat modelling.

Like any process, the threat modelling process has its basic steps that can be used for developing applications or applications that need further improvement [28]:

- Identification of assets;
- Creating architecture reviews;
- Decomposition of the application;
- Identification of threats;
- Documentation of threats;
- Threat Assessment.

The abovementioned procedure for creating threat model will be applied to WoT-based door management system. Although there are many tools that can be utilized for automated threat modelling, we use Microsoft Threat Modeling Tool (MTMT).

MTMT is a freeware tool that helps to identify threats in the software design phase. This tool is a key element of Microsoft SDL. MTMT enables potential security issues to be identified and mitigated early, when it is relatively straightforward and cost-effective to address. As a result, there is a decrease in overall development costs. The MTMT enables any developer or software architect to:

- Communicate about the security design of their systems;
- Analyse those designs for potential security issues using a proven methodology;
- Suggest and manage mitigations for security issues [29].

The latest version used is the Microsoft Threat Modeling Tool 2016. MTMT uses Data Flow Diagram (DFD) to model threats, and one of its biggest drawbacks is its inability to run on any computer system other than Microsoft. The tool works on a drag and drop principle to create a DFD for each use case or function. This diagram is then analysed using the STRIDE model to identify possible threats. Six major model creation facilities are also available: process, multiple processes, external interactor, database, data flow, and confidence boundaries [30].

3.2. A WoT-based Door Management System

The door management system, whether in a home or business environment, either through direct access or through a network gateway, allows remote verification of whether a door (lock) in an object is locked or unlocked. The controls (smartphone, tablet, laptop, desktop computer, etc.) and door (lock) communicate using web technologies. The door (lock) has a locking sensor.

Figure 3 shows the physical layout of door management system elements. Designed architecture is divided into several zones that ultimately form one whole.

The principle of operation is as follows: the user opens a browser and a web page to access the WoT device, i.e. door, which is a web server. The website must be authenticated for the device to know that it is being communicated by an authorized user. After granted access, the user is shown a door map of a specific object. The

doors when unlocked are painted green and when they are locked red. There is a switch next to each door on the display. Clicking the switch changes the status of the lock from unlocked to locked and vice versa, and this moment of change is recorded with a timestamp. The system also allows scheduling when the lock should be unlocked and when locked.

The first zone is the User zone from which the user sends a request to access the system. The request for access to the system is sent via a User browser that is connected to the User zone by an Internet connection (2G-4G, Wireless Fidelity (Wi-Fi)).

The next zone is the WoT device zone, where the Wi-Fi router connects to the User's browser, also by an Internet connection. The Wi-Fi router is further connected via Bluetooth to a WoT device, after which authentication and connection to the web server is performed.

The web server connects to two zones, the Administrator zone and the Door zone. Administrator connects to the web server through the Administrator browser, while the Door map connects to the web server via Bluetooth. The door map is connected by wire to a locking sensor.

For better understanding and analysis of system vulnerabilities, it is necessary to decompose the architecture into smaller parts by identifying trust boundaries.

There are several trust-based boundaries in a door management system. The Internet Trust Limit is the first trust boundary of a door management system. The boundary is between the end user and the browser. After authentication, there is another trust boundary with the web server. The third boundary of trust is between the web server and the user's browser.

Nine connections are shown on the MTMT diagram of the door management system architecture. The first connection is displayed between the user and his browser. User sends a web server access request through the browser. Connection between the End User and the User Browser is made via Wi-Fi or 2G-4G. There is also Internet trust boundary in this connection.

The following connection is a two-way link between the User's Browser and a Wi-Fi router that allows you to connect to the Internet. The Wi-Fi router further connects to the Web site, and it is also a two-way link. Another connection that leads to authentication is a connection between Wi-Fi router and Web site. After authentication, the web server is accessed. The connection is a two-way Bluetooth connection, and a trust boundary is passed to the web server. Connection between the web server and the Admin Browser is two-way, achieved through 2G-4G or Wi-Fi, and goes over the trust boundary.

The following connection is between the web server and the Door Map. The door map represents the database that the user accesses in order to have access to all the

The answers to the questions are given in the form of an estimate, then they are assigned values (high, medium, low). The values represent the severity level and are expressed in numbers: 1 - low, 2 - medium, 3 - high. After that, all ratings are summed up and a final rating for a specific threat is obtained, ranging from 5 to 15. The scale determines the risk:

- High risk: 12-15;
- Medium risk: 8-11;
- Low risk: 5-7.

Table II shows the number of occurrences of a given attack level within the STRIDE attack classification. When it comes to high-risk threats, we can see that most of these threats fall into the category of DoS, although spoofing and Elevation of privilege are not negligible. Then, most medium-risk threats fall into Elevation of privilege and DoS categories. These categories are the ones that threaten

this system the most as well. Finally, when it comes to low-risk threats, the highest number also come from Elevation of privilege and DoS categories.

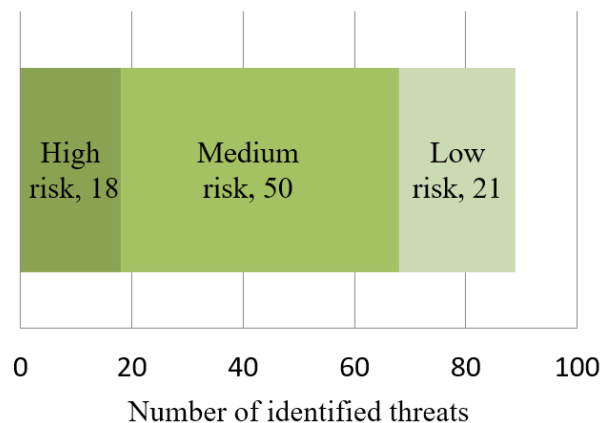


Figure 5: The degree of risk of threats by the DREAD method

Table I: DREAD evaluation of threats

Threats	D	R	E	A	D	Total	Mark
Relation: User Browser - Wi-Fi router							
Spoofing of Source Data Store Wi-Fi router	3	3	2	1	3	12	High
Relation: User - User browser							
Data Flow HTTPS Is Potentially Interrupted	2	2	1	3	1	9	Medium
Relation: Administrator Browser- Web Server							
Cross Site Request Forgery	3	2	3	3	1	12	High
Relation: Authentication – Web site							
Elevation Using Impersonation	3	2	2	2	2	11	Medium
Relation: Web site - Wi-Fi router							
Weak Access Control for a Resource	3	2	2	2	3	12	High
Relation: User Browser - Wi-Fi router							
Data Store Inaccessible	2	1	1	2	1	7	Low

Legend: HTTPS (HyperText Transfer Protocol Secure), Wi-Fi (Wireless Fidelity).

Table II: Risk level per STRIDE category

Threats	High risk rating	Medium risk rating	Low risk rating
Spoofing	5	8	1
Tempering	0	6	0
Repudiation	2	4	4
Information disclosure	1	1	1
Denial of service	6	15	7
Elevation of privilege	4	16	8

5. CONCLUSION

The concept of the door management system, analysed in this paper, is based on WoT. WoT describes a future where everyday objects are fully integrated within the Web. Data transmission in the WoT concept is done through a public network, which is an aggravating security issue.

In order to successfully identify threats to a WoT-based system being designed (future systems), it is advisable to create a threat model whose further analysis can identify the greatest vulnerabilities of the system. For more accurate results, it is necessary to know the system, its elements, modes, technologies, etc. Therefore, in this paper, security threats of WoT-based system for distance management of doors were identified by creating the threat model in MTMT tool.

The process of identifying threats in the MTMT tool, which is based on STRIDE methodology, resulted with 89 different threats. Specifically, for this system, the biggest threat is the Elevation of privilege (32.58%), then the DoS (28%). By using DREAD approach, most threats are assessed to be medium risk (50), which means that they are not prioritized but should not be ignored. Medium-risk threats mainly relate to DoS attacks and attempts to access false identities. With regard to high-risk threats (18), some of the threats that can be extracted are: Bluetooth data flow is potentially interrupted, web server process memory is compromised, data flow through the wire is potentially interrupted, end-user fraud by an external entity, etc. High-risk attacks are reflected in DoS and Elevation of privilege. Low-risk threats (21), although not a major threat to the system, need to be addressed before they receive higher-risk ratings and they are most reflected also in Elevation of privilege and DoS attacks. In order to sum, the application of threat modelling process to WoT-based system is one useful step given that the identification of potential threats contribute to the system design and security.

As for the future research for door management system, first of all it is necessary to consider the architecture in detail, then it is necessary to build a higher-level architecture compared to the one observed in this paper. More importantly, it is necessary to include the conclusions of this paper in the design of the system and its further developments. These finding and conclusion may be very useful in design phase of similar systems as well.

REFERENCES

- [1] R. Shahan: Azure Internet of Things: Internet of Things (IoT) security architecture, Microsoft Azure, 2018, Available at: <https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture>
- [2] R. Sobers: 110 Must-Know Cybersecurity Statistics for 2020, Inside Out Security Blog, 2020, Available at: <https://www.varonis.com/blog/cybersecurity-statistics/>
- [3] S. Baraković, et al.: Security Issues in Wireless Networks: An Overview, Proceedings of the 11th International Symposium on Telecommunications, (BIH-TEL 2016), Sarajevo, Bosnia and Herzegovina, 2016
- [4] 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](https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648006(v=pandp.10)?redirectedfrom=MSDN)
- [5] D. Mocri, Y. Chen, P. Musilek: IoT-based Smart Homes: A Review of System Architecture, Software, Communications, Privacy and Security. Internet of Things 1-2: pp. 81-98, 2018
- [6] E. Cero, J. Baraković Husić, S. Baraković: IoT's tiny steps towards 5G: Telco's Perspective, Symmetry, vol. 9, no. 10, pp. 213, 2017
- [7] Technopedia: Internet of Things (IoT), 2019, Available at: <https://www.techopedia.com/definition/28247/internet-of-things-iot>
- [8] P. Stokes, 4 stages of IoT architecture, Data Driven Investor, 2018, Available at: <https://medium.com/datadriveninvestor/4-stages-of-iot-architecture-explained-in-simple-words-b2ea8b4f777f>
- [9] F. Allhoff, A. Henschke: The Internet of Things: Foundational Ethical Issues. Internet of Things 1-2 (2018): pp. 55-66, 2018
- [10] N.K. Tran, Q.Z. Sheng, M.A. Babar, L. Yao: Searching The Web of Things: State of the Art, Challenges, and Solutions, ACM Computer Survey 50, 4, 2017
- [11] S. Duquennoy, G. Grimaud, J.J. Vandewalle: The Web of Things: Interconnecting Devices with High Usability and Performance, International Conference on Embedded Software and Systems, 2009. Available at: <https://ieeexplore.ieee.org/abstract/document/5066664>
- [12] M. Kovatsch, R. Matsukura, M. Lagally, T. Kawaguchi, K. Toumura, K. Kajimoto: WoT architecture, W3C, 2020, Available at: <https://www.w3.org/TR/wot-architecture/>
- [13] S. Satapathy: Threat Modeling in Web Applications, Department of Computer Science and Engineering, India, 2014
- [14] Y.H. Hwang: IoT Security & Privacy: Threats and Challenges, Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security, Singapore, 2015
- [15] Abomhara, et al.: Security and privacy in the Internet of Things: Current status and open issues, Proceedings of International Conference on Privacy and Security in Mobile Systems, Aalborg, Denmark, 2014
- [16] C. Atac, S. Akleylek: A Survey on Security Threats and Solutions in the Age of IoT, European Journal of Science and Technology, 2019, Available at: <https://dergipark.org.tr/tr/download/article-file/661535>
- [17] M. Silaghi, A. Maraj, T. Atkinson: The Device War – The War Between IOT Brands In A Household, Florida Institute of Tehnology, 2018, Available at: https://www.researchgate.net/publication/330035067_The_Device_War_-_The_War_Between_IOT_Brands_In_A_Household
- [18] M. Frustaci, P. Pasquale, G. Aloï, G. Fortino: Evaluating critical security issues of the IoT world: Present and Future challenges, IEEE Internet of Things Journal, vol. 5, no. 4, 2017, Available at: https://www.researchgate.net/publication/320680302_Evaluating_critical_security_issues_of_the_IoT_world_Present_and_Future_challenges
- [19] K. Tabassum, A. Ibrahim, S. A. El Rahman: Security Issues and Challenges in IoT, Proceedings of the International Conference on Computer and Information Sciences (ICCIS), 2019, Available at: https://www.researchgate.net/publication/333158390_Security_Issues_and_Challenges_in_IoT
- [20] A. Mawgoud, N. E. M. Khalifa, M. H. N. Taha: Security Threats of Social Internet of Things in the Higher Education Environment, Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications, 2020, Available at: https://www.researchgate.net/publication/334655853_Security_Threats_of_Social_Internet_of_Things_in_the_Higher_Education_Environment

- [21] D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac: Internet of things: Vision, applications and research challenges, *Ad Hoc Networks*, 2012, Available at: <https://www.sciencedirect.com/science/article/abs/pii/S1570870512000674>
- [22] The Cyber Security Challenges in the IoT Era, European Commission, 2019, Available at: <https://cordis.europa.eu/event/id/147582-the-cyber-security-challenges-in-the-iot-era>
- [23] E. Reshetova, M. McCool: Web of Things (WoT) Security and Privacy Guidelines, W3C, 2019, Available at: <https://www.w3.org/TR/wot-security/>
- [24] J.D. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla, A. Murukan: Improving Web Application Security: Threats and Countermeasures, Microsoft Corporation, 2003, Available at: [https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644\(v=pandp.10\)](https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10))
- [25] A. Shostack: Threat Modeling: Designing for Security. John Wiley & Sons, Inc., 2014
- [26] H. Mahmood: Application Threat Modeling using DREAD and STRIDE, Infosec Blog, 2017, Available at: <https://haiderm.com/application-threat-modeling-using-dread-and-stride/>
- [27] D. Eng: Integrated Threat Modelling, The University of Oslo, 2017, Available at: <https://www.duo.uio.no/bitstream/handle/10852/55699/dae-thesis.pdf?sequence=1&isAllowed=y>
- [28] Centar informacijske sigurnosti (CIS): Modeliranje sigurnosnih prijetnji (Threat modeling), 2012, Available at: <https://www.cis.hr/files/dokumenti/CIS-DOC-2012-05-049.pdf>
- [29] Microsoft Corporation: Threat Modeling: Microsoft Threat Modeling Tool, Available at: <https://www.microsoft.com/en-us/securityengineering/sdl/threat-modeling>
- [30] S. Kadhivelan Prakash, A. Söderberg-Rivkin: Threat Modelling and Risk Assessment Within Vehicular Systems, Chalmers University of Technology, University of Gothenburg, Department of Computer Science and Engineering Göteborg, Sweden, 2014, Available at: <http://publications.lib.chalmers.se/records/fulltext/202917/202917.pdf>

BIOGRAPHY

Jasmina Kulović, received her B.Sc. and M.Sc. degrees in communication technologies from the Faculty of traffic and communication, University of Sarajevo (Bosnia and Herzegovina), in 2017 and 2019, respectively. During her education she actively participated in the development of various projects.

Sabina Baraković is an Associate Professor at the University of Sarajevo and American University in Bosnia and Herzegovina. 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, Qatar, etc.) Her research interests include multidimensional QoE modeling of multimedia, mobile Web-based applications, and unified communications, QoS/QoE/QoL management, cybersecurity and threat modelling in smart environments and IoT/WoT.

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 IC1304, IC1303 and CA16226. Her research interests include variety of topics in networked multimedia services, QoS/QoE/QoL management, 5G-IoT communications.