

Original scientific paper/Izvorni naučni rad

CASE STUDY: SECURITY OF SYSTEM FOR REMOTE MANAGEMENT OF WINDOWS

STUDIJA SLUČAJA: SIGURNOST SISTEMA ZA DALJINSKO UPRAVLJANJE PROZORIMA

Tarik Dervišević^{1,2}, Sabina Baraković^{2,3}, Jasmina Baraković Husić²

Abstract: In the process of designing and forming each system, it is necessary to identify potential vulnerabilities and threats to that system and to include appropriate countermeasures. The process that helps to find the problem in the first phase of design is called threat modeling. Threat modeling is based on the idea that every system has valuable resources that need to be protected. These resources have certain weak points that internal or external threats can use to harm them, while there are as well countermeasures used to mitigate them. Therefore, this paper analyses the security of a Web of Things (WoT)-based system for remote management of windows, which is in the design stage by using a threat modeling approach based on STRIDE and DREAD. The results obtained through Microsoft Threat Modeling Tool (MTMT) justified the use of threat modeling in the design phase given that we have identified in total 118 threats, with Elevation of privilege class of threats being the most prominent ones. The Information disclosure threats are found to be the ones characterized as medium and low risk ones, while the most represented high-risk threats again come from the Elevation of privilege class of threats.

Keywords: application security, cyber-security, DREAD, human factor, MTMT, network security, STRIDE

Sažetak: Prilikom dizajniranja sistema, važno je razumjeti potencijalne prijetnje prema tom sistemu i uključiti odgovarajuće protumjere dok se isti dizajnira. Proces koji se koristi za pronalaženje problema u početnoj fazi dizajna je modelovanje prijetnji. Modelovanje prijetnji se zasniva na ideji da svaki sistem ima vrijedne resurse koje je potrebno zaštititi. Ti resursi imaju određene slabe tačke koje unutrašnje ili vanjske prijetnje mogu iskoristiti da im naštetite, ali postoje i odgovarajući mehanizmi odbrane koji ih ublažavaju. Stoga, ovaj rad, u fazi dizajna analizira sigurnost sistema za daljinsko upravljanje prozorima, temeljenog na Webu stvari (eng. Web of Things, WoT), pomoću pristupa modeliranja prijetnji na temelju STRIDE i DREAD. Rezultati dobiveni pomoću Microsoftovog alata za modeliranje prijetnji (eng. Microsoft Threat Modeling Tool, MTMT) opravdali su upotrebu modeliranja prijetnji u fazi dizajniranja. Identificirano je ukupno 118 prijetnji, pri čemu su prijetnje iz klase podizanje privilegija najistaknutije prijetnje. Prijetnje otkrivanjem informacija okarakterizirane su kao one prijetnje sa srednjim i niskim rizicima, dok najrizičnije prijetnje dolaze iz klase podizanja privilegija.

Ključne riječi: sigurnost aplikacija, kibernetička sigurnost, DREAD, ljudski factor, MTMT, mrežna sigurnost, STRIDE

INTRODUCTION

Cybersecurity challenges and issues are on the rise on a day-to-day basis [1]. This is a hot topic for organizations and businesses of all sizes across every industry. Recent trends and cybersecurity statistics reveal a great increase in hacked and breached data from sources that are increasingly common in a workplace, like mobile and Internet of Things (IoT) devices [1]. By raising the level of knowledge of Information Communication Technology (ICT), as well as developing solutions and possibilities of a computer networks and systems, the level of abuse has also risen. The fact is also that our data is being more frequently transmitted via wireless mobile networks which consequently leads to increased number of victims of illicit

cybercrime activities which causes many losses, either in data, money, or lives [2].

Some of the current trends in cybersecurity are related to the types of attacks, methods of prevention and affected industries. Other trends are related to finding new methods and technologies to [3]:

- Reducing cybersecurity vulnerabilities;
- Improving network security;
- Using of automation in cybersecurity;
- Increasing of data privacy and compliance; and
- Improving the collecting and analysis of data.

Cybersecurity trends which are related to the types of attack are:

- *Phishing attacks mediums are changing* [4]: Cybercriminals in 2019 didn't use only emails as a medium for phishing attacks (even though it is a still popular method for phishing attacks). Phishing attacks nowadays involves general Short Message Service (SMS) texting attacks ("smishing"), Social networks (Facebook, Twitter, Instagram, LinkedIn, etc.) and even phone calls with a live person ("vishing");

¹ Infobip, Bosnia nad Hercegovina,

² University of Sarajevo, Bosnia nad Hercegovina

³ Ministry of Security of Bosnia and Hercegovina
barakovic.sabina@gmail.com

Paper submitted: March 2020 Paper accepted: May 2020

- *Increased use of mobile devices by employees as a security vulnerability for the organization:* The mobility offered by mobile devices makes life more convenient. Mobile devices can be used for handling personal and business communications. Research from the RSA's 2019 Current State of Cybercrime whitepaper shows that 70% of fraudulent transactions originated from the mobile channel in 2018 [5]. Furthermore, fraud from mobile apps has increased 680% since 2015, making it a huge channel of opportunity for cybercrime. Considering all of this, it is understandable that this practice spells out concerns for businesses;
- *Attacks on local governments and enterprises via ransomware:* According to Malwarebytes research, the ransomware are on the rise for enterprises. From the fourth quarter 2018 to the first quarter of 2019, the ransomware was increased by 195%, respectively 500% from the first quarter of 2018 to the first quarter of 2019. Even governments aren't safe from ransomware. Cybersecurity trends show that besides enterprises, the governments are going to be increasingly common targets for ransomware [6];
- *Increasing emphasis on data privacy, sovereignty, and compliance:* Since the rollout of the European Union's General Data Protection Regulation (GDPR), many countries and industries have begun taking harder looks at their existing data privacy-related regulations in order to develop, pass, and implement new regulations that will ensure higher data security and privacy standards; and
- *Increasing investments in cybersecurity automation:* Automation is very important advantage in cybersecurity and this statement is confirmed by a recent Ponemon Institute survey of more than 1.400 ICT security practitioners. The survey shows that 79% of respondents either currently use 29% of automation tools and platforms within their organization or 50% of them plan to use within the next six months to three years. This movement towards the use of automation aims to reduce the burden on understaffed cybersecurity teams and increase efficiency [7].

Cybersecurity trends that are mentioned for 2019 are likely to carry over into 2020 [1]. However, three main trends for 2020 can be summarized as follows:

- *Cybersecurity spending will continue to increase:* Data from IDC show that global spending on cybersecurity solutions, such as hardware, software, and services, is anticipated to top \$103 billion in 2019. That's an estimated increase of 9.4% over 2018 and they also expect this rate of growth in 2020 [8]. The three industries that spent mostly on security solutions in 2019 are: banking, discrete manufacturing, and governments;
- *The growing impact of Artificial Intelligence (AI) and Machine Learning (ML) on cybersecurity:* ML and AI are developing cybersecurity as a whole and these areas are going to be more explored in 2020. Data from a Capgemini Research Institute [8] survey support the idea that AI is vital to an organization for help

in cybersecurity defense. 75% of surveyed executives reported that AI helps their organizations respond more quickly to breaches and 69% of the organizations reported that AI is necessary to respond to cyber-attacks. Data from Research and Markets report projected that the market for AI in cybersecurity is going to reach 38.2 billion by 2026 [8]; and

- *Cyber-attacks on utilities and public infrastructure will continue to increase:* Utilities and public infrastructure provide critical infrastructure for millions of people and governments around the world, but they often operate using old, outdated technologies that are not prepared to deal with major cybersecurity threats.

Taking into account all previously stated trends in cyberspace when it comes to its security, it is evident that it is important to incorporate security and privacy into the system design in the early stage in order to prevent insecurity in ICT domain. One of the manners to do that is to analyze security and vulnerabilities of systems through the threat modeling process.

Therefore, this paper aims to conduct the abovementioned modeling in order to analyze potential security threats to a specific ICT system. We will perform the case study analysis on the Web of Things (WoT) system for remote management of windows, which is in the design stage. The contribution of this research reflects in identification of threats, which can raise awareness on system security holes and be further incorporated in design of the subject system.

The structure of the paper is as follows: After the introductory part, Section 1 addresses the security of ICT systems, where the threat modeling process is described together with the segments important for security. Section 2 describes the system for remote management of windows and the conducted threat modeling process. Results analysis and discussion are given in Section 3, while Section 4 concludes the paper.

1. SECURITY OF ICT SYSTEMS

ICT systems are built using information and communication technologies in order to enable interconnecting of remote computer systems. Information technologies represent hardware and software, which allow access, downloading, organizing, manipulation, and information presentation. Communication technologies represent telecommunication equipment, which allows sending and receiving data.

Each ICT system consists of different segments that work together to achieve common goal. Security weaknesses of ICT system can be located in the next three segments, which will be addressed in more detail in the following text:

- Network segment;
- Application segment and
- Human segment.

1.1. Network Security

The safe network is as strong as the weakest layer. However, the data layer of the Open System Interconnection (OSI) model is considered as potentially the weakest layer. Organizations usually implement security solutions such as firewalls, Intrusion Prevention System (IPS), or Virtual Private Network (VPN). In that way, they protect elements from the network layer to the application layer of the OSI model. However, if the data layer is the target of the attack all other layers will be threatened as well.

Common attacks that target the data layer [9] and the best practices for avoiding these attacks and reducing their impact are represented in Table I.

All layers must be considered when designing a network security. Potential vulnerabilities and threats should be identified for each layer. According to the best practices, it is necessary to reduce the impact of those vulnerabilities and threats on the network as one segment of the ICT system [2].

1.2. Application Security

Considering that tools that offer the possibility of developing the applications with significant functionality and

faster than ever, nowadays exist, and with pressure from the business side, the solution must be ready as soon as possible. Because of that, the security of these applications is ignored. Application security is important because today's applications are often available over various networks and they are connected to the cloud, which makes them exposed to various threats and breaches [10].

The Open Web Application Security Project (OWASP) is a non-profit organization that provides information about application security. For 2019, OWASP has ranked 10 application security risks [11], which are represented in Table II following the best practices for reducing these risks.

1.3. Human Factor

The human factor is the weakest point for the system's security [12]. This opinion is shared with many security experts and because of that, human factor must be considered when developing a system. Social engineering and phishing are some of many types of attacks that can target humans, which is one of the most important segments of the system.

Table I: Common attacks and best practices for protecting the data layer

Attacks	Best practices
CDP Reconnaissance Attack	Disable CDP on edge ports that are connected to the untrusted devices and, in that way, limit the use of CDP on devices.
Telnet Attacks	Using the SSH protocol, strong passwords, access-lists (ACL), AAA with either TACACS+ or RADIUS protocols.
MAC Address Table Flooding Attack	Implement port security on the devices.
VLAN Attacks	Configure access links, disable auto trunking mode, manually enable trunk links, change the default native VLAN, implement port-security.
DHCP Attacks	Configure DHCP snooping and implementation port security.

Legend: AAA (Authentication, Authorization, Accounting), ACL (Access Control List), CDP (Cisco Discovery Protocol), DHCP (Dynamic Host Configuration Protocol), RADIUS (Remote Authentication Dial-In User Service), SSH (Secure Shell), TACACS (Terminal Access Controller Access- Control System), VLAN (Virtual Local Area Network).

Table II: Common attacks and best practices for protecting the application segment

Risks	Best practices
Injection	Application security testing
Broken Authentication	Multi-factor authentication
Sensitive Data Exposure	Data Encryption
XML External Entity	Static application security testing
Broken Access Control	Penetration testing
Security Misconfiguration	Dynamic application security testing
Cross-Site Scripting	Encoding data and input validation.
Insecure deserialization	Using application security tool and penetration testing.
Using Components with Known Vulnerabilities	Software composition analysis and static analysis
Insufficient Logging and Monitoring	Think like an attacker and keep the goals of an attacker in mind

Legend: XML (Extensible Markup Language).

1.4. Threat Modeling Basics

To make sure that the ICT system is secure, every segment of the ICT system must be protected from external and internal threats. To achieve this goal, as already stated, the threat modeling process is recommended. Threat modeling is based on the idea that every system has valuable resources that need to be protected and these resources have certain weak points that internal or external threats can use to harm them [13]. By using the threat modeling process in designing and developing each system, we accomplish the identification of potential vulnerabilities and threats to which we can implement appropriate countermeasures, resulting in the protected system.

The threat modeling process consists of six sub-processes [13]:

- *Identification of resources*: Identification of the valuable resources that the system must protect;
- *Creating an architecture overview*: Document the architecture of the system by using simple diagrams and tables;
- *Application decomposing*: Creating a security profile for the system by application decomposing;
- *Threats identification*: Identify the threats that could affect the system using knowledge of the system architecture, potential vulnerabilities of the system while keeping the goals of an attacker in mind;
- *Documenting threats*: Document each threat that has been identified using a common threat template that defines a core set of attributes for each threat; and
- *Threats rating*: Using the appropriate methodology rate the threats to prioritize and address the most significant threats first.

There are many methods and methodologies to conduct threat identification in threat modeling [14]. However, the most mature methodology so far is STRIDE [15][16]. We will use this methodology in threat identification phase. STRIDE is the acronym made out of initial letter of different attack types that it covers. Therefore, threats identified in threat modeling process using STRIDE methodology can be categorized into six categories:

- **Spoofing (S)**: Spoofing is an attempt to gain access to the system by using a false identity;
- **Tampering (T)**: Tampering is the unauthorized data modification;
- **Repudiation (R)**: Repudiation is user's ability to deny that they performed specific actions or transactions;
- **Information disclosure (I)**: Information disclosure represents unwanted exposure of private data;
- **Denial of service (D)**: Denial of service (DoS) is the process of making a system or application unavailable;
- **Elevation of privilege (E)**: Elevation of privilege occurs when the user with limited privileges assumes the identity of a privileged user and in that way can get privileged access to an application/system.

Further on, the risk of threats identified by STRIDE methodology can be calculated using many rating approaches. One of them, which will be used in this paper, is DREAD methodology [17]. DREAD is also an acronym made out of notions that describe the questions one needs to ask when rating each threat, i.e.:

- **Damage potential**: How big is the damage if the vulnerability is exploited?
- **Reproducibility**: How easy is it to reproduce the attack?
- **Exploitability**: How easy is it to launch an attack?
- **Affected users**: As a rough percentage, how many users are affected?
- **Discoverability**: How easy is it to find the vulnerability?

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

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

Security in general starts with threat model [17]. The main objective of the threat modeling process is to understand how attacker might be able to compromise a system and then make sure appropriate mitigations are in place. This should be an inevitable step in the system designing, because it allows us to understand the potential threats to the system and react in timely fashion.

2. CASE STUDY – THREAT MODELING OF SYSTEM FOR REMOTE MANAGEMENT OF WINDOWS

Existing web standards and tools provide an ideal solution for data exchange between interconnected devices and applications, which represent the vision of the concept of web technologies. One of those systems is a system for remote management of windows, which offers remote control using web technologies, i.e., WoT concept [18]. WoT represents solution for enabling worldwide interoperability for the IoT systems through the Web. WoT is the concept of standardizing the communication channel at the application layer which enables management of IoT systems.

The system for remote management of windows functions the following way: End-user uses the browser to access web page over which he/she can manage the windows. The web page has an authentication mechanism that provides that only authorized users have access to the system. After a successful login, the user can manage the condition of windows (open/closed). The system can also be an automated system because it offers options for planning when the windows are going to be open/closed. The architec-

ture of the system for remote management of windows in given in Figure 1.

In accordance with the threat modeling process explained in the previous section, the first step is to identify resources and security goals. The security goals of the system for remote management of windows are availability, security, privacy, reliability, and scalability. Valuable resources of this system are data (user data such as passwords, user's identity, name, surname, photo, etc.) and assets where windows are located.

The second step includes architecture overview. The architecture of the system for remote management of windows can be decomposed into six zones. Namely, for architecture decomposition, we have used Data Flow Diagram (DFD) method given in Figure 2. Architecture represents a logical layout of elements for this system and connections between these elements:

- User zone (U): Over this zone a user can manipulate with windows by sending request towards the system;
- Router zone (R): Represents a zone which enables user's connection to the Internet;
- Frontend zone (F): Represents a zone which offers authentication and data presentation;
- WoT server zone (W): Represents the "brain" of the system and this zone is consisted of the WoT server and Structured Query Language (SQL) database;
- Sensor zone (S): Consists of the sensor that reverts data if the window is open; and

- System administrator zone (SA): Represents a zone where system administrator can do administration tasks, such as data filtering, management of the system operation, etc.

In order to conduct the third and the fourth step of the threat modeling process, i.e., architecture decomposition and threat identification, we have used the Microsoft Threat Modeling Tool (MTMT) [19], which is based on STRIDE methodology.

The remaining steps of threat modeling process, i.e., results of threat identification and their ratings are given in next section.

3. RESULTS ANALYSIS

By using previously described MTMT tool we have identified 118 threats for the subject system for remote management of windows. The STRIDE categorization of threats is represented in Table III.

Based on the obtained results, we can conclude that in the analysis of WoT-based system for remote management of windows elevation of privilege attacks have the highest probability of occurrence (32%). The second place is taken by DoS threats (24%), while Spoofing (19%), Repudiation (11%), Tampering (9%), and Information disclosure (5%) rank from third to sixth place, respectively.

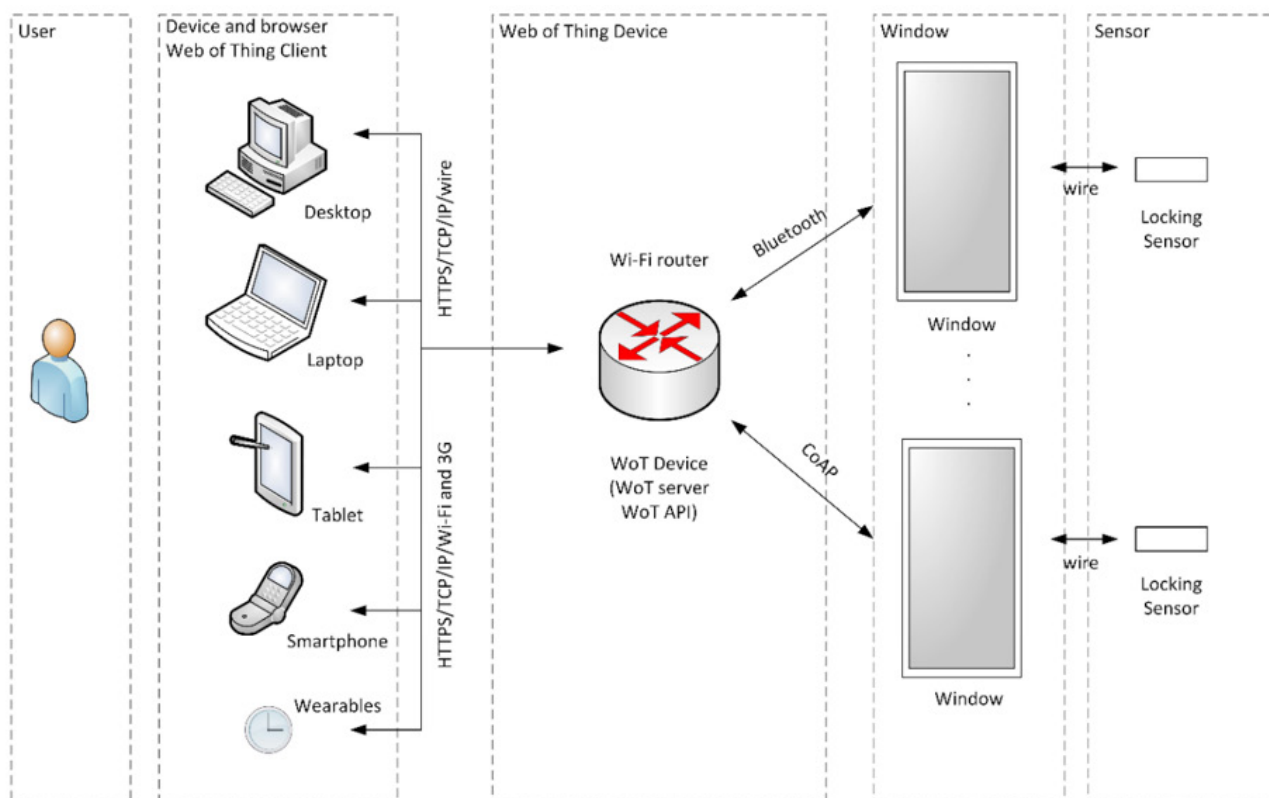


Figure 1: The high-level architecture of a system for remote management of windows

Legend: 3G (3rd Generation), API (Application Programming Interface), CoAP (Constrained Application Protocol), HTTPS (HyperText Transfer Protocol Secure), IP (Internet Protocol), TCP (Transmission Control Protocol), Wi-Fi (Wireless Fidelity), WoT (Web of Things).

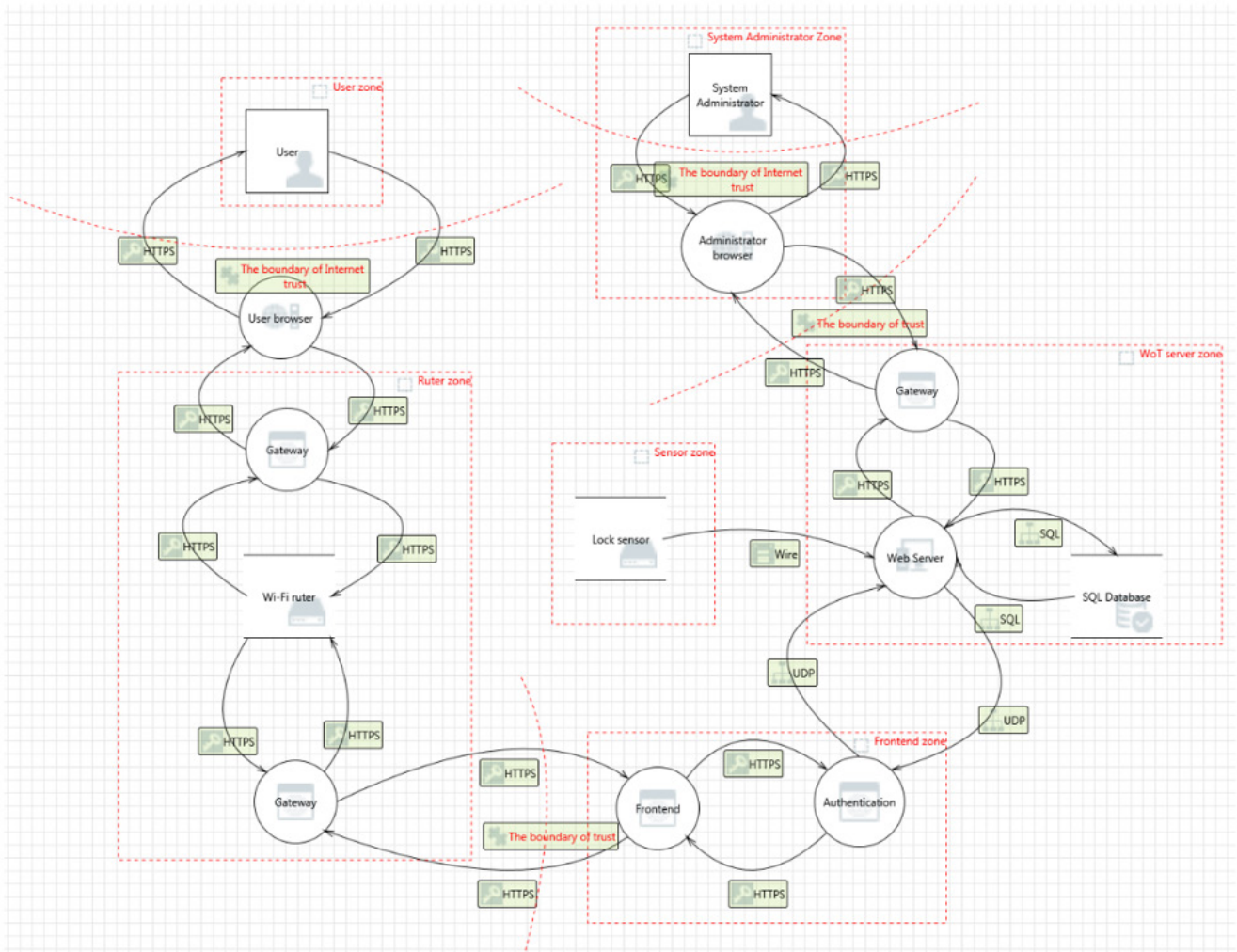


Figure 2: The Data Flow Diagram of a WoT-based system for remote management of windows

The final step in this threat modeling process is rating the threats by using previously described DREAD methodology. The conclusion from using this method for calculating the risks of the identified threats by STRIDE methodology for a WoT-based system for remote management of windows is that 32.20% of identified threats have high risk, 62.71% threats have a medium risk, and 4.23% threats have a low risk.

Table IV represents the percentages of risks for relations between elements of the system and it represents the sum of risks for each identified zone of the system, which are classified per high, medium, and low level of risk. These results are combined with the ones shown on Figure 3.

Figure 3 shows a distribution of different STRIDE category threats in different zones of the considered WoT-based system for remote management of windows. We can conclude from the graph and table information that the Router and WoT zones are the most vulnerable ones, while the Frontend zone is the least vulnerable. Elevation of privilege is the most represented threat in high risk zones, i.e., Router and WoT zone, but also in Frontend zone (as low-risk zone). For this threat, the

implementation of security solutions should be considered as the highest priority. DoS threats are in the second place. Middle-risk zones, i.e., user, administrator and sensor zone are mostly characterized by DoS, Elevation of privilege and Spoofing attacks.

Finally, Table V represents the best practices for the defense of attack for each category of threats identified by STRIDE methodology.

Table III: Number of identified threats and percentages for analyzed system for remote management of windows

Threat Category	Number of Threats and Percentages
Spoofing	22 (18.64%)
Tampering	11 (9.32%)
Elevation of Privilege	38 (32.20%)
Denial of Service	28 (23.72%)
Repudiation	13 (11.01%)
Information Disclosure	6 (5.08%)

Table IV: Percentages of risks for relations between elements of the system and the sum of risks for each identified zone of the system

Zones	Relations	Risk					
		High (%)		Medium (%)		Low (%)	
			SUM		SUM		SUM
User Zone	User Browser (user)	1.68	3.38	5.07	9.3	0.84	1.68
	Gateway Browser (user)	1.69		4.23		0.84	
Router Zone	Browser (user) Gateway	2.54	4.24	4.23	11.01	0	0.84
	Gateway Wi-Fi router	0		3.39		0	
	Frontend Gateway	1.69		3.39		0.84	
Frontend Zone	Gateway Frontend	0	2.54	5.93	11.85	0	0.84
	Fronted Authentication	0		1.7		0	
	Web-server Authentication	2.54		4.23		0.84	
WoT Server Zone	Authentication Web Server	4.23	12.7	5.93	12.7	0	0
	Web Server SQL data base	1.69		4.23		0	
	Gateway Web Server	2.53		0		0	
	Browser (Administrator) Gateway	4.23		2.54		0	
System Administrator Zone	Gateway Browser (Administrator)	2.54	5.08	4.23	9.32	0	0.84
	System Administrator Browser (Administrator)	2.54		5.09		0.84	
Sensor Zone	Sensor Web Server	4.23	4.23	5.08	5.08	0	0

Legend: SQL (Structured Query Language), Wi-Fi (Wireless Fidelity), WoT (Web of Things).

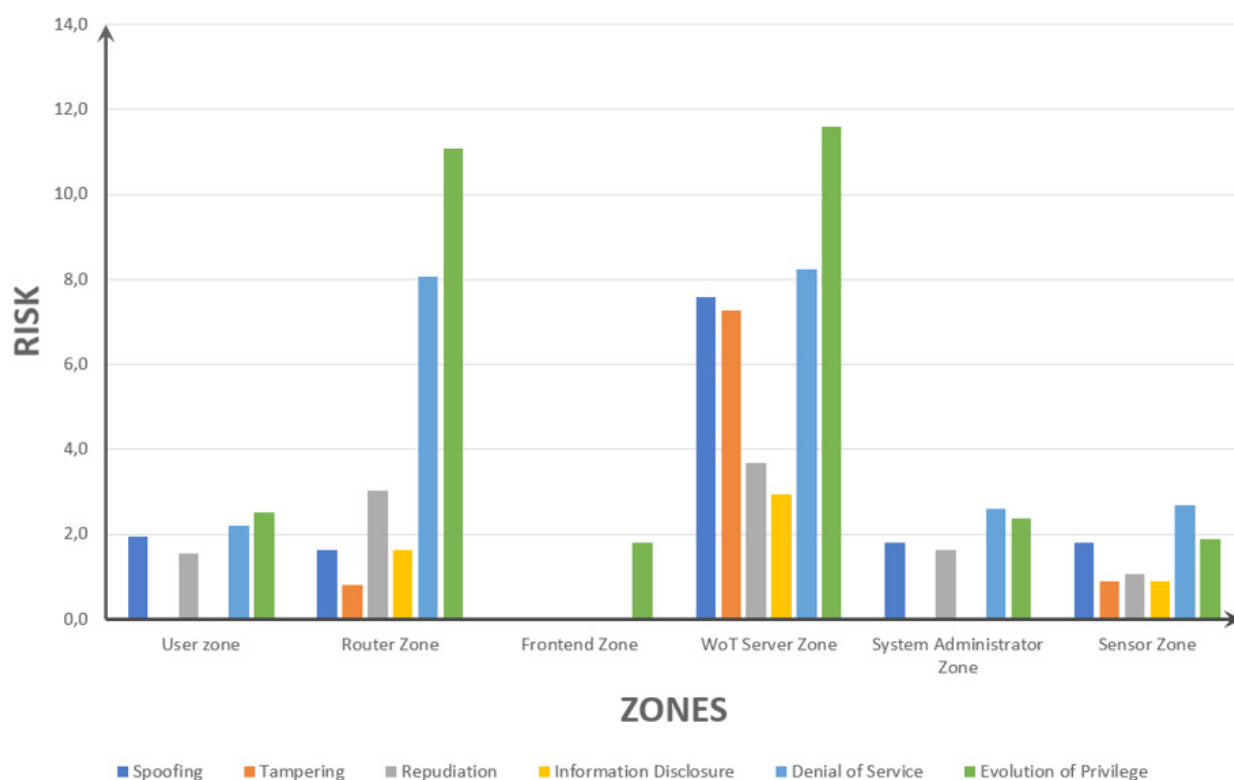


Figure 3: Distribution of STRIDE category threats in different zones of the system

Table V: The best practices for the defense of STRIDE threats

Threat Category	Best Practices
Spoofing	Strong authentication, credentials encryption, Secure Sockets Layer (SSL)
Tampering	Strong authorization, digital signatures, use tamper-resistant protocols and protocols which provide message integrity
Repudiation	Create secure audit trails and use digital signatures
Information Disclosure	Use strong authorization and encryption, use protocols that provide message confidentiality.
Denial of Service	Input validation and filtering, use throttling techniques
Elevation of Privilege	Follow the principle of least privilege and use least privileged service accounts to run processes and access resources

4. CONCLUSION

Cybersecurity consideration is very important for each modern system based on IoT and WoT technologies. In this paper, we have analyzed the security of the WoT-based system, i.e., a system for remote management of windows by using the threat modeling approach. In general, security starts with the threat model. Its main objective is to understand the potential threats to the system and allow the designer team to implement appropriate security solutions in the initial phase. Given that the considered system is in the initial design phase, for efficient implementing security solutions we wanted to identify and rate the potential threats and vulnerabilities through the threat modeling approach.

After we have identified the resources and security goals, we overviewed and decomposed the system architecture (DFD), and moved to threat identification. For identifying threats we used the MTMT tool, which is based on STRIDE methodology, while for their rating we used the DREAD approach. MTMT identified 118 different threats for the observed system architecture. After summarizing the results and analyzing them, we conclude that the greatest number of threats (38) falls into the category of Elevation of privilege. This class of threats characterized the most risky zones of the system, i.e., Router and WoT zone, but the Frontend one as well, which is marked as a low-risk zone of the system.

Information disclosure class of threats are at the same time the ones characterized as medium and low risk ones, while the most represented high-risk threats come from the Elevation of privilege class of threats. Considering this, the appropriate countermeasures for these threats should be inspected first, and then the relevant countermeasures for the highest to the lowest risk should be implemented. Since the analyzed system is still in the design phase, the obtained results will contribute to the implementation of the principle security and privacy by design, thereby increasing the security of the system as a final product. For future research, it is necessary to consider in more detail the architecture of the considered WoT-based system for remote management of windows, i.e., to build a higher-level architecture model compared to one observed in this paper.

REFERENCES

- [1] R. Sobers: 110 Must-Know Cybersecurity Statistics for 2020, Inside Out Security Blog, 2020, Available at: <https://www.varonis.com/blog/cybersecurity-statistics/>
- [2] 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
- [3] C. Crane: The Top Cyber Security Trends in 2019 (and What to Expect in 2020), 2019, Available at: <https://www.thesslstore.com/blog/the-top-cyber-security-trends-in-2019-and-what-to-expect-in-2020/>
- [4] Verizon: Data Breach Investigations Report, 2019
- [5] RSA: 2019 Current State of Cybercrime - The Digital Transformation of Cybercrime, 2019, Available at: <https://www.rsa.com/content/dam/en/white-paper/2019-current-state-of-cybercrime.pdf>
- [6] Malwarebytes LABS: Cybercrime tactics and techniques Q1 2019, 2019, Available at: https://resources.malwarebytes.com/files/2019/04/MWB-CTNT-2019-state-of-malware_FINAL.pdf
- [7] Ponemon Institute: Staffing the IT Security Function in the Age of Automation: A Study of Organizations in the United States, United Kingdom and APAC, 2019, Available at: <https://www.domaintools.com/content/2019-ponemon-report-staffing-it-age-automation.pdf>
- [8] IDC: Worldwide Spending on Security Solutions Forecast to Reach \$103.1 Billion in 2019, According to a New IDC Spending Guide, 2019, Available at: <https://www.idc.com/getdoc.jsp?containerId=prUS44935119>
- [9] NetAcad: CCNA Security, 2019
- [10] S. Baraković, J. Baraković Husić: Short and Sweet: Cloud Computing and Its Security, Proceedings of the 11th International Symposium on Telecommunications, (BIHTEL 2016), Sarajevo, Bosnia and Herzegovina, 2016
- [11] OWASP: Top 10 Web Application Security Risks, 2019, Available at: <https://owasp.org/www-project-top-ten/>
- [12] K. D. Mitnick, W. L. Simon. The Art of Deception: Controlling the Human Element of Security. Wiley, 1st edition, 2003

- [13] M. Curphey, J. Scambray, E. Olson: Improving Web Application Security, Threats and Countermeasures, 2003
- [14] N. Shevchenko, T. A. Chick, P. O’Riordan, T. Scanlon, C. Woody: Threat modeling: A summary of available methods, 2018, Available: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=524448>
- [15] A. Shostack: Threat Modeling: Designing for Security. John Wiley & Sons, Inc., 2014
- [16] M. Haider: Application Threat Modelling using DREAD and STRIDE, Infosec Blog, 2017, Available at: <https://haiderm.com/application-threat-modeling-using-dread-and-stride/>
- [17] 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>
- [18] 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/>
- [19] Microsoft Corporation: Threat Modeling: Microsoft Threat Modeling Tool, 2020, Available at: <https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>

BIOGRAPHY

Tarik Dervišević, graduated at the Faculty of Traffic and Communication, University of Sarajevo, direction Communication technology, and received a Bachelor’s degree in 2017. In the same year, he enrolled in a Master’s program on the same faculty and direction and in 2019 he received a Master’s degree. He is employed as a Core Operation Technician in Infobip, a company that is a global leader in omnichannel communication.

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 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.