Impact Evaluation of DDoS Attacks Using IoT Devices

Ronierison Maciel*, Jean Araujo†, Carlos Melo*, Paulo Pereira*, Jamilson Dantas*,
Júlio Mendonça*, and Paulo Maciel*
*Centro de Informática, Universidade Federal de Pernambuco, Recife, Brazil
†Unidade Acadêmica de Garanhuns, Universidade Federal Rural de Pernambuco, Garanhuns, Brazil
{rsm4, casm3, prps, jrd, jrmn, prmm}@cin.ufpe.br, jean.teixeira@ufrpe.br†

2021 IEEE International Systems Conference (SysCon) | 978-1-6654-4439-2/20/$31.00 ©2021 IEEE | DOI: 10.1109/SysCon48628.2021.9447145

***Abstract*—Distributed Denial-of-Service (DDoS) attacks can occur anytime, everywhere, and most normally occur with little or no warning. Most small and medium businesses (SMBs) usually are not prepared to deal with this type of attack. The companies must have at least a bandwidth higher than the attack, an infrastructure with redundant components, regular backups, and firewalls capable of monitoring the threats. Otherwise, the services provided by the companies' support can be interrupted, increasing the chances of financial losses. Hierarchical modeling approaches are often used to evaluate the availability of such systems. It can represent different failures and repair events in distinct parts of the system. In this way, this paper proposes hierarchical models that describe the behavior of major IT systems and IoT device components and assess the DDoS effects on system availability. Therefore, we evaluate the impact of the DDoS attacks on computing systems using IoT devices in attack amplification. We assessed equations that estimate the attack feasibility, pain factor, attack propensity, attacker benefits, and technical ability. They enable a direct analytical solution for large systems. The attack tree indices show the impact of simultaneous attacks on a computer system and the several threats that will maximize the system downtime. The attack tree investigation results allow for planning and improving the system's availability, maintainability, and reliability.**

Keywords—DDoS; IoT; Malware; Attack Tree; Threats

I. Introduction

Information and communications technology (ICT) has become an essential and indispensable part of our daily lives. A well-known technology part is Internet-connected smart devices, and ubiquitous connectivity [1]. The Internet of Things (IoT) is changing the way that humans and technology interact. IoT devices are mainly found in smart homes that auditors and adjust the environment to better suit the users [2]. With the recent rapid development of the IoT, the interest in understanding emerging cyber threats in IoT has been increasing [3].

Vulnerabilities in IoT devices can be applied in DDoS attacks on a large scale. For example, Mirai bots were used to perform DDoS attacks using IoT devices [4]. In another situation, the enterprise KrebsOnSecurity suffers a DDoS attack of 620 Gigabytes per second; the attack lasted seventy-seven hours and was powered by 380,000 insecure IoT devices [5]. IoT hacking is a new phenomenon, but it has demonstrated a massive potential for destruction within a relatively short timeline. For example, the Mirai bots use an auto-replication module that looks for vulnerable devices by scanning the whole Internet [6].

It estimated that the cybercrime cost exceeds up to US$ 10.5 trillion until 2025 [7]. The same report stated that the majority of IoT attacks in 2018 were originated from Brazil (18%), followed by China (15%), Japan (9%), Poland (7%), US (7%), and Iran (6%) [8]. Also, more than half of the attempted attacks using IoT devices targeted SSH assistance. Remark that malicious activities can result in enterprises' operational needs, data center control, health systems, and real-time operating systems.

Some studies have been conducted to verify DDoS attacks using IoT devices. In Yigit et al. [1], the authors proposed one solution of attack protection with minimization of costs using attack graphs for IoT systems. Already in Sun et al. [9], the authors introduced a novel framework for modeling and clustering the attacker activity patterns based on honeypots' data. Was employed fuzzy and fast fuzzy design for in IoT malware detection using classification decision tree and random forests [10]. Maciel et al. [11] show the main threats that takes a system to stay down, DDoS attack methods using amplification, flooding, applications, and protocol exploitations, all utilizing the attacker, handler, bots, and victims. Moreover, most articles in the literature do not have broad menace coverage and not applicable attacks using IoT devices orchestration.

This paper proposes strategies to assess DDoS attacks' impact using IoT devices through Attack Tree (AT) modeling. It differs from the other articles because we developed a model that can analyze the attack likelihood, attack cost, attack benefits, attack feasibility, attack propensity, and the pain factor of environments that use venerable IoT devices. In this way, we can evaluate in detail the impact of DDoS attacks that uses IoT devices.

This paper arranged as follows. Section II presents an overview of IoT security and its main threats in DDoS attack utilization and conceptual knowledge regarding AT focused on IoT devices. Section III presents the AT model proposed and describes both target and attacker profiles. Section IV presents case studies demonstrating the feasibility of the proposed model. Section V shows our final remarks, discusses the main contributions and limitations of this paper, and indicates some future lines of research.

II. Background

The section depicts the most current safety threats on IoT devices, focusing on DDoS attacks and Attack Tree modeling concepts.

978-1-6654-4439-2/21/$31.00 ©2021 IEEE

A. Main threats of DDoS attacks

Distributed Denial-of-Service (DDoS) based attacks continuously evolve, increasing their complexity and range, thereby making it more challenging to perform timely and accurate detection. That attack type can be taken out on a particular device and follows authorized user traffic, which hinders it from mitigating it. Its main goal is to destabilize or suspend the victim's workstation or service by sending abnormal or large packets, burdening the target device [12].

The reflection-based volumetric attack's purpose is to use the available bandwidth size of a specific company. The interlopers own botnets to create a large traffic amount in the victim networks: backdoors viruses illegally take over machines to amplify this type of attack. Backdoor is wicked software that affects the victim and provides full access to its computer and its resources [13].

Given these conditions, the computer becomes part of a robot network (botnets), an acronym for machines that perform illegal actions which the user does not know, commonly known as a zombie computer network [14].

Computational threats impact operational losses and other aspects [15]. The main risks are:

- *Backdoor:* The intruder attaches to the machine with few or no authentication and performs commands.
- *Botnet:* All affected devices with the botnet corresponding receive the same directions from a single command-and-control server.
- *Malicious code injector:* Methods used by hackers for injecting ill-disposed codes from an unknown place in the system and trying to steal or manipulate an authorized user's data.

B. IoT markets

Businesses like healthcare, automotive, home, building, retail, energy, manufacturing, mobility, transport, logistics, and media are leading the IoT business (see Figure 1). Also, there are vulnerabilities in these devices that they're used to perform DDoS attacks. Figure 1 summarizes how IoT devices have been employed in these markets as follows.

- *Healthcare:* The data transmission improved monitoring of patients as well as people and equipment [16];
- *Home and Building:* Through their mobile devices connected to computers, managers can control the temperature, security, and maintenance of their buildings and homes [17];
- *Retail:* We have improved customer satisfaction by analyzing data regarding the supply chain, integrated customer service, and e-commerce efficiency [17];
- *Energy:* The use of smart meters and the grid results in savings and reduced energy consumption [18];
- *Manufacturing:* Traffic management and intelligent lighting, power, cooling, and emergency systems [16];

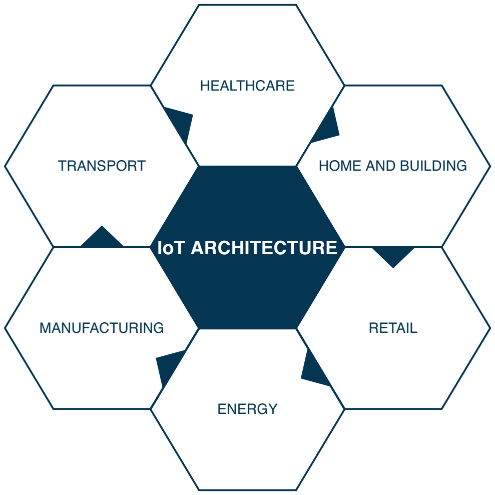


Fig. 1. IoT markets

- *Transport:* They have increased safety and reduction in pollution due to real-time traffic alerts, vehicle diagnostics, and predictive driving or commuting behavior [18].

The global IoT market size stood at US$ 250 billion in 2019 and is projected to reach US$ 1,463.19 billion by 2027, exhibiting a Compound Annual Growth Rate or (CARG) of 25.9% during the forecast period. The associated technologies such as digital twin came to leverage artificial intelligence and 5G infrastructure, contributing to the cybernetic attack's ability and amplifications [19].

C. IoT vulnerabilities

The quick internet of things (IoT) development goes cyberattacks simple and effective due to the security lack in these devices. Thereby, the attackers can use IoT devices, create botnets, and launch distributed denial of service (DDoS) attacks against networks. Next, we explain the vulnerabilities with the most impact on victims.

The IoT devices show your weaknesses to be explored easily. Some of the most common vulnerabilities are:

- *Username enumeration:* A malicious actor can use brute-force to either guess or confirm valid users in a system.
- *Weak Passwords:* The password is easy to detect by both human beings or computational systems. For example, people usually use a simple password, names children, animals, houses numbers, and others not to forget them.
- *Account Lockout:* The attacker can exhaust the invalid login attempt limit for a given account; that account may be locked out against the owner's wishes.

However, security-related factors are essential to ensure these devices' reliability, and manufacturers must comply with a pattern to ensure these devices' security. One way to help quantify and analyze these threats is to use AT models [20].

D. Attack tree modeling

Security professionals have been considering how to prevent downtime to market flow due to virtual attacks. The consideration to studies has done formed not only in the specialist literature but also in the general media. Given the likely extent of financial losses, companies need to adopt strategies to decrease these threats. Besides, there have been improvements in technology and instrument to build protections upon these perils.

Attack Tree is an emerging and encouraging method that aims to overcome economic losses by recognizing threats [21], [22]. AT clarifications are helpful as they can provide intelligence regarding computational threats in institutions. Some ways to do this include: (1) indicating occurrence probabilities to substantial observed dangers; (2) investigators can model the attacker's behavior and determine how long it takes for the attacker to crash a system; (3) The examiner should further tell how much the victim should advance to avoid any intervention on its infrastructure. With this data, it is possible to assess the security developed in a pattern including more terrific threat potential refinement.

The AT description is structured and hierarchically distributed. AT uses a bottom-up strategy. We begin from the leaf nodes, in which ill-disposed actions can perform. Then, the logical operators OR or AND can model the combined the supposed attack effects. A more computation is done for each logical operator to reach the attacker's main objective finally. The successful attack likelihood at AND gate, modeled in an AT, is calculated by Equation (1). The successful attack likelihood of an OR gate is determined by Equation (2). Both equations are described in the interim $[0, 1]$. n represents the daughter nodes number in the tree, and the occurrence likelihood $(Prob_i)$ describes the successful attack likelihood [23].

$$PA_{AND} = \prod_{i=1}^{n} Prob_i \tag{1}$$

$$PA_{OR} = 1 - \prod_{i=1}^{n} (1 - Prob_i) \tag{2}$$

III. Proposed Model

This section exhibits the recommended AT model to examine the primary attack methods DDoS using IoT devices. We choose the scenario and construct a model-based on possible attacks using these devices. Additionally, those vulnerable IoT device threats are potential to the real environment.

In Figure 2, the agent examines Command-and-Control servers (CC). Then, malicious requests are sent to IoT devices and wait for answers. The next step is to find out vulnerable devices and then choose the target for the DDoS attack. We detail each attack step.

- *Malicious agent:* Responsible for malicious sending codes to IoT devices.
- *CC Server:* The computer has issues directives to digital devices and is a target to infect with rootkits or other malware types, such as ransomware.
- *Send malicious code scanner:* The malicious code describes broad system security category terms that include attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.
- *Scanner:* Any device connected to the Internet can be part of the IoT and crawled over the network. The metrics adopted in
- *Vulnerable IoT devices:* The IoT devices connected to an exposed network can carry out an attack.
- *Target:* The attack victim.

The metrics adopted in this paper estimates the costs, attacker's benefits, feasibility, pain factor, attacker propensity, and technical ability. Nonetheless, the price considered here is linked to the value that the attacker is willing to pay to achieve success in his task.

The cost to attack $(Cost_i)$ metrics adopted in the AT formalism. The Equation (3) show the cost per gate AND, while Equation (4) presents the cost per gate OR. This equation's domain is $[0, \infty]$ because it bottle be known whereby an intruder requires to spend [23].

$$CA_{AND} = \sum_{i=1}^{n} Cost_i \tag{3}$$

$$CA_{OR} = \frac{\sum_{i=1}^{n} Prob_i \cdot Cost_i}{\sum_{i=1}^{n} Prob_i} \tag{4}$$

Attacker's Benefits (AB) say the advantages that an attacker will become by a successful attack. It can be determined by Equation (5). The W_i weighting also $Prob_i$ likelihood variables related to estimating AB are given in Table III and in Figure 3(c).

$$AB = \sum_{i=1}^{n} (W_i \cdot Prob_i) \tag{5}$$

The feasibility (FA) metric defines the attack ease in the evaluated scenario. It is measured as a geometric average trying to compare multiple characteristics. As displayed in Equation (6), we adopted $Cost_i$, Noticeability (Not_i), and Technical Ability (Tea_i) [24]. The taken these properties values are exhibited in Figure 3.

$$FA = \sqrt[N]{\prod_{i=1}^{N} Cost_i \cdot Not_i \cdot Tea_i} \tag{6}$$

Pain Factor (PF) shows the problem that the victim will feel if the invasion happens. It is an evaluated intervention that will hurt the target system. It can be measured by Equation (7). The values W_i are weighting related, and $Prob_i$ likelihood presented in Table III indicators profiles, whose contents exhibited in Figure 3(e).

$$PF = \sum_{i=1}^{n} (W_i \cdot Prob_i) \tag{7}$$

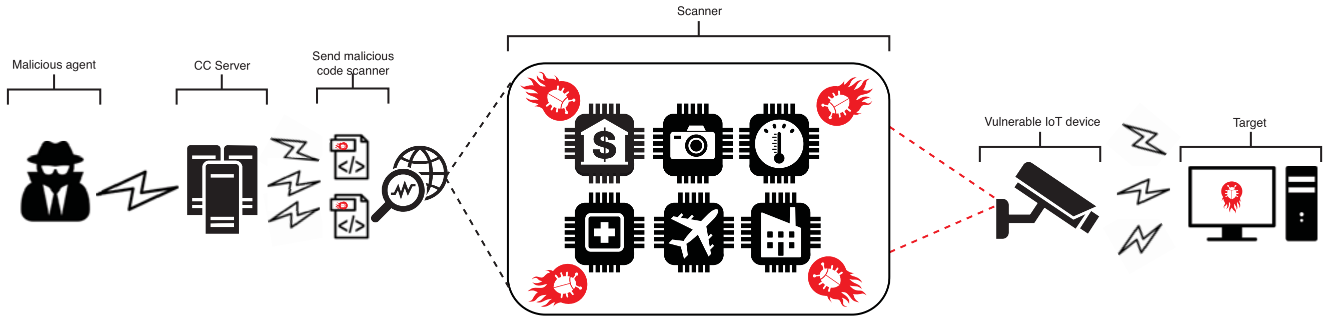


Fig. 2. The attack scenario DDoS using IoT

The attack propensity presented in Equation (8) assumes the feasibility combinations (FeA) and the Attacker's Benefits (AtB) from an invasion outline. The purpose is to present a possibility to the attack percentage metric. It corresponds to the instant in which the threat agent operates the target system.

$$PA = FA \cdot BA \tag{8}$$

The technical ability indicator is presented in Figure 3(a), which portrays the ability to subvert the evaluated scenario according to the values defined in Table II. The occurrence probability indicator shown in Figure 3(b) represents the relationship between the occurrence likelihood and the willingness probability, how much the attacker this willing to attack [25]. Figure 3(c) shows an attack cost based on how much an attacker can spend to reach his goal [26]. Figure 3(d) estimates the attack benefit noticeability. Therefore, the operational losses indicator presented in Figure 3(e) shows the victim's financial losses due to an attack. The reputation losses in Figure 3(f) arise from the attack impact.

IV. Case Study

The case research was adopted to give a real-world approximation scenario. Currently, many businesses are choosing security models to decrease the invasions that they are suffering. These attacks occur in different parts, whether in the industry, school, and medical assistance areas.

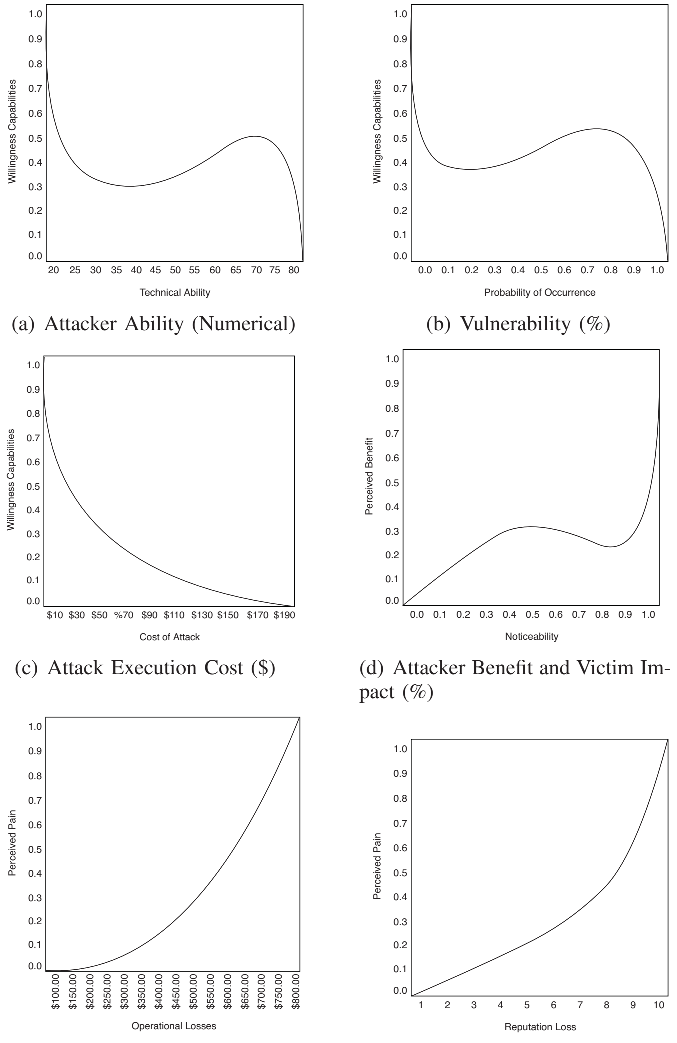
A. Input Parameters

To assess the stated model, we chose the input parameters exhibited in the Tables I, II, and III. The charges applied for the AT model node components, attack rate per month for each threat, each visibility threat into the intruder, money amount spent by an attacker to perform the intervention and the victim to defend his organization, and threat impact it happens obtained from [27].

Table I shows the used impact information to describe all potential consequences in any system.

Table II lists the agent knowledge level regarding the sabotage determined for the scene or also the threat agent's technical ability (see Amenaza [28]). Table II identifies threat agents' technical skills according to their experience level [28].

The attack tree presents logic gates and details the possible threats through failure on firewall or software attack. Over loss,



(a) Attacker Ability (Numerical)

(b) Vulnerability (%)

(c) Attack Execution Cost ($)

(d) Attacker Benefit and Victim Impact (%)

(e) Victim Losses ($)

(f) Victim Loss (Numerical)

Fig. 3. Indicators profiles

TABLE I. Reputation Loss - Victim

Range	$Impact_i$	Impact Definition
$1 \leqslant I < 4$	None	Minor influence on the system.
$4 \leqslant I < 7$	Low	A moderate impact on the system.
$7 \leqslant I < 10$	Medium	Significant damage results to the system.
10	High	The system effectively jeopardized, inoperable.

TABLE II. TECHNICAL ABILITY - ATTACKER

Tea_i	Agent knowledge	Definition knowledge
$20 - 30$	Average user	Can easily surf the Internet, minor the system understanding
$30 - 40$	Power user	Low programming skills
$40 - 60$	Advanced user	IT security professional
$60 - 80$	User super seasoned	For all reasonable purposes, this would be not easy

a firewall can be obtained by network attack or phishing, and through this, it is possible to exploit software bugs and your leaves. However, software attacks have your leaves. The threats in Table III related to OR gates are access by firewall failure or software attack. Also, AND gates software flaw exploitation. But, other gates we can see in Figure 4.

TABLE III. ATTACK INPUT PARAMETERS

	$Cost_i$	$Prob_i$		Opl_i		Not_i
$Threats$	($)	(%)	Tea_i	($)	$Impact_i$	(%)
UDP	60.00	20	30	240.000	High	20
NTP	100.00	20	80	600.000	High	20
SNMP	60.00	20	40	120.000	High	10
DNS	100.00	20	50	300.000	High	20
SSDP	600.00	40	30	340.000	High	40
Spear phishing	200.00	10	80	400.000	Medium	10
Whaling	200.00	10	80	500.000	High	10
Baiting	200.00	10	60	500.000	Medium	10
SQL injection	120.00	20	20	400.000	High	20
XSS	60.00	30	80	280.000	Medium	30
Rootkits	60.00	30	20	300.000	Medium	30
Trojan	60.00	10	20	200.000	Medium	10
Viruses	60.00	10	10	200.000	Medium	10
Worms	60.00	10	10	150.000	Medium	10
Spyware	60.00	40	10	110.000	Medium	40
Backdoor	60.00	30	70	200.000	Medium	30

In this case study, we adopted relative values cyberattacks using IoT devices to fill the tree leaves, demonstrating the impact of these attacks on a victim; the attacks were diversified to the environment real simulation. In the next subsection, we discuss the result analysis obtained with the model.

B. Result Analysis

Given the stated scenario and the assessed model, we got results for the attack likelihood, attack cost, attacker's benefits, feasibility, pain factor, attack propensity, and technical ability. The attack likelihood present 84% chance occur any attack, using Equation (1) AND gate and Equation (2) OR gate. However, results regarding the attack cost the agent malicious spend values US$ 78 to US$ 98 dollars using the Equation (3) AND gate and Equation (4) OR gate.

Figure 5 gives the easiest attack techniques. The Viruses, worms, and Spyware has a 69% occurrence chance, followed by UDP, SNMP, and SSDP, with a 65% occurrence likelihood.

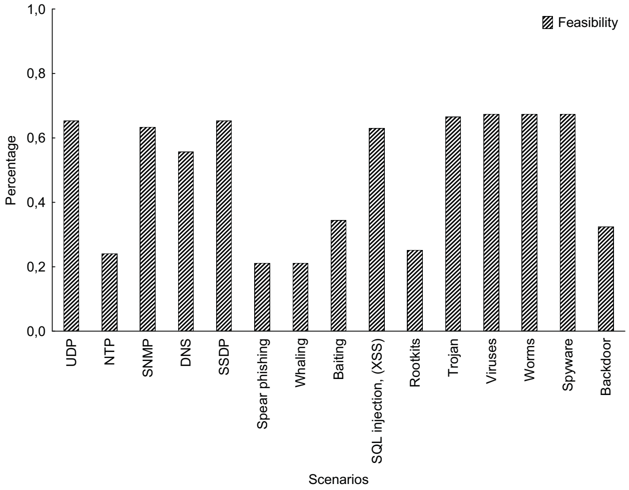


Fig. 5. Feasibility

Figure 6 demonstrates organizations' pain factor due to attack occurrences. The pain factor comprises several prejudicial factors to organizations in the evaluated circumstances, namely operational, financial, and reputation losses. The menaces listed in decreasing order were found to have the next occurrence likelihood: the SSDP attack method 58%, the NTP method 49%, SQL injection, and Cross-Site Scripting (XSS) 45%.

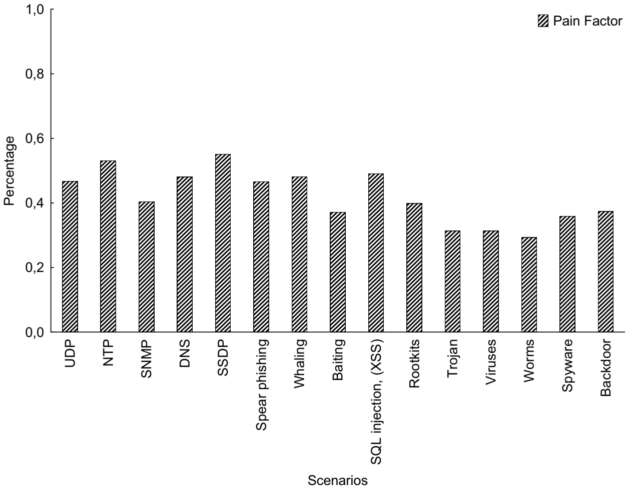


Fig. 6. Pain Factor

Figure 7 explains the attack methods that most likely to occur. The factors contributing to this result include the attacker's technical ability, threat perception, attack cost, attack ease, and the attack's benefits. Given this, we obtained the attack propensities to occur. We observed the threats that are most likely to the occurrence, the characteristic set. As it has a 28% affair, SQL injection and Cross-Site Scripting (XSS) has the highest propensity, followed by SSDP with a 25% probability, and the Spyware technique had a 23% chance of occurring.

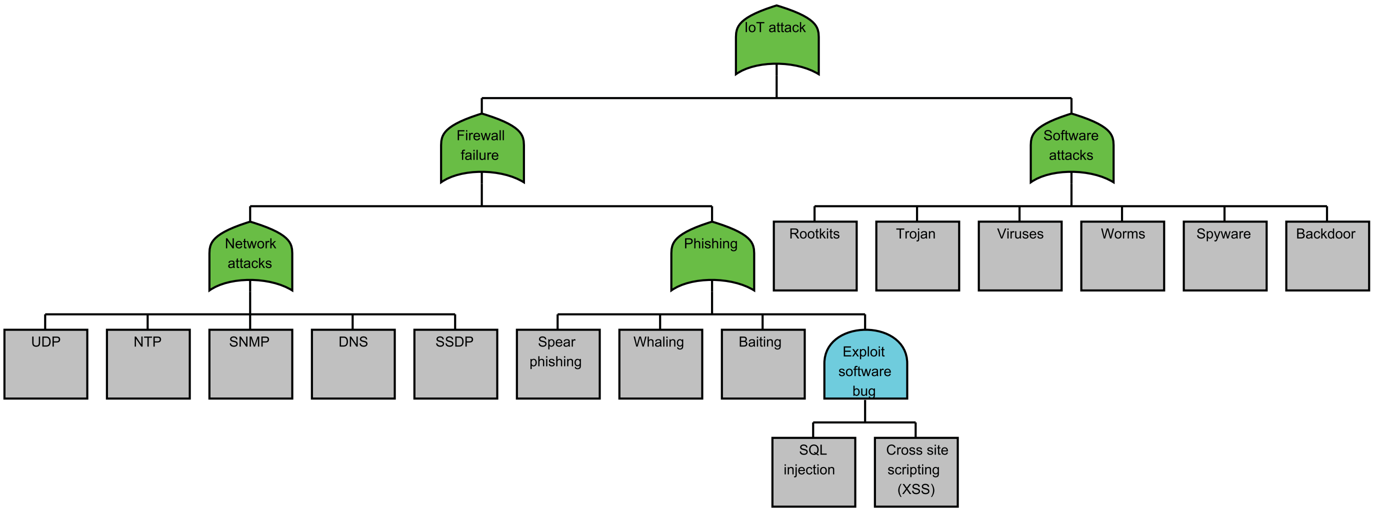


Fig. 4. Model Attack Tree

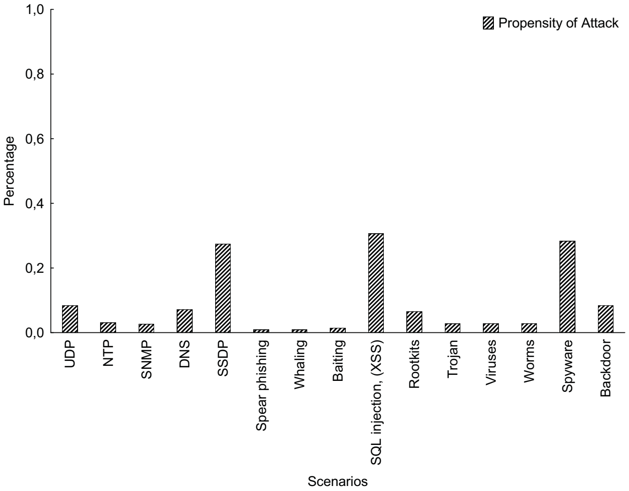


Fig. 7. Attack Propensity

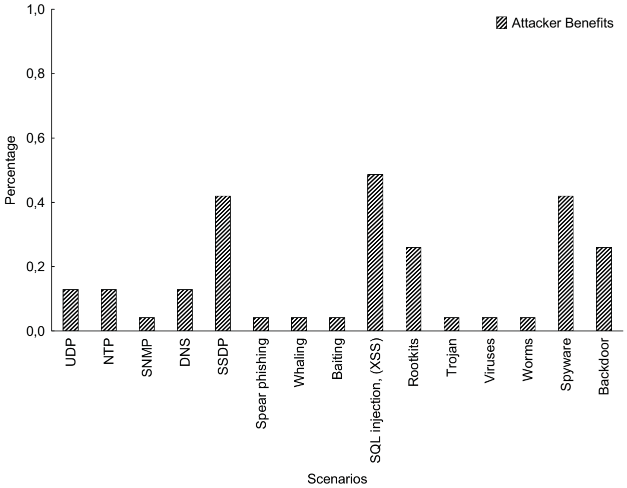


Fig. 8. Attacker's Benefits

Figure 8 depicts the possible invasion gains for the threats main. The primary attacked service is SQL injection, Cross-Site Scripting (XSS), followed by Spyware, SSDP, and Backdoor. These are the main threats that the security analyst will have to pay the most attention to and devote the most effort. The attacker will have a 45% obtaining benefits chance using the SQL injection and XSS attack. In contrast, as a using result of the Spyware and SSDP methods, he will have a 40% obtaining benefits likelihood.

Figure 9 shows the technical abilities needed by the attacker to perform an attack. Understanding the invader skills can reduce the attack outcomes. As can be observed, the two most knowing the attacker technical abilities are Viruses, Worms, Spyware, technique, with 90% of knowledge to subvert the system, and SQL injection, XSS, and UDP technique, with 85% of expertise.

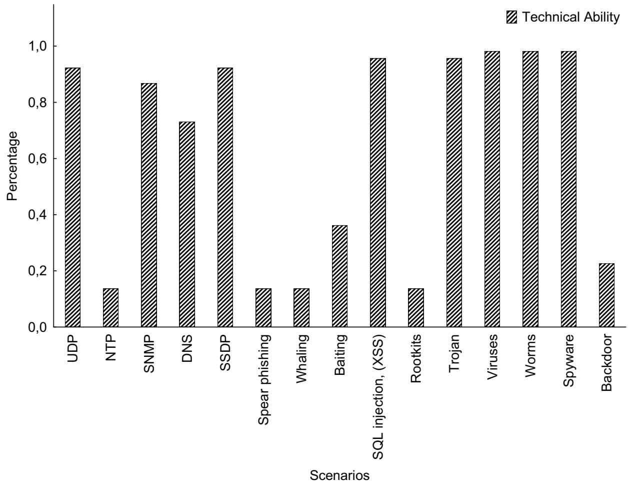


Fig. 9. Technical Ability

The evaluated results refer to the attack probability occurrence from the victim's perspective. The relevant consequence shows us which techniques are employed in the analyzed context. However, the victim can make individual decisions regarding the threat. The study addresses only attack-oriented threats from attacks of distributed-denial-of-service (DDoS) using IoT devices. Moreover, the AT is used to model any threat risk analysis. The outcomes show that the victims' most vulnerable points can be avoided by observing the study outcome collected, prevent cost and service downtime.

V. Final Remarks

This article described an analytical-based approach to evaluate the distributed denial-of-service attacks impact using IoT devices directed to a computer system. An AT simulation model was intended as an evaluation method to obtain the results for several interest metrics and the solution's benefits by measuring and adjusting specific computing components for the analytical solution and the simulation models. The collected results showed that the distributed denial-of-service techniques with IoT devices impacted the victim significantly. The attack occurrence likelihood is 84%. Also, there is a feasibility of 69% using the UDP, SNMP, and SSDP technique. Another evaluated metrics is the pain factor, which has a 58% occurrence probability and the attack propensity, with a 23% happening chance.

In a forthcoming study, we aim to use AT models to assess the physical attack impacts in cloud computing infrastructures using IoT devices exposed using multivariate analysis metrics.

VI. Acknowledgements

We want to thank the Coordination for the Improvement of Higher Education Personnel – CAPES, and MoDCS Research Group for their support.

References

[1] B. Yiğit, G. Gür, F. Alagöz, and B. Tellenbach, "Cost-aware securing of iot systems using attack graphs," *Ad Hoc Networks*, vol. 86, pp. 23 – 35, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870518301239

[2] N. Akatyev and J. I. James, "Evidence identification in iot networks based on threat assessment," *Future Generation Computer Systems*, vol. 93, pp. 814 – 821, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17300857

[3] C. Fernandez-Gago, F. Moyano, and J. Lopez, "Modelling trust dynamics in the internet of things," *Information Sciences*, vol. 396, pp. 72–82, 2017.

[4] R. Maciel, J. Araujo, C. Melo, J. Dantas, and P. Maciel, "Impact assessment of multi-threats in computer systems using attack tree modeling," in *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Oct 2018, pp. 2448–2453.

[5] "Mirai ddos attack against krebsonsecurity cost device owners $300,000," https://www.zdnet.com/article/mirai-botnet-attack-against-krebsonsecurity-cost-device-owners-300000/, accessed: 2019-04-06.

[6] B. Afzal, M. Umair, G. A. Shah, and E. Ahmed, "Enabling iot platforms for social iot applications: vision, feature mapping, and challenges," *Future Generation Computer Systems*, vol. 92, pp. 718–731, 2019.

[7] "Cybercrime to cost the world $10.5 trillion annually by 2025," https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021, accessed: 2020-10-12.

[8] "The Hunt for IoT: multi-purpose attack thingbots threaten internet stability and human life," https://www.f5.com/labs/articles/threat-intelligence/the-hunt-for-iot--multi-purpose-attack-thingbots-threaten-intern, accessed: 2019-04-06.

[9] P. Sun, J. Li, M. Z. A. Bhuiyan, L. Wang, and B. Li, "Modeling and clustering attacker activities in iot through machine learning techniques," *Information Sciences*, vol. 479, pp. 456–471, 2019.

[10] E. M. Dovom, A. Azmoodeh, A. Dehghantanha, D. E. Newton, R. M. Parizi, and H. Karimipour, "Fuzzy pattern tree for edge malware detection and categorization in iot," *Journal of Systems Architecture*, 2019.

[11] R. Maciel, J. Araujo, J. Dantas, C. Melo, E. Guedes, and P. Maciel, "Impact of a ddos attack on computer systems: An approach based on an attack tree model," in *2018 Annual IEEE International Systems Conference (SysCon)*. IEEE, 2018, pp. 1–8.

[12] T. OWASP, "10 2010," *The Ten Most Critical Web Application Security Risks*, vol. 30, 2010.

[13] E. Skoudis and L. Zeltser, *Malware: Fighting malicious code*. Prentice Hall Professional, 2004.

[14] J. T. M. Garre, M. G. Pérez, and A. Ruiz-Martínez, "A novel machine learning-based approach for the detection of ssh botnet infection," *Future Generation Computer Systems*, vol. 115, pp. 387–396, 2021.

[15] D. Ewald, "The proposal of fuzzy observation and detection of massive data ddos attack threat," *Uncertainty and Imprecision in Decision Making and Decision Support: New Challenges, Solutions and Perspectives: Selected Papers from BOS-2018, held on September 24-26, 2018, and IWIFSGN-2018, held on September 27-28, 2018 in Warsaw, Poland*, vol. 1081, p. 363, 2020.

[16] J. A. Jerkins, "Motivating a market or regulatory solution to iot insecurity with the mirai botnet code," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2017, pp. 1–5.

[17] D. Minoli, K. Sohraby, and B. Occhiogrosso, "Iot considerations, requirements, and architectures for smart buildings—energy optimization and next-generation building management systems," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 269–283, 2017.

[18] O. Vermesan, P. Friess *et al.*, *Internet of things-from research and innovation to market deployment*. River publishers Aalborg, 2014, vol. 29.

[19] "Internet of Things Market Size: iot industry report," https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307, accessed: 2020-04-06.

[20] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the internet of things (iot)," *IEEE Internet Initiative*, vol. 1, pp. 1–86, 2015.

[21] P. Suhasaria, A. Garg, A. Agarwal, and K. Selvakumar, "Distributed denial of service attacks: A survey," *Imperial Journal of Interdisciplinary Research*, vol. 3, no. 2, 2017.

[22] R. Maciel, J. Araujo, C. Melo, J. Dantas, and P. Maciel, "Impact assessment of multi-threats in computer systems using attack tree modeling," in *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 2018, pp. 2448–2453.

[23] K. S. Edge, G. C. Dalton, R. A. Raines, and R. F. Mills, "Using attack and protection trees to analyze threats and defenses to homeland security," in *Military Communications Conference, 2006. MILCOM 2006. IEEE*. IEEE, 2006, pp. 1–7.

[24] T. R. Ingoldsby, "Attack tree-based threat risk analysis," *Amenaza Technologies Limited*, pp. 3–9, 2010.

[25] D. Ren, S. Du, and H. Zhu, "A novel attack tree based risk assessment approach for location privacy preservation in the vanets," in *Communications (ICC), 2011 IEEE International Conference on*. IEEE, 2011, pp. 1–5.

[26] B. Schneier, "Attack trees," *Dr. Dobb's journal*, vol. 24, no. 12, pp. 21–29, 1999.

[27] C. C. ENISA, "Benefits, risks and recommendations for information security," *European Network and Information Security*, 2012.

[28] T. R. Ingoldsby, "Amenaza demos," *Amenaza Technologies Limited*, 2010. [Online]. Available: https://www.amenaza.com/demos/introduction_to_securitree.html