Exploration of Impactful Countermeasures on IoT Attacks

Salim Chehida, Abdelhakim Baouya, Marius Bozga, Saddek Bensalem

Exploration of Impactful Countermeasures on IoT Attacks

Salim Chehida*, Abdelhakim Baouya†, Marius Bozga‡ and Saddek Bensalem§
Univ. Grenoble Alpes, CNRS, VERIMAG
F-38000,Grenoble, France
Email: { *salim.chehida, †abdelhakim.baouya, ‡marius.bozga, §saddek.bensalem }@univ-grenoble-alpes.fr

***Abstract*—Risks mitigation in IoT based systems is one of the recent challenges in both academia and industry. In this work, we propose an approach based on the attack-defense tree to assess the relevant countermeasures for protecting IoT infrastructure. To this end, an attack strategy exploration tool built on the top of the statistical model checker and genetic algorithm is used to select high impactful countermeasures. From that result, defense strategies are highlighted while a compromise guarantee between successful attacks, the cost incurred and the time to perform a sequence of attack actions. We report experiments applied over IoT network attacks.**

***Index Terms*—Risks Analysis ; IoT Based Systems; Attacks Assessment; Attack-Defense Trees; Defense Strategies Exploration**

I. Introduction

The growth of damage caused by attacks on IoT systems requires the definition of a rigorous methodology allowing to failure of attackers' strategies. The attacks are due to numerous vulnerabilities related to the large number of devices that can be used in the IoT systems and also the diversity of communication technologies that link these devices. Attackers exploit different vulnerabilities to circumvent the security countermeasures and damage the target system.

Various techniques can be used by the attackers which highlight the urgent need for proposing methods and tools that help security experts to analyze the potential attacks and define reliable defense configurations. Attacks require resources (equipment, tools, etc.) and time to be set up. The attacker takes into account these considerations and tries to increase the probability of success with a limited amount of resources. In the paper, we aim to identify a sufficient set of relevant countermeasures while finding a balance between the attack cost and its probability of success.

As shown in Figure 1, our approach consists of four steps: the two first steps start by collecting quantitative metrics of existing attacks on IoT systems and countermeasures used to protect the systems against those attacks. The third step consists of the construction of the Attack-Defense Tree (ADT) [1] as a logical formula while combining attacks and countermeasures. The fourth step provides the adequate countermeasures called "defense configuration" with the highest impact on attacks.

Attack-Defense Exploration tool [2] employed in this paper is built upon a Statistical Model Checking (SMC) tool [3] and the Genetic Algorithm (GA) [4]. GA synthesizes strategies that minimize the attack cost and maximizes the probability of an attack to succeed, whereas, SMC estimates the cost and the probability of an attack being successful under each strategy. Finally, an Impact-Optimal Defense (IO-Def) heuristic evaluates the impact of the defenses on the attack cost to pinpoint defense actions portraying a good balance between defenses and their provided impact on the attack cost regarding the organization's defense budget. Also, a benchmark description regarding the existing approaches is portrayed in paper [2].

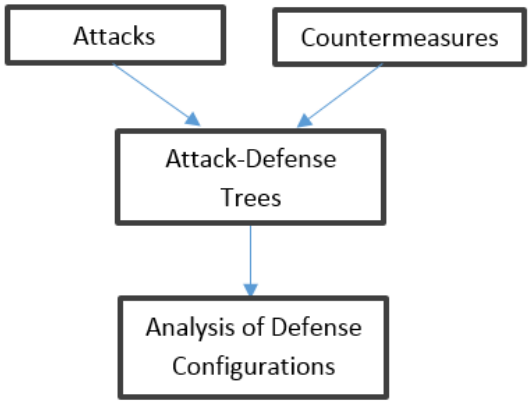

Fig. 1. Generic Attack-Defense Exploration Approach.

II. Attacks assessment

To evaluate and analyze different attacks that target IoT systems, certain metrics can be used. In our approach, attacks are characterized by the following metrics:

- LB: lower time bound in days needed to achieve the attack.
- UB: upper time allowed to perform the attack.
- $Cost$: charge of resources (stated in terms of dollars) required to perform the attack.
- Env : probability of attack success.

In the recent year, with the growth of IoT applications (smart buildings, health monitoring, energy management, etc.) and threats affecting these applications, several surveys and research papers such as [5], [6], [7] and [8] have highlighted the security issues by providing the potential attacks at each layer (application, support, communication, and perception) of IoT architecture. The authors in [5] provide a quantitative assessment of attacks by evaluating the probability of success, the impact, and the risk level. Starting from these studies, we identify the potential attacks and their characteristics.

TABLE I
IoT Network Attacks

ID	Name Attack	LB	UB	Cost	Env
SFA	Selective forwarding attacks	0	20	16 250	0.65
SiA	Sinkhole attacks	0	20	16 250	0.65
WoA	Wormhole attacks	0	20	16 250	0.65
SyA	Sybil attacks	0	20	16 250	0.65
TAA	Traffic analysis attacks	0	20	15 000	0.75
MMA	Man in the Middle Attacks	0	20	12 500	0.75
DoS	Denial of Service Attacks	0	20	15 000	0.75
SpA	Spoofing Attacks	0	20	13 000	0.65
UnA	Unauthorized Access	0	20	16 250	0.65
DDoS	Distributed Denial of Service	0	20	15 000	0.75
SCA	Side-Channel Attacks	0	20	10 500	0.35

Table I presents the attacks that target the communication layer. In this study, we consider 20 days as the time interval allowed to perform each attack. The probability of the specific attack being achieved is taken from [5]. The estimated cost of each attack is calculated using the formula from [9]:
$Cost = (probability/risk) \times impact$

A brief description of the attacks is given below:

(a) *Selective Forwarding Attacks* : In this attack, malicious node declines to transmit some packets in order to destroy the routing paths in the IoT network [5].

(b) *Sinkhole Attacks* : The attackers attempt to direct the IoT network traffic to a specific device to make it look attractive to other nodes [10].

(c) *Wormhole Attacks* : The attackers use malicious node to record packets at one location in the IoT network and then forward the network traffic data ignoring the intermediate nodes [11].

(d) *Sybil Attacks*: In this attack, malicious node claims multiple identities to mislead other nodes in the IoT network in order to impersonate them and gain access to the IoT system [12].

(e) *Traffic Analysis Attacks* : The attackers capture and analyze the IoT network packets to gather significant information, such as network flows or the payload of decrypted packets in the communication between devices [5].

(f) *Man in the Middle Attacks*: The attackers try to monitor and eavesdrop the communication between two IoT devices in order to access private data. They use malicious node to store and forward all data communicated between devices in order to violate the security of restricted data in IoT system [5].

(g) *Denial of Service Attacks*: The attackers try to create massive traffic in IoT networks in order to consume the resources and reduce the performance of the IoT system making IoT services unavailable. In Distributed Denial of Service (DDoS), devices are attacked from multiple sources in a distributed manner.

(h) *Spoofing Attacks*: The attackers attempt to get access to information from a valid tag or a valid IP address of authorized devices and then send malicious data with the obtained information in order to make these data seem valid [7].

(i) *Unauthorized Access* : The attackers try to obtain significant information from IoT devices to be able to access IoT services through authentication mechanisms.

(j) *Side-Channel Attacks* : The attackers attempt to acquire secret keys from the encryption protocols and then use them to decrypt the exchanged data and access the confidential information.

III. Countermeasures

Countermeasures are mechanisms that can be deployed to defend the system and thwart attacks exploiting its vulnerabilities. Several surveys like [5] and [7] have collected the different countermeasures for addressing attacks on IoT systems. In this work, we based on the study proposed by [6] that presents the recent countermeasures against the attacks identified in the previous section.

(a) *EPIC* : The framework proposed by [13] to protect IoT network against traffic analysis by preventing adversaries intercept the internet traffic. The framework integrates secure multi-hop routing protocols to guarantee the source/destination unlinkability and ensure the confidentiality of users' data.

(b) *SRAM-PUF*: The protocol proposed by [14] to check the authenticity of edge devices by using unclonable device IDs. It reduces the risk of spoofing attacks as well as unauthorized access by preventing adversaries from usurping the identity of devices.

(c) *SRPL*: Secure routing protocol proposed by [15] that uses the Hash Chain Authentication (HCA) technique to prevent malicious nodes from exploiting control messages values to create a fake topology. SRPL deals with several attacks like sinkhole attacks and selective forwarding attacks.

(d) *INTI*: Intrusion Detection System proposed by [16] to detect sinkhole attacks in IoT networks that use 6LoWPAN protocol. It analyzes the behavior of each node in the network and then identifies and isolates the malicious nodes launching the attacks.

(e) *C-IDS*: IDS proposed by [17] to detect wormhole attacks in IoT networks. The system combines the unsupervised clustering (using K-means) and Decision Tree techniques to identify the wormhole nodes.

(f) *SecTrust*: Trust aware RPL routing protocol proposed by [18] to make routing decisions and detect malicious nodes. The protocol allows to identify and isolate nodes that launch Sybil attacks.

(g) *SMQTT*: A secure extension of MQTT (Message Queue Telemetry Transport) protocol proposed by [19] to ensure Device to Device (D2D) security. SMQTT integrates Attribute-Based Encryption (ABE) algorithm to secure IoT networks against Man in the Middle Attacks.

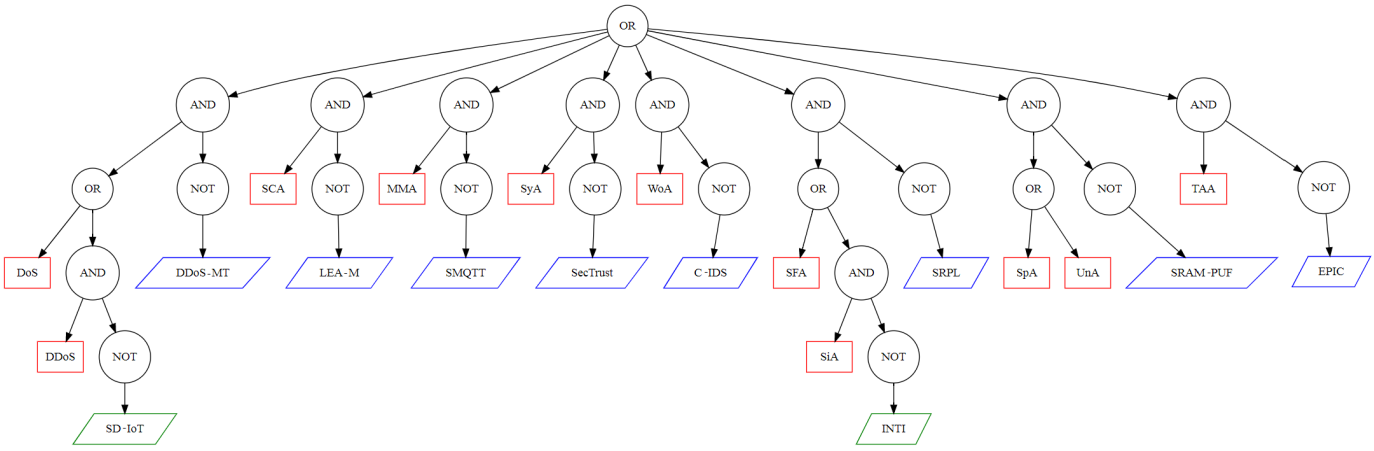

Fig. 2. Attack-Defense Tree.

(h) *DDoS-MT*: The framework proposed by [20] to detect and block DDoS attacks and DoS attacks. DDoS-MT is composed of an analysis module that checks whether the incoming traffic is suspicious or not and a monitoring module that categorizes the suspicious traffic to DoS or DDoS.

(i) *SD-IoT* : The framework proposed by [21] that uses SDx (Software-Defined anything) paradigm and a technique called CSV (Cosine Similarity of Vectors) to detect and mitigate DDoS attacks.

(j) *LEA-M*: Encryption algorithm [22] based on LEA (Lightweight Encryption Algorithm) that masks secret keys of cryptographic implementations rendering side-channel attacks hard.

IV. Attack-Defense Tree

Several works have employed *Trees* for attacks modeling and risk analysis. For instance, Attacks Trees (ATs) [23] are used for modeling the combinations of attacks that allow achieving a malicious goal. Extensions of ATs such as Defense Trees (DTs) [24] were proposed to incorporate defense mechanisms. In this work, we use Attack-Defense Trees (ADT) [1] that integrate ATs and DTs concepts.

Figure 2 shows the ADT that models the various combinations of attacks presented in Section II and countermeasures discussed in the previous Section. Attack nodes are represented by rectangles and defense nodes by parallelograms (impactful defenses in blue and not impactful defenses in green). We express the combinations between the nodes by operators (AND, OR, NOT) depicted by ellipses.

For example, both *Spoofing Attacks* (SpA) and *Unauthorized Access Attacks* (UnA) can be blocked by the countermeasure *SRAM-PU*. ADT will be used to analyze attacks and explore impactful defense configurations.

V. Analysis of Defense configurations

Attack-Defense Exploration tool [2] starts by exploring the cost-effective attacks that are most likely to succeed, then it identifies a set of countermeasures that block these attacks. The selected countermeasures increase the attack's cost. It is good to block all possible attacks in ADT, but for organizations with a limited defense budget, it is important to select countermeasures that make the system harder to attack.

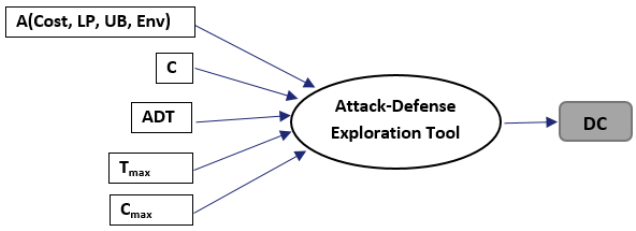

Fig. 3. Attack-Defense Exploration Tool.

As shown in Figure 3, the input of the tool is the risk assessment model composed of a set of attacks `A` with their characteristics (`Cost`, `LP`, `UB`, `Env`), a set of countermeasures `C`, `ADT` expressed as logic formula, and the constraints T_{max} (time to perform attacks) and C_{max} (budget of resources used in attacks). The output is a defense configuration `DC` composed of a set of impactful countermeasures.

The tool allows also to generate the graphical representation of ADT as in Figure 2 showing the selected countermeasures (impactful defenses) in blue parallelograms and the other not impactful defenses in green parallelograms.

The analysis of the risk assessment model consists of exploring the defense configurations that have the largest impact on certain attacker profiles, based on budget and time constraints.

In Table II, we distinguish two configurations that correspond to organizations with sufficient (`DC1`) and limited (`DC2`) defense budgets. In both cases, we consider the same time constraint T_{max}=`300 days`.

In `DC1`, we consider attackers with important resources C_{max}=`500 000 $` used to perform attacks defined in Table I. The exploration results presented in Figure 2 and Table II show that role played by countermeasures "`INTI`" and "`SD-IoT`" is negligible. According to the analysis carried out,

DC1 can also block other attacker profiles with C_{max}=100 000 $ and T_{max}=300 days, or with C_{max}=150 000 $ and T_{max}=150 days.

For organizations with limited budget, the configuration DC2 = {EPIC, SRAM-PUF, SMQTT, DDoS-MT} can be deployed to block the most cost-effective attacks with budgetary constraint C_{max} = 49 000 $ and time constraint T_{max}=300 days. DC2 is also impactful for attackers with budget C_{max} = 50 000 $ and time constraint T_{max}=150 days.

TABLE II
DEFENSE CONFIGURATIONS

DC	C_{max}	T_{max}	Countermeasures
1	500 000	300	EPIC, SRAM-PUF, SRPL, C-IDS, SecTrust, SMQTT, DDoS-MT, LEA-M
2	49 000	300	EPIC, SMQTT, DDoS-MT, SRAM-PUF

VI. CONCLUSION

In this paper, we have proposed an approach for the automatic identification of impactful countermeasures that can increase the cost of attacks and decrease their probability of success. A balance between defenses and their impact on attack cost is realized to produce security configuration related to IoT infrastructure. The security expert can select the best configuration according to the organization's budget. We have applied our approach to IoT network attacks. We are planning in the future to enhance the approach by introducing more quality metrics such as energy.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Union through the BRAIN-IoT project H2020-EU.2.1.1. Grant agreement ID: 780089.

REFERENCES

[1] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer, "Foundations of Attack–Defense Trees," in *Formal Aspects of Security and Trust*, P. Degano, S. Etalle, and J. Guttman, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, vol. 6561, pp. 80–95.

[2] B. L. Mediouni, A. Nouri, M. Bozga, A. Legay, and S. Bensalem, "Mitigating Security Risks Through Attack Strategies Exploration," in *Leveraging Applications of Formal Methods, Verification and Validation. Verification*, T. Margaria and B. Steffen, Eds. Cham: Springer International Publishing, 2018, vol. 11245, pp. 392–413.

[3] B. L. Mediouni, A. Nouri, M. Bozga, M. Dellabani, A. Legay, and S. Bensalem, "SBIP 2.0: Statistical Model Checking Stochastic Real-time Systems," in *ATVA 2018 - 16th International Symposium Automated Technology for Verification and Analysis*. Los Angeles, CA, United States: Springer, Oct. 2018, pp. 536–542.

[4] B. L. Mediouni, S. Niar, R. Benmansour, K. Benatchba, and M. Koudil, "A bi-objective heuristic for heterogeneous MPSoC design space exploration," in *2015 10th International Design & Test Symposium (IDT)*. Dead Sea, Amman, Jordan: IEEE, Dec. 2015, pp. 90–95.

[5] P. I. Radoglou Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, "Securing the Internet of Things: Challenges, threats and solutions," *Internet of Things*, vol. 5, pp. 41–70, Mar. 2019.

[6] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, p. 102481, Jan. 2020.

[7] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[8] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, Jan. 2015.

[9] 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 *MILCOM 2006 - 2006 IEEE Military Communications conference*, 2006, pp. 1–7.

[10] M. M. Ahemd, M. A. Shah, and A. Wahid, "IoT security: A layered approach for attacks defenses," in *2017 International Conference on Communication Technologies (ComTech)*, April 2017, pp. 104–110.

[11] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, Oct 2017.

[12] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, July 2015, pp. 180–187.

[13] J. Liu, C. Zhang, and Y. Fang, "EPIC: A Differential Privacy Framework to Defend Smart Homes Against Internet Traffic Analysis," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1206–1217, Apr. 2018.

[14] U. Guin, A. Singh, M. Alam, J. Canedo, and A. Skjellum, "A Secure Low-Cost Edge Device Authentication Scheme for the Internet of Things," in *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*. Pune: IEEE, Jan. 2018.

[15] G. Glissa, A. Rachedi, and A. Meddeb, "A Secure Routing Protocol Based on RPL for Internet of Things," in *2016 IEEE Global Communications Conference (GLOBECOM)*. Washington, DC, USA: IEEE, Dec. 2016, pp. 1–7.

[16] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. Ottawa, ON, Canada: IEEE, May 2015, pp. 606–611.

[17] P. Shukla, "ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things," in *2017 Intelligent Systems Conference (IntelliSys)*. London: IEEE, Sep. 2017, pp. 234–240.

[18] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things," *Future Generation Computer Systems*, vol. 93, pp. 860–876, Apr. 2019.

[19] M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," in *2015 Fifth International Conference on Communication Systems and Network Technologies*. Gwalior, India: IEEE, Apr. 2015, pp. 746–751.

[20] V. Adat and B. B. Gupta, "A DDoS attack mitigation framework for internet of things," in *2017 International Conference on Communication and Signal Processing (ICCSP)*. Chennai: IEEE, Apr. 2017, pp. 2036–2041.

[21] D. Yin, L. Zhang, and K. Yang, "A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework," *IEEE Access*, vol. 6, pp. 24 694–24 705, 2018.

[22] J. Choi and Y. Kim, "An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system," in *2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, 2016, pp. 1–4.

[23] S. Mauw and M. Oostdijk, "Foundations of Attack Trees," in *Information Security and Cryptology - ICISC 2005*, D. H. Won and S. Kim, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, vol. 3935, pp. 186–198.

[24] S. Bistarelli, F. Fioravanti, and P. Peretti, "Defense trees for economic evaluation of security investments," in *First International Conference on Availability, Reliability and Security (ARES'06)*, April 2006, pp. 8 pp.–423.