A Survey on IoT Security and its Vulnerabilities with First Empirical Look on Internet-scale IoT Exploitations

John Bennet J

Department of Computer Science and Engineering, Bethlahem Institute of Engineering, Karungal, Tamilnadu, India.

***

Abstract- The security issue impacting the Internet-of-Things (IoT) paradigm has recently attracted significant attention from the research community. In this context, we initially provide a comprehensive classification of state-of-the-art surveys, which address various dimensions of the IoT paradigm. This aims at facilitating IoT research endeavors by amalgamating, comparing and contrasting dispersed research contributions. Subsequently, we provide a unique taxonomy, which sheds the light on IoT vulnerabilities, their attack vectors, impacts on numerous security objectives, attacks which exploit such vulnerabilities, corresponding remediation methodologies and currently offered operational cyber security capabilities to infer and monitor such weaknesses. Additionally, motivated by the lack of empirical (and malicious) data related to the IoT paradigm, this work also presents a first look on Internet-scale IoT exploitations by drawing upon more than 1.2 GB of macroscopic, passive measurements' data. Insightful findings, inferences and outcomes in addition to open challenges and research problems are also disclosed in this work, which we hope would pave the way for future research endeavors addressing theoretical and empirical aspects related to the imperative topic of IoT security.

Index Terms—Internet of Things, IoT Vulnerabilities, IoT Data, IoT Security, Network Security

1. INTRODUCTION

People-centric IoT solutions, for instance, significantly enhance daily routines of elderly and disabled people, thus increasing their autonomy and self-confidence. Implantable and wearable IoT devices monitor and extract vital measurements to enable the real-time emergency alerting in order to increase patients' chances of survival. This emerging technology is also being leveraged to reduce response times in reacting to abrupt health incidents such as the sudden infant death syndrome during sleep.

Safety-centric IoT solutions endeavor to minimize hazardous scenarios and situations. For example, the concept of connected vehicles prevents the driver from deviating from proper trajectory paths or bumping into objects. Moreover, IoT sensors at factories monitor environmental pollution and chemical leaks in water supply, while smoke, toxic gases and temperature sensors coupled with warning systems prevent ecological disasters. Indeed, a number of case-studies have reported on the significant impact of IoT on natural resources' integrity and consumption.

The undeniable benefits proposed by the IoT paradigm, nevertheless, are coupled with serious security flaws. Profit-driven businesses and time-to-market along with the shortage of related legislation have stimulated manufacturers to overlook security considerations and to design potentially vulnerable IoT devices, opening the door for adversaries, which often exploit such devices with little or no effort. Moreover, poorly designed devices allow the execution of arbitrary commands and re-programming of device firmware. Among the many cases that recently attracted the public attention, the cyber attack provides a clear example of the severity of the threat caused by incrementing exploited IoT devices.

While the disclosure of private and confidential information coupled with the launch of debilitating DoS attacks cause various privacy violations and business disruptions, the most significant danger from exposed IoT devices remains the threat to people's lives and well-being. While benefits from using these IoT devices and corresponding technologies possibly outweigh the risks, undoubtedly, IoT security at large should be carefully and promptly addressed.

Several technical difficulties, including limited storage, power, and computational capabilities, challenge addressing various IoT security requirements. For instance, the simple issue of unauthorized access to IoT devices by applying default user credentials remains largely unsolved. IoT manufacturers, though aware of this flaw, do not mitigate this risk by design, making consumers take responsibility of this technical task and to update their device firmware.

2. RELATED SURVEYS

The rapid growth and adoption of the IoT paradigm have induced enormous attention from the research community. Tohighlight the latest findings and research directions in such an evolving field, a plethora of surveys were put forward to shed the light on recent IoT trends and challenges such as (i) protocols and enabling technologies, (ii) application domains, (iii) context awareness, (iv) legal frameworks, (v) attacks against IoT, (vi) access models, (vii) security protocols, and (viii) intrusion detection techniques.

A. IoT Architectures and Corresponding Technologies

In this we discussed two different perspectives of IoT research, namely, Internet-oriented or Things-oriented. Research challenges and the most relevant enabling technologies with a focus on their role rather than their technical details

According to the results, these three epochs are respectively labeled as (i) tagged things, (ii) a web of things, and (iii) social IoT, cloud computing, and semantic data.

B. IoT Security

Very recently, a quantitative and a qualitative evaluation of available access control solutions for IoT. The highlighted solution achieved various security requirements, noting that the adoption of traditional approaches cannot be applied directly to IoT in many cases. We also declared that centralized and distributed approaches could complement each other when designing IoT-tailored access control.

Additionally, on numerous security features in addition to elaborating on the challenges of a distributed architecture to understand its viability for IoT. We concluded that while a distributed architecture might reduce the impact caused by a successful attack, it might also augment the number of attack vectors.

3. TAXONOMY OF IOT VULNERABILITIES: LAYERS, IMPACTS, ATTACKS, REMEDIATION AND SITUATIONAL AWARENESS CAPABILITIES

In this section, we elaborate on the proposed taxonomy by focusing on the IoT vulnerabilities as they inter-relay with several dimensions.

IoT Vulnerabilities

Based on the previously outlined methodology, an exhaustive analysis of the research works related to the field of IoT security yielded nine (9) classes of IoT vulnerabilities. Before we introduce the taxonomy, we describe such vulnerabilities, which aim at paving the way the elaboration of their multidimensional taxonomy as thoroughly described further in this section. For each class of vulnerabilities, we pinpoint a number of representative research works in their corresponding contexts.

Deficient physical security. The majority of IoT devices operate autonomously in unattended environments. Consequently, an attacker would cause physical damage to the devices, possibly unveiling employed cryptographic schemes, replicating their firmware using malicious node, or simply corrupting their control or cyber data.

Insufficient energy harvesting. IoT devices characteristically have limited energy and do not necessary possess the technology or mechanisms to renew it automatically

Inadequate authentication. The unique constraints within the context of the IoT paradigm such as limited energy and computational power challenge the implementation of complex authentication mechanisms.

Improper encryption. Data protection is of paramount importance in IoT realms, especially those operating in critical CPS (i.e., power utilities, manufacturing plants, building automation, etc). It is known that encryption is an effective mechanism to store and transmit data in a way that only authorized users can utilize it. As the strength of cryptosystems depend on their designed algorithms, resource limitations of the IoT affects the robustness, efficiency and efficacy of such algorithms. To this end, an attacker might be able to circum- vent the deployed encryption techniques to reveal sensitive information or control operations with limited, feasible effort. Representative research contributions in this context include [66]–[71].

Unnecessary open ports. Various IoT devices have unnecessarily open ports while running vulnerable services, permitting an attacker to connect and exploit a plethora of vulnerabilities.

Insufficient access control. Strong credential management ought to protect IoT devices and data from unauthorized access. It is known that the majority of IoT devices in conjunction with their cloud management solutions do not force a password of sufficient complexity

A. Security Impact

Given the extracted IoT vulnerabilities, we now elaborate on their impact on core security objectives, namely, confidentiality, integrity, availability, and accountability consistent with the taxonomy of Figure 2.

1) Confidentiality: This security objective is designed to protect assets from unauthorized access and is typically enforced by strict access control, rigorous authentication procedures, and proper encryption. Nevertheless. This work thus demonstrated that it is feasible to reveal a secret PIN sequence of key-based security systems, which included ATM and electronic door entries. Additionally, conducted penetration testing, fingerprinting, process enumeration, and vulnerability scanning of numerous consumer IoT devices.

Investigation unveiled that a large number of devices have unnecessary open ports which could be easily leveraged to leak confidential information related to operating systems, device types and transferred data.

2) Integrity: The integrity objective typically guarantees the detection of any unauthorized modifications and is routinely enforced by strict auditing of access control, rigorous hashing and encryption primitives, interface restrictions, input validations, and intrusion detection methods. These attacks undeniably cause disruptions and safety degradations. The researchers, nevertheless, pinpointed that the Malfunction Management Unit (MMU) typically maintains safety by switching the controller to a known-safe mode in case of a detected integrity violation. We noted that auditing mechanisms and restricting administrator access would contribute to better device security, thus reducing integrity issues.

3) Availability: In this context, two groups of availability issues associated with wireless visual sensor networks. These concerns include hardware and coverage failures. While the first group deals with issues such as damage devices, energy depletion and nodes' disconnection, the second group refers to the quality of the information transmitted by the device.

4) In this context, Ur et al. [51] investigated ownership rules, roles, and integrity monitoring capabilities of numerous types of home automation devices. We pinpointed various access control issues such as insufficiency of audit mechanisms and ability to evade the

A. Challenge 2. Inadequacy of Scalable Vulnerability Assessment Solutions

As noted, empirical measurements for inferring IoT maliciousness is essential, yet solely insufficient to secure the IoT paradigm. Indeed, vulnerable yet unexploited IoT devices cannot be addresses by employing the latter approach. Consequently, numerous devices remain vulnerable for future exploitation. Hence, such methods lack device variability and scalability. In this context, there is a need for IoT-tailored test beds which would enable

B. Challenge 4. Immaturity of Security Protocol Standardization and Reactive Frameworks

While many research efforts consider the IoT protocol's standardization, it is clear that they require future enhancement to tackle their limitations. Moreover, the heterogeneity of the IoT paradigm dictates generalization. Indeed, the immaturity of this standardization effort in combination with emerging attacks against the IoT paradigm indicates the need for standardization endeavors at large.

applied integrity rules.

IOT VULNERABILITIES: LESSONS LEARNED AND FUTURE PERSPECTIVE

In this section, we outline a number of research and operational challenges and pinpoint several initiatives (both technical and non-technical) for future work, which we believe are worthy of being pursued in this imperative

D. Challenge 1. Lack of Large-scale Identification Techniques of Exploited IoT Devices

One of the most significant challenges for future work is the design and implementation of Internet-scale solutions for addressing the IoT security problem. The widespread deployment of IoT in different private environments prevents visibility of IoT-related security incidents and thus hinders the adequate analysis of such data in order to identify, attribute and mitigate maliciousness.

E. Challenge 3. Limited Security-related Awareness Capabilities for IoT Users

This challenge addresses secure access to IoT devices and their data. It is indisputable that the ability to gain access to IoT devices by either brute-forcing their default credentials or by exploiting certain vulnerabilities remains a primary attack vector. Further, while using traditional password-based access methods seem to be the most frequently employed, new techniques rooted in biometric and context-aware methods are currently emerging for the IoT.

C. Challenge 5. Lack of Secure Software Development Processes

To assure sufficient level of IoT software security, proper and prompt operational actions should be established for the identified vulnerabilities. Another problem of significant importance is related to secure IoT code. IoT applications rely on tailored software applications, which could characteristically be vulnerable. We also noticed the lack of methods which aim at vetting deployed IoT code.

CONCLUSION

The IoT paradigm refers to scenarios where network connectivity and computing capability extends to embedded comprehensive study emanates many open research questions in the context of the security of the IoT paradigm. Specifically, Internet-scale solutions addressing the IoT security issue remain one of the most prominent challenges towards IoT resiliency. Research efforts are also required in the context of studying IoT-specific attacks and their malicious signatures. Indeed, such knowledge is essential in providing effective remediation solutions. Further, suitable schemes, which take into account IoT-specific threats coupled with their unique characteristics, undoubtedly require to be designed and integrated into firmware development cycles to contribute to securing IoT devices.

This survey and the initial empirical exploration presents a solid foundation for future research efforts. To this end, we foresee a number of future initiatives as briefed in this survey, including, exploring diverse strategies which aim at inferring malicious IoT devices in a large-scale for prompt remediation, empirical studies to investigate and characterize the generated traffic of such compromised IoT devices and formal attribution methodologies which would generate insightful inferences related to the causes and intentions of such Internet-wide IoT exploitations.

REFERENCES

[1] M. C. Domingo, "An overview of the internet of things for people with disabilities," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 584–596, 2012.

[2] M. Chan, D. Estève, J.-Y. Fourniols, C. Escriba, and E. Campo, "Smart wearable systems: Current status and future challenges," *Artificial intelligence in medicine*, vol. 56, no. 3, pp. 137–156, 2012.

[3] A. G. Ferreira, D. Fernandes, S. Branco, J. L. Monteiro, J. Cabral, A. P. Catarino, and A. M. Rocha, "A smart wearable system for sudden infant death syndrome monitoring," in *Industrial Technology (ICIT), 2016 IEEE International Conference on*. IEEE, 2016, pp. 1920–1925.

[4] I. Bisio, A. Delfino, F. Lavagetto, and A. Sciarrone, "Enabling iot for in-home rehabilitation: Accelerometer signals classification methods for activity and movement recognition," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 135–146, 2017.

[5] Stanford University, "The autism glass project at stanford medicine," http://autismglass.stanford.edu/.

[6] Patel, Prachi, "Autism glass takes top student health tech prize," https://www.scientificamerican.com/article/autism-glass-takes-top- student-health-tech-prize-slide-show1/.

[7] R. Coppola and M. Morisio, "Connected car: technologies, issues, future trends," *ACM Computing Surveys (CSUR)*, vol. 49, no. 3, p. 46, 2016.

[8] Centric Digital, "Internet of things applications part 2: The min- ing industry," https://centricdigital.com/blog/digital-trends/internet-of- things-applications-pt2-the-mining-industry/.

[9] Inter-American Development Bank (IDB),in association with the Korea Research Institute for Human Settlements (KRIHS), "Smart cities - international case studies," http://www.iadb.org/en/topics/emerging-and-sustainable-cities/ international-case-studies-of-smart-cities,20271.html.

[10] M. Stanislav and T. Beardsley, "Hacking iot: A case study on baby monitor exposures and vulnerabilities," *Rapid 7*, 2015.

[11] Franceschi-Bicchierai, Lorenzo, "How this internet of things stuffed animal can be remotely turned into a spy device," https://motherboard.vice.com/en us/article/qkm48b/how-this-internet- of-things-teddy-bear-can-be-remotely-turned-into-a-spy-device.

[12] ——, "Internet of things teddy bear leaked 2 million parent and kids message recordings," https://motherboard.vice.com/en us/article/ pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and- kids-message-recordings.

[13] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer*, vol. 50, no. 2, pp. 76–79, 2017.

[14] B. Herzberg, D. Bekerman, and I. Zifman, "Breaking down mirai: An iot ddos botnet analysis," https://www.incapsula.com/blog/malware- analysis-mirai-ddos-botnet.html, october, 2016.

Weagle,Stephanie, "Financial impact of mirai ddos attack on dyn revealed in new data," https://www.corero.com/blog/797-financial- impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data.html.