Elias Bou-Harb
Nataliia Neshenko

Cyber Threat Intelligence for the Internet of Things

Springer

Cyber Threat Intelligence for the Internet of Things

Elias Bou-Harb • Nataliia Neshenko

Cyber Threat Intelligence for the Internet of Things

Springer

Elias Bou-Harb
Information Systems and Cyber Security
The University of Texas at San Antonio
San Antonio, TX, USA

Nataliia Neshenko
Computer & Electrical Engineering
Florida Atlantic University
Boca Raton, FL, USA

ISBN 978-3-030-45857-7 ISBN 978-3-030-45858-4 (eBook)
https://doi.org/10.1007/978-3-030-45858-4

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Advancements in computing, communication, and sensing technologies are making it possible to embed, control, and gather vital information from tiny devices that are being deployed and utilized in practically every aspect of our modernized society. From smart home appliances to municipal water and electric industrial facilities to our everyday work environments, the next Internet frontier dubbed as the Internet of Things (IoT) is promising to revolutionize our lives and tackle some of our nation's most pressing challenges. While the seamless interconnection of IoT devices with the physical realm is envisioned to bring a plethora of critical improvements on many aspects and in diverse domains, it will undoubtedly pave the way for attackers that will target and exploit such devices, threatening the integrity of their data and the reliability of critical infrastructure. Furthermore, such compromised devices will undeniably be leveraged as the next generation of botnets, given their increased processing capabilities and abundant bandwidth. The aim of this book is to generate cyber threat intelligence related to Internet-scale inference and evaluation of malicious activities generated by compromised IoT devices to facilitate prompt detection, mitigation, and prevention of IoT exploitation.

In this context, the book initially provides 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, it provides 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 cybersecurity capabilities to infer and monitor such weaknesses. This aims at providing the reader with a multidimensional research perspective related to IoT vulnerabilities, including their technical details and consequences, which is postulated to be leveraged for remediation objectives. While several demonstrations exist in the literature describing the exploitation procedures of a number of IoT devices, the real time inference, characterization, and analysis of unsolicited IoT devices that are currently deployed in the wild are still in their infancy. The book addresses this imperative task by leveraging active and passive measurements to report on unsolicited Internet-scale

IoT devices. This work renders a first step towards exploring the utilization of passive measurements in combination with the results of active measurements to shed the light on the Internet-scale insecurities of the IoT paradigm. By correlating results of Internet-wide scanning with Internet background radiation traffic, this work discloses numerous compromised IoT devices in diverse sectors, including critical infrastructure and smart home appliances. To this end, it also analyzes their generated traffic to create effective mitigation signatures that could be deployed at local IoT realms. To support large-scale empirical data analytics in the context of IoT, the inferred and extracted IoT malicious raw data through an authenticated platform is made available. The outcomes of this work confirm the existence of such compromised devices on an Internet scale, while the generated inferences and insights are postulated to be employed for inferring other similarly compromised IoT devices, in addition to contributing to IoT cybersecurity situational awareness.

San Antonio, TX, USA — Elias Bou-Harb
Boca Raton, FL, USA — Nataliia Neshenko
January 2020

Acknowledgements

This work was supported by a grant from the U.S. National Science Foundation (NSF) (Office of Advanced Cyberinfrastructure (OAC) #1953050).

Contents

Chapter 1
Introduction

The conception of the prominent Internet-of-Things (IoT) notion is envisioned to improve the quality of modern life. People-centric IoT solutions, for instance, significantly enhance daily routines of elderly and disabled people, thus increasing their autonomy and self-confidence [8]. 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 [5]. 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 [9]. Moreover, advanced solutions for in-home rehabilitation strive to revolutionize physical therapy [3], while the Autism Glass [18] aims at aiding autistic children to recognize emotions of other people in real-time [16].

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. Further, such concept enables the automatic emergency notification of nearest road and medical assistance in case of accidents [6]. Additionally, autonomous, self-driving mining equipment keeps workers away from unsafe areas, while location and proximity IoT sensors allow miners to avoid dangerous situations [7]. Moreover, deployed 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 [14]. Indeed, a number of case-studies report on the significant impact of IoT on natural resources' integrity and consumption. For instance, water pressure sensors in pipelines monitor flow activity and notify operators in case of a leak, while smart IoT devices and systems enable citizens to control water and energy consumption [14]. In fact, the IoT notion is introducing notable solutions for contemporary operations, well-being and safety. In this context, several ongoing IoT endeavors, such as those illustrated in Fig. 1.1, promise to transform modern life and business models, hence improving efficiency, service level, and customer satisfaction.

E. Bou-Harb, N. Neshenko, *Cyber Threat Intelligence for the Internet of Things*,
https://doi.org/10.1007/978-3-030-45858-4_1