

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>

© Springer Nature Switzerland AG 2020

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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
Boca Raton, FL, USA
January 2020

Elias Bou-Harb
Nataliia Neshenko

Acknowledgements

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

Contents

- 1 Introduction 1**
 - 1.1 Context and Motivation 2
 - 1.2 Objectives and Contributions 3
 - 1.3 Notes on This Book’s Organization 5
 - References 5
- 2 Taxonomy of IoT Vulnerabilities 7**
 - 2.1 Research Trends in the Field 8
 - 2.2 Research Methodology 12
 - 2.3 IoT Vulnerabilities 13
 - 2.4 Taxonomy Overview 15
 - 2.5 Layers..... 17
 - 2.5.1 Device-Based Vulnerabilities 17
 - 2.5.2 Network-Based Vulnerabilities..... 18
 - 2.5.3 Software-Based Vulnerabilities 20
 - 2.6 Security Impact..... 22
 - 2.6.1 Confidentiality 23
 - 2.6.2 Integrity 24
 - 2.6.3 Availability 25
 - 2.7 Attacks..... 26
 - 2.7.1 Attacks Against Confidentiality and Authentication 26
 - 2.7.2 Attacks Against Data Integrity 28
 - 2.7.3 Attacks Against Availability 31
 - 2.8 Remediation 33
 - 2.8.1 Access and Authentication Controls 33
 - 2.8.2 Software Assurance 38
 - 2.8.3 Security Protocols 39

2.9	Situational Awareness Capabilities	41
2.9.1	Vulnerability Assessment	42
2.9.2	Honeypots	43
2.9.3	Network Discovery	44
2.9.4	Intrusion Detection	45
	References	50
3	Towards Inferring IoT Maliciousness	59
3.1	Inference of IoT Exploitation.....	59
3.1.1	Exploiting Darknet Data.....	60
3.1.2	Probing Inference	62
3.1.3	Correlation with Active Measurements.....	63
3.1.4	Generating IoT-Specific Malicious Signatures	64
3.2	Empirical Evaluation.....	65
3.2.1	First Empirical Look on Internet-Scale Exploitation of IoT Devices	65
3.2.2	Characterization and Signature Generation.....	68
3.2.3	A Closer Look into Hosting Environment.....	71
	References	75
4	Generating and Sharing IoT-Centric Cyber Threat Intelligence	77
4.1	Server Core Function	77
4.1.1	Data Aggregation Module	78
4.1.2	Data Processing Module.....	78
4.1.3	Auxiliary Functions.....	80
4.2	Client-Side Core Components	80
4.3	Performance Evaluation	82
	References	84
5	Concluding Remarks and Future Perspective	85
5.1	Challenges and Future Perspective	86
	References	89