

University of New Hampshire

University of New Hampshire Scholars' Repository

Master's Theses and Capstones

Student Scholarship

Fall 2020

Internet-of-Things (IoT) Security Threats: Attacks on Communication Interface

Mohammad Mezanur Monjur
University of New Hampshire, Durham

Follow this and additional works at: <https://scholars.unh.edu/thesis>

Recommended Citation

Monjur, Mohammad Mezanur, "Internet-of-Things (IoT) Security Threats: Attacks on Communication Interface" (2020). *Master's Theses and Capstones*. 1388.
<https://scholars.unh.edu/thesis/1388>

This Thesis is brought to you for free and open access by the Student Scholarship at University of New Hampshire Scholars' Repository. It has been accepted for inclusion in Master's Theses and Capstones by an authorized administrator of University of New Hampshire Scholars' Repository. For more information, please contact Scholarly.Communication@unh.edu.

INTERNET-OF-THINGS (IOT) SECURITY THREATS: ATTACKS ON
COMMUNICATION INTERFACE

BY

MOHAMMAD MEZANUR RAHMAN MONJUR

DISSERTATION

Submitted to the University of New Hampshire
in Partial Fulfillment of the Requirements for the Degree of

Master of Science
in
Electrical and Computer Engineering

September, 2020

This thesis will be examined by and approved in partial fulfillment of the requirements for the degree of Master of Science in Electrical Engineering by:

Thesis Director, Qiaoyan Yu, Ph.D.

Associate Professor

Department of Electrical & Computer Engineering

Md Shaad Mahmud, Ph.D.

Assistant Professor

Department of Electrical & Computer Engineering

Dongpeng Xu, Ph.D.

Assistant Professor

Department of Computer Science

On July, 2020

Original approval signatures are on file with the University of New Hampshire Graduate School.

ACKNOWLEDGEMENTS

First and foremost, I want to say thank you to my advisor Dr. Qiaoyan Yu. I received an enormous amount of help from her in both my course work and the project. Besides the academic aspect, she also gave me a lot of advice and encouragement when I made important decisions about my career. Most importantly, she helped me build up my interest and confidence in my research work.

I would like to thank Dr. Md Shaad Mahmud and Dr. Dongpeng Xu for their willingness to provide help on my thesis and other graduation work as my thesis committee members.

I would also like to thank my fellow graduate students in the UNH Reliable VLSI Systems Lab: Zhiming Zhang, Pruthvy Yellu, and Sandeep Sunkavilli. I got a lot of help and advice from them on my research, and I had a great time working with them.

Finally, I wish to thank my family for their support and care. I could not have come to this far in my life without their constant support, encouragement, and sacrifices of my family. Their support and care helped me overcome setbacks and stay focused on my graduate study.

Contents

Acknowledgements	iii
List of Tables	viii
List of Figures	ix
Abstract	xii
1 Introduction	1
1.1 Internet of Things	1
1.2 IoT Applications Vulnerability	3
1.3 Key Contributions	6
1.4 Thesis Outline	7
2 Background	10
2.1 Security Concerns on IoT Applications	10
2.2 IoT Protocol	11
2.2.1 Network Layer	11
2.2.2 Internet Layer	12
2.2.3 Transport Layer	12
2.2.4 Application Layer	13

2.3	IoT Vulnerability	13
2.3.1	Software Vulnerability	13
2.3.2	Network Vulnerability	15
2.3.3	Hardware Vulnerability	17
2.3.4	Chip Level Vulnerability	18
2.4	Conclusion	19
3	Bluetooth Low Energy Bulb Attack	20
3.1	Introduction	20
3.2	Preliminaries	21
3.2.1	Air-Gapped Networks	21
3.2.2	Smart Bulbs	22
3.2.3	Covert Data Exfiltration	25
3.3	Threat Model	27
3.3.1	Attack Condition	27
3.3.2	Smart Light Bulb Attack Model	27
3.4	Proposed Data Exfiltration	29
3.4.1	Exploiting Weaknesses of Bluetooth Protocol Stack to Develop At- tack Surface	29
3.4.2	Plans for Data Exfiltration	31
3.5	Implementation Covert Data Channel 1	32
3.5.1	Assumption, Tools, and Setup	32
3.5.2	Experiment	32
3.6	Implementation Covert Data Channel 2	35
3.6.1	Assumption, Tools and Setup	35

3.6.2	Experiment	37
3.7	Implementation Covert Data Channel 3	39
3.7.1	Assumption, Tools and Setup	39
3.7.2	Experiment	40
3.8	Conclusion	43
4	Physical Attack Implementation on Communication Protocols	44
4.1	Introduction	44
4.2	Background	45
4.2.1	Sensor Network	45
4.2.2	Temperature Sensor	46
4.3	Methodology	47
4.3.1	Attack Scenario 1	47
4.3.2	Attack Scenario 2	48
4.3.3	Experimental Setup	49
4.4	Experiment Results	50
4.5	Conclusion	52
5	Analog Trojan	53
5.1	Introduction	53
5.2	Attacks Crossing Analog and Digital Domains	55
5.2.1	Attack Models	56
5.2.2	Demonstration of Attack Examples	57
5.2.3	Challenges on Analog Attack Detection	60
5.3	Proposed Method for Analog Trojan Detection	61

5.4	Experimental Results	63
5.4.1	Effectiveness of Obfuscated Attack Detection	64
5.5	Hardware Cost	67
5.6	Conclusion	67
6	Conclusion and Future Work	68
6.1	Conclusion	68
6.2	Future Work	71
	References	72