

Solutions for Internet of Things Security Challenges: Trust & Authentication

Jason M. McGinthy

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Computer Engineering

Alan J. Michaels, Co-chair
T. Charles Clancy, Co-chair
Matthew Hicks
Allen B. MacKenzie
Walid Saad

June 18, 2019
Blacksburg, Virginia

Keywords: Security, Internet of Things, Standardization, Authentication, Lightweight
Copyright 2019, Jason M. McGinthy

Solutions for Internet of Things Security Challenges: Trust & Authentication

Jason M. McGinthy

(ABSTRACT)

The continuing growth of Internet-connected devices presents exciting opportunities for future technology. These Internet of Things (IoT) products are being manufactured and interleaved with many everyday activities, which is creating a larger security concern. Sensors will collect previously unimaginable amounts of private and public data and transmit all of it through an easily observable wireless medium in order for other devices to perform data analytics. As more and more devices are produced, many are lacking a strong security foundation in order to be the “first to market.” Moreover, current security techniques are based on protocols that were designed for more-capable devices such as desktop computers and cellular phones that have ample power, computational ability, and memory storage. Due to IoT’s technological infancy, there are many security challenges without proper solutions. As IoT continues to grow, special considerations and protections must be in place to properly secure this data and protect the privacy of its users. This dissertation highlights some of the major challenges related to IoT and prioritizes their impacts to help identify where gaps are that must be filled. Focusing on these high priority concerns, solutions are presented that are tailored to IoT’s constraints. A security feature-based framework is developed to help characterize classes of devices to help manage the heterogeneous nature of IoT devices and networks. A novel physical device authentication method is presented to show the feasibility in IoT devices and networks. Additional low-power techniques are designed and evaluated to help identify different security features available to IoT devices as presented in the aforementioned framework.

Solutions for Internet of Things Security Challenges: Trust & Authentication

Jason M. McGinthy

(GENERAL AUDIENCE ABSTRACT)

The Internet has been gaining a foothold in our everyday lives. Smart homes, smart cars, and smart cities are becoming less science fiction and more everyday realities. In order to increase the public's general quality of life, this new Internet of Things (IoT) technological revolution is adding billions of devices around us. These devices aim to collect unforeseen amounts of data to help better understand environments and improve numerous aspects of life. However, IoT technology is still in its infancy, so there are still many challenges still remaining. One major issue in IoT is the questionable security for many devices. Recent cyber attacks have highlighted the shortcomings of many IoT devices. Many of these device manufacturers simply wanted to be the first in a niche market, ignoring the importance of security. Proper security implementation in IoT has only been done by a minority of designers and manufacturers. Therefore, this document proposes a secure design for all IoT devices to be based. Numerous security techniques are presented and shown to properly protect the data that will pass through many of these devices. The overall goal for this proposed work aims to have an overall security solution that overcomes the current shortfalls of IoT devices, lessening the concern for IoT's future use in our everyday lives.

Dedication

To my family.

Acknowledgments

I would not have been able to achieve this goal without the support and encouragement of many people in my life. First, I would like to thank my wonderful wife, Janice. Without your support, I would have never been able to have the peace of mind to complete this journey. Your proof-reading and suggestions helped make this a document instead of technical jargon. You handled a busy household, completed your own degree, and never failed at making a good point when I needed advice. Next, I would like to thank my advisor, Dr. Alan Michaels, for continually encouraging and challenging me to push through roadblocks and put words on paper. Your guidance was monumental in helping me accomplish this dream. Finally, I would also like to thank the Department of Computer and Cyber Sciences at the United States Air Force Academy for giving me this opportunity to follow my dream. I look forward to returning and imparting the wisdom I have gained through this process into future Air Force officers.

Contents

List of Figures	xi
-----------------	----

List of Tables	xiv
----------------	-----

1 Introduction	1
1.1 The Internet	1
1.2 Evolution of IoT	2
1.2.1 The S in IoT is for Security	3
1.3 IoT Scenarios	3
1.3.1 Industry 4.0	4
1.3.2 Critical Infrastructures	5
1.3.3 Automotive	7
1.3.4 Wireless Avionics Intra-communication	8
1.3.5 Healthcare	10
1.3.6 Smart Consumer & Homes	11
1.4 Challenges in IoT Security	13
1.4.1 Standardization	13
1.4.2 Trust & Authentication	15
1.4.3 Privacy	15
1.4.4 Information Security	16
1.4.5 Network Attacks	19
1.4.6 Latency	20
1.4.7 Wireless Communications	20
1.4.8 Version Control & Updates	20
1.4.9 Physical Attacks	21

1.4.10	SWaP	22
1.5	Motivation for Efficiently Scalable Security in IoT	22
1.6	Outline and Research Contributions	24
1.6.1	Journal Manuscripts	25
1.6.2	Conference Papers	25
2	Feature-based Security Standardization	27
2.1	Acknowledgements	27
2.2	Background	28
2.3	Feature-based Security Levels	29
2.3.1	Class 3	31
2.3.2	Class 2	32
2.3.3	Class 1	33
2.3.4	Class 0	33
2.4	General Security Features	34
2.4.1	Physical Device Security	35
2.4.2	Trusted Execution Environment	35
2.4.3	Memory	36
2.4.4	Data Considerations	36
2.4.5	Clocks and Synchronization	37
2.4.6	Power Management	38
2.4.7	Boot Procedure	38
2.4.8	Key Management	38
2.4.9	Pseudorandom Number Generator	39
2.4.10	Encryption	40
2.4.11	Message Validation	42
2.4.12	Hash Engine	43
2.4.13	Modulation	43
2.4.14	TRANSEC	44

2.4.15	Data Logging	45
2.5	Summary	45
3	Authentication using Neural Network-Based Specific Emitter Identification	47
3.1	Acknowledgements	48
3.2	Recent Work	49
3.3	Security Background	49
3.3.1	IoT Security	50
3.3.2	Multi-factor Authentication	52
3.4	IoT Model	53
3.4.1	Network Configuration	53
3.4.2	Devices	56
3.5	SEI Background	57
3.5.1	Traditional SEI Techniques	57
3.5.2	NN Approaches to SEI	58
3.5.3	Considered Approach	58
3.6	NN-based SEI for IoT	62
3.6.1	One-Way SEI	63
3.6.2	Mutual Authentication Through a Secondary Device	64
3.6.3	Authentication-as-a-Service	64
3.7	IoT Implementation Results	65
3.8	Summary	67
4	Low-Power PRNG-based Key Derivation Function	69
4.1	Acknowledgements	69
4.2	Background and Related Work	70
4.2.1	Comparison to TLS 1.3 HKDF	71
4.3	Key Derivation	73

4.3.1	Selected Techniques	75
4.3.2	Aliasing	78
4.3.3	Entropy	82
4.3.4	Randomness	84
4.3.5	Correlation	86
4.4	Results	86
4.4.1	Aliasing	86
4.4.2	Entropy	86
4.4.3	Randomness	87
4.4.4	Correlation	87
4.5	PRNG-Based Security	88
4.5.1	NIST Statistical Test Suite	89
4.5.2	Law of the Iterated Logarithm	90
4.5.3	Joint Entropy	92
4.6	Non-Standard Length Key Derivation	92
4.7	Software and Hardware Performance Characterization	92
4.7.1	Software Implementation	93
4.7.2	Hardware Implementations	96
4.8	Summary	98
5	Lightweight Encryption using Galois Extension Field Arithmetic	100
5.1	Acknowledgements	100
5.2	Background	101
5.3	Stream-Cipher Cryptography using Galois Extension Field Multiplication . .	102
5.4	Evaluation of Randomness	106
5.5	MSP430 Implementation	108
5.6	Applications of Selectively Invertible Galois Extension Field Techniques . . .	110
5.7	Summary	111

6	Semi-Coherent Transmission Security	112
6.1	Acknowledgements	113
6.2	System Overview	113
6.2.1	Spread Spectrum Modulation	113
6.2.2	Semi-Coherent TRANSEC	114
6.2.3	Session Key Protection	115
6.3	System Design	115
6.3.1	Perturbation Types	116
6.3.2	Phase Modulation	117
6.3.3	Discrete Phase State Mapping	122
6.3.4	Energy Per Symbol Calculations	123
6.4	Exemplary Design	123
6.5	Simulation Results	124
6.5.1	Calculated Performance Loss	124
6.5.2	Symbol Energy Calculations	125
6.6	Summary	126
7	Conclusions and Future Research	128
7.1	Security Level-based Standardization Framework	130
7.2	Neural Network-based Specific Emitter Identification	131
7.3	PRNG-based Key Derivation Function	133
7.4	Galois Extension Field Cryptographic Functions	134
7.5	Semi-Coherent Transmission Security	134
7.6	Ideal Contribution Use Cases	135
7.7	Final Remarks	136
	Bibliography	138