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

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