Defense Against Integrity and Privacy Attacks

in

The Internet of Things

A thesis submitted in fulfillment
of the requirements for the degree of

Doctor of Philosophy

by

Imran Makhdoom
School of Electrical and Data Engineering
Faculty of Engineering and Information Technology
University of Technology Sydney
NSW 2007, Australia

August 2020

ABSTRACT

The world is resorting to the Internet of Things for ease of control and monitoring of smart devices. The ubiquitous use of the Internet of Things ranges from Industrial Control Systems to e-Health, e-Commerce, smart cities, supply chain management, smart cars, and a lot more. Such reliance on the Internet of Things is resulting in a significant amount of data to be generated, collected, processed, and analyzed. The big data analytics is no doubt beneficial for business development. However, at the same time, numerous threats such as attacks on message and device integrity, the vulnerability of end-devices to malware attacks, physical compromise of devices, and threats to user data security and privacy pose a great danger to the sustenance of Internet of Things. Therefore, it is the need of the hour to develop a security mechanism for the Internet of Things systems to ensure the integrity and privacy of data being processed by these systems.

This study thus endeavors to highlight most of the known threats at various layers of the Internet of Things architecture with a focus on the anatomy of some of the significant attacks. The research also construes a detailed attack methodology adopted by some of the most successful malware attacks on the Internet of Things, including Industrial Control Systems and Cyber Physical Systems. The study further infers an attack strategy of a Distributed Denial of Service attack through the Internet of Things botnet followed by requisite security measures. The illustration of attack methodologies is followed by a composite guideline for the development of an Internet of Things security framework based on industry best practices.

Sequel to the Internet of Things threat modeling, this research investigates the use of blockchain technology to protect the Internet of Things against data integrity and privacy attacks. Hence, to arrive at intelligible conclusions, a systematic study of the peculiarities of the Internet of Things environment, including its security and performance requirements and progression in blockchain technologies, is carried out. Moreover, this thesis also identifies unique challenges to blockchain's adoption in the Internet of Things and recommends a possible way forward.

Based on a systematic and analytical review of blockchain technology, this study proposes a privacy-preserving and secure data sharing framework for smart cities. The proposed scheme preserves user data privacy by dividing the blockchain network into various channels, where every channel comprises a finite number of authorized organizations and processes a specific type of data such as health, smart car, smart energy, or financial details. Moreover, access to users' data within a channel is controlled by embedding access control rules in the smart contracts. The

devised solution also conforms to some of the essential requirements outlined in the European Union General Data Protection Regulation.

Another important contribution of this work is the conception and design of a novel Internet of Things centric consensus protocol with the Internet of Things focused transaction validation rules. The proposed Proof-of-Honesty consensus protocol not only reduces the possibility of Byzantine behavior by block proposers (validator/mining nodes) during the consensus process but is also scalable with low communication complexity. It is believed that the proposed consensus protocol will prove to be a governing factor for the Internet of Things systems considering to adopt blockchain technology.

Correspondingly, the main conclusion of this research and evaluation is that a sensibly selected and carefully designed blockchain-based IoT application can provide some assurance to the users concerning the security and privacy of their data. In this context, the focus should be on developing an IoT-centric consensus protocol with an intelligent misbehavior detection mechanism to detect and identify malicious miner/validator nodes. Moreover, validation of IoT devices' integrity is also an open challenge that requires due attention.

STATEMENT OF ORIGINAL AUTHORSHIP

I, Imran Makhdoom, declare that this thesis is submitted in fulfillment of the requirements for the award of the degree of Doctor of Philosophy in the School of Electrical and Data Engineering, Faculty of Engineering and Information Technology, at the University of Technology Sydney.
This thesis is wholly my work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.
This document has not been submitted for qualifications at any other academic institution.
This research is supported by the Australian Government Research Training Program.
This research was also [partially] supported by funding from Food Agility CRC Ltd, funded under the Commonwealth Government CRC Program. The CRC Program supports industry-led collaboration between industry, researchers, and the community.

Signed:

Production Note:
Signature removed prior to publication.

Imran Makhdoom
3 August 2020

STATEMENT OF THE TYPE OF THESIS

The thesis is structured as a single manuscript comprising a combination of chapters. Whereas, the chapters other than the Introduction Chapter, are the compilation of published/publishable work.

ACKNOWLEDGEMENTS

I express my profound gratitude to my supervisors, A/Prof Mehran Abolhasan (Principal Supervisor), A/Prof Justin Lipman (Co-Supervisor), and Dr. Wei Ni (External Supervisor) for their fruitful guidance and support throughout my Ph.D. candidature. Their encouragement and regular interactive meetings made my experience very productive. I am especially thankful to Dr. Mehran for his kind support that enabled me to focus on my research. He was also very supportive in terms of providing assistance to me to attend international conferences.

I am also thankful to the University of Technology Sydney for giving me the opportunity to pursue my Ph.D. studies by granting me scholarships to cover my tuition fee and living expenses. I also acknowledge the handwork put in by the School of Electrical and Data Engineering staff to provide efficient admin and academic support to the research students.

In the end, I would like to extend my gratitude to my parents for their kind prayers, my lovely wife for taking care of me and the kids, and also for bearing with me during hard times.

LIST OF PUBLICATIONS

Journal Papers

J-1. I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, "Anatomy of Threats to the Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1636-1675, Secondquarter 2019. **Research Question 1**

J-2. I. Makhdoom, M. Abolhasan, H. Abbas and W. Ni, "Blockchain's Adoption in IoT: The Challenges, and a Way Forward," Journal of Network and Computer Applications, vol. 125, pp. 251–279, 2018. **Research Question 2**

J-3. I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman and W. Ni, "PrivySharing: A Blockchain-Based Framework for Privacy-Preserving and Secure Data Sharing in Smart Cities," Computers & Security, vol. 88, pp. 101653, 2020. **Research Question 3**

Conference Papers

C-1. I. Makhdoom, M. Abolhasan, H. Abbas and W. Ni, "Blockchain for IoT: The Challenges and a Way Forward," in 15^{th} International Conference on Security and Cryptography (SECRYPT), Porto, Portugal, Jul. 2018, pp. 428-439. **Research Question 2**

C-2. I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman and W. Ni, "PrivySharing: A Blockchain-Based Framework for Privacy-Preserving and Secure Data Sharing in Smart Cities," in 16^{th} International Conference on Security and Cryptography (SECRYPT), Prague, Czech Republic, Jul. 2019, pp. 363-371. **Research Question 3**

C-3. I. Zhou, I. Makhdoom, M. Abolhasan, J. Lipman and S. Negin, "A Blockchain-based File-sharing System for Academic Paper Review," in 13^{th} International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, Queensland, Australia, Dec. 2019, pp. 1-10.

C-4. I. Makhdoom, F. Tofigh, I. Zhou, M. Abolhasan and J. Lipman, "PLEDGE: A Proof-of-Honesty based Consensus Protocol for Blockchain-based IoT Systems," **In press** in the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, Canada, May. 2020. **Research Question 4**

Patents

P-1. I. Makhdoom, F. Tofigh, “A Method of Electronic Device Integrity Check Based on Device Digital Genome (D2iGen),” Australia Patent 2018204784, Jun. 29, 2018.

CONTENTS

List of Figures

List of Tables

List of Acronyms

ADEPT	Autonomous Decentralized Peer-to-Peer Telemetry
ADS	Alternate Data Streams
AI	Artificial Intelligence
AP	Attribute Provider
API	Application Program Interface
App	Application
Approx	Approximately
ARP	Address Resolution Protocol
ASIC	Application Specific Integrated Circuit
AT&T	American Telephone & Telegraph
Avg	Average
BFT	Byzantine Fault Tolerance
BLE	Bluetooth Low Energy
BNC	Business Network Card
BPDIMS	Blockchain-based Personal Data and Identity Management System
BSN	Biomedical Sensor Network
BSoD	Blue Screen of Death
CA	Certificate Authority
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CASB	Cloud Access Security Broker
CC	Channel Configuration
CCS	Command and Control Server
CERT	Computer Emergency Response Team
CH	Cluster Head
Ch	Channel
CIoT	Cognitive IoT
CMSP	Channel Membership Service Provider
CN	Core Network
CoAP	Constrained Application Protocol
CPS	Cyber Physical System

CSMA	Carrier Sense Multiple Access
CTO	Chief Technology Officer
DApps	Decentralized Applications
DAC	Decentralized Autonomous Corporation
DAG	Directed Acyclic Graph
DAO	Decentralized Autonomous Organization
DARPA	Defense Advanced Research Projects Agency
DBFT	Delegated Byzantine Fault Tolerance
DDoS	Distributed Denial of Service
DKOM	Direct Kernel Object Manipulation
DH	Diffie Hellman
DHT	Distributed Hash Table
DLT	Distributed Ledger Technology
DNS	Domain Name System
DoS	Denial of Service
DPoS	Delegated Proof of Stake
DSS	Digital Signature Standard
DTLS	Datagram Transport Layer Security
DVR	Digital Video Recorder
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-only Memory
eNB	evolve NodeB
EU	European Union
EU GDPR	European Union General Data Protection Regulation
EVM	Extended Verification Module
FCM	Fuzzy Cognitive Maps
Fintech	Financial Technology
FMC	Follow Me Cloud
FTP	File Transfer Protocol
FTTH	Fiber-To-The-Home
GDPR	General Data Protection Regulation
GSM	Global System for Mobile Communications
HDFS	Hadoop Distributed File System
HIPPA	Health Insurance Portability Accountability Act
IAT	Import Address Table
ICS	Industrial Control System
ID	Identity
IDM	Identity Management
IDP	Identity Provider
IDS	Intrusion Detection System
IMA	Integrity Measurement Architecture

IoT	Internet of Things
IoV	Internet of Vehicles
IPFS	Interplanetary File System
IPS	Intrusion Protection System
ISMS	Information Security Management System
ITS	Intelligent Transportation System
JTAG	Joint Test Action Group
KSI	Keyless Signature Infrastructure
LDAP	Lightweight Directory Access Protocol
LMSP	Local Membership Service Provider
LTE	Long Term Evolution
MAC	Medium Access Control
MB	Megabytes
MBR	Master Boot Record
MCMC	Markov Chain Monte Carlo
MEC	Mobile Edge Computing
MITM	Man-In-The-Middle Attack
MMC	Mobile Micro Cloud
ML	Machine Learning
MSISDN	Mobile Station International Subscriber Directory Number
MSP	Membership Service Provider
M2M	Machine-to-Machine
ms	Milliseconds
NC	Network Configuration
NMS	Network Management System
NMSP	Network Membership Service Provider
NIST	National Institute of Standards and Technology
O	Organization
OAuth	Open Authorization
ODS	Ordering Service
OFC	Optical Fiber Cable
OOK	On-Off-Keying
OPC	Open Platform Communications
OS	Operating System
OSI	Open Systems Interconnection
OSN	Online Social Networks
OTA	Over-The-Air
OTAA	Over-The-Air Activation
OWAC	One Way Accountable Channel
OWASP	Open Web Application Security Project
P2P	Peer-to-Peer

P2PKH	Pay to Public Key Hash
PBFT	Practical Byzantine Fault Tolerance
PII	Personally Identifiable Information
PIPEDA	Personal Information Protection and Electronic Documents Act
PKG	Public Key Generator
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PoA	Proof-of-Activity
PoC	Proof-of-Concept
PoET	Proof-of-Elapsed-Time
PoS	Proof-of-Stake
PoT	Proof-of-Trust
PoW	Proof-of-Work
PoH	Proof-of-Honesty
PubKeyHash	Public Key Hash
PubKeyScript	Public Key Script
QoS	Quality of Service
RAT	Remote Access Trojan
RCA	Root Certificate Authority
RFID	Radio Frequency Identification
RPL	Routing Protocol for Lossy Networks
RT-IoT	Real-Time Internet of Things
SCADA	Supervisory Control and Data Acquisition
SCC	Small Cell Cloud
SCeNB	Small Cell evolve NodeB
SCM	Supply Chain Management
SDN	Software Defined Network
SED	Self Encrypting Drives
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SigScript	Signature Script
SMB	Server Message Block
SMP	Security Management Provider
SoC	System on Chip
SSH	Secure Shell
TCG	Trusted Computing Group
TCS	Trusted Candidate Set
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TOR	The Onion Router
TPM	Trusted Platform Module

TPS	Transactions Per Second
TX	Transaction
UART	Universal Asynchronous Receiver Transmitter
UDP	User Datagram Protocol
UE	User Equipment
UI	User Interface
UMTS	Universal Mobile Telecommunications Service
USD	United States Dollar
VANET	Vehicular Ad-Hoc Networks
Ver	Version
VPN	Virtual Private Network
V2V	Vehicle-to-Vehicle
VRF	Verifiable Random Function
WAP	Wireless Application Protocol
WebRTC	Web Real-Time Communications
WSN	Wireless Sensor Network
WWW	World Wide Web
XPolM	Cross-Polarization Modulation
XSS	Cross-Site Scripting
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks