Advanced Sciences and Technologies for Security Applications

The series Advanced Sciences and Technologies for Security Applications comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

More information about this series at http://www.springer.com/series/5540

Cristina Alcaraz
Editor

Security and Privacy Trends in the Industrial Internet of Things

Springer

Editor
Cristina Alcaraz
Computer Science Department
University of Malaga
Malaga, Spain

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-030-12329-1 ISBN 978-3-030-12330-7 (eBook)
https://doi.org/10.1007/978-3-030-12330-7

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

We are increasingly witnessing how the industry in general is modernizing its underlying critical systems to move toward the fourth industrial revolution, commonly known as Industry 4.0. This new industrial paradigm encompasses, among others, the Industrial Internet of Things (IIoT) as one of the most relevant technologies of the today's industry. Through IIoT, it is possible to open the industrial connections to address effective and more extensive controls, allowing monitoring from anywhere, at any time, and in anyhow, and in this way to increase the effectiveness and reliability of production states, reduce operational costs, and improve the overall market economy.

Although there exist already consortiums and bodies working on the deployment of this technology, there are also diverse entities (academy, governments, international organizations, and industries) working on many aspects related to security and privacy. Particularly, certain interest issues deserve to be considered in their own right. For example, the hardware and software limitations of the vast majority of the IIoT devices do not help provide complex and robust security approaches; and the current predominance to lead advanced persistent attacks in the diverse industrial sectors brings about numerous security risks. There exists a special attraction to track and exploit zero-day vulnerabilities in order to proceed with potential attacks related to information exfiltration, data manipulation, false data injection, or end users' privacy violation. In addition to this, the incorporation of IIoT-related technologies in Industry 4.0 does not help avoid these types of risks. Cyber-physical systems, cloud/fog computing, big data, digital twins, and the diverse emergent technologies that need to collaborate each other for the convergence IT (information technologies) – OT (operational technologies) certainly add new security and privacy risks that should widely be considered from the security point of view.

Therefore, the present volume highlights all these issues from the beginning, showing the current research challenges and ongoing work lines, with an eye toward keeping the operability of the underlying critical systems and their monitoring infrastructures. Diverse standpoints are addressed, capturing a theoretical analysis of the current situation and the benefits and drawbacks that the IIoT technology

itself can bring to the operational processes. Part of these analyses likewise involves the provision of lightweight approaches based on cryptographic algorithms, access control, anomaly detection, intrusion detection methodologies, or remote attestation algorithms. But beyond this, privacy techniques are also addressed in this book to evaluate the impact of the problem and its occurrence in determined critical environments such as smart health ecosystems. In counterpart to the theoretical procedures, practical researches in the IIoT security field are equally keys to demonstrate the validity of the approaches and their applications in critical scenarios. In this case, the design of IIoT-based testbeds and their influence on research procedures undoubtedly constitute a fundamental part to consolidate the new security and privacy trends on IIoT and its real application.

This book can therefore serve as a timely introduction to the state of the art of the technology of IIoT, trying to aid researchers to gain an overview of a field that is still largely unexplored, industries interested in modernizing their infrastructures from a secure perspective, and lecturers wishing to prepare future Industry 4.0 experts with solid criterion and contents.

Malaga, Spain Cristina Alcaraz
December 2018

Contents

List of Abbreviations

2PAKE	Two-party password authenticated key exchange
6LoWPAN	IPv6 over low-power wireless personal area networks
ABAC	Attribute-based access control
ACC	Authenticated control center
ACI	Access control information
ACL	Access control list
ADF	Access control decision function
ADI	Access control decision information
ADS	Anomaly detection system
ADU	Application data unit
AE	Authenticated encryption
AEAD	Authenticated encryption with associated data
AEF	Access control enforcement function
AI	Artificial intelligence
AJAX	Asynchronous JavaScript and XML
ALKE	Authenticated lightweight key exchange
AM	Attribute manager
AMI	Advanced metering infrastructure
AMQP	Advanced Message Queuing Protocol
API	Application programming interface
APT	Advanced persistent threat
ASC	Authenticated Stream-Cipher
ASLR	Address space layout randomization
BIBD	Balanced incomplete block design
BLE	Bluetooth low energy
C&C	Command-and-control
CAD	Computer-aided design
CAM	Computer-aided manufacturing
CapBAC	Capability-based access control
CDM	Central detection module
CH	Context handler

CI	Critical infrastructure
CIM	Computer-integrated manufacturing
CIR	Channel impulse response
CNN	Convolutional neural networks
COM	Component object model
CPPS	Cyber-physical production system
CPS	Cyber-physical system
CTF	Capture-the-flag
D-IDS	Distributed-IDS
DAG	Directed acyclic graph
DAO	Destination advertisement object
DAO-ACK	Destination advertisement object acknowledgment
DCOM	Distributed component object mode
DCS	Distributed control system
DDH	Decisional Diff ie-Hellman
DDoS	Distributed denial of service
DHT	Distributed hash table
DIO	DODAG information object
DIS	DODAG information solicitation
DNP3	Distributed network protocol 3
DODAG	Destination-oriented DAG
DoS	Denial-of-service
DPI	Deep packet inspection
DTMC	Discrete-time Markov models
EHR	Electronic health record
EKF	Extended Kalman filter
EMS	Energy management system
ENIP	EtherNet/IP
EPC	Electronic product code
EPIC	Electric power and intelligent control
EPP	Event processing point
ETSI	European Telecommunications Standards Institute
ETX	Expected transmission time
GDPR	General data protection regulation
GE	Gate equivalent
GPAKE	Password authenticated group key exchange
GQ	Generalized quadrangles
H4.0	Hospital 4.0
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital information systems
HITECH	Health Information Technology for Economic and Clinical Health
HMI	Human machine interfaces
I4.0	Industry 4.0
IAC	Industrial automation and control
ICS	Industrial control system

ICT	Information and communication technology
IDS	Intrusion detection system
IED	Intelligent electronic device
IEEE	Institute of Electrical and Electronics Engineers (IEEE)
IETF	Internet Engineering Task Force
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IMIoT	Industrial Medical Internet of Thing
IoT	Internet of Thing
IoTEED	IoT Trusted Execution Environment for Edge Devices
IPFIX	Internet Protocol Flow Information eXport
IPS	Intrusion prevention system
IR	Industrial Revolution
ISA	International Society for Automation
IT	Information technology
ITS	Intelligent transportation system
ITU	International Telecommunications Union
LAN	Local area network
LC	Lightweight cryptography
LLN	Routing protocol for lossy and low power network
LS	Local stage
LSFA	Leaked-state-forgery attack
LTI	Linear time-invariant
LUT	Look-up table
LWAE	Lightweight AE scheme
M2M	Machine to machine
MAC	Message authentication code
MACRA	Medicare Access and CHIP Reauthorization Act
MI	Mutual information
MILS	Multiple independent levels of security
MitM	Man-in-the-middle
ML	Machine learning
MMS	Manufacturing message specification
MQTT	Message queuing telemetry transport
MR	Medical record
MSPC	Multivariate statistical process control
MTU	Master terminal unit
NFC	Near field communication
NGAC	Next generation access control
NIDS	Network intrusion detection systems
NIST	National Institute of Standards and Technology
OCM	Online compression model
OF	Objective function
OLE	Object linking and embedding
OPC	Process control

ORNL	Oak Ridge National Laboratories
OS	Operating system
OSI	Open system interconnection
OT	Operational technology
P2P	Peer-to-peer
PAP	Policy authorization point
PC	Principal component
PCA	Principal component analysis
PDP	Policy decision point
PDU	Protocol data unit
PEP	Policy enforcements point
PID	Protocol identifier
PIP	Policy information point
PKI	Public key infrastructure
PLC	Programmable logic controller
PRBG	Pseudorandom bit generator
PS	Policy store
PUB	Public utility board
PV	Photovoltaic
RAM	Random access memory
RAP	Resource access point
RAT	Remote Access Trojan
RBAC	Role-based access control
RF	Radio frequency
RFID	Radio frequency identification
RIO	Remote input/output
RN	Reference number
RO	Reverse osmosis
ROP	Return-oriented programming
RPL	Routing protocol for low power and lossy network
RSS	Received signal strength
RTS	Real-time digital power systems
RTU	Remote terminal unit
SBIBD	Symmetric Balanced Incomplete Block Design
SCADA	Supervisory control and data acquisition
SCVAE	Squeezed Convolutional Variational AutoEncoder
SDN	Software-defined networking
SM	Session manager
SMAC	Sequential missing attribute collection
SPC	Statistical process control
SPKI	Simple public key infrastructure
SPL	Smart production logistic
SQL	Structured Query Language
SSL	Secure Sockets Layer
SUTD	Singapore University of Technology and Design

SWaT	Secure water treatment
TAE	Tweakable authenticated encryption
TC	Traff ic control
TID	Transaction identifier
TIHM	Technology Integrated Health Management
TLS	Transport Layer Security
TPM	Trusted Platform Module
UCIoT	Usage control in the Internet of Things
UCON	Usage control
UCS	Usage control system
UDP	User Datagram Protocol
UID	Unit identifier
UPS	Uninterruptible power supply
VLAN	Virtual local area network
VM	Virtual machine
VPN	Virtual private network
W3C	World Wide Web Consortium
WADI	Water distribution
WAN	Wide area network
WPT	Water plant testbed
WSN	Wireless sensor network
XACML	Extensible Access Control Markup Language
ZDI	Zero-day initiative