EDITED BY
CHARLES A. KAMHOUA | LAURENT L. NJILLA
ALEXANDER KOTT | SACHIN SHETTY

MODELING AND DESIGN OF SECURE INTERNET OF THINGS

IEEE PRESS
WILEY

Table of Contents

- Cover
- About the Editors
- List of Contributors
- Foreword
- Preface
- 1 Introduction
  - 1.1 Introduction
  - 1.2 Overview
  - 1.3 Roadmap
  - 1.4 Summary and Future Work
  - References
- Part I: Game Theory for Cyber Deception
  - 2 Game-Theoretic Analysis of Cyber Deception
    - 2.1 Introduction
    - 2.2 Game Theory in Security
    - 2.3 Binary State Space: Leaky Deception Using Signaling Game with Evidence
    - 2.4 Continuous State Space: Knowledge Acquisition and Fundamental Limits of Deception
    - 2.5 Adaptive Strategic Cyber Defense for APT in Critical Infrastructure Network
    - 2.6 Conclusion
    - References
  - 3 A Hypergame-Based Defense Strategy Toward Cyber Deception in Internet of Battlefield Things (IoBT)

3.1 Introduction
3.2 Modeling the Spread of an Attack
3.3 Experiments
3.4 Conclusion
References
4 Cooperative Spectrum Sharing and Trust Management in IoT Networks
4.1 Introduction
4.2 Problem Statement
4.3 Overview to Physical Layer Secrecy
4.4 Introduction to Stackelberg Games
4.5 Proposed Game-Theoretic Spectrum Leasing Model to Enhance Secrecy Rate
4.6 Conclusion
A. Appendix
References
5 Adaptation and Deception in Adversarial Cyber Operations
5.1 Introduction
5.2 Key Aspects of Recent Game Theory Successes
5.3 Real-World Adversarial Situations
5.4 Paradoxes and Paradoxes Resolved
5.5 Summary
Acknowledgments
References
6 On Development of a Game-Theoretic Model for Deception-Based Security
6.1 Introduction

6.2 Related Research
6.3 Game-Theoretic Deception Model
6.4 Deception Using *N* Computing Devices
6.5 Deception in a Tree-Based Network Structure
6.6 Simulation Results
6.7 Conclusion
References
7 Deception for Cyber Adversaries
7.1 Introduction
7.2 Background
7.3 The Taxonomy for Cyber Deception
7.4 Game-Theoretic Model for Cyber Deception
7.5 Open Challenges and Opportunities
7.6 Summary
References
Part II: IoT Security Modeling and Analysis
8 Cyber-Physical Vulnerability Analysis of IoT Applications Using Multi-Modeling
8.1 Introduction
8.2 Vulnerabilities in IoT
8.3 Multi-modeling Approach for CPS Vulnerability Analysis
8.4 Open Questions and Future Research Directions
References
9 Securing Smart Cities
9.1 Foreword

9.2 Detection, Identification, Fingerprinting, and Behavioral Monitoring in Smart Cities
9.3 Modeling Smart Cities
9.4 The Future: Connecting and Federating IoT Technologies in Smart Cities
9.5 Epilogue
Acknowledgment
References
10 Modeling and Analysis of Integrated Proactive Defense Mechanisms for Internet of Things
10.1 Introduction
10.2 Related Work
10.3 System Model
10.4 Proposed Proactive Defense Mechanisms
10.5 Numerical Results and Analysis
10.6 Conclusions and Future Work
References
11 Addressing Polymorphic Advanced Threats in Internet of Things Networks by Cross-Layer Profiling
11.1 Introduction
11.2 System Model
11.3 Attack Surface Analysis
11.4 A Security Layer
11.5 Conclusion
References
12 Analysis of Stepping-Stone Attacks in Internet of Things Using Dynamic Vulnerability Graphs
12.1 Introduction
12.2 Background

12.3 Stepping-Stone Dynamics
12.4 Min-Plus Algebra
12.5 Discussion
12.6 Conclusions
Acknowledgment
References
13 Anomaly Behavior Analysis of IoT Protocols
13.1 Introduction
13.2 IoT Architecture
13.3 IoT Threat Modeling Methodology
13.4 Application of the Threat Modeling Concepts to Different Protocols
13.5 Conclusion and Future Work
References
14 Dynamic Cyber Deception Using Partially Observable Monte-Carlo Planning Framework
14.1 Introduction
14.2 Related Work
14.3 The Dynamic Deception Model
14.4 Defender's Action
14.5 Online Deception Algorithm
14.6 IoT Aware Smart Healthcare Architecture
14.7 Experimental Results and Discussion
14.8 Conclusion
References
15 A Coding Theoretic View of Secure State Reconstruction
15.1 Introduction and Motivation
15.2 Problem Definition and Model

15.3 Secure State Reconstruction as Error Correction
15.4 Connections to Classical Coding Theory
15.5 Sparse Strong Observability, Hamming Distance, and Secure State Reconstruction
15.6 Decoding Algorithms
References
16 Governance for the Internet of Things
16.1 Introduction
16.2 Risk and Resilience
16.3 Strategies of IoT and Digital Economy Governance
16.4 Applying Resilience to IoT Governance
16.5 Conclusions
References
Part III: IoT Security Design
17 Secure and Resilient Control of IoT-Based 3D Printers
17.1 Introduction
17.2 Problem Formulation
17.3 Equilibrium Analysis of the Cyber-Physical Games
17.4 Simulation Results
17.5 Conclusions
References
18 Proactive Defense Against Security Threats on IoT Hardware
18.1 Introduction
18.2 Hardware Security Threats
18.3 Countermeasure Against SCAs

18.4 Countermeasure Against HTs
18.5 Countermeasure Against Software Security Threats
18.6 Conclusion
References
19 IoT Device Attestation
19.1 Introduction
19.2 Background on Attestation
19.3 Notable Approaches
19.4 Discussion and Future Directions
Acknowledgments
References
20 Software-Defined Networking for Cyber Resilience in Industrial Internet of Things (IIoT)
20.1 Introduction
20.2 Related Work
20.3 System Model
20.4 Security Risk Levels and Impact on QoS
20.5 Optimal Security Countermeasure Selection Problem Formulation
20.6 Simulation Results
20.7 Conclusion
Acknowledgment
Disclaimer
References
21 Leverage SDN for Cyber-Security Deception in Internet of Things
21.1 Introduction
21.2 Literature Review

21.3 Design
21.4 Evaluation
21.5 SDN for Distributed Networks
21.6 Conclusion
References
22 Decentralized Access Control for IoT Based on Blockchain and Smart Contract
22.1 Introduction
22.2 Access Control in IoT
22.3 Blockchain and Smart Contract
22.4 Blockchain-Based Security Solutions to IoT
22.5 BlendCAC: A Case Study
22.6 Conclusions
References
23 Intent as a Secure Design Primitive
23.1 Introduction
23.2 A LangSec Primer
23.3 An ELFbac Primer
23.4 Building a Secure Implementation of AMQP
23.5 Evaluation Techniques
23.6 Conclusions
23.7 Further Reading
Acknowledgments
References
24 A Review of Moving Target Defense Mechanisms for Internet of Things Applications
24.1 Introduction
24.2 Internet of Things

24.3 Software Defined Networking Background
24.4 Moving Target Defense
24.5 Moving Target Defense for IoT
24.6 Future Research Challenges
24.7 Conclusion
References
25 Toward Robust Outlier Detector for Internet of Things Applications
25.1 Introduction
25.2 State of the Art Anomaly Detection Techniques
25.3 Problem Statement and Proposed Outlier Detector
25.4 Future Research Directions
25.5 Conclusions
References
26 Summary and Future Work
26.1 Summary
26.2 The Future
Index
End User License Agreement

List of Tables

Chapter 2

Table 2.1 $\sigma^{R^*}(1 \mid m, e)$ in pooling PBNE with $\beta > 1 - \alpha$.

Table 2.2 $\sigma^{R^*}(1 \mid m, e)$ in pooling PBNE with $\beta > 1 - \alpha$.

Chapter 3

Table 3.1 October 2018 CVSS score distribution published by NVD.

Table 3.2 The adversary's perceived matrix game.

Table 3.3 The reduced game for the adversary.

Table 3.4 The defender's perceived matrix game.

Table 3.5 The reduced game for the defender.

Table 3.6 Adversary's perceived game in the experiment.

Table 3.7 Defender's perceived game in the experiment.

Table 3.8 Percentiles of time and proportion with $K = 35$.

Table 3.9 Percentiles of time and proportion with $K = 20$.

Table 3.10 Percentiles of time and proportion with $K = 420$.

Table 3.11 Percentiles of time and proportion with $K = 200$.

Chapter 4

Table 4.1 Applications of game theory in communication networks.

Table 4.2 Simulation parameters.

Chapter 6

Table 6.1 Notations used in analysis.

Table 6.2 Payoff matrix for system(S) and attacker (A).

Chapter 10

Table 10.1 Real node and vulnerability information.

Table 10.2 Decoy node and vulnerability information.

Table 10.3 Design parameters, their meanings, and the default values.

Chapter 11

Table 11.1 An enumeration of the various components (computational capabiliti...

Table 11.2 Attack surface: enumeration of vulnerabilities, attacks, and impac...

Table 11.3 A complete description of the set of features used in our system.

Chapter 12

Table 12.1 Host configuration, function information, and vulnerability scores...

Table 12.2 Stepping-stone cost evolution from every source node to the target...

Table 12.3 Stepping-stone cost evolution from every source; notice that after...

Chapter 13

Table 13.1 End nodes layer.

Table 13.2 Communications plane.

Table 13.3 Services layer.

Table 13.4 Applications layer.

Table 13.5 IEEE 802.11 physical layer standards.

Table 13.6 Wireless attacks.

Table 13.7 Intrusion detection system rules.

Table 13.8 Bluetooth feature set.

Chapter 17

Table 17.1 System parameters.

Chapter 19

Table 19.1 Common symbols and terminology used in this chapter.

Table 19.2 Comparison of different approaches.

Chapter 20

Table 20.1 Range of basic parameters for security level.

Table 20.2 Parameters for evaluating security level.

Table 20.3 Parameters for evaluating delay and throughput.

Chapter 23

Table 23.1 Syntax and usage of Hammer.

Table 23.2 Syntax and usage for the keywords used in the Mithril Domain-speci...

Table 23.3 Number of vulnerabilities reported by the common vulnerabilities a...

Chapter 24

Table 24.1 IoT technologies developed for each OSI layer and their implementa...

Table 24.2 Constrained device categories (RFC 7228).

List of Illustrations

Chapter 1

Figure 1.1 IoT system architecture.

Figure 1.2 Book roadmap.

Figure 1.3 Cyber kill chain.

Chapter 2

Figure 2.1 Signaling games with evidence add a detector block (shown on the ...

Figure 2.2 PBNE differs within five prior probability regimes. In the Zero-D...

Figure 2.3 PBNE in each of the parameter regions defined in Figure 2.2. For

Figure 2.4 Signaling games with evidence acquisition by investigation. The p...

Figure 2.5 The APTs' life cycle includes a sequence of phases and stages suc...

Figure 2.6 Value function $\bar{U}^{R*}_{k':K}(x_{k'})$ under different expanded states $\{x_{k-}, \alpha_{k-},$

Figure 2.7 The effect of the defender's belief.

Chapter 3

Figure 3.1 A sample network topology.

Figure 3.2 The adversary's strategies in Round 1.

Figure 3.3 The adversary's strategies in Round 2.

Figure 3.4 Two-layer binary network with one target node.

Figure 3.5 Boxplots with $K = 35$. From left to right: (a) total time to explo...

Figure 3.6 Boxplots with $K = 20$. From left to right: (a) total time to explo...

Figure 3.7 Six-layer binary network.

Figure 3.8 Boxplots with $K = 420$. From left to right: (a) total time to expl...

Figure 3.9 Boxplots with $K = 200$. From left to right: (a) total time to expl...

Chapter 4

Figure 4.1 Comparison of information secrecy and cryptography methods.

Figure 4.2 Wiretap model.

Figure 4.3 The Gaussian wiretap channel.

Figure 4.4 The relay channel.

Figure 4.5 The relay channel using encoder and decoder.

Figure 4.6 Relaying for secrecy.

Figure 4.7 Cooperative jamming for enhancing the secrecy.

Figure 4.8 Active cooperation (DF or CF).

Figure 4.9 Enhancing secrecy with cooperation and game theory.

Figure 4.10 An example of spectrum leasing to secondary IoT devices in excha...

Figure 4.11 System model of proposed spectrum leasing scheme between the PU ...

Figure 4.12 The proposed Stackelberg game model.

Figure 4.13 Probability of selecting unreliable nodes over time [70].

Figure 4.14 Cooperation phase (α β) versus the distance between th...

Chapter 6

Figure 6.1 Three-node structure depicting the attack–defense strategies.

Figure 6.2 *N* node structure depicting the attack–defense strategies.

Figure 6.3 System model for deception in a tree-based network structure.

Figure 6.4 System utility versus number of computing devices. From the figur...

Figure 6.5 Expected utility of the system and the attacker with varying numb...

Figure 6.6 Optimal NE-based strategy (P_S^*) of the system with varying probabil...

Figure 6.7 Optimal NE-based strategy (P_A^*) of the attacker with varying probab...

Chapter 7

Figure 7.1 Typical lifecycle of cyber deception for cyber adversaries.

Figure 7.2 Typical cyber infrastructure components where deception can be in...

Figure 7.3 Taxonomy of information protection mechanisms using deception tec...

Figure 7.4 Framework to incorporate deception for cyber defense.

Figure 7.5 A typical cryptographic system.

Figure 7.6 Control theory model where feedback helps stabilize the system.

Figure 7.7 Taxonomy of cyber-deception techniques.

Figure 7.8 Cybersecurity deception concept.

Figure 7.9 An adversary scans the defender's IoT devices and the defender de...

Figure 7.10 Loss of the IoT system and gain of the attacker when there is no...

Chapter 8

Figure 8.1 Vulnerability propagation across the different layers of a CPS.

Figure 8.2 Example multi-domain system model hierarchy. A system captures th...

Figure 8.3 Example 2D and 3D analysis of a circuit board in a system context...

Figure 8.4 Example signal with RF energy insertion.

Figure 8.5 Functional blocks of the IoT sensor node.

Figure 8.6 Internal model of the core BLE platform.

Figure 8.7 PCB design.

Figure 8.8 Links between hardware events and behavior models.

Figure 8.9 Example testbench for RF susceptibility.

Figure 8.10 Model for SI wave analysis.

Figure 8.11 Evaluation results.

Chapter 9

Figure 9.1 Different granularities of analyzing smart-city devices. (1) Dete...

Figure 9.2 Ground truth (top) versus clustering results (bottom). Despite ma...

Figure 9.3 Ground truth (top) versus clustering results (bottom). The cluste...

Figure 9.4 Graph-based temporal modeling of a scenario where traffic lights ...

Chapter 10

Figure 10.1 Example of a software-defined IoT network.

Figure 10.2 Workflow for security analysis.

Figure 10.3 Performance comparison of the four MTD schemes with low-intellig...

Figure 10.4 Performance comparison of the four MTD schemes with medium-intel...

Figure 10.5 Performance comparison of the four MTD schemes with low-intellig...

Chapter 11

Figure 11.1 Security layer for smart home (SLaSH).

Figure 11.2 Cross-layer security to thwart advanced persistent threats in th...

Chapter 12

Figure 12.1 Network topology.

Figure 12.2 A vulnerability graph derived from the network topology presente...

Figure 12.3 Physical network represented with a 10-node undirected graph G. ...

Figure 12.4 A vulnerability multigraph derived from G at any time t_1. For ex...

Figure 12.5 Vulnerability multigraph derived from G at any time t_2. In this ...

Figure 12.6 A 10-node vulnerability graph $G = G_p$ with node 1 as a target nod...

Figure 12.7 A 10-node vulnerability graph G_q derived from graph G_p where the...

Chapter 13

Figure 13.1 Rise of wearables and future wearable technology.

Figure 13.2 Growth of IoT by 2020.

Figure 13.3 Attack sophistication versus intruder technical knowledge.

Figure 13.4 The timeline of cyber-threads scope of damage and impact time.

Figure 13.5 IoT architecture.

Figure 13.6 Application of IoT architecture to a Smart speaker.

Figure 13.7 IoT threat modeling framework.

Figure 13.8 Wi-Fi frame structure.

Figure 13.9 Wi-Fi header.

Figure 13.10 Wi-Fi protocol state machine.

Figure 13.11 Anomaly behavior analysis.

Figure 13.12 Feature set.

Figure 13.13 Wireless n-gram (W-gram).

Figure 13.14 Feature set to fingerprinting data-structure mapping.

Figure 13.15 IEEE 802.11 behavior analysis module.

Figure 13.16 Wi-Fi testbed.

Figure 13.17 False negative versus frame drop rate.
Figure 13.18 Flowscore value to rule comparison.
Figure 13.19 Correct attack classification (percentage) versus frame drop ra...
Figure 13.20 Bluetooth piconet.
Figure 13.21 Bluetooth state machine.
Figure 13.22 Feature set to n-grams.
Figure 13.23 Bluetooth observation-flow.
Figure 13.24 Bluetooth IDS architecture.
Figure 13.25 Bluetooth test bed.
Figure 13.26 Rate of learning of unique n-grams.
Figure 13.27 Unique n-grams for an n-gram size.
Figure 13.28 Precision for various classifiers.
Figure 13.29 Recall for various classifiers.
Figure 13.30 RoC area for various classifiers.
Chapter 14
Figure 14.1 Dynamic deception model.
Figure 14.2 An illustration of POMCP in an environment with 2 actions, 2 obs...
Figure 14.3 A sample exploit dependency graph with a real network (left) and...
Figure 14.4 IoT aware Smart Healthcare System with network decoys.
Figure 14.5 Sample evolution of deception policy when an attacker is in a re...
Figure 14.6 Sample evolution of deception policy when the attacker is in the...

Figure 14.7 Performance evaluation.

Figure 14.8 Discounted cost.

Chapter 17

Figure 17.1 The architecture of the IoT-based 3D-printing system and the pot...

Figure 17.2 The dynamical model of the extruder moving in one dimension: the...

Figure 17.3 The linearized model of the rotor and extruder: we linearize the...

Figure 17.4 The sequential architecture of the *FlipIt* game: at each time slo...

Figure 17.5 The structure of the Stackelberg game-theoretic framework: the p...

Figure 17.6 (a) The tracking performance under the control of the normal use...

Figure 17.7 The input of the control in different cases: in the normal case,...

Figure 17.8 (a) Case 1 (No Defense Strategies): When there is no defense str...

Figure 17.9 The relationship among α, γ, and p_a^*: (i) when we decrea...

Figure 17.10 Given different move-cost ratio α, we use mapping $T_S(\cdot)$ t...

Chapter 18

Figure 18.1 Hardware security threats from multiple stages of IC design flow...

Figure 18.2 Hardware Trojan. (a) Structure of hardware Trojan, (b) combinati...

Figure 18.3 Hardware Trojan taxonomy [26].

Figure 18.4 Contaminated FPGA design suite leading to a stealthy modificatio...

Figure 18.5 Attack surfaces on the Xilinx FPGA design flow. The rectangles r...

Figure 18.6 An example of practical attack performed through the FPGA editor...

Figure 18.7 An example of practical attack performed through Quartus Chip Pl...

Figure 18.8 Dynamic masking plus error deflection method for thwarting CPA a...

Figure 18.9 High-level overview of the proposed countermeasure.

Figure 18.10 Router architecture used in this work. One proposed input and o...

Figure 18.11 Traffic hotspot migration and bandwidth depletion induced by HT...

Figure 18.12 FPGA mapping modified by proposed defense line 1. Three parts i...

Figure 18.13 Schematic diagram of proposed defense line 2.

Figure 18.14 Schematic diagram of the hot-swappable submodule assembling tec...

Figure 18.15 Hardware Trojan hit rate reduction by proposed defense line 1 a...

Figure 18.16 Hardware Trojan hit rate for (a) c432, and (b) nine benchmark c...

Chapter 19

Figure 19.1 Flow of operations in SMART. A remote V sends a request to a dev...

Figure 19.2 C-FLAT test implementation model. Trampolines are used to enter ...

Chapter 20

Figure 20.1 Interaction of roles in different EDS domains through secure com...

Figure 20.2 Internal and external WAN attacks.

Figure 20.3 Security and QoS framework for SDN-enabled EDS.

Figure 20.4 Pareto front.

Figure 20.5 NSGA-II procedure.

Figure 20.6 Pareto front to maintain delay ≤100 ms when $N = 10$.

Figure 20.7 Pareto front with constraint $Thr \geq 97\%$ when $N = 14$.

Figure 20.8 Pareto front with constraint $Thr \geq 97\%$ when $N = 14$.

Figure 20.9 Pareto front with no constraint when $N = 14$.

Chapter 21

Figure 21.1 Architecture of cooperative IoT security.

Figure 21.2 SDN workflow.

Figure 21.3 Experimental topology.

Figure 21.4 GENI experiments (Controller 1's network). (a) Attack alert time...

Figure 21.5 GENI experiments (Controller 2's network). (a) Information shari...

Figure 21.6 Hardware experiments. (a) Attack alert time. (b) Flow installati...

Chapter 22

Figure 22.1 Capability-based access control model.

Figure 22.2 Work process in blockchain.

Figure 22.3 BlendCAC system architecture.

Figure 22.4 Experimental results of BlendCAC: (a) access authorization succe...

Chapter 23

Figure 23.1 ELFbac and LangSec both enforce human intent by codifying the sp...

Figure 23.2 Chomsky hierarchy extended with LangSec boundaries.

Figure 23.3 Full recognition before computation.

Figure 23.4 Building the state machine using Mithril.

Figure 23.5 The finite state machine represented by our OpenSSH ELFbac polic...

Figure 23.6 (a) State machine. (b) Mithril policy that mitigates Spectre var...

Figure 23.7 Flow of messages in the AMQP protocol.

Figure 23.8 AMQP Client state machine. The client initiates the connection w...

Figure 23.9 AMQP Broker State Machine diagram showing the various states and...

Figure 23.10 (a) Packet format of a generic AMQP packet. The number of bytes...

Figure 23.11 Design of our AMQP parser implementation.

Figure 23.12 Conversion of a syntax structure for a packet format into Hamme...

Chapter 24

Figure 24.1 Three-different domains – IoT, SDN, and MTD.

Figure 24.2 Essential building blocks of an IoT environment.

Figure 24.3 Traditional network switches versus SDN-based switches.

Figure 24.4 Proposed MTD classification for the dynamic network. This classi...

Figure 24.5 An example of host-centric approach: TAP-based port and address ...

Figure 24.6 An example of network-centric architecture with three additional...

Figure 24.7 An example of network-centric architecture with two additional g...

Figure 24.8 Proposed SDN-based MTD classification. This classification is de...

Figure 24.9 SDN shuffle protocol operations. The dotted lines are optional p...

Figure 24.10 RHM operations comparison when a client tries to access the ser...

Figure 24.11 PHEAR per-switch basis operations.

Figure 24.12 Proposed MTD for IoT classification. The classification is deri...

Figure 24.13 The creation, usage, and deletion of an obscured IPv6 address t...

Figure 24.14 The translation service operations at the network layer.

Figure 24.15 SDN-based switches for Smart Home.

Figure 24.16 SDN-based vehicular network.

Figure 24.17 (a) MTD for IIoT systems and (b) optimal design of an MTD techn...

Chapter 25

Figure 25.1 Proposed anomaly detector.

Figure 25.2 Time series traffic data at different locations.

Figure 25.3 Spatial correlation of traffic flow between different positions....

Figure 25.4 Actual and predicted traffic count values.

Figure 25.5 Time-series traffic gradient for different window size.

IEEE Press
445 Hoes Lane
Piscataway, NJ 08854

Modeling and Design of Secure Internet of Things

Edited by

Charles A. Kamhoua

Laurent L. Njilla

Alexander Kott

Sachin Shetty

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication data applied for

ISBN: 9781119593362

Set in 9.5/12.5pt STIXTwoText by SPi Global, Pondicherry, India

Cover Design: Wiley
Cover Image: © Photographer is my life./Getty Images

About the Editors

Charles A. Kamhoua is a Senior Electronics Engineer at the Network Security Branch of the US Army Research Laboratory (ARL) in Adelphi, MD, where he is responsible for conducting and directing basic research in the area of game theory applied to cyber security. Prior to joining the Army Research Laboratory, he was a researcher at the US Air Force Research Laboratory (AFRL), Rome, New York, for 6 years and an educator in different academic institutions for more than 10 years. He has held visiting research positions at the University of Oxford and Harvard University. He has coauthored more than 200 peer-