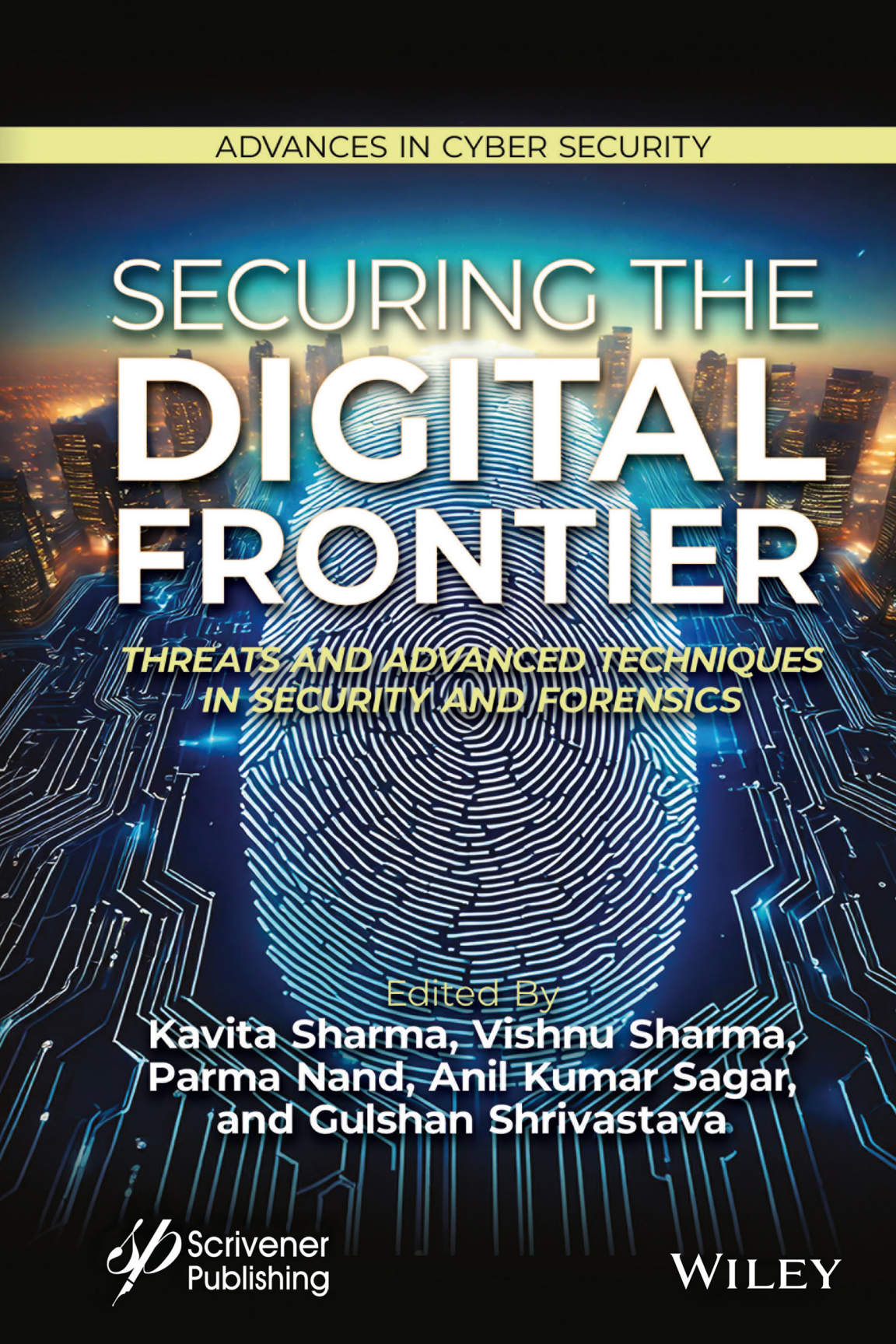
ADVANCES IN CYBER SECURITY



SECURING THE DIGITAL FRONTIER

THREATS AND ADVANCED TECHNIQUES IN SECURITY AND FORENSICS

Edited By
Kavita Sharma, Vishnu Sharma, Parma Nand, Anil Kumar Sagar, and Gulshan Shrivastava

Scrivener Publishing

WILEY

Securing the Digital Frontier

Scrivener Publishing
100 Cummings Center, Suite 541J
Beverly, MA 01915-6106

Advances in Cyber Security

Series Editors: Rashmi Agrawal and D. Ganesh Gopal

Scope: The purpose of this book series is to present books that are specifically designed to address the critical security challenges in today's computing world including cloud and mobile environments and to discuss mechanisms for defending against those attacks by using classical and modern approaches of cryptography, blockchain and other defense mechanisms. The book series presents some of the state-of-the-art research work in the field of blockchain, cryptography and security in computing and communications. It is a valuable source of knowledge for researchers, engineers, practitioners, graduates, and doctoral students who are working in the field of blockchain, cryptography, network security, and security and privacy issues in the Internet of Things (IoT). It will also be useful for faculty members of graduate schools and universities. The book series provides a comprehensive look at the various facets of cloud security: infrastructure, network, services, compliance and users. It will provide real-world case studies to articulate the real and perceived risks and challenges in deploying and managing services in a cloud infrastructure from a security perspective. The book series will serve as a platform for books dealing with security concerns of decentralized applications (DApps) and smart contracts that operate on an open blockchain. The book series will be a comprehensive and up-to-date reference on information security and assurance. Bringing together the knowledge, skills, techniques, and tools required of IT security professionals, it facilitates the up-to-date understanding required to stay one step ahead of evolving threats, standards, and regulations.

Publishers at Scrivener
Martin Scrivener (martin@scrivenerpublishing.com)
Phillip Carmical (pcarmical@scrivenerpublishing.com)

Securing the Digital Frontier

Threats and Advanced Techniques in Security and Forensics

Edited by

Kavita Sharma

Vishnu Sharma

Parma Nand

Anil Kumar Sagar

and

Gulshan Shrivastava

WILEY

This edition first published 2025 by John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA and Scrivener Publishing LLC, 100 Cummings Center, Suite 541J, Beverly, MA 01915, USA

For more information about Scrivener publications please visit www.scrivenerpublishing.com.

Wiley Global Headquarters
111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Library of Congress Cataloging-in-Publication Data

ISBN 978-1-394-26888-7

Front cover images supplied by Adobe Firefly
Cover design by Russell Richardson

Set in size of 11pt and Minion Pro by Manila Typesetting Company, Makati, Philippines

Printed in the USA

10 9 8 7 6 5 4 3 2 1

Contents

Preface **xix**

1 Pegasus—A Menace to Privacy and Security **1**
Raunaq Khurana and Shilpa Mahajan
1.1 Introduction 1
1.2 Working of Pegasus 4
1.2.1 Pegasus Attacking iOS 8
1.2.2 Pegasus Impacting Android 9
1.2.3 Differentiating Android and iOS Pegasus 10
1.3 Literature Review 10
1.4 Methodologies 12
1.5 Pegasus Implantation Techniques 12
1.6 Mitigation Measures 13
1.7 Conclusion 14
References 14

2 Data Privacy and Compliance in Information Security **17**
Rakesh Nayak, Umashankar Ghugar, Praveen Gupta, Satyabrata Dash and Nishu Gupta
2.1 Introduction 18
2.2 Discussion on Risks, Consequences, and Security Measures for Data Privacy 19
2.2.1 Getting Around the Compliance Landscape in Information Security 22
2.2.2 Legal Frameworks: Protecting Privacy Rights, CCPA, and GDPR 23
2.2.2.1 General Data Protection Regulation (GDPR) 23
2.2.2.2 California Consumer Privacy Act (CCPA) 24
2.2.3 Challenges in Achieving Compliance and the Repercussions of Noncompliance 24

2.2.4 Principles to Follow to Ensure Data Privacy and Compliance 26
2.2.5 Integrated Approach: Audits, Access Controls, Encryption, and Privacy Awareness 27
2.3 Data Privacy and Compliance in Information Security: The Changing Nature 28
2.4 Continuous Learning and Adaptation: Keeping Pace with Emerging Technologies and Regulations 31
2.5 Conclusion 32
References 33

3 Unveiling Cyber Threats and Digital Forensics 35
Nidhi Gupta, Arpita Trivedi, Parveen P. Terang and Hasmat Malik
3.1 Information Security 36
3.1.1 Issues and Challenges 36
3.1.2 Digital Forensics 37
3.2 Cyberattacks 39
3.2.1 System Exploitation 39
3.2.2 Phishing 40
3.2.3 Man in the Middle Attack 41
3.2.4 Denial of Service 42
3.2.5 Ransomware 43
3.3 Protection Techniques 44
3.3.1 Firewalls 45
3.3.2 Threat Modeling 46
3.3.3 Penetration Testing 48
3.3.4 Encryption 50
3.3.5 Access Control 52
3.4 Internet of Medical Things 53
3.5 Conclusion 54
References 54

4 A Customised Privacy Preservation Mechanism for Cyber-Physical Systems 59
Manas Kumar Yogi and A.S.N. Chakravarthy
4.1 Introduction 59
4.1.1 Role of CPS 60
4.1.2 Privacy Preservation in CPS 61
4.1.3 Motivation for CPS Privacy 62

4.2 Background 64
4.2.1 Current Trends in CPS Privacy 64
4.2.2 Trade-Off Between Privacy and Data Utility 65
4.2.3 Challenges in Variable Differential Privacy Implementation 66
4.3 Motivation 73
4.3.1 Variants of Differential Privacy 73
4.3.2 Impact of Noise Addition in Variants of Differential Privacy 74
4.4 Proposed Mechanism 76
4.4.1 Algorithm: Customized Differential Privacy 78
4.4.2 Algorithm: Privacy-Utility Balancing in Differential Privacy 80
4.5 Experimental Results 81
4.5.1 Interpretations of the Results 82
4.5.2 The Advantages of Using Customized Privacy Budgets are Evident in the Following Ways 84
4.6 Future Directions 84
4.7 Conclusion 88
References 88

5 Securing the Future: Emerging Threats and Countermeasures in Cryptography 91
Debosree Ghosh, Kishore Ghosh, Chandrima Chakraborty, Atanu Datta and Somsubhra Gupta
5.1 Introduction 92
5.2 Quantum Computing and Post-Quantum Cryptography 92
5.3 Cryptanalysis: Cracking the Code 93
5.4 Side-Channel Attacks: Stealthy and Insidious 95
5.5 Fault Attacks: Exploiting Implementation Weaknesses 96
5.5.1 Permanent Fault Attacks 97
5.5.2 Transient Fault Attacks 97
5.6 Hardware Security Modules (HSMS) 97
5.6.1 HSMs Offer a Range of Features that Make Them a Critical Component of Modern Information Security Systems 98
5.6.2 HSMs Applications in Various Industries and Scenarios 99
5.7 Secure Implementations: From Theory to Reality 99

5.8 A Holistic Approach to Cryptography 99
5.9 Quantum Key Distribution (QKD) 100
5.10 Internet of Things in Cryptography 102
5.11 Artificial Intelligence in Cryptography 103
5.12 Cryptarithmetic 104
5.13 The Road Ahead: Future Trends and Prospects 105
5.14 Conclusion 106
Bibliography 106

6 Cyber Threats and Its Impact on Electronic Transactions 109
Ramalingam Dharmalingam and Vaishnavi Dharmalingam
6.1 Introduction 109
6.2 Digital Transformation and Cybersecurity 111
6.3 Evolution of Cyber Threats 112
6.3.1 Telephone Hacks in the 1950s 113
6.3.2 Introduction of Computer Virus in the 1970s and 1980s 113
6.3.3 Widespread Malware Attacks in the 1990s 114
6.3.4 The Turn of the Century 114
6.3.5 Threat to the Connected "Things" in the 2020s 115
6.4 Emerging Cyber Threats 115
6.4.1 Malware Delivery 116
6.4.2 Fileless Malware 119
6.4.3 Legitimate Service Abuse 119
6.4.4 Botnet Renovations 119
6.4.5 Search Engine Optimization and Malicious Advertising 120
6.4.6 Security Tools as a Malware 120
6.4.7 Web Shells Deep Dive 121
6.4.8 Domain-Generating Algorithms 121
6.4.9 AI-Enabled Cyber Attacks 121
6.5 Impacts of Data Breaches in the Financial Sector 121
6.6 Cybersecurity Standards, Frameworks, and Benchmarks 124
6.7 Innovative Approaches to Cyber-Incident Management 127
6.7.1 International and Multistakeholder Collaboration 127
6.7.2 Cognitive Analytics in Cybersecurity Management 128
6.7.3 Security Automation for Combating Cyberattacks 128
6.8 Conclusion 129
References 129

7 A Robust Model for Enabling Insider Threat Detection and Prevention: Techniques, Tools, and Applications 133
A. Sheik Abdullah, Shivansh Dhiman and Arif Ansari
7.1 Introduction 134
7.2 Structure 135
7.3 Impact of Insider Threats on Modern Organizations 137
7.3.1 Types of Insider Threats 137
7.3.2 Importance of Understanding the Impact of Insider Threats 139
7.3.3 The Magnitude of the Threat 140
7.3.4 Why are Insider Threats so Dangerous? 141
7.5 Challenges in Insider Threat Detection 142
7.6 Techniques for Insider Threat Detection 144
7.7 Robust Model 146
7.7.1 Shortcomings in Current Insider Threat Detection Models 147
7.7.2 Required Algorithms and Tools for Robust Model 148
7.7.2.1 Supervised Learning Model 149
7.7.2.2 Complex Event Processing 150
7.7.3 Integration Model 152
7.7.4 Pseudocode 154
7.8 Application and Case Studies 156
7.8.1 Introduction 156
7.8.2 How the Integration Works 156
7.8.3 Case Studies 157
7.9 Other Important Insider Threat Prevention Strategies 158
7.10 Ethical Considerations 160
7.11 Future Trends 163
7.12 Conclusion 165
References 166
Authored Book 167
References 167

8 Digital Vulnerabilities Unveiled: A Multidisciplinary Exploration of Emerging Threats to Security and Privacy in the Age of Networked Communication 169
Priya Sachdeva and Archan Mitra
8.1 Introduction 170
8.1.1 Objectives 171
8.2 Theoretical Foundation 172

8.2.1 Conceptual Foundations 172
8.2.2 The Literary Nexus 173
8.3 Methodological Framework 174
8.3.1 Data Collection 174
8.3.2 Data Analysis 175
8.3.3 Integration of Multidisciplinary Perspectives 175
8.3.4 Ethical Considerations 175
8.4 Emergent Themes 176
8.4.1 Misinformation and Fake News 176
8.4.2 Data Breaches Put Personal Information at Risk 176
8.4.3 The Role of Humans in Phishing and other Forms of Social Engineering 177
8.5 Interdisciplinary Insights 178
8.5.1 Connecting Threads 178
8.5.2 Dialogue Across Disciplines 178
8.6 Pedagogical Implications 179
8.6.1 The Development of Curriculum 179
8.6.2 Education that Promotes Ethical and Effective Communication 180
8.7 Findings and Discussion 181
8.7.1 Survey Findings 181
8.7.2 Findings from the Interview 181
8.7.3 Discussion 182
8.8 Integration and Synthesis 185
8.8.1 Bringing Together Multidisciplinary Perspectives 185
8.8.2 Policy and Practice Recommendations 186
8.9 Conclusion 187
References 188
Appendix A: Survey Instrument 190

9 Tools of Emancipation as Global Web and its Digital Ecosystem: Steering IoT Landscape, Cloud Computing Unravel Safe Spaces Lensing New Cyber Risks and Emerging Threats 197
Bhupinder Singh and Christian Kaunert
9.1 Introduction 198
9.1.1 Background of Study 199
9.1.2 Objectives 200
9.1.3 Scope of the Study 200
9.1.4 Structure of the Chapter 201

9.2 Tools of Emancipation on the World Wide Web: Conceptual Framework and Definition 202
9.2.1 Historical Evolution 202
9.2.2 Contemporary Significance 203
9.3 IoT Landscape and Its Overview: Opportunities and Challenges 203
9.4 Cloud Computing: Pillar for Safe Spaces Protection 204
9.4.1 Fundamental Concepts of Cloud Computing 205
9.4.2 Security Aspects of Cloud Services 206
9.4.3 Cloud-Based Solutions for Safe Spaces 206
9.5 Cyber Risks and Emerging Threats—Current Landscape of Cyber Threats 206
9.6 Tools of Emancipation: Digital Tools for Positive Purposes and Potential for Using Technology 207
9.7 Assimilating Tools of Emancipation, Cloud Computing, and IoT 208
9.8 Embryonic Updated Technologies and Future Tendencies 209
9.9 New Cyber Risks and Emerging Threats 210
9.9.1 Policy Implications, Societal and Ethical Considerations Concerning Safe Spaces Lensing New Cyber Risks and Emerging Threats 211
9.10 Conclusion and Future Scope 212
References 213

10 IoT and Smart Device Security: Emerging Threats and Countermeasures 217
Geo Francis E., S. Sheeja, Antony John E.F. and Jismy Joseph
10.1 Introduction to IoT and Smart Devices 217
10.1.1 Definition and Scope 220
10.1.2 Growth and Importance of IoT 221
10.1.3 Smart Device Landscape 222
10.2 Vulnerabilities in IoT Devices 223
10.2.1 Insecure Device Design and Configuration 224
10.2.2 Weak Authentication and Authorization 224
10.2.3 Lack of Device Updates and Patch Management 225
10.3 Emerging Threats in IoT Security 226
10.3.1 Botnets and DDoS Attacks 226
10.3.2 Data Breaches and Privacy Risks 226
10.3.3 Physical Damage and Safety Concerns 227
10.4 Attack Vectors in IoT 228

10.4.1 Network Exploitation 228
10.4.2 Firmware and Software Exploits 229
10.4.3 Social Engineering and Phishing 229
10.5 Countermeasures for IoT Security 230
10.5.1 Secure Device Design Principles 230
10.5.2 Authentication and Encryption 231
10.5.3 Network Segmentation and Monitoring 231
10.5.4 Security Updates and Patch Management 232
10.6 Case Studies in IoT Security 232
10.6.1 Notable IoT Security Incidents 233
10.6.2 Successful IoT Security Implementations 234
10.7 Future Trends and Challenges in IoT Security 236
10.7.1 Artificial Intelligence and Machine Learning in IoT Security 236
10.7.2 Regulatory and Legal Considerations 236
10.7.3 Securing Emerging IoT Technologies 237
10.8 Conclusion 238
10.8.1 Recap of Key Points 238
10.8.2 Importance of IoT Security Implementation 239
10.8.3 Future Outlook for IoT Security 239
References 240

11 Secured IoT with LWC and Blockchain 243
Srishti Priya Chaturvedi, Ajay Yadav, Santosh Kumar and Rahul Mukherjee
11.1 Introduction 244
11.1.1 IoT Architecture 247
11.1.1.1 Three-Layered IoT Architecture 247
11.1.1.2 Five-Layered IoT Architecture 248
11.1.1.3 Cloud and Fog/Edge-Based IoT Architecture 249
11.2 Applications of IoT 251
11.2.1 Smart Home 251
11.2.2 Smart Healthcare 252
11.2.3 Industrial IoT 252
11.2.4 Smart Agriculture 252
11.2.5 Smart Mobility 252
11.2.6 Smart Grid 253
11.2.7 Environment Monitoring 253
11.3 Different Security Attacks on IoT Layers 254

11.3.1 Active Attack 254
11.3.1.1 Security Attacks on Perception/ Physical Layer 255
11.3.1.2 Security Attacks on Network Layer 256
11.3.1.3 Security Attacks on Processing Layer 257
11.3.1.4 Security Attacks on Application Layer 257
11.3.1.5 Security Attacks on Business Layer 258
11.3.2 Passive Attack 259
11.3.2.1 Eavesdropping 259
11.3.2.2 Traffic Analysis 259
11.4 Solution to IoT Security Attacks 259
11.4.1 IoT Security Using Blockchain Technology 259
11.4.1.1 Network Layer 260
11.4.1.2 Consensus Layer 260
11.4.1.3 Data Layer 260
11.4.1.4 Execution Layer 261
11.4.1.5 Application Layer 261
11.4.2 Blockchain-Based IoT Applications 261
11.4.2.1 Cyber-Physical Systems 262
11.4.2.2 Intelligent Transportation System 262
11.4.2.3 Smart City 262
11.4.2.4 Supply Chain Management 262
11.4.2.5 Underwater Things 262
11.4.3 IoT Security Using Lightweight Cryptography 262
11.4.3.1 Lightweight Cryptography 264
11.5 Conclusion 265
References 266

12 Social Engineering Attacks: Detection and Prevention 269
Rajat Singh, Priyanka Soni and Animaw Kerie
12.1 Introduction 269
12.1.1 Strong Affect 270
12.1.2 Overloading 271
12.1.3 Reciprocation 271
12.1.4 Deceptive Relationship 271
12.1.5 Diffusion of Moral Duty and Responsibility 271
12.1.6 Authority 271
12.1.7 Consistency and Commitment 272
12.2 Life Cycle of Social Engineering 272

12.2.1 Selection of Target and Reconnaissance 272
12.2.2 Planning and Preparation 273
12.2.3 Initiation of Contact 273
12.2.4 Fostering Trust and Manipulation 273
12.2.5 Elicitation and Exploitation 273
12.2.6 Launch of Attack 273
12.2.7 Maintaining the Access 274
12.2.8 Covering the Trails 274
12.3 Types of Social Engineering 274
12.3.1 Phishing 275
12.3.2 Vishing 275
12.3.3 Grooming 275
12.3.4 Identity Theft 275
12.3.5 Quid Pro Quo Attacks 276
12.3.6 Dumpster Diving Attacks 276
12.3.7 Diversion Theft Attacks 276
12.3.8 Tailgating 276
12.3.9 File Masquerade 277
12.3.10 Water-Holing 277
12.4 Social Engineering Attacks Using Advanced Techniques 277
12.5 Social Engineering Attack Detection Models 278
12.5.1 SEADM 278
12.5.2 SEADMv2 279
12.5.3 SEADer 280
12.5.4 SEADer++ V2 281
12.6 Detection of Social Engineering Links 281
12.7 Preventive Approaches 282
12.7.1 SIEM 282
12.7.2 Next-Gen Cloud-Based WAF 283
12.7.3 "Human-as-a-Security-Sensor Framework" 283
12.7.4 Awareness Programs 284
12.7.5 Prevention Protocols 284
12.8 Preventive Measures Against Social Engineering Attacks 285
12.8.1 Avoid Clicking Unknown Links 285
12.8.2 Use Multi-Factor Authentication 286
12.8.3 Verify Email Sender's Identity 286
12.8.4 Check for SSL Certificate 286
12.8.5 Check for Updates 286
12.8.6 Pay Attention to Your Digital Footprint 286
12.9 Conclusion 286
References 287

13 Multilayer Perceptron of Occlusion and Pose-Sensitive Ear Attributes for Social Engineering Attack Mitigation 291
O. Taiwo Olaleye, Oluwasefunmi Arogundade, Adebayo Abayomi-Alli, Wilson Ahiara, Temitope Ogunbiyi, Segun Akintunde, Segun Dada and Olalekan Okewale
13.1 Introduction 292
13.1.1 Biometric Authentication and Social Engineering Attacks 293
13.1.1.1 Strengths of Biometric Authentication 293
13.1.1.2 Weaknesses of Biometric Authentication 293
13.2 Literature Review 295
13.2.1 Black Ear Inclusivity in Biometric Authentication Systems 296
13.3 Materials and Methods 299
13.3.1 Data Acquisition 299
13.3.2 Feature Extraction 299
13.3.2.1 Color Layout Filter 299
13.3.2.2 Edge Histogram Filter 300
13.3.3 One-Hot Encoding 301
13.3.4 Predictive Analytics by the Perceptron 303
13.3.5 Parameter Optimization of MLP 303
13.4 Result and Discussion 305
13.4.1 Performance Metrics of MLP on Occlusion and Pose Sensitive Ear Facial Dataset 305
13.4.2 Performance Metrics of MLP on Occlusion and Pose Sensitive Ear Facial Dataset After One-Hot Encoding 306
13.4.3 Performance Metrics of MLP on Occlusion and Pose Sensitive Ear Facial Dataset with Parameter Optimization 307
13.4.4 Performance Metrics of MLP on Occlusion and Pose Sensitive Ear Facial Dataset After One-Hot Encoding with Parameter Optimization 308
13.4.5 Overall Evaluation of MLP on the Experimental Measures 309
13.5 Conclusion 311
References 312

14 Study and Analysis of Cyberbullying Message Detection and Prevention Using Machine Learning Techniques 315
S. Shanmugam, S. Gunasekaran and N. Anusha
14.1 Introduction 316
14.2 Literature Survey 318
14.2.1 Identifying Cyberbullies Through Twitter Data Analysis 318
14.2.2 Cyber Bullying Detection on Social Media Using Machine Learning 318
14.2.3 Cyberbullying in Schools: A Research of Gender Differences 319
14.2.4 Automated Detection of Cyberbullying Using Machine Learning 319
14.3 Implementation of Cyberbullying Model 320
14.3.1 Dataset Description 320
14.3.2 Architecture and Functionalities of the Proposed System 321
14.3.2.1 NLP Toolkit for Implementation 322
14.3.3 Performance Evaluation Measures 324
14.4 Evaluation and Comparison of Machine Learning Techniques for Cyber Bullying 325
14.5 Conclusion 329
References 329

15 Future Directions in Digital Forensics and Cybersecurity 333
Elipe Arjun and Priyanka Singh
15.1 Overview of Digital Forensics and Cyber Forensics 333
15.2 Introduction 335
15.2.1 Rapid Technological Evolution 337
15.2.2 An Ever-Changing Threat Landscape 337
15.3 Technologies and Their Impact 337
15.3.1 Balancing Opportunity and Threat 337
15.4 Impact of Emerging Technologies on Digital Forensics and Cybersecurity 338
15.4.1 Artificial Intelligence (AI) and Machine Learning (ML) 338
15.4.2 Quantum Computing 340
15.4.3 5G Technology 340
15.4.4 Blockchain Technology 340
15.4.5 Biometric Technologies 340
15.4.6 Cloud Computing 341

15.4.7 IoT (Internet of Things) 341
15.4.8 Automated Threats and Botnets 342
15.4.9 Augmented Reality (AR) Virtual Reality (VR) and Autonomous Systems and AI-Driven Attacks 342
15.5 Cybersecurity and Digital Forensics: Threats and Opportunities 342
15.5.1 Threats 343
15.5.2 Opportunities 344
15.6 Future of Digital Forensics 346
15.6.1 Emerging Trends and Future Directions in Digital Forensics 347
15.6.2 Potential Benefits and Challenges of These Emerging Trends of Digital Forensics 348
15.6.3 Significant Challenges in Modern Digital Forensics, Both from an Ethical and Technological Perspective 349
15.7 The Future of Cybersecurity 350
15.7.1 Overview of Future Directions and Emerging Trends in Cybersecurity 350
15.7.2 Emerging Trends and Potential Benefits Include 351
15.7.3 Challenges in Cybersecurity 352
15.8 Collaboration and Interdisciplinary Approaches 353
15.8.1 Ways in Which Digital Forensics and Cyber Security Might Collaborate 353
15.9 Ethics and Human Factors in Future Digital Forensics and Cybersecurity 356
15.9.1 Why Do we Need Ethics in Technology? 356
15.9.2 What Does Ethics Have to Do with Cybersecurity and Digital Forensics? 357
15.9.3 Potential Benefits 358
15.10 Challenges and Opportunities of Digital and Cyber-Forensics 359
15.10.1 Challenges 359
15.10.2 Opportunities 360
15.11 Conclusion 360
15.11.1 Summary of Key Points 361
15.11.2 Discussion of Importance 361
15.11.3 Conclusion and Implications for Future Research and Practice 362
References 363

16 Tomorrow's Shields: Exploring Future Trends in Cyber Security and Forensics **367**
Mridu Sharma, Ravshish Kaur Kohli and Kunal Sharma
16.1 Introduction 368
16.2 Recent Digital Forensic Trends 369
16.2.1 Cloud Forensics 369
16.2.2 Social Media Forensics 370
16.2.3 IoT Forensics 372
16.3 Threats Faced by Digital Forensics 374
16.3.1 Technical Challenges 374
16.3.2 Operational Challenges 375
16.3.3 Personnel-Related Challenges 376
16.4 Opportunities 378
16.4.1 USB Forensics 378
16.4.2 Intrusion Detection 379
16.4.3 Artificial Intelligence 380
16.5 Conclusion 382
References 382

Index **387**

Preface

Welcome to *Securing the Digital Frontier: Threats and Advanced Techniques in Security and Forensics*. In today's interconnected world, where our lives are increasingly intertwined with technology, safeguarding our digital information cannot be overstated. This book is a comprehensive exploration of the evolving landscape of cybersecurity, offering insights into the latest threats, innovative techniques, and proactive measures employed to protect our digital assets.

Chapter 1, "Pegasus - A Menace to Privacy and Security," sheds light on the Pegasus spyware developed by the Israeli-based cyber group NSO. Authors Raunaq Khurana and Shilpa Mahajan examine the workings of this advanced spyware, which exploits zero-day vulnerabilities to access and collect data from target systems without user consent. Through detailed analysis and case studies, the chapter highlights Pegasus's challenges. It encourages using advanced technologies such as AI and ML/DL to develop effective countermeasures.

In Chapter 2, "Data Privacy and Compliance in Information Security," authors Rakesh Nayak, Umashankar Ghugar, Praveen Gupta, Satyabrata Dash, and Nishu Gupta explore the sophisticated relationship between data privacy and compliance in information security. They discuss the challenges, regulations, and best practices in protecting sensitive data in today's digital age, emphasizing the importance of implementing robust security measures and fostering privacy awareness within organizations.

Chapter 3, "Unveiling Cyber Threats: Exploring Crime, Security Techniques, and Digital Forensics," authored by Nidhi Gupta, Arpita Trivedi, Parveen P Terang, and Hasmat Malik, delves into the escalating landscape of cybercrimes and the various advanced techniques used to protect devices from cyberattacks. The chapter also highlights the importance of digital forensics in investigating cybercrimes and identifying perpetrators.

In Chapter 4, "A Customised Privacy Preservation Mechanism for Cyber-Physical Systems," authors Manas Kumar Yogi and A.S.N. Chakravarthy advocate for a novel privacy approach for cyber-physical systems, allowing users to customize their privacy settings based on their usage. The chapter explores the trade-off between privacy and utility in CPS entities and presents a provisional privacy-preserving method designed to enhance data utility while maintaining user privacy.

Chapter 5, "Securing the Future: Emerging Threats and Countermeasures in Cryptography," authored by Debosree Ghosh, Kishore Ghosh, Chandrima Chakraborty, Atanu Datta, and Somsubhra Gupta, focuses on emerging threats to cryptographic systems and innovative countermeasures. The chapter highlights the importance of post-quantum cryptography and secure implementation practices in safeguarding data security in an evolving digital landscape.

In Chapter 6, "Cyber Threats and its Impact on Electronic Transactions," authors Ramalingam Dharmalingam and Vaishnavi Dharmalingam explore the impact of cyber threats on electronic transactions, particularly during the COVID-19 pandemic. The chapter discusses the growth of digital transformation, current cyberattacks, and frameworks for combating cyber threats, emphasizing the need for collaborative efforts to secure future transactions.

Chapter 7, "A Robust Model for Enabling Insider Threat Detection and Prevention: Techniques, Tools, and Applications," authored by A Sheik Abdullah, Shivansh Dhiman, and Arif Ansari, addresses the growing threat of insider threats in organizations. The chapter explores techniques and tools for accurately detecting and mitigating insider threats, leveraging machine learning, artificial intelligence, and behavioral analytics.

In Chapter 8, "Digital Vulnerabilities Unveiled: A Multidisciplinary Exploration of Emerging Threats to Security and Privacy in the Age of Networked Communication," authors Priya Sachdeva and Archan Mitra offer a multidisciplinary analysis of digital vulnerabilities, highlighting the interplay between socio-technical factors underlying security issues. The chapter emphasizes the value of interdisciplinary approaches in comprehending and solving complex security challenges.

Chapter 9, "Tools of Emancipation as Global Web and its Digital Ecosystem: Steering IoT Landscape, Cloud Computing Unravel Safe Spaces Lensing New Cyber Risks and Emerging Threats," authored by Bhupinder Singh and Christian Kaunert, explores the symbiosis of tools of emancipation, the global web, and the digital ecosystem in navigating cybersecurity challenges. The chapter discusses the role of IoT and cloud computing in

mitigating cyber risks and proposes strategies for fortifying safe spaces in the digital realm.

Chapter 10, "IoT and Smart Device Security: Emerging Threats and Countermeasures," authored by Geo Francis E, S. Sheeja, Anotony Johen E.F., and Jismy Joseph, delves into the security challenges posed by IoT devices and explores emerging threats and countermeasures. The chapter emphasizes the importance of addressing IoT vulnerabilities and implementing robust security measures to safeguard data privacy and integrity.

In Chapter 11, "Secured IoT with LWC and Blockchain," authors Srishti Priya Chaturvedi, Ajay Yadav, Santosh Kumar, and Rahul Mukherjee discuss lightweight encryption and blockchain solutions for securing the Internet of Things. The chapter explores using lightweight cryptographic algorithms and decentralized blockchain structures to protect IoT ecosystems from cyber threats.

Chapter 12, "Social Engineering Attacks: Detection and Prevention," authored by Rajat Singh, Priyanka Soni, and Animaw Kerie, focuses on social engineering attacks and proposes detection and prevention techniques. The chapter discusses various social engineering attack models and preventive measures, including security information and event management (SIEM) systems and human-as-a-security-sensor frameworks.

In Chapter 13, "Multilayer Perceptron of Occlusion and Pose-Sensitive Ear Attributes for Social Engineering Attack Mitigation," authors O. Taiwo Olaleye, Oluwasefunmi Arogundade, Adebayo Abayomi-Alli, Wilson Ahiara, Temitope Ogunbiyi, Segun Akintunde, Segun Dada, and Olalekan Okewale explore the use of multilayer perceptron for detecting social engineering attacks. The chapter investigates the effectiveness of MLP in handling occlusion and pose variations, offering insights into its potential applications in digital forensics.

Chapter 14, "Study and Analysis of Cyberbullying Message Detection and Prevention Using Machine Learning Techniques," authored by Dr. S. Gunasekaran, Dr. S. Shanmugam, and Dr. N. Anusha, focuses on detecting and preventing cyberbullying using machine learning techniques. The chapter compares different machine-learning approaches for cyberbullying detection and proposes future research directions for improving detection accuracy.

Chapter 15, "Future Directions in Digital Forensics and Cybersecurity," authored by Elipe Arjun and Priyanka Singh, offers insights into the future trends and challenges in digital forensics and cybersecurity. The chapter explores the potential impact of emerging technologies like quantum computing and AI on cybersecurity practices, emphasizing the need for interdisciplinary collaboration and ethical considerations.

In Chapter 16, "Tomorrow's Shields: Exploring Future Trends in Cyber Security and Forensics," authors M. Sharma, R.K. Kohli, and K. Sharma provide a holistic perspective on future trends in security and forensics. The chapter discusses emerging technologies, regulatory frameworks, and industry trends shaping the future of cybersecurity, highlighting the importance of proactive measures and continuous learning in combating evolving threats.

We extend our sincere gratitude to all the authors who contributed their expertise & insights to this book. Their dedication and passion for advancing cybersecurity knowledge have made this book a valuable resource for researchers, practitioners, and students alike.

We hope that *Securing the Digital Frontier: Threats and Advanced Techniques in Security and Forensics* catalyzes ongoing discussions & collaborative efforts to fortify our digital defenses and navigate the ever-changing cybersecurity landscape.

Dr. Kavita Sharma
Galgotias College of Engineering & Technology, Greater Noida, India
Dr. Vishnu Sharma
ITS Engineering College, Greater Noida, India
Dr. Parma Nand
Sharda University, Greater Noida, India
Dr. Anil Kumar Sagar
Sharda University, Greater Noida, India
Dr. Gulshan Shrivastava
Bennett University, Greater Noida, India

1

Pegasus—A Menace to Privacy and Security

Raunaq Khurana* and Shilpa Mahajan

Department of Computer Science, The NorthCap University, Gurugram, Haryana, India

Abstract

The Israeli-based cyber group NSO developed Pegasus, a spyware that can access and collect data from a target system without the user's consent. Pegasus commonly exploits zero-day vulnerabilities, which are system weaknesses that the manufacturer has not addressed or is unaware of. This chapter thoroughly examines the Pegasus spyware, highlighting its unique features that pose significant challenges in its detection as compared to other malicious software. It presents an extensive analysis of Pegasus on both iOS and Android operating systems, with the intention of educating readers about its capabilities and advocating for the use of advanced technologies such as AI, ML/DL to develop effective countermeasures against spyware, malware, and adware. The chapter also includes various case studies that illustrate the transformation of Pegasus over time and the measures taken to prevent its infiltration into user devices. To facilitate reader's understanding, the chapter provides essential security checklists that help identify Pegasus's monitoring mechanisms.

***Keywords*:** Malware/spyware, encryption, vulnerability, vishing

1.1 Introduction

Spyware is harmful software made with the intention of stealing data from a system and sharing it with unidentified outside third parties. Pegasus is a sophisticated programme that can break into mobile devices like smartphones and tablets and eventually go over security precautions like internal

**Corresponding author*: raunaq.khurana18@gmail.com

Kavita Sharma, Vishnu Sharma, Parma Nand, Anil Kumar Sagar and Gulshan Shrivastava (eds.)
Securing the Digital Frontier: Threats and Advanced Techniques in Security and Forensics, (1–16)

encryption and two-factor authentication to allow hackers complete access to the targeted device once it is plugged in. If that is the case, Pegasus can control all communication between devices, including calls, messages, emails, microphone and camera providers, location data, contacts and calendars [1]. The memory consumption can be discovered using covert methods, CPU cycles, and network traffic monitoring, despite the fact that the Pegasus file store was initially intended to target officials, politicians, journalists, and influencers.

Pegasus tool is produced by the Israeli company NSO Group. This surveillance tool is designed purposely to monitor specific individuals for national security. Although this tool is developed to be used by the government agencies but it has been a subject of significant controversies. These controversies arises as they are considered to be threat to human privacy, an abuse to human rights and potential misuse of surveillance technologies.

The allegation involves that government is spying on its officials and political opponents and even individuals or not even legitimate targets for surveillance. NSO group gave his assurance that their tool is used for legitimate purposes like for frightening crimes and terrorism. However, number of evidences and investigations have suggested that Pegasus has been used for questionable purposes by some people.

The way that this tool operates is by taking advantage of flaws in mobile devices, especially smartphones, to access personal data, including calls, texts, emails, and other communications. It may also be used to activate the camera and microphone, monitor the device's position, and do a variety of other things, thereby transforming it into a robust surveillance tool.

The properties of Pegasus are thoroughly covered in this chapter, with special emphasis placed on those aspects that set it isolated from different spyware and malware in terms of difficulty in detection [2]. It also explains how Pegasus operates on both iOS and Android operating systems and suggests using advanced technologies like machine learning and AI to develop systems that can identify and prevent Pegasus, safeguarding devices from adware, malware, or spyware. Additionally, the chapter presents case studies demonstrating Pegasus's evolution over time and proposes methods to prevent spyware from infiltrating and spreading on user devices. By following the practical safety guidelines outlined in this chapter, readers can learn how to protect themselves from Pegasus's surveillance tool.

- Investigating the market origins and distribution of Pegasus.
- Examining how Pegasus operates and its ability to turn smartphones into listening devices by exploiting multiple vulnerabilities.

- Proposing various techniques to detect potential Pegasus attacks.
- Sharing advice on how to recognize the presence of Pegasus spyware on a device.
- Suggesting the utilization of command-line or terminal utilities to lower the likelihood of being affected by the Pegasus spyware.
- Providing practical recommendations to enhance awareness and protect devices from Pegasus spyware.

Spyware attacks have become increasingly sophisticated in recent years. In the past, malicious software could be installed by opening a suspicious email as early as a decade ago [3]. However, Pegasus spyware has now adopted a "mobile first" strategy, whereby it impersonates its users by sending links in text messages that appear to be from trusted sources. Clicking on these links gives Pegasus access to sensitive information, such as location data and financial information. From 2016 to 2021, Pegasus has become even more advanced and now uses "zero-click" technology, which relies on zero-day threats that are unknown to the user and remain unpatched [4]. To limit the success of Pegasus on user devices, the research paper titled "Pegasus: A Privacy Killer" recommends adopting basic precautions, like avoid unknown links, categorization of devices, and using reliable VPNs for all devices [5, 6]. Pegasus uses complex zero-day infection vectors to infiltrate devices. Once installed, try different ways to get access to victim's data and transmits it to the server [7]. The way how Pegasus can attack and exploit your phone can be seen in Figure 1.1.

1) It uses GPS information to identify and differentiate targets and obtain precise information
2) The Pegasus spyware does not require coordination with local Mobile Network Operators (MNOs), making it independent of service providers.
3) It control both the content and devices it infects by utilizing proprietary protocols and SSL, commonly used in complex communications, which allows it to surpass encrypted information.
4) The surveillance includes monitoring various applications, such as Instagram, Twitter, WhatsApp, Skype, Viber etc.
5) Monitor VoIP and voice calls in real time (call interception).
6) Pegasus can recognize operational identities without the need for regularly switching virtual identities or while continuously surveilling/observing the device.

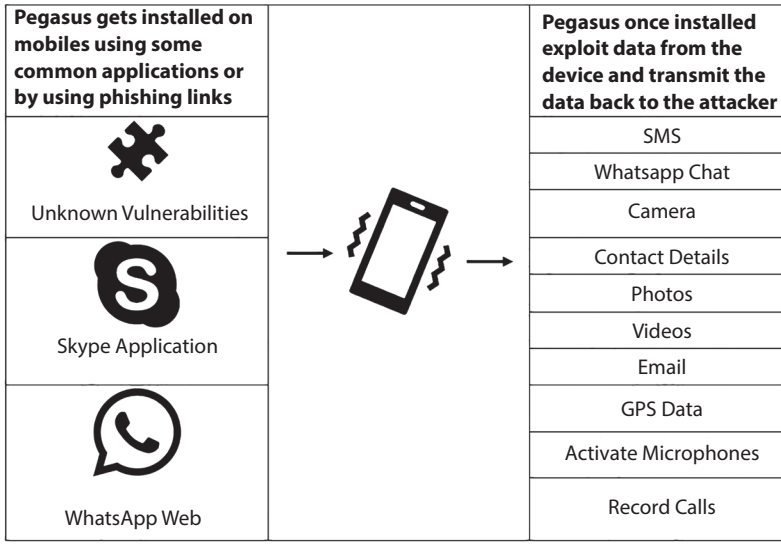


Figure 1.1 Pegasus impact.

1.2 Working of Pegasus

This spyware name Pegasus is a highly advance and dangerous tool that exploits "Zero-day Vulnerability," a security weakness for which no patch or update is available or known by the manufacturer. Pegasus can silently infiltrate various Android and iOS devices and covertly monitor all device activities. By exploiting vulnerabilities in third-party spyware, Pegasus can take complete control of the device, allowing the attacker to perform various actions. To protect against such attacks, users must take proactive measures, such as installing antivirus software, regularly updating device firmware, and being vigilant when clicking on links from unknown sources.

Pegasus can access data like access your messages, location tracking, content surfing, can make calls from compromised phones, call logs can be accessed, access to photo, camera and Microphone can be accessed and an delete data and even retrieve the deleted files from the mobiles. Pegasus spyware directly transmit the data obtained from target's phone straight to the data server of NSO group [8].

Pegasus spyware is a highly advanced malware that can be installed easily through physical contact, text or email and through calls and messages. It exploits vulnerabilities that have not been updated with a patch or are not known to the relevant parties. It can infiltrate a device through a missed call on WhatsApp or an iMessage on iPhones [9]. The Pegasus spyware utilizes a zero-click method that does not require any user interaction, making it challenging to detect. Even if a user tries to delete a suspicious message, the spyware can persist on the device and infect it [10].

Pegasus spyware is a highly sophisticated tool that can decrypt end-to-end encrypted messages and files, making it a potent weapon in espionage [11, 12]. Recent findings indicate that the latest versions of Pegasus can infiltrate devices through missed calls and delete the call logs to cover up the attack, making it harder to detect and track its actions. This poses a significant challenge for users who may not even be aware that their devices have been compromised [13].

A diagram depicting the general workflow of Pegasus can be seen in Figure 1.2.

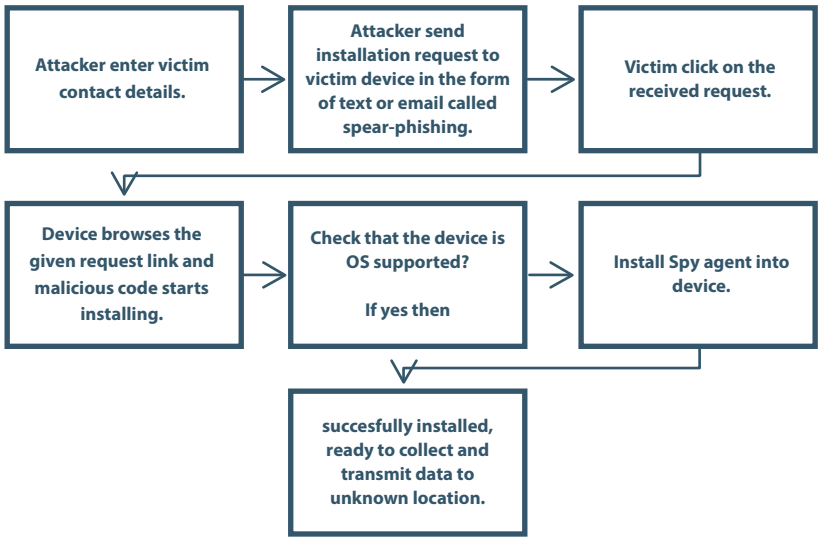


Figure 1.2 Pegasus workflow.

The workflow of Pegasus on a normal device vs. an infected device can be seen in Figure 1.3. It is interesting to find how an infected device behave differently from the normal device. In normal device, the common phasis include

Device Setup	*The user purchases a new mobile device and goes through the initial setup process, which typically includes connecting to Wi-Fi, signing in with their Apple ID or Google Account, and configuring settings.*
App Installation	*Users can install applications from authorized application marketplaces such as the Apple App Store or Google Play Store. These apps undergo a vetting process to ensure they do not contain malicious code.*
Regular Usage	*The individual utilizes the device for a multitude of functions, including placing calls, sending messages, surfing the web, and accessing applications. The device operates normally without any unexpected behavior.*

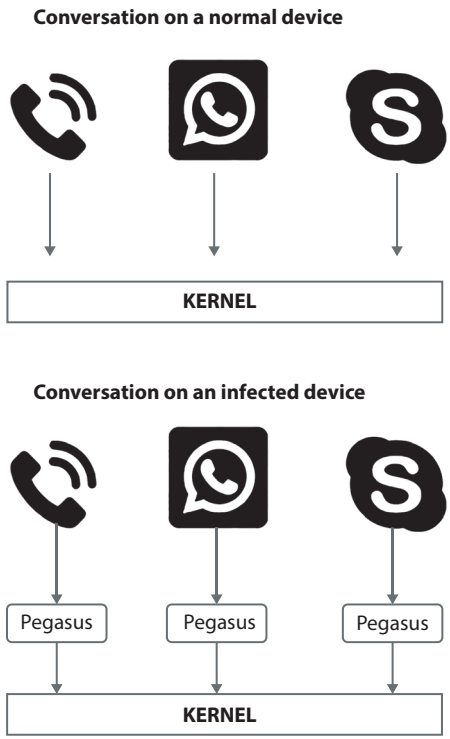


Figure 1.3 Work-flow of normal device vs infected device.