Abusing The Internet Of Things Blackouts Freakouts And Stakeouts

This book discusses novel intelligent-system algorithms and methods in cybernetics, presenting new approaches in the field of cybernetics and automation control theory. It constitutes the proceedings of the Cybernetics and Automation Control Theory Methods in Intelligent Algorithms Section of the 8th Computer Science On-line Conference 2019 (CSOC 2019), held on-line in April 2019.

Drawing on the popular Economic Social and Research Council (ESRC) seminar series, this book examines social issues and anxieties, and the solutions to them, through the concept of moral panic.

Substance abuse is one of the most frequent and serious problems encountered by human service workers, criminal justice professionals, and clinicians. Unfortunately, many professionals in these fields receive little, if any, formal training about this problem. Our planned encyclopedia presents state-of-the-art research and evidence-based applications in A-to-Z format. Rather than create a compendium of specific drugs and drug effects, for which there are any number of fine titles already available, the focus will be upon practical knowledge and skills for pre-service and in-service human service professionals, including substance abuse counselors and prevention specialists.

This book is a marvellous thing: an important intervention in the policy debate about information security and a practical text for people trying to improve the situation. — Cory Doctorowauthor, co-editor of Boing Boing A future with billions of connected "things" includes monumental security concerns. This practical book explores how malicious attackers can abuse popular IoT-based devices, including wireless LED lightbulbs, electronic door locks, baby monitors, smart TVs, and connected cars. If you’re part of a team creating applications for Internet-connected devices, this guide will help you explore security solutions. You’ll not only learn how to uncover vulnerabilities in existing IoT devices, but also gain deeper insight into an attacker’s tactics. Analyze the design, architecture, and security issues of wireless lighting systems Understand how to breach electronic door locks and their wireless mechanisms Examine security design flaws in remote-controlled baby monitors Evaluate the security design of a suite of IoT-connected home products Scrutinize security vulnerabilities in smart TVs Explore research into security weaknesses in smart cars Delve into prototyping techniques that address security in initial designs Learn plausible attacks scenarios based on how people will likely use IoT devices

Society is now completely driven by data with many industries relying on data to conduct business or basic functions within the organization. With the efficiencies that big data bring to all institutions, data is continuously being collected and analyzed. However, data sets may be too complex for traditional data-processing, and therefore, different strategies must evolve to solve the issue. The field of big data works as a valuable tool for many different industries. The Research Anthology on Big Data Analytics, Architectures, and Applications is a complete reference source on big data analytics that offers the latest, innovative architectures and frameworks and explores a variety of applications within various industries. Offering an international perspective, the applications discussed within this anthology feature global representation. Covering topics such as advertising curricula, driven supply chain, and smart cities, this research anthology is ideal for data scientists, data analysts, computer engineers, software engineers, technologists, government officials, managers, CEOs, professors, graduate students, researchers, and academicians.

This book introduces readers to the tools needed to protect IT resources and communicate with security specialists when there is a security problem. The book covers a wide range of security topics including Cryptographic Technologies, Network Security, Security Management, Information Assurance, Security Applications, Computer Security, Hardware Security, and Biometrics and Forensics. It introduces the concepts, techniques, methods, approaches, and trends needed by security specialists to improve their security skills and capabilities. Further, it provides a glimpse into future directions where security techniques, policies, applications, and theories are headed. The book represents a collection of carefully selected and reviewed chapters written by diverse security experts in the listed fields and edited by prominent security researchers. Complementary slides are available for download on the book’s website at Springer.com.

The two-volume set LNICST 150 and 151 constitutes the thoroughly refereed post-conference proceedings of the First International Internet of Things Summit, IoT360 2014, held in Rome, Italy, in October 2014. This volume contains 74 full papers carefully reviewed and selected from 118 submissions at the following four conferences: the First International Conference on Cognitive Internet of Things Technologies, COIOTE 2014; the First International Conference on Pervasive Games, PERGAMES 2014; the First International Conference on IoT Technologies for HealthCare, HealthyIoT 2014; and the First International Conference on IoT as a Service, IoTaaS 2014. The papers cover the following topics: user-centric IoT; artificial intelligence techniques for the IoT; the design and deployment of pervasive games for various sectors, such as health and wellbeing, ambient assisted living, smart cities and societies, education, cultural heritage, and tourism; delivery of electronic healthcare; patient care and medical data management; smart objects; networking considerations for IoT; platforms for IoTaaS; adapting to the IoT environment; modeling IoTaaS; machine to machine support in IoT.

Lawyer's Desk Book is an extraordinary guide that you can't afford to be without. Used by over 150,000 attorneys and legal professionals, this must-have reference supplies you with instant, authoritative legal answers, without exorbitant research fees. Packed with current, critical information, Lawyer's Desk Book includes: Practical guidance on virtually any legal matter you might encounter: real estate transactions, trusts, divorce law, securities, mergers and acquisitions, computer law, tax planning, credit and collections, employer-employee relations, personal injury, and more - over 75 key legal areas in all! Quick answers to your legal questions, without having to search stacks of material, or wade through pages of verbiage. Key citations of crucial court cases, rulings, references, code sections, and more. More than 1500 pages of concise, practical, insightful information. No fluff, no filler. Just the facts you need to know. The Lawyer's Desk Book, 2017 Edition incorporates recent court decisions, legislation, and administrative rulings. Federal statutes and

revised sentencing guides covered in this edition reflect a growing interest in preventing terrorism, punishing terror-related crimes, and promoting greater uniformity of sentencing. There is also new material on intellectual property law, on legislation stemming from corporate scandals, such as the Sarbanes- Oxley Act, and on legislation to cut individual and corporate tax rates, such as the Jobs and Growth Tax Relief Reconciliation Act. Chapters are in sections on areas including business planning and litigation, contract and property law, and law office issues.

This book focuses on recent advances and different research areas in multi-modal data fusion under healthcare informatics and seeks out theoretical, methodological, well-established and validated empirical work dealing with these different topics. This book brings together the latest industrial and academic progress, research, and development efforts within the rapidly maturing health informatics ecosystem. Contributions highlight emerging data fusion topics that support prospective healthcare applications. The book also presents various technologies and concerns regarding energy aware and secure sensors and how they can reduce energy consumption in health care applications. It also discusses the life cycle of sensor devices and protocols with the help of energy-aware design, production, and utilization, as well as the Internet of Things technologies such as tags, sensors, sensing networks, and Internet technologies. In a nutshell, this book gives a comprehensive overview of the state-of-the-art theories and techniques for massive data handling and access in medical data and smart health in IoT, and provides useful guidelines for the design of massive Internet of Medical Things. Presents a rigorous introduction to theoretical foundations and practical solutions for Internet of Medical Things; Covers data handling, intelligence and security and related issues to guide the massive data handling techniques for healthcare; Includes examples and case studies for further study for academics, researchers, and professionals.

A compelling argument that the Internet of things threatens human rights and security and that suggests policy prescriptions to protect our future The Internet has leapt from human-facing display screens into the material objects all around us. In this so-called Internet of Things—connecting everything from cars to cardiac monitors to home appliances—there is no longer a meaningful distinction between physical and virtual worlds. Everything is connected. The social and economic benefits are tremendous, but there is a downside: an outage in cyberspace can result not only in a loss of communication but also potentially a loss of life. Control of this infrastructure has become a proxy for political power, since countries can easily reach across borders to disrupt real-world systems. Laura DeNardis argues that this diffusion of the Internet into the physical world radically escalates governance concerns around privacy, discrimination, human safety, democracy, and national security, and she offers new cyber-policy solutions. In her discussion, she makes visible the sinews of power already embedded in our technology and explores how hidden technical governance arrangements will become the constitution of our future.

This publication highlights the fast-moving technological advancement and infiltration of Artificial Intelligence into society. Concepts of evolution of society through interconnectivity are explored, together with how the fusion of human and technological interaction leading to Augmented Humanity is fast becoming more than just an endemic phase, but a cultural phase shift to digital societies. It aims to balance both the positive progressive outlooks such developments bring with potential issues that may stem from innovation of this kind, such as the invasive procedures of bio hacking or ethical connotations concerning the usage of digital twins. This publication will also give the reader a good level of understanding on fundamental cyber defence principles, interactions with Critical National Infrastructure (CNI) and the Command, Control, Communications and Intelligence (C3I) decision-making framework. A detailed view of the cyber-attack landscape will be garnered; touching on the tactics, techniques and procedures used, red and blue teaming initiatives, cyber resilience and the protection of larger scale systems. The integration of AI, smart societies, the human-centric approach and Augmented Humanity is discernible in the exponential growth, collection and use of [big] data; concepts woven throughout the diversity of topics covered in this publication; which also discusses the privacy and transparency of data ownership, and the potential dangers of exploitation through social media. As humans are become ever more interconnected, with the prolificacy of smart wearable devices and wearable body area networks, the availability of and abundance of user data and metadata derived from individuals has grown exponentially. The notion of data ownership, privacy and situational awareness are now at the forefront in this new age.

Elvy explores the consumer ramifications of the Internet of Things through the lens of the commercial law of privacy and security.

Use the Internet. Know its dangers. Internet use is catching on faster than any form of technology ever invented. Its potential for human benefit is beyond measure. But it is not without problems: • Marriages break up over emotional relationships forged in chat rooms. • College students risk grades and health to spend time online. • Child abusers lure kids by contact through the internet. • Adults spend fortunes to subscribe to internet pornography. These people have crossed the boundary between healthy use and obsessive preoccupation with this versatile electronic medium. An avid net-surfer himself, therapist Gregory Jantz has seen an increasing number of clients coming to his counseling centers for help with internet abuse. Jantz writes for two audiences: those who are worried about a loved one's use of the net, and internet users who may have a problem. He offers both groups concrete and biblical steps for working towards change.

This volume presents in-depth studies on leading themes in education policy and intercultural communication in contemporary Asia, covering empirical as well as theoretical approaches, and offering both an in-depth investigation of their implications, and a synthesis of areas where these topics cohere and point to advances in description, analysis and theory, policy and applications. The studies address key questions that are essential to the future of education in an Asia where intercultural communication is ever more important with the rise of the ASEAN Economic Community and other international initiatives. These questions include the properties of the increasing globalisation of communication and how it plays out in Asia, especially but not exclusively with reference to English, and how we can place intercultural communication in this context, as well as studies that highlight intercultural communication and its underlying value

systems and ideologies in Asia.

This book constitutes the proceedings of the 7th International Conference on Internet of Things (IoT) Technologies for HealthCare, HealthyIoT 2020, held in Viana do Castello, Portugal, in December 2020. Due to Covid-19 pandemic the conference was held virtually. The IoT as a set of existing and emerging technologies, notions and services can provide many solutions to delivery of electronic healthcare, patient care, and medical data management. The 12 revised full papers presented were carefully reviewed and selected from 27 submissions. The papers are grouped in topics on physical data tracking wearables, applications and systems; psychological data tracking wearables, applications and systems; scenarios and security.

The life and times of the Smart Wife--feminized digital assistants who are friendly and sometimes flirty, occasionally glitchy but perpetually available. Meet the Smart Wife--at your service, an eclectic collection of feminized AI, robotic, and smart devices. This digital assistant is friendly and sometimes flirty, docile and efficient, occasionally glitchy but perpetually available. She might go by Siri, or Alexa, or inhabit Google Home. She can keep us company, order groceries, vacuum the floor, turn out the lights. A Japanese digital voice assistant--a virtual anime hologram named Hikari Azuma--sends her "master" helpful messages during the day; an American sexbot named Roxxxy takes on other kinds of household chores. In The Smart Wife, Yolande Strengers and Jenny Kennedy examine the emergence of digital devices that carry out "wifework"--domestic responsibilities that have traditionally fallen to (human) wives. They show that the principal prototype for these virtual helpers--designed in male-dominated industries--is the 1950s housewife: white, middle class, heteronormative, and nurturing, with a spick-and-span home. It's time, they say, to give the Smart Wife a reboot. What's wrong with preferring domestic assistants with feminine personalities? We like our assistants to conform to gender stereotypes--so what? For one thing, Strengers and Kennedy remind us, the design of gendered devices re-inscribes those outdated and unfounded stereotypes. Advanced technology is taking us backwards on gender equity. Strengers and Kennedy offer a Smart Wife "manifesta," proposing a rebooted Smart Wife that would promote a revaluing of femininity in society in all her glorious diversity.

This book provides use case scenarios of machine learning, artificial intelligence, and real-time domains to supplement cyber security operations and proactively predict attacks and preempt cyber incidents. The authors discuss cybersecurity incident planning, starting from a draft response plan, to assigning responsibilities, to use of external experts, to equipping organization teams to address incidents, to preparing communication strategy and cyber insurance. They also discuss classifications and methods to detect cybersecurity incidents, how to organize the incident response team, how to conduct situational awareness, how to contain and eradicate incidents, and how to cleanup and recover. The book shares real-world experiences and knowledge from authors from academia and industry. Shares cases studies on using ML and AI to predict and preempt cyber attacks; Describes security attacks, trends, and scenarios along with attack vectors for various domains and industry sectors; Includes detail on incident planning, detection methods, containing incidents, and clean up and recovery.

Use this hands-on guide to understand the ever growing and complex world of digital security. Learn how to protect yourself from digital crime, secure your communications, and become anonymous online using sophisticated yet practical tools and techniques. This book teaches you how to secure your online identity and personal devices, encrypt your digital data and online communications, protect cloud data and Internet of Things (IoT), mitigate social engineering attacks, keep your purchases secret, and conceal your digital footprint. You will understand best practices to harden your operating system and delete digital traces using the most widely used operating system, Windows. Digital Privacy and Security Using Windows offers a comprehensive list of practical digital privacy tutorials in addition to being a complete repository of free online resources and tools assembled in one place. The book helps you build a robust defense from electronic crime and corporate surveillance. It covers general principles of digital privacy and how to configure and use various security applications to maintain your privacy, such as TOR, VPN, and BitLocker. You will learn to encrypt email communications using Gpg4win and Thunderbird. What You'll Learn Know the various parties interested in having your private data Differentiate between government and corporate surveillance, and the motivations behind each one Understand how online tracking works technically Protect digital data, secure online communications, and become anonymous online Cover and destroy your digital traces using Windows OS Secure your data in transit and at rest Be aware of cyber security risks and countermeasures Who This Book Is For End users, information security professionals, management, infosec students

This book offers a timely and detailed exploration and analysis of key contemporary issues and challenges in child sexual abuse, which holds great relevance for scholarly, legal, policy, professional and clinical audiences worldwide. The book draws together the best current evidence about the nature, aetiology, contexts, and sequelae of child sexual abuse. It explores the optimal definition of child sexual abuse, considers sexual abuse in history, and explores new theoretical understandings of children's rights and other key theories including public health and the Capabilities Approach, and their relevance to child sexual abuse prevention and responses. It examines a selection of the most pressing legal, theoretical, policy and practical challenges in child sexual abuse in the modern world, in developed and developing economies, including institutional child sexual abuse, female genital cutting, child marriage, the use of technology for sexual abuse, and the ethical responsibility and legal liability of major state and religious organisations, and individuals. It examines recent landmark legal and policy developments in all of these areas, drawing in particular on extensive developments from Australia in the wake of its Royal Commission Into Institutional Responses to Child Sexual Abuse. It also considers the best evidence about promising strategies and future promising directions in enhancing effective prevention, intervention and responses to child sexual abuse.

Cybersexism is rampant and can exact an astonishingly high cost. In some cases, the final result is suicide. Bullying, stalking, and trolling are just the beginning. Extreme examples such as GamerGate get publicized, but otherwise the online abuse of women is largely underreported. Haters combines a history of online sexism with suggestions for solutions. Using current events and the latest available research into cybersexism, Bailey Poland questions the motivations behind cybersexist activities and explores methods to reduce footprints of Internet misogyny, drawing parallels between online and offline abuse. By exploring the cases of Alyssa Funke, Rehtaeh Parsons, Audrie Pott, Zoe Quinn, Anita Sarkeesian, Brianna Wu, and others, and her personal experiences with sexism, Poland develops a compelling method of combating sexism online.

The advent of internet of things (IoT) has influenced and revolutionized the information systems and computing technologies. A computing concept where physical objects used in daily life, will identify themselves by getting connected to the internet is called IoT. Physical objects embedded with electronic, radio-frequency identification, software, sensors, actuators and smart objects converge with the internet to accumulate and share data in IoT. IoT is expected to bring in extreme changes and solutions to most of the daily problems in the real world. Thus, IoT provides connectivity for everyone and everything at any time. The IoT embeds some intelligence in Internet connected objects to communicate, exchange information, take decisions, invoke actions and provide amazing services. It has an imperative economic and societal impact for the future construction of information, network, and communication technology. In the upcoming years, the IoT is expected to bridge various technologies to enable new applications by connecting physical objects together to support the intelligent decision making. As the most cost-effective and performant source of positioning and timing information in outdoor environments, the global navigation satellite systems(GNSS) has become an essential element of major contemporary technology developments notably including the IoT, Big Data, Smart Cities and Multimodal Logistics. By 2020, there will be more than 20 billion interconnected IoT devices, and its market size may reach $1.5 trillion. Projections for the impact of IoT on the Internet and economy are impressive, with some anticipating as many as 100 billion connected IoT devices and a global economic impact of more than $11 trillion by 2025. Regulators can play a role in encouraging the

development and adoption of the IoT, by preventing abuse of market dominance, protecting users and protecting Internet networks while promoting efficient markets and the public interest. Regulators can consider and identify some measures to foster development of the IoT. Encourage development of LTE?A and 5G wireless networks, and keep need for IoT?specific spectrum under review. Universal IPv6 adoption by governments in their own services and procurements, and other incentives for private sector adoption. Increasing interoperability through competition law and give users a right to easy access to personal data. Support global standardization and deployment of remotely provisioned SIMs for greater machine to machine competition. Particular attention will be needed from regulators to IoT privacy and security issues, which are key to encouraging public trust in and adoption of the technology. This paper focuses specifically on the essential technologies that enable the implementation of IoT and the general layered architecture of IoT, the market of IoT and GNSS technologies and their impact of the world economy, application domain of IoT and finally the Policy and regulatory implications and best practices.

With the threats that affect every computer, phone or other device connected to the internet, security has become a responsibility not just for law enforcement authorities or business leaders, but for every individual. Your family, information, property, and business must be protected from cybercriminals in the office, at home, on travel, and in the cloud. Understanding Security Issues provides a solid understanding of the threats, and focuses on useful tips and practices for protecting yourself, all the time, everywhere and anywhere you go. This book discusses security awareness issues and how you can take steps to reduce the risk of becoming a victim: The threats that face every individual and business, all the time. Specific indicators of threats so that you understand when you might be attacked and what to do if they occur. The security mindset and good security practices. Assets that need to be protected at work and at home. Protecting yourself and your business at work. Protecting yourself and your family at home. Protecting yourself and your assets on travel.

This book constitutes the refereed proceedings of the 17th International Conference on Mobile Web and Intelligent Information Systems, MobiWIS 2021, held as a virtual event, in August 2021. The 15 full papers presented in this book were carefully reviewed and selected from 40 submissions. The papers of MobiWIS 2021 deal focus on topics such as security and privacy; web and mobile applications; networking and communication; intelligent information systems; and IoT and ubiquitous computing.

Hackers, cyber-criminals, Dark Web users, and techno-terrorists beware! This book should make you think twice about attempting to do your dirty work in the smart cities of tomorrow. Scores of cities around the world have begun planning what are known as “smart cities.” These new or revamped urban areas use the latest technology to make the lives of residents easier and more enjoyable.They will have automated infrastructures such as the Internet of Things, “the Cloud,” automated industrial controls, electronic money, mobile and communication satellite systems, wireless texting and networking. With all of these benefits come new forms of danger, and so these cities will need many safeguards to prevent cyber criminals from wreaking havoc. This book explains the advantages of smart cities and how to design and operate one. Based on the practical experience of the authors in projects in the U.S. and overseas in Dubai, Malaysia, Brazil and India, it tells how such a city is planned and analyzes vital security concerns that must be addressed along the way. Most of us will eventually live in smart cities. What are the advantages and the latest design strategies for such ventures? What are the potential drawbacks? How will they change the lives of everyday citizens? This book offers a preview of our future and how you can help prepare yourself for the changes to come.

An investigation of how-to guides for sensor technologies Sensors are increasingly common within citizen-sensing and DIY projects, but these devices often require the use of a how-to guide. From online instructional videos for troubleshooting sensor installations to handbooks for using and abusing the Internet of Things, the how-to genres and formats of digital instruction continue to expand and develop. As the how-to proliferates, and instructions unfold through multiple aspects of technoscientific practices, Jennifer Gabrys asks why the how-to has become one of the prevailing genres of the digital. How to Do Things with Sensors explores the ways in which things are made do-able with and through sensors and further considers how worlds are made sense-able and actionable through the instructional mode of citizen-sensing projects. Forerunners: Ideas First Short books of thought-in-process scholarship, where intense analysis, questioning, and speculation take the lead

Child Sexual Abuse: Forensic Issues in Evidence, Impact, and Management approaches the issue of child sexual abuse from several viewpoints. First, child abuse will be considered from both victimization and offending perspectives and, although empirical scholarship will inform much of the content, there will be applied material from experts and practitioners in the field - from policing to child safety to intelligence. This is a significant divergence from literature most commonly provided in the market. Additionally, contemporary scholarship on issues surrounding child abuse includes (but is not limited to) typologies (such as psychological, sexual and physical abuse, and neglect), risk and protective factors (at individual and community levels), recognition, responses, biopsychosocial outcomes (dealt with in discrete chapters), public policy, prevention, institutional abuse, children and corrections, treatment and management (including global comparisons), and myths and fallacies (e.g. outcomes for children of same-sex marriages).

The rise of intelligence and computation within technology has created an eruption of potential applications in numerous professional industries. Techniques such as data analysis, cloud computing, machine learning, and others have altered the traditional processes of various disciplines including healthcare, economics, transportation, and politics. Information technology in today’s world is beginning to uncover opportunities for experts in these fields that they are not yet aware of. The exposure of specific instances in which these devices are being implemented will assist other specialists in how to successfully utilize these transformative tools with the appropriate amount of discretion, safety, and awareness. Considering the level of diverse uses and practices throughout the globe, the fifth edition of the Encyclopedia of Information Science and Technology series continues the enduring legacy set forth by its predecessors as a premier reference that contributes the most cutting-edge concepts and methodologies to the research community. The Encyclopedia of Information Science and Technology, Fifth Edition is a three-volume set that includes 136 original and

previously unpublished research chapters that present multidisciplinary research and expert insights into new methods and processes for understanding modern technological tools and their applications as well as emerging theories and ethical controversies surrounding the field of information science. Highlighting a wide range of topics such as natural language processing, decision support systems, and electronic government, this book offers strategies for implementing smart devices and analytics into various professional disciplines. The techniques discussed in this publication are ideal for IT professionals, developers, computer scientists, practitioners, managers, policymakers, engineers, data analysts, and programmers seeking to understand the latest developments within this field and who are looking to apply new tools and policies in their practice. Additionally, academicians, researchers, and students in fields that include but are not limited to software engineering, cybersecurity, information technology, media and communications, urban planning, computer science, healthcare, economics, environmental science, data management, and political science will benefit from the extensive knowledge compiled within this publication.

This book explores the interconnected ways in which the control of knowledge has become central to the exercise of political, economic, and social power. Building on the work of International Political Economy scholar Susan Strange, this multidisciplinary volume features experts from political science, anthropology, law, criminology, women's and gender studies, and Science and Technology Studies, who consider how the control of knowledge is shaping our everyday lives. From "weaponised copyright" as a censorship tool, to the battle over control of the internet's "guts," to the effects of state surveillance at the Mexico–U.S. border, this book offers a coherent way to understand the nature of power in the twenty-first century.

This book constitutes the proceedings of the 15th International Conference on Distributed Computing and Internet Technology, ICDCIT 2019, held in Bhubaneswar, India, in January 2019. The 18 full papers and 14 short papers presented together with 5 invited papers were carefully reviewed and selected from 115 submissions. The papers present research in three areas: distributed computing, Internet technologies, and societal applications.

In recent years, the need for smart equipment has increased exponentially with the upsurge in technological advances. To work to their fullest capacity, these devices need to be able to communicate with other devices in their network to exchange information and receive instructions. Computational Intelligence in the Internet of Things is an essential reference source that provides relevant theoretical frameworks and the latest empirical research findings in the area of computational intelligence and the Internet of Things. Featuring research on topics such as data analytics, machine learning, and neural networks, this book is ideally designed for IT specialists, managers, professionals, researchers, and academicians.

Development in information and communication technologies has led to the advancement of business and enabled enterprises to produce on a global scale. Productivity is a key function in maintaining a competitive advantage in today's market. The internet of things has rapidly become prevalent in the productivity efforts of businesses. Understanding these technologies and how to implement them into current business practices is vital for researchers and practitioners. Internet of Things (IoT) Applications for Enterprise Productivity is a collection of innovative research on the advancing methods productivity efforts of business through the implementation of the internet of things. While highlighting topics including employee motivation, enterprise productivity, and supply chain tracking, this book is ideally designed for manufacturing professionals, industrialists, engineers, managers, practitioners, academicians, and students seeking current research on enterprise production systems and its transformation using internet of things technologies.

This book presents refereed proceedings of the First International Conference on Advances in Cyber Security, ACeS 2019, held in Penang, Malaysia, in July-August 2019. The 25 full papers and 1 short paper were carefully reviewed and selected from 87 submissions. The papers are organized in topical sections on internet of things, industry and blockchain, and cryptology; digital forensics and surveillance, botnet and malware, and DDoS and intrusion detection/prevention; ambient cloud and edge computing, wireless and cellular communication.

Written by all-star security experts, Practical IoT Hacking is a quick-start conceptual guide to testing and exploiting IoT systems and devices. Drawing from the real-life exploits of five highly regarded IoT security researchers, Practical IoT Hacking teaches you how to test IoT systems, devices, and protocols to mitigate risk. The book begins by walking you through common threats and a threat modeling framework. You'll develop a security testing methodology, discover the art of passive reconnaissance, and assess security on all layers of an IoT system. Next, you'll perform VLAN hopping, crack MQTT authentication, abuse UPnP, develop an mDNS poisoner, and craft WS-Discovery attacks. You'll tackle both hardware hacking and radio hacking, with in-depth coverage of attacks against embedded IoT devices and RFID systems. You'll also learn how to: • Write a DICOM service scanner as an NSE module • Hack a microcontroller through the UART and SWD interfaces • Reverse engineer firmware and analyze mobile companion apps • Develop an NFC fuzzer using Proxmark3 • Hack a smart home by jamming wireless alarms, playing back IP camera feeds, and controlling a smart treadmill The tools and devices you'll use are affordable and readily available, so you can easily practice what you learn. Whether you're a security researcher, IT team member, or hacking hobbyist, you'll find Practical IoT Hacking indispensable in your efforts to hack all the things REQUIREMENTS: Basic knowledge of Linux command line, TCP/IP, and programming

Addiction is a powerful and destructive condition impacting large portions of the population around the world. Addiction takes many forms and has the potential to impact individuals of all ages, socio-economic statuses, and ethnic backgrounds. Substance Abuse and Addiction: Breakthroughs in Research and Practice is an authoritative resource that comprehensively examines the prevalence, assessment, causes, and impacts of substance abuse and addiction from cultural, legal, psychosocial, theoretical, and medical viewpoints. Highlighting a range of pertinent topics such as technological addictions, drug treatment, and addictive behaviors, this publication is an ideal reference source for psychologists, researchers, mental health professionals, clinicians, academicians, and graduate-level students seeking current research on the prevention, assessment, and rehabilitation of substance abuse and addiction.