Abusing The Internet Of Things: Blackouts, Freakouts, And Stakeouts

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

"The beauty of this important book lies in its conclusion... This book provides the roadmap that has led us to our current dilemmas and offers the path forward to a truly just society for all." -Terry Fulmer, PhD, RN, FAAN, President of The John A. Hartford Foundation Delivering the first comprehensive analysis of elder justice and its implications for policy and practice, this book offers a promising approach that ensures the rights, safety, and security of all older Americans. It explains the antecedents of elder justice in the fields of elder abuse, aging, and public health, and describes the opportunities for achieving more comprehensive, cohesive, and integrated public policy. The text examines the cumulative impact of ageism, racism, sexism, heterosexism, class, and other forms of disadvantage and isolation on the lives of older adults and how these contribute to poverty, disease, disability, abuse, and neglect. It draws from the fields of public health and health equity, and plans devised by international organizations that frame elder abuse as a human rights issue. Practical and achievable goals in the prevention of elder abuse aid policy makers, program developers, grant-makers, and service providers in the fields of gerontology, social work, public health, and nursing in their efforts towards elder abuse prevention. Key Features: Identifies institutionalized ageism in public policy and practice Proposes core principles of elder justice to guide policy and service development Introduces knowledge and techniques from the fields of elder abuse and public health Provides greater understanding of social determinants and how they are addressed in the public health arena Offers techniques for improving access to the legal system for people with physical, cognitive, and communication disabilities Offers practical and achievable goals; objectives and recommendations; and models for state, national, and international policy and programs.

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.

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.

Architectures, Protocols and Standards

17th International Conference, MobiWIS 2021, Virtual Event, August 23–25, 2021, Proceedings

Mobile Web and Intelligent Information Systems

A Practical Guide to Hacking the Internet of Things

Using it Without Abusing it

How Smart TVs, Smart Cars, Smart Homes, and Smart Cities are Changing the World

Forensic Issues in Evidence, Impact, and Management

The definitive guide to hacking the world of the Internet of Things (IoT) -- Internet connected devices such as medical devices, home assistants, smart home appliances and more. 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

The old Internet typically connected personal computers. But a radically new Internet is emerging. Some call it an "Internet of Things" (IoT) or "Internet of Everything" (IoE). The IoT won't just connect people: it'll connect "smart" homes, appliances, cars, aircraft (a.k.a. drones)… offices, factories, cities… the world. By some estimates, the IoE will explode into a $19 trillion market in just a few years. If that happens… when that happens… it will transform your life. ¿ You need to know what's coming. But, until now, most guides to the Internet of Everything have been written for technical experts. Now, the world's #1 author of beginning technology books has written the perfect introduction for every consumer and citizen. In The Internet of Things, Michael Miller reveals how a new generation of autonomously connected smart devices is emerging, and how it will enable people and devices to do more things, more intelligently, and more rapidly. ¿ Miller demystifies every type of smart device, both current and future. Each chapter ends with a special "...and You" section, offering up-to-the-minute advice for using today's IoE technologies or preparing for tomorrow's. ¿ You'll also discover the potential downsides and risks associated with intelligent, automatic interaction. When all your devices can communicate with each other (and with the companies that sell and monitor them), how private is your private life? Do the benefits outweigh the risks? And what does a connected world do when the connections suddenly go down? Packed with scenarios and insider interviews,The Internet of Things makes our future utterly, vividly real.

This book presents refereed proceedings of the Third International Conference on Advances in Cyber Security, ACeS 2021, held in Penang, Malaysia, in August 2021. The 36 full papers were carefully reviewed and selected from 92 submissions. The papers are organized in the following topical sections: Internet of Things, Industry 4.0 and Blockchain, and Cryptology; Digital Forensics and Surveillance, Botnet and Malware, DDoS, and Intrusion Detection/Prevention; Ambient Cloud and Edge Computing, SDN, Wireless and Cellular Communication; Governance, Social Media, Mobile and Web, Data Privacy, Data Policy and Fake News.

There is great confusion about what the Internet of Things means. This book lays out a technological future based on the intersection of evolutionary psychology, shared functionality desires, and a long-term vision of human society. Broken into three themes of Prediction, Interface, and Evolution, it's an attempt to show what's coming so that we can start getting ready. Regardless of what forms it may take during gestation, this book describes what the Real Internet of Things will inevitably become.

Big Data and The Internet of Things

Digital Forensics and Internet of Things

Getting Started with the Internet of Things

Blackouts, Freakouts, and Stakeouts

Enterprise Information Architecture for A New Age

Practical Internet of Things Security

The Smart Wife

What is the Internet of Things? It's billions of embedded computers, sensors, and actuators all connected online. If you have basic programming skills, you can use these powerful little devices to create a variety of useful systems—such as a device that waters plants when the soil becomes dry. This hands-on guide shows you how to start building your own fun and fascinating projects. Learn to program embedded devices using the .NET Micro Framework and the Netduino Plus board. Then connect your devices to the Internet with Pachube, a cloud platform for sharing real-time sensor data. All you need is a Netduino Plus, a USB cable, a couple of sensors, an Ethernet connection to the Internet—and your imagination. Develop programs with simple outputs (actuators) and inputs (sensors) Learn about the Internet of Things and the Web of Things Build client programs that push sensor readings from a device to a web service Create server programs that allow you to control a device over the Web Get the .NET classes and methods needed to implement all of the book's examples

IOT AND WIRELESS SENSOR NETWORKS WRITTEN BY Dr. Durga Bhavani Dasari, Dr.MD.Javeed Ahammed, Dr.Sushma Jaiswal, Mr.V.Kamalkumar

Gain a strong foundation of Arduino-based device development, from which you can go in any direction according to your specific development needs and desires. You'll build Arduino-powered devices for everyday use, and then connect those devices to the Internet. You'll be introduced to the building blocks of IoT, and then deploy those principles to by building a variety of useful projects. Projects in the books gradually introduce the reader to key topics such as internet connectivity with Arduino, common IoT protocols, custom web visualization, and Android apps that receive sensor data on-demand and in realtime. IoT device enthusiasts of all ages will want this book by their side when developing Android-based devices. If you're one of the many who have decided to build your own Arduino-powered devices for IoT applications, then Building Arduino Projects for the Internet of Things is exactly what you need. This book is your single resource--a guidebook for the eager-to-learn Arduino enthusiast--that teaches logically, methodically, and practically how the Arduino works and what you can build with it. Written by a software developer and solution architect who got tired of hunting and gathering various lessons for Arduino development as he taught himself all about the topic. For Arduino enthusiasts, this book not only opens up the world of IoT applications, you will also learn many techniques that likely would not be obvious if not for experience with such a diverse group of applications What You'll Learn Create an Arduino circuit that senses temperature Publish data collected from an Arduino to a server and to an MQTT broker Set up channels in Xively Using Node-RED to define complex flows Publish data visualization in a web app Report motion-sensor data through a mobile app Create a remote control for house lights Set up an app in IBM Bluematrix Who This Book Is For IoT device enthusiasts of all ages will want this book by their side when developing Android-based devices.

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).

Why Siri, Alexa, and Other Smart Home Devices Need a Feminist Reboot

Understanding Power Structures in the 21st Century

Impact and Challenges

A practitioner's guide to securing connected industries

Third International Conference, ACeS 2021, Penang, Malaysia, August 24–25, 2021, Revised Selected Papers

Abusing the Internet of Things

Internet of Things

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.

A guided tour through the Internet of Things, a networked world of connected devices, objects, and people that is changing the way we live and work. We turn on the lights in our house from a desk in an office miles away. Our refrigerator alerts us to buy milk on the way home. A package of cookies on the supermarket shelf suggests that we buy it, based on past purchases. The cookies themselves are on the shelf because of a "smart" supply chain. When we get home, the thermostat has already adjusted the temperature so that it's toasty or bracing, whichever we prefer. This is the Internet of Things—a networked world of connected devices, objects, and people. In this book, Samuel Greengard offers a guided tour through this emerging world and how it will change the way we live and work. Greengard explains that the Internet of Things (IoT) is still in its early stages. Smart phones, cloud computing, RFID (radio-frequency identification) technology, sensors, and miniaturization are converging to make possible a new generation of embedded and immersive technology. Greengard traces the origins of the IoT from the early days of personal computers and the Internet and examines how it creates the conceptual and practical framework for a connected world. He explores the industrial Internet and machine-to-machine communication, the basis for smart manufacturing and end-to-end supply chain visibility; the growing array of smart consumer devices and services—from Fitbit fitness wristbands to mobile apps for banking; the practical and technical challenges of building the IoT; and the risks of a connected world, including a widening digital divide and threats to privacy and security. Finally, he considers the long-term impact of the IoT on society, narrating an eye-opening "Day in the Life" of IoT connections circa 2025.

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.

Apress is proud to announce that Rethinking the Internet of Things was a 2014 Jolt Award Finalist, the highest honor for a programming book. And the amazing part is that there is no code in the book. Over the next decade, most devices connected to the Internet will not be used by people in the familiar way that personal computers, tablets and smart phones are. Billions of interconnected devices will be monitoring the environment, transportation systems, factories, farms, forests, utilities, soil and weather conditions, oceans and resources. Many of these sensors and actuators will be networked into autonomous sets, with much of the information being exchanged machine-to-machine directly and without human involvement. Machine-to-machine communications are typically terse. Most sensors and actuators will report or act upon small pieces of information - "chirps". Burdening these devices with current network protocol stacks is inefficient, unnecessary and unduly increases their cost of ownership. This must change. The architecture of the Internet of Things must evolve now by incorporating simpler protocols toward at the edges of the network, or remain forever inefficient. Rethinking the Internet of Things describes reasons why we must rethink current approaches to the Internet of Things. Appropriate architectures that will coexist with existing networking protocols are described in detail. An architecture comprised of integrator functions, propagator nodes, and end devices, along with their interactions, is explored.

Internet of Things for Architects

Internet of Things (IoT) Applications for Enterprise Productivity

Hidden Dangers of the Internet

Internet of Things (IoT)

Experiments with Real-World Applications

Internet of Things (IoT) and Related Abuses, New Ways of Working, Teleworking, Tele-learning, Unpaid Care and Housework, Women in Leadership and Decision-making Process

Proceedings of 8th Computer Science On-line Conference 2019, Vol. 3

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.
Connect your organization to the Internet of Things with solid strategy and a proven implementation plan Building Internet of Things provides front-line business decision makers with a practical handbook for capitalizing on this latest transformation. Focusing on the business implications of Internet of Things (IoT), this book describes the sheer impact, spread, and opportunities arising every day, and how business leaders can implement IoT today to realize tangible business advantages. The discussion delves into IoT from a business, strategy and organizational standpoint, and includes use-cases that illustrate the ripple effect that this latest disruption brings; you'll learn how to fashion a viable IoT plan that works with your organization's strategy and direction, and how to implement that strategy successfully by integrating IoT into your organization tomorrow. For business managers, the biggest question surrounding the Internet of Things is what to do with it. This book examines the way IoT is being used today—and will be used in the future—to help you craft a robust plan for your organization. Grasp the depth and breadth of the Internet of Things Create a secure IoT recipe that aligns with your company's strategy Capitalize on advances while avoiding disruption from others Leverage the technical, organizational, and social impact of IoT In the past five years, the Internet of Things has become the new frontier of technology that has everyone talking. It seems that almost every week a major vendor announces a new IoT strategy or division; is your company missing the boat? Learn where IoT fits into your organization, and how to turn disruption into profit with the expert guidance in Building the Internet of Things.
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.

The ebook edition of this title is Open Access and freely available to read online This handbook features theoretical, empirical, policy and legal analysis of technology facilitated violence and abuse (TFVA) from over 40 multidisciplinary scholars, practitioners, advocates, survivors and technologists from 17 countries

Implement New Business Models, Disrupt Competitors, Transform Your Industry

Principles, Paradigms and Applications of IoT

The Definitive Guide to Attacking the Internet of Things

Elder Justice, Ageism, and Elder Abuse

Digital Privacy and Security Using Windows

Cybernetics and Automation Control Theory Methods in Intelligent Algorithms

Connecting Sensors and Microcontrollers to the Cloud

DIGITAL FORENSICS AND INTERNET OF THINGS It pays to be ahead of the criminal, and this book helps organizations and people to create a path to achieve this goal. The book discusses applications and challenges professionals encounter in the burgeoning field of IoT forensics. IoT forensics attempts to align its workflow to that of any forensics practice—investigators identify, interpret, preserve, analyze and present any relevant data. As with any investigation, a timeline is constructed, and, with the aid of smart devices providing data, investigators might be able to capture much more specific data points than in a traditional crime. However, collecting this data can often be a challenge, as it frequently doesn't live on the device itself, but rather in the provider's cloud platform. If you can get the data off the device, you'll have to employ one of a variety of methods given the diverse nature of IoT devices hardware, software, and firmware. So, while robust and insightful data is available, acquiring it is no small undertaking. Digital Forensics and Internet of Things encompasses: State-of-the-art research and standards concerning IoT forensics and traditional digital forensics Compares and contrasts IoT forensic techniques with those of traditional digital forensics standards Identifies the driving factors of the slow maturation of IoT forensic standards and possible solutions Applies recommended standards gathered from IoT forensic literature in hands-on experiments to test their effectiveness across multiple IoT devices Provides educated recommendations on developing and establishing IoT forensic standards, research, and areas that merit further study. Audience Researchers and scientists in forensic sciences, computer sciences, electronics engineering, embedded systems, information technology.

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.

Take a practioner’s approach in analyzing the Internet of Things (IoT) devices and the security issues facing an IoT architecture. You’ll review the architecture's central components, from hardware communication interfaces, such as UARTand SPI, to radio protocols, such as BLE or ZigBee. You'll also learn to assess a device physically by opening it, looking at the PCB, and identifying the chipsets and interfaces. You'll then use that information to gain entry to the device or to perform other actions, such as dumping encryption keys and firmware. As the IoT rises to one of the most popular tech trends, manufactures need to take necessary steps to secure devices and protect them from attackers. The IoT Hacker's Handbook breaks down the Internet of Things, exploits it, and reveals how these devices can be built securely. What You’ll LearnPerform a threat model of a real-world IoT device and locate all possible attacker entry points Use reverse engineering of firmware binaries to identify security issues Analyze,assess, and identify security issues in exploited ARM and MIPS based binariesSniff, capture, and exploit radio communication protocols, such as Bluetooth Low Energy (BLE), and ZigBee Who This Book is For Those interested in learning about IoT security, such as pentesters working in different domains, embedded device developers, or IT people wanting to move to an Internet of Things security role.

Enterprise Information Architecture for a New Age: Big Data and The Internet of Things, provides guidance in designing an information architecture to accommodate increasingly large amounts of data, massively large amounts of data, not only from traditional sources, but also from novel sources such everyday objects that are fast becoming wired into global Internet. No business can afford to be caught out by missing the value to be mined from the increasingly large amounts of available data generated by everyday devices. The text provides background as to how analytical solutions and enterprise architecture methodologies and concepts have evolved (including the roles of data warehouses, business intelligence tools, predictive analytics, data discovery, Big Data, and the impact of the Internet of Things). Then you’re taken through a series of steps by which to define a future state architecture and create a plan for how to reach that future state. Enterprise Information Architecture for a New Age: Big Data and The Internet of Things helps you gain an understanding of the following: Implications of Big Data from a variety of new data sources (including data from sensors that are part of the Internet of Things) upon an information architecture How establishing a vision for data usage by defining a roadmap that aligns IT with line-of-business needs is a key early step The importance and details of taking a step-by-step approach when dealing with shifting business challenges and

changing technology capabilities How to mitigate risk when evaluating existing infrastructure and designing and deploying new infrastructure Enterprise Information Architecture for a New Age: Big Data and The Internet of Things combines practical advice with technical considerations. Author Robert Stackowiak and his team are recognized worldwide for their expertise in large data solutions, including analytics. Don't miss your chance to read this book and gain the benefit of their advice as you look forward in thinking through your own choices and designing your own architecture to accommodate the burgeoning explosion in data that can be analyzed and converted into valuable information to drive your business forward toward success.

What Everyone Needs to Know®

Information, Technology and Control in a Changing World

White-Collar Crime Online

Research Anthology on Big Data Analytics, Architectures, and Applications

A Scalable Approach to Connecting Everything

Advances in Cyber Security

What Organisations and Institutions Need to Do

The Internet of Things (IoT) is the notion that nearly everything we use, from gym shorts to streetlights, will soon be connected to the Internet; the Internet of Everything (IoE) encompasses not just objects, but the social connections, data, and processes that the IoT makes possible. Industry and financial analysts have predicted that the number of Internet-enabled devices will increase from 11 billion to upwards of 75 billion by 2020. Regardless of the number, the end result looks to be a mind-boggling explosion in Internet connected stuff. Yet, there has been relatively little attention paid to how we should go about regulating smart devices, and still less about how cybersecurity should be enhanced. Similarly, now that everything from refrigerators to stock exchanges can be connected to a ubiquitous Internet, how can we better safeguard privacy across networks and borders? Will security scale along with this increasingly crowded field? Or, will a combination of perverse incentives, increasing complexity, and new problems derail progress and exacerbate cyber insecurity? For all the press that such questions have received, the Internet of Everything remains a topic little understood or appreciated by the public. This volume demystifies our increasingly "smart" world, and unpacks many of the outstanding security, privacy, ethical, and policy challenges and opportunities represented by the IoE. Scott J. Shackelford provides real-world examples and straightforward discussion about how the IoE is impacting our lives, companies, and nations, and explain how it is increasingly shaping the international community in the twenty-first century. Are there any downsides of your phone being able to unlock your front door, start your car, and control your thermostat? Is your smart speaker always listening? How are other countries dealing with these issues? This book answers these questions, and more, along with offering practical guidance for how you can join the effort to help build an Internet of Everything that is as secure, private, efficient, and fun as possible.

An Industrial IoT Approach for Pharmaceutical Industry Growth, Volume Two uses an innovative approach to explore how the Internet of Things (IoT) and big data can improve approaches and make discoveries. Rapid growth of the IoT has encouraged many companies in the manufacturing sector to make use of this technology to unlock its potential. Using clear language and real-world case studies, this book discusses systems level from both a human-factors point-of-view and the perspective of networking, databases, privacy and anti-spoofing.

The wide variety in topics presented offers multiple perspectives on how to integrate the Internet of Things into pharmaceutical manufacturing. This book represents a useful resource for researchers in pharmaceutical sciences, information and communication technologies, and those who specialize in healthcare and pharmacovigilance. Emphasizes efficiency in pharmaceutical manufacturing through an IoT/Big Data approach Explores cutting-edge technologies through sensor enabled environments in the pharmaceutical industry Discusses system levels from both a human-factors point-of-view and the perspective of networking, databases, privacy and anti-spoofing

A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world About This Book Learn to design and implement cyber security strategies for your organization Learn to protect cyber-physical systems and utilize forensic data analysis to beat vulnerabilities in your IoT ecosystem Learn best practices to secure your data from device to the cloud Gain insight into privacy-enhancing techniques and technologies Who This Book Is For This book targets IT Security Professionals and Security Engineers (including pentesters, security architects and ethical hackers) who would like to ensure security of their organization's data when connected through the IoT. Business analysts and managers will also find it useful. What You Will Learn Learn how to break down cross-industry barriers by adopting the best practices for IoT deployments Build a rock-solid security program for IoT that is cost-effective and easy to maintain Demystify complex topics such as cryptography, privacy, and penetration testing to improve your security posture See how the selection of individual components can affect the security posture of the entire system Use Systems Security Engineering and Privacy-by-design principles to design a secure IoT ecosystem Get to know how to leverage the burdgening cloud-based systems that will support the IoT into the future. In Detail With the advent of Intenret of Things (IoT), businesses will be faced with defending against new types of threats. The business ecosystem now includes cloud computing infrastructure, mobile and fixed endpoints that open up new attack surfaces, a desire to share information with many stakeholders and a need to take action quickly based on large quantities of collected data. . It therefore becomes critical to ensure that cyber security threats are contained to a minimum when implementing new IoT services and solutions. . The interconnectivity of people, devices, and companies raises stakes to a new level as computing and action become even more mobile, everything becomes connected to the cloud, and infrastructure is strained to securely manage the billions of devices that will connect us all to the IoT. This book shows you how to implement cyber-security solutions, IoT design best practices and risk mitigation methodologies to address device and infrastructure threats to IoT solutions. This book will take readers on a journey that begins with understanding the IoT and how it can be applied in various industries, goes on to describe the security challenges associated with the IoT, and then provides a set of guidelines to architect and deploy a secure IoT in your Enterprise. The book will showcase how the IoT is implemented in early-adopting industries and describe how lessons can be learned and shared across diverse industries to support a secure IoT. Style and approach This book aims to educate readers on key areas in IoT security. It walks readers through engaging with security challenges and then provides answers on how to successfully manage IoT security and build a safe infrastructure for smart devices. After reading this book, you will understand the true potential of tools and solutions in order to build real-time security intelligence on IoT networks.

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

Computational Intelligence in the Internet of Things

First International Conference, ACeS 2019, Penang, Malaysia, July 30 – August 1, 2019, Revised Selected Papers

Practical Industrial Internet of Things Security

Practical IoT Hacking

The Emerald International Handbook of Technology-Facilitated Violence and Abuse

Rethinking the Internet of Things

Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security

This book addresses researchers and graduate students at the forefront of study/research on the Internet of Things (IoT) by presenting state-of-the-art research together with the current and future challenges in building new smart applications (e.g., Smart Cities, Smart Buildings, and Industrial IoT) in an efficient, scalable, and sustainable way. It covers the main pillars of the IoT world (Connectivity, Interoperability, Discoverability, and Security/Privacy), providing a comprehensive look at the current technologies, procedures, and architectures.

The high profile reporting of child sexual abuse carried out by Jimmy Savile over decades has had far reaching-consequences, raising public awareness and concern, yet we continue to uncover new cases of institutional abuse which have been taking place under the radar for years. This book distils the learning from 80+ public inquiries relating to Savile as well as related cases of institutional abuse and analyses the key findings. It examines what we now know about offending within organisations and institutions, and how organisational failures can enable abusers. Each chapter also outlines solutions, offering perspectives for individuals and organisations on what practical action they can take to minimise risk in the settings in which they work. The book includes chapters specifically dedicated to the NHS, sports organisations and schools, and is necessary reading for professionals with responsibility for safeguarding in any

setting.

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.

A Systematic Approach to Learn the Principles, Paradigms and Applications of Internet of Things DESCRIPTION In this book, Principles, Paradigm frameworks, and Applications of IoT (Internet of Things) in the modern era are presented. It also provides a sound understanding of the IoT concepts, architecture, and applications, and improves the awareness of readers about IoT technologies and application areas. A key objective of this book is to provide a systematic source of reference for all aspects of IoT. This book comprises nine chapters with close co-operation and contributions from four different authors, spanning across four countries and providing a global, broad perspective on major topics on the Internet of Things. KEY FEATURES - IoT applications in various sectors like Education, Smart City, Politics, Healthcare, Agriculture, etc. - Adoption of the IoT technology and strategies for various sectors - To present case studies and innovative applications of the IoT - To analyze and present the state of the art of the IoT and related technologies and methodologies - To propose new models, practical solutions and technological advances of the IoT WHAT WILL YOU LEARN - Become aware of the IoT components, their connectivity to form the IoT altogether, and future possibilities with IoT. - Understand how the various components of cloud computing work together to form the basic architecture of cloud computing. - Examine the relationship between the various layers in the IoT architecture. - Understand the programming framework for the Internet of Things (IoT) and various programming paradigms. WHO THIS BOOK IS FOR This book is intended for professionals, researchers, instructors, and designers of a smart system, who will benefit from reading this book. TABLE OF CONTENTS 1. IoT Introduction 2. IoT Architectures and Protocols 3. Programming Framework for IoT 4. Virtualization and IoT 5. Security, Privacy and Challenges in IoT 6. IoT Applications Areas 7. IoT and Cloud 8. Smart City Using IoT integration 9. Case Studies 10. Important Key Terms 11. References

Child Sexual Abuse

Building Arduino Projects for the Internet of Things
The Real Internet of Things
Deviance, Organizational Behaviour and Risk
IOT AND WIRELESS SENSOR NETWORKS
Protecting Children and Adults from Abuse After Savile
Volume 2

On the International Women's Day, let us recall the context in which the current event is taking place. Just about a year ago, the World Health Organisation proclaimed the COVID 19 as the global pandemics. In the scope of several weeks, it has affected all the countries in the world and persists until this day, in spite of the existence of vaccines. Hence, further societal developments are uncertain and more changes within it are to be expected. In the sections below, the Policy Department tries to address the selected sectors of society affecting women and girls by changes resulting from the effects of the COVID 19 pandemics.

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

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.

Take your idea from concept to production with this unique guide Whether it's called physical computing, ubiquitous computing, or the Internet of Things, it's a hot topic in technology: how to channel your inner Steve Jobs and successfully combine hardware, embedded software, web services, electronics, and cool design to create cutting-edge devices that are fun, interactive, and practical. If you'd like to create the next must-have product, this unique book is the perfect place to start. Both a creative and practical primer, it explores the platforms you can use to develop hardware or software, discusses design concepts that will make your products eye-catching and appealing, and shows you ways to scale up from a single prototype to mass production. Helps software engineers, web designers, product designers, and electronics engineers start designing products using the Internet-of-Things approach Explains how to combine sensors, servos, robotics, Arduino chips, and more with various networks or the Internet, to create interactive, cutting-edge devices Provides an overview of the necessary steps to take your idea from concept through production If you'd like to design for the future, Designing the Internet of Things is a great place to start.

Encyclopedia of Information Science and Technology, Fifth Edition

Designing the Internet of Things

The IoT Hacker's Handbook

Building the Internet of Things

An Industrial IoT Approach for Pharmaceutical Industry Growth

Women's Rights and Well-being in a Post-Covid World

A Practical Guide

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.

Learn to design, implement and secure your IoT infrastructure Key Features Build a complete IoT system that is the best fit for your organization Learn about different concepts, technologies, and tradeoffs in the IoT architectural stack Understand the theory, concepts, and implementation of each element that comprises IoT design—from sensors to the cloud Implement best practices to ensure the reliability, scalability, robust communication systems, security, and data analysis in your IoT infrastructure Book Description The Internet of Things (IoT) is the fastest growing technology market. Industries are embracing IoT technologies to improve operational expenses, product life, and people's well-being. An architectural guide is necessary if you want to traverse the spectrum of technologies needed to build a successful IoT system, whether that's a single

device or millions of devices. This book encompasses the entire spectrum of IoT solutions, from sensors to the cloud. We start by examining modern sensor systems and focus on their power and functionality. After that, we dive deep into communication theory, paying close attention to near-range PAN, including the new Bluetooth ® 5.0 specification and mesh networks. Then, we explore IP-based communication in LAN and WAN, including 802.11ah, 5G LTE cellular, SigFox, and LoRaWAN. Next, we cover edge routing and gateways and their role in fog computing, as well as the messaging protocols of MQTT and CoAP. With the data now in internet form, you'll get an understanding of cloud and fog architectures, including the OpenFog standards. We wrap up the analytics portion of the book with the application of statistical analysis, complex event processing, and deep learning models. Finally, we conclude by providing a holistic view of the IoT security stack and the anatomical details of IoT exploits while countering them with software defined perimeters and blockchains. What you will learn Understand the role and scope of architecting a successful IoT deployment, from sensors to the cloud Scan the landscape of IoT technologies that span everything from sensors to the cloud and everything in between See the trade-offs in choices of protocols and communications in IoT deployments Build a repertoire of skills and the vernacular necessary to work in the IoT space Broaden your skills in multiple engineering domains necessary for the IoT architect Who this book is for This book is for architects, system designers, technologists, and technology managers who want to understand the IoT ecosphere, various technologies, and tradeoffs and develop a 50,000-foot view of IoT architecture.

Skillfully navigate through the complex realm of implementing scalable, trustworthy industrial systems and architectures in a hyper-connected business world. Key Features Gain practical insight into security concepts in the Industrial Internet of Things (IIoT) architecture Demystify complex topics such as cryptography and blockchain Comprehensive references to industry standards and security frameworks when developing IIoT blueprints Book Description Securing connected industries and autonomous systems is a top concern for the Industrial Internet of Things (IIoT) community. Unlike cybersecurity, cyber-physical security is an intricate discipline that directly ties to system reliability as well as human and environmental safety. Practical Industrial Internet of Things Security enables you to develop a comprehensive understanding of the entire spectrum of securing connected industries, from the edge to the cloud. This book establishes the foundational concepts and tenets of IIoT security by presenting real-world case studies, threat models, and reference architectures. You'll work with practical tools to design risk-based security controls for industrial use cases and gain practical know-how on the multi-layered defense techniques including Identity and Access Management (IAM), endpoint security, and communication infrastructure. Stakeholders, including developers, architects, and business leaders, can gain practical insights in securing IIoT lifecycle processes,

standardization, governance and assess the applicability of emerging technologies, such as blockchain, Artificial Intelligence, and Machine Learning, to design and implement resilient connected systems and harness significant industrial opportunities. What you will learn Understand the crucial concepts of a multi-layered IIoT security framework Gain insight on securing identity, access, and configuration management for large-scale IIoT deployments Secure your machine-to-machine (M2M) and machine-to-cloud (M2C) connectivity Build a concrete security program for your IIoT deployment Explore techniques from case studies on industrial IoT threat modeling and mitigation approaches Learn risk management and mitigation planning Who this book is for Practical Industrial Internet of Things Security is for the IIoT community, which includes IIoT researchers, security professionals, architects, developers, and business stakeholders. Anyone who needs to have a comprehensive understanding of the unique safety and security challenges of connected industries and practical methodologies to secure industrial assets will find this book immensely helpful. This book is uniquely designed to benefit professionals from both IT and industrial operations backgrounds.

The Internet of Things