Programming And Cloning Automotive Transponder Equipped

This Bosch Bible fully explains the theory, troubleshooting, and service of all Bosch systems from D-Jetronic through the latest Motronics. Includes high-performance tuning secrets and information on the newest KE- and LH-Motronic systems not available from any other source.

This book provides an insight into the 'hot' field of Radio Frequency Identification (RFID) Systems In this book, the authors provide an insight into the field of RFID systems with an emphasis on networking aspects and research challenges related to passive Ultra High Frequency (UHF) RFID systems. The book reviews various algorithms, protocols and design solutions that have been developed within the area, including most recent advances. In addition, authors cover a wide range of recognized problems in RFID industry, striking a balance between theoretical and practical coverage. Limitations of the technology and state-of-the-art solutions are identified and new research opportunities are addressed. Finally, the book is authored by experts and respected researchers in the field and every chapter is peer reviewed. Key Features: Provides the most comprehensive analysis of networking aspects of RFID systems, including tag identification protocols and reader anti-collision algorithms Covers in detail major research problems of passive UHF systems such as improving reading accuracy, reading range and throughput Analyzes other "hot topics" including localization of passive RFID tags, energy harvesting, simulator and emulator design, security and privacy Discusses design of tag antennas, tag and reader circuits for passive UHF RFID systems Presents EPCGlobal architecture framework, middleware and protocols Includes an accompanying website with PowerPoint slides and solutions to the problems http://www.site.uottawa.ca/~mbolic/RFIDBook/ This book will be an invaluable guide for researchers and graduate students in electrical engineering and computer science, and researchers and developers in telecommunication industry.

This book describes the evolving CBRN risk landscape and highlights advances in the “core” CBRN technologies, including when combined with (improvised) explosive devices (CBRNe threats). It analyses how associated technologies create new safety and security risks, challenging certain assumptions that underlie current control regimes. The book also shows how technologies can be enablers for more effective strategies to mitigate these risks. 21st-century safety and security risks emanating from chemical, biological, radiological and nuclear materials – whether resulting from natural events, accidents or malevolent use - are increasingly shaped by technologies that enable their development, production or use in ways that differ from the past. Artificial intelligence, the use of cyberspace, the revolution in the life sciences, new manufacturing methods, new platforms and equipment for agent delivery, hypersonic weapons systems, information tools utilised in hybrid warfare – these and other technologies are reshaping the global security environment and CBRN landscape. They are leading to a growing potential for highly targeted violence, and they can lead to greater instability and vulnerability worldwide. At the same time, technology offers solutions to manage CBRN risks. Examples are faster detection, more accurate characterisation of the nature and origin of CBRN agents, new forensic investigation methods, or new medical treatments for victims of CBRN incidents. New educational concepts help to foster a culture of responsibility in science and technology and strengthen governance. New training methods help develop practical skills to manage CBRN risks more effectively. The book concludes that there is a growing need for a holistic framework towards CBRN risk mitigation. Traditional arms control mechanisms such as global, regional or bilateral treaties and export controls are still needed, as they provide a necessary legal and institutional framework. But laws and technology denial alone will not suffice, and institutional mechanisms can at times be weak. Given the pace of technological progress and the diffusion of critical knowledge, tools and materials, policymakers must accept that CBRN risks cannot be eliminated altogether. Instead, society has to learn to manage these risks and develop resilience against them. This requires a “softer”, broadly based multi-stakeholder approach involving governments, industry, the research and development communities, educators, and civil society. Furthermore, educating policymakers that cutting-edge technologies may seriously affect global strategic stability could create incentives for developing a more creative and contemporary arms control strategy that fosters cooperation rather than incremental polarisation.

This edition of Parker's California Business & Professions Code is from our Parker's California Code Business Series and is a convenient desktop reference containing the California code and regulations you use most in your business practice. This single volume contains the complete primary law plus annotations and other features to help you find what you need quickly and expand your research.

Most innovations in the car industry are based on software and electronics, and IT will soon constitute the major production cost factor. It seems almost certain that embedded IT security will be crucial for the next generation of applications. Yet whereas software safety has become a relatively well-established field, the protection of automotive IT systems against manipulation or intrusion has only recently started to emerge. Lemke, Paar, and Wolf collect in this volume a state-of-the-art overview on all aspects relevant for IT security in automotive applications. After an introductory chapter written by the editors themselves, the contributions from experienced experts of different disciplines are structured into three parts. "Security in the Automotive Domain" describes applications for which IT security is crucial, like immobilizers, tachographs, and software updates. "Embedded Security Technologies" details security technologies relevant for automotive applications, e.g., symmetric and asymmetric cryptography, and wireless security. "Business Aspects of IT Systems in Cars" shows the need for embedded security in novel applications like location-based navigation systems and personalization. The first book in this area of fast-growing economic and scientific importance, it is indispensable for both researchers in software or embedded security and professionals in the automotive industry.

Modern cars are more computerized than ever. Infotainment and navigation systems, Wi-Fi, automatic software updates, and other innovations aim to make driving more convenient. But vehicle technologies haven’t kept pace with today’s more hostile security environment, leaving millions vulnerable to attack. The Car Hacker’s Handbook will give you a deeper understanding of the computer systems and embedded software in modern vehicles. It begins by examining vulnerabilities and providing detailed explanations of communications over the CAN bus and between devices and systems. Then, once you have an understanding of a vehicle’s communication network, you’ll learn how to intercept data and perform specific hacks to track vehicles, unlock doors, glitch engines, flood communication, and more. With a focus on low-cost, open source hacking tools such as Metasploit, Wireshark, Kayak, can-utils, and ChipWhisperer, The Car Hacker’s Handbook will show you how to: –Build an accurate threat model for your vehicle –Reverse engineer the CAN bus to fake engine signals –Exploit vulnerabilities in diagnostic and data-logging systems –Hack the ECU and other firmware and embedded systems –Feed exploits through infotainment and vehicle-to-vehicle communication systems –Override factory settings with performance-tuning techniques –Build physical and virtual test benches to try out exploits safely If you’re curious about automotive security and have the urge to hack a two-ton computer, make

The Car Hacker’s Handbook your first stop.

Infrastructure for Homeland Security Environments Wireless Sensor Networks helps readers discover the emerging field of low-cost standards-based sensors that promise a high order of spatial and temporal resolution and accuracy in an ever-increasing universe of applications. It shares the latest advances in science and engineering paving the way towards a large plethora of new applications in such areas as infrastructure protection and security, healthcare, energy, food safety, RFID, ZigBee, and processing. Unlike other books on wireless sensor networks that focus on limited topics in the field, this book is a broad introduction that covers all the major technology, standards, and application topics. It contains everything readers need to know to enter this burgeoning field, including current applications and promising research and development; communication and networking protocols; middleware architecture for wireless sensor networks; and security and management. The straightforward and engaging writing style of this book makes even complex concepts and processes easy to follow and understand. In addition, it offers several features that help readers grasp the material and then apply their knowledge in designing their own wireless sensor network systems: * Examples illustrate how concepts are applied to the development and application of * wireless sensor networks * Detailed case studies set forth all the steps of design and implementation needed to solve real-world problems * Chapter conclusions that serve as an excellent review by stressing the chapter's key concepts * References in each chapter guide readers to in-depth discussions of individual topics This book is ideal for networking designers and engineers who want to fully exploit this new technology and for government employees who are concerned about homeland security. With its examples, it is appropriate for use as a coursebook for upper-level undergraduates and graduate students.

Defines, and occasionally diagrams, all electronic terms and expressions in dictionary form, with a section of related tables and data

"This book presents case studies, literature reviews, ethnographies, and frameworks supporting the emerging technologies of RFID implants while also highlighting the current and predicted social implications of human-centric technologies"--Provided by publisher.

* Pro ASP.NET 2.0 Website Programming shows how to provide users and customers with ASP.NET 2.0 websites that are easy-to-use, perform well, and secure. * This book clearly explains how to handle all of the common website tasks effortlessly: including logging in, displaying important customer information, querying data, reporting. and security. * With this book, readers will learn ASP.NET 2.0 and how to apply it to solve real business problems.

This practical, tutorial-style book uses the Kali Linux distribution to teach Linux basics with a focus on how hackers would use them. Topics include Linux command line basics, filesystems, networking, BASH basics, package management, logging, and the Linux kernel and drivers. If you're getting started along the exciting path of hacking, cybersecurity, and pentesting, Linux Basics for Hackers is an excellent first step. Using Kali Linux, an advanced penetration testing distribution of Linux, you'll learn the basics of using the Linux operating system and acquire the tools and techniques you'll need to take control of a Linux environment. First, you'll learn how to install Kali on a virtual machine and get an introduction to basic Linux concepts. Next, you'll tackle broader Linux topics like manipulating text, controlling file and directory permissions, and managing user environment variables. You'll then focus in on foundational hacking concepts like security and anonymity and learn scripting skills with bash and Python. Practical tutorials and exercises throughout will reinforce and test your skills as you learn how to: - Cover your tracks by changing your network information and manipulating the rsyslog logging utility - Write a tool to scan for network connections, and connect and listen to wireless networks - Keep your internet activity stealthy using Tor, proxy servers, VPNs, and encrypted email - Write a bash script to scan open ports for potential targets - Use and abuse services like MySQL, Apache web server, and OpenSSH - Build your own hacking tools, such as a remote video spy camera and a password cracker Hacking is complex, and there is no single way in. Why not start at the beginning with Linux Basics for Hackers?

A rollicking rural yarn from the bestselling author of North Star and Morgan's Law.

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.

Within the past four decades a powerful scientific methodology has emerged that promises to dramatically recast our concept of nature and mankind's place in it. Unlike the traditional analytical approach which breaks nature down into smaller and smaller constituent parts, chaos theory, the theory of self-organization, and other so-called sciences of complexity, explore dynamic systems in their totalities, so as to lay bare the great constants governing their emergence, organization, and evolution. Using the tools of complexity, researchers recently have made breakthroughs in the understanding of such divers phenomena as weather systems, economies, and even the most daunting scientific mystery of all, the mind as an emergent property of the brain's dense neuronal mazes.

This book consists of a collection of works on utilizing the automatic identification technology provided by Radio Frequency Identification (RFID) to address the problems of global counterfeiting of goods. The book presents current research, directed to securing supply chains against the efforts of counterfeit operators, carried out at the Auto-ID Labs around the globe. It assumes

very little knowledge on the part of the reader on Networked RFID systems as the material provided in the introduction familiarizes the reader with concepts, underlying principles and vulnerabilities of modern RFID systems.
This reference guide to creating high quality security software covers the complete suite of security applications referred to as end2end security. It illustrates basic concepts of security engineering through real-world examples.
This volume offers an overview of the processes of zoonotic viral emergence, the intricacies of host/virus interactions, and the role of biological transitions and modifying factors. The themes introduced here are amplified and explored in detail by the contributing authors, who explore the mechanisms and unique circumstances by which evolution, biology, history, and current context have contrived to drive the emergence of different zoonotic agents by a series of related events.
Car keys have developed from the simple systems which were no more advanced than the front door key of a house to very advanced forms that use onboard computers for their operation. Modern vehicles also have push button remote locking/unlocking, it is rare these days to push your Car Key into the barrel to open it. Most cars now use Remote Control Keys to open. These improvements in the Car Keys Systems, has however made it difficult for genuine car owners to duplicate their Car keys or get a replacement when they lose them. The process requires specialize skills and knowhow for even a regular locksmith. This book has therefore been written to inform and guides anyone who wants to develop the skills required to duplicate or replace keys of modern cars.
This book provides the technical essentials, state-of-the-art knowledge, business ecosystem and standards of Near Field Communication (NFC)by NFC Lab – Istanbul research centre which conducts intense research on NFC technology. In this book, the authors present the contemporary research on all aspects of NFC, addressing related security aspects as well as information on various business models. In addition, the book provides comprehensive information a designer needs to design an NFC project, an analyzer needs to analyze requirements of a new NFC based system, and a programmer needs to implement an application. Furthermore, the authors introduce the technical and administrative issues related to NFC technology, standards, and global stakeholders. It also offers comprehensive information as well as use case studies for each NFC operating mode to give the usage idea behind each operating mode thoroughly. Examples of NFC application development are provided using Java technology, and security considerations are discussed in detail. Key Features: Offers a complete understanding of the NFC technology, including standards, technical essentials, operating modes, application development with Java, security and privacy, business ecosystem analysis Provides analysis, design as well as development guidance for professionals from administrative and technical perspectives Discusses methods, techniques and modelling support including UML are demonstrated with real cases Contains case studies such as payment, ticketing, social networking and remote shopping This book will be an invaluable guide for business and ecosystem analysts, project managers, mobile commerce consultants, system and application developers, mobile developers and practitioners. It will also be of interest to researchers, software engineers, computer scientists, information technology specialists including students and graduates.
The chapters in this open access book arise out of the EU Cost Action project Cryptacus, the objective of which was to improve and adapt existent cryptanalysis methodologies and tools to the ubiquitous computing framework. The cryptanalysis implemented lies along four axes: cryptographic models, cryptanalysis of building blocks, hardware and software security engineering, and security assessment of real-world systems. The authors are top-class researchers in security and cryptography, and the contributions are of value to researchers and practitioners in these domains. This book is open access under a CC BY license.
From the former president of MIT, the story of the next technology revolution, and how it will change our lives. A century ago, discoveries in physics came together with engineering to produce an array of astonishing new technologies: radios, telephones, televisions, aircraft, radar, nuclear power, computers, the Internet, and a host of still-evolving digital tools. These technologies so radically reshaped our world that we can no longer conceive of life without them. Today, the world’s population is projected to rise to well over 9.5 billion by 2050, and we are currently faced with the consequences of producing the energy that fuels, heats, and cools us. With temperatures and sea levels rising, and large portions of the globe plagued with drought, famine, and drug-resistant diseases, we need new technologies to tackle these problems. But we are on the cusp of a new convergence, argues world-renowned neuroscientist Susan Hockfield, with discoveries in biology coming together with engineering to produce another array of almost inconceivable technologies—next-generation products that have the potential to be every bit as paradigm shifting as the twentieth century’s digital wonders. The Age of Living Machines describes some of the most exciting new developments and the scientists and engineers who helped create them. Virus-built batteries. Protein-based water filters. Cancer-detecting nanoparticles. Mind-reading bionic limbs. Computer-engineered crops. Together they highlight the promise of the technology revolution of the twenty-first century to overcome some of the greatest humanitarian, medical, and environmental challenges of our time.
Real-Time Systems Development introduces computing students and professional programmers to the development of software for real-time applications. Based on the academic and commercial experience of the author, the book is an ideal companion to final year undergraduate options or MSc modules in the area of real-time systems design and implementation. Assuming a certain level of general systems design and programming experience, this text will extend students’ knowledge and skills into an area of computing which has increasing relevance in a modern world of telecommunications and ‘intelligent’ equipment using embedded microcontrollers. This book takes a broad, practical approach in discussing real-time systems. It covers topics such as basic input and output; cyclic executives for bare hardware; finite state machines; task communication and synchronization; input/output interfaces; structured design for real-time systems; designing for multitasking; UML for real-time systems; object oriented approach to real-time systems; selecting languages for RTS development; Linux device drivers; and hardware/software co-design. Programming examples using GNU/Linux are included, along with a supporting website containing slides; solutions to problems; and software examples. This book will appeal to advanced undergraduate Computer Science students; MSc students; and, undergraduate software engineering and electronic engineering students. * Concise treatment delivers material in manageable sections * Includes handy glossary, references and practical exercises based on familiar scenarios * Supporting website contains slides, solutions to problems and software examples
Whether you want to learn lockpicking or locksmithing, or choose locks that are virtually impossible to defeat, this classic will meet your needs. The top reference in the field since 1976, this book is perfect for everyone from beginners who

want to master techniques step by illustrated step, to pros who need an up-to-date, comprehensive shop manual. The Sixth Edition features: •Complete, illustrated coverage from a master locksmith. •Techniques and tips for lockpicking and fixing. •Safe opening and servicing techniques. •Coverage of electronic and high-security mechanical locks. •Auto lock opening and servicing how-tos. •An all-new Registered Locksmith test. •How to conduct a home security survey •How to start and run a locksmithing business, or get hired as a locksmith.

Forensic Investigation of Stolen-Recovered and Other Crime-Related Vehicles provides unique and detailed insights into the investigations of one of the most common crime scenes in the world. In addition to a thorough treatment of auto theft, the book covers vehicles involved in other forms of crime—dealing extensively with the various procedures and dynamics of evidence as it might be left in any crime scene. An impressive collection of expert contributors covers a wide variety of subjects, including chapters on vehicle identification, examination of burned vehicles, vehicles recovered from under water, vehicles involved in terrorism, vehicle tracking, alarms, anti-theft systems, steering columns, and ignition locks. The book also covers such topics as victim and witness interviews, public and private auto theft investigations, detection of trace evidence and chemical traces, vehicle search techniques, analysis of automotive fluids, vehicle registration, document examination, and vehicle crime mapping. It is the ultimate reference guide for any auto theft investigator, crime scene technician, criminalist, police investigator, criminologist, or insurance adjuster. Extensively researched and exceptionally well-written by internationally-recognized experts in auto theft investigation and forensic science All the principles explained in the text are well-illustrated and demonstrated with more than 450 black and white and about 100 full-color illustrations, many directly from real cases Serves as both a valuable reference guide to the professional and an effective teaching tool for the forensic science student

Explaining the contemporary role of management accounting in organisations, this book is useful for the Australian business environment. It provides coverage of the management accounting concepts that are relevant to the Australian economy.

Set deep in the heart of Texas, bestselling author Kimberly Raye's sizzling new series proves that men, women, and moonshine make one dangerous combination... RECIPE FOR DISASTER The most infamous moonshiners in Lone Star history, the Tuckers and the Sawyers have been feuding for over a hundred years. Sure, the days of buckshot and bloodshed are long gone, but it's not over yet. To save the family business, Callie Tucker has to find the recipe for the legendary Texas Thunder moonshine. But first she'll need to make a devil's bargain—with a red-hot hellraiser named Brett Sawyer. ROMANCE WITH A KICK A Sawyer through and through, Brett was raised to never trust a Tucker—especially one as pretty as Callie. But desperate times call for desperate measures. With his ranch going bankrupt, Brett agrees to help Callie find the recipe, sell the rights, and split the profits. Of course, it won't be easy for these two enemies to work together. But it's even harder to ignore the sparks of attraction—when just one kiss delivers a kick stronger than any swig of moonshine...

In today’s modernized world, new research and empirical findings are being conducted and found within various professional industries. The field of engineering is no different. Industrial and material engineering is continually advancing, making it challenging for practitioners to keep pace with the most recent trends and methods. Engineering professionals need a handbook that provides up-to-date research on the newest methodologies in this imperative industry. The Handbook of Research on Developments and Trends in Industrial and Materials Engineering is a collection of innovative research on the theoretical and practical aspects of integrated systems within engineering. This book provides a forum for professionals to understand the advancing methods of engineering. While highlighting topics including operations management, decision analysis, and communication technology, this book is ideally designed for researchers, managers, engineers, industrialists, manufacturers, academicians, policymakers, scientists, and students seeking current research on recent findings and modern approaches within industrial and materials engineering.

This book presents high-quality original contributions on the development of automatic traffic analysis systems that are able to not only anticipate traffic scenarios, but also understand the behavior of road users (vehicles, bikes, trucks, etc.) in order to provide better traffic management, prevent accidents and, potentially, identify criminal behaviors. Topics also include traffic surveillance and vehicle accident analysis using formal concept analysis, convolutional and recurrent neural networks, unsupervised learning and process mining. The content is based on papers presented at the 1st Italian Conference for the Traffic Police (TRAP), which was held in Rome in October 2017. This conference represents a targeted response to the challenges facing the police in connection with managing massive traffic data, finding patterns from historical datasets, and analyzing complex traffic phenomena in order to anticipate potential criminal behaviors. The book will appeal to researchers, practitioners and decision makers interested in traffic monitoring and analysis, traffic modeling and simulation, mobility and social data mining, as well as members of the police.

The development of low-cost, compact digital storage, sensors and radio modules allows us to embed digital memories into products to record key events. Such computationally enhanced products can perceive and control their environment, analyze their observations, and communicate with other smart objects and human users. Digital product memories (DPMs) will play a key role in the upcoming fourth industrial revolution based on cyber-physical production systems, resulting in improvements in traceability and quality assurance, more efficient and flexible production, logistics, customization, and recycling, and better information for the consumer. SemProM was a major industrial and academic research project that examined all aspects of the design and implementation of semantic product memories, and this book is a comprehensive assessment of the results achieved. The introductory chapters explain the fundamental ideas and the organization of the related project, while the remaining parts explain how to build, model and process DPMs, multimodal interaction using them, and selected applications. This work is inherently multidisciplinary and the related ideas, technologies, and implementations draw on results in fields such as semantic technologies, machine-to-machine

communication, intelligent sensor networks, instrumented environments, embedded systems, smart objects, RFID technology, security, and privacy. The contributing authors are leading scientists and engineers, representing key academic teams and companies. The book explains successful deployment in applications such as manufacturing, green logistics, retail, healthcare, and food distribution, and it will be of value to both researchers and practitioners.

Find out what Blockchain is, how it works, and what it can do for you Blockchain is the technology behind Bitcoin, the revolutionary 'virtual currency' that's changing the way people do business. While Bitcoin has enjoyed some well-deserved hype, Blockchain may be Bitcoin's most vital legacy. Blockchain For Dummies is the ideal starting place for business pros looking to gain a better understanding of what Blockchain is, how it can improve the integrity of their data, and how it can work to fundamentally change their business and enhance their data security. Blockchain For Dummies covers the essential things you need to know about this exciting technology's promise of revolutionizing financial transactions, data security, and information integrity. The book covers the technologies behind Blockchain, introduces a variety of existing Blockchain solutions, and even walks you through creating a small but working Blockchain-based application. Blockchain holds the promise to revolutionize a wide variety of businesses. Get in the know about Blockchain now with Blockchain For Dummies and be ready to make the changes to business that your colleagues and competitors will later wish they'd done. Discover ten ways Blockchain can change business Find out how to apply a Blockchain solution See how to make data more secure Learn how to work with vendors Filled with vital information and tips on how this paradigm-changing technology can transform your business for the better, this book will not only show you Blockchain's full potential, but your own as well!

Car Key Programming GuideLulu Press, Inc

Major revelations about the US government’s drone program—bestselling author Jeremy Scahill and his colleagues at the investigative website The Intercept expose stunning new details about America’s secret assassination policy. When the US government discusses drone strikes publicly, it offers assurances that such operations are a more precise alternative to troops on the ground and are authorized only when an “imminent” threat is present and there is “near certainty” that the intended target will be killed. The implicit message on drone strikes from the Obama administration has been trust, but don’t verify. The online magazine The Intercept exploded this secrecy when it obtained a cache of secret slides that provide a window into the inner workings of the US military’s kill/capture operations in Afghanistan, Yemen, and Somalia. Whether through the use of drones, night raids, or new platforms yet to be employed, these documents show assassination to be central to US counterterrorism policy. The classified documents reveal that Washington’s fourteen-year targeted killing campaign suffers from an overreliance on flawed signals intelligence, an apparently incalculable civilian toll, and an inability to extract potentially valuable intelligence from terror suspects. This campaign, carried out by two presidents through four presidential terms, has been deliberately obscured from the public and insulated from democratic debate. The Assassination Complex allows us to understand at last the circumstances under which the US government grants itself the right to sentence individuals to death without the established checks and balances of arrest, trial, and appeal. The book will include original contributions from Glenn Greenwald and Edward Snowden. Originally published in hardcover in 2019 by Doubleday.

This is the third revised edition of the established and trusted RFID Handbook; the most comprehensive introduction to radio frequency identification (RFID) available. This essential new edition contains information on electronic product code (EPC) and the EPC global network, and explains near-field communication (NFC) in depth. It includes revisions on chapters devoted to the physical principles of RFID systems and microprocessors, and supplies up-to-date details on relevant standards and regulations. Taking into account critical modern concerns, this handbook provides the latest information on: the use of RFID in ticketing and electronic passports; the security of RFID systems, explaining attacks on RFID systems and other security matters, such as transponder emulation and cloning, defence using cryptographic methods, and electronic article surveillance; frequency ranges and radio licensing regulations. The text explores schematic circuits of simple transponders and readers, and includes new material on active and passive transponders, ISO/IEC 18000 family, ISO/IEC 15691 and 15692. It also describes the technical limits of RFID systems. A unique resource offering a complete overview of the large and varied world of RFID, Klaus Finkenzeller’s volume is useful for end-users of the technology as well as practitioners in auto ID and IT designers of RFID products. Computer and electronics engineers in security system development, microchip designers, and materials handling specialists benefit from this book, as do automation, industrial and transport engineers. Clear and thorough explanations also make this an excellent introduction to the topic for graduate level students in electronics and industrial engineering design. Klaus Finkenzeller was awarded the Fraunhofer-Smart Card Prize 2008 for the second edition of this publication, which was celebrated for being an outstanding contribution to the smart card field.