Card Essentials Rfid Mifare Desfire Ev1

The definitive guide to understanding RFID technology's benefits and implementation.

This book constitutes the thoroughly refereed post-worksop proceedings of the 7th International Workshop Radio Frequency Identification: Security and Privacy Issues. RFIDSec 2011, held in Amherst, Massachusetts, USA, in June 2011. The 12 revised full papers presented were carefully reviewed and selected from 21 initial submissions for inclusion in the book. The papers focus on minimalism in cryptography, on-tag cryptography, securing RFID with physics, and protocol-level security in RFID.

From its well-chosen essays to its thorough editorial apparatus to its practical organization, The Compact Reader provides instructors with the fundamental support they need to get students writing purposefully. The distinctive dual organization -- rhetorical and thematic -- introduces students to essential strategies of writing while engaging them with brief readings on captivating topics. For the instructor who wants a concise, effective means for teaching students to think critically about the connection between form and content, The Compact Reader is the perfect choice.

Explore embedded systems pentesting by applying the most common attack techniques and patterns Key Features Learn various pentesting tools and techniques to attack and secure your hardware infrastructure Find the glitches in your hardware that can be a possible entry point for attacks Discover best practices for securely designing products Book Description Hardware pentesting involves leveraging hardware interfaces and communication channels to find vulnerabilities in a device. Practical Hardware Pentesting will help you to plan attacks, hack your embedded devices, and secure the hardware infrastructure. Throughout the book, you will see how a specific device works, explore the functional and security aspects, and learn how a system senses and communicates with the outside world. You will start by setting up your lab from scratch and then gradually work with an advanced hardware lab. The book will help you get to grips with the global architecture of an embedded system and sniff on-board traffic. You will also learn how to identify and formalize threats to the embedded system and understand its relationship with its ecosystem. Later, you will discover how to analyze your hardware and locate its possible system vulnerabilities before going on to explore firmware dumping, analysis, and exploitation. Finally, focusing on the reverse engineering process from an attacker point of view will allow you to understand how devices are attacked, how they are compromised, and how you can harden a device against the most common hardware attack vectors. By the end of this book, you will be well-versed with security best practices and understand how they can be implemented to secure your hardware. What you will learn Perform an embedded system test and identify security critical functionalities Locate critical security components and buses and learn how to attack them Discover how to dump and modify stored information Understand and exploit the relationship between the firmware and hardware Identify and attack the security functions supported by the functional blocks of the device Develop an attack lab to support advanced device analysis and attacks Who this book is for This book is for security professionals and researchers who want to get started with hardware security assessment but don't know where to start. Electrical engineers who want to understand how their devices can be attacked and how to protect against these attacks will also find this book useful.

Wireless and Mobile Networks

Professional Android Sensor Programming

Theories, Methods, Tools and Technologies

Dragon Boy

A Major Reform in Progress

Development and Implementation of RFID Technology

The Art and Science of NFC Programming

NFC is a world standard since 2004 which is now within every smartphone on the market. Such a standard enables us to do mobile transactions (mobile payment) in a secure way along with many other information- based tap’n play operations. This book has a double role for computer scientists (from bachelor students in CS to IT professionals).

This document provides info. to organizations on the security capabilities of Bluetooth and provide recommendations to organizations employing Bluetooth technologies on securing them effectively. It discusses Bluetooth technologies and security capabilities in technical detail. This document assumes that the readers have at least some operating system, wireless networking, and security knowledge. Because of the constantly changing nature of the wireless security industry and the threats and vulnerabilities to the technologies, readers are strongly encouraged to take advantage of other resources (including those listed in this document) for more current and detailed information. Illustrations.

An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements.

Radio Frequency Identification System SecurityIOS Press

Everyday Surveillance

Security of Ubiquitous Computing Systems

Electronic access control systems. Core interoperability protocol based on Web services

20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers

Radio Frequency Identification System Security

Proprietary Burglar Alarm Units and Systems, UL 1076

Trusted Systems

Handbook of Signal Processing Systems is organized in three parts. The first part motivates representative applications that drive and apply state-of-the art methods for design and implementation of signal processing systems; the second part discusses architectures for implementing these applications; the third part focuses on compilers and simulation tools, describes models of computation and their associated design tools and methodologies. This handbook is an essential tool for professionals in many fields and researchers of all levels.

The idea for the book has been taken from true events during the fantastic life of the author. Some of the characters are real and have played a solid role of shaping the author into the man he is today. The author met God when he was seven years old. The angel Tonghunkas Tan Bonus is real; the mother of Jesus Christ is real—the author visited with them three to four hours. This great event is absolutely true. The author’s polygraph test will be released in his next book, For Whom the Bullets Kill. He will also tell readers where heaven truly is, what it looks like, and much more. The events with the dignitaries were real but have been embellished for the excitement and entertainment of the reader. Again, this book was written to captivate the reader’s attention but, most importantly, covers true events that will enlighten the religious beliefs we Americans are blessed to have freedom to worship every day. If my book offends anyone, I offer the humblest apologies; if my book entertains anyone, then all my labors will have been worthwhile. I thank God that I am an American and have the right to write what I please. I also feel I have earned that right by having fought wars for my country and also for the people while serving as a police officer.

When we think of surveillance in our society, we usually imagine “Big Brother” scenarios with the government tracking our every move. The actual surveillance of our everyday lives is much more subtle, however, and may be more insidious. William G. Staples shows how our lives are tracked by both public and private organizations—sometimes with our consent, and sometimes without—through our internet use, cell phones, public video cameras, credit cards, license plates, shopping habits, and more. Everyday Surveillance is a provocative exploration of the myriad ways we are watched each day, and how this surveillance shapes our lives. Thoroughly revised, the second edition considers new topics, such as the rise of social media, and updates research throughout. Everyday Surveillance introduces students to concepts of social control and incites classroom discussion about how surveillance impacts the ways we understand people and our lives at home, work, school, or in the community.

This book constitutes the thoroughly refereed post-conference proceedings of the 13th International Conference on Information Security and Cryptology, held in Seoul, Korea, in December 2010. The 28 revised full papers presented were carefully selected from 99 submissions during two rounds of reviewing. The conference provides a forum for the presentation of new results in research, development, and applications in the field of information security and cryptology. The papers are organized in topical sections on cryptanalysis, cryptographic algorithms, implementation, network and mobile security, symmetric key cryptography, cryptographic protocols, and side channel attack.

RFID

Deploying Radio Frequency Identification Systems

The RF in RFID

Selected Topics

Critical Infrastructure Security and Resilience

Mobile Computing, Applications, and Services

RFID Field Guide

The book generously covers a wide range of aspects and issues related to RFID systems, namely the design of RFID antennas, RFID readers and the variety of tags (e.g. UHF tags for sensing applications, surface acoustic wave RFID tags, smart RFID tags), complex RFID systems, security and privacy issues in RFID applications, as well as the selection of encryption algorithms. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices but also for experienced technical professionals and RFID aficionados.

The book presents the proceedings of the 4th EAI International Conference on Management of Manufacturing Systems (MMS 2019), which took place in Krynica Zdroj, Poland, on October 8-10, 2019. The conference covered Management of Manufacturing Systems with support for Industry 4.0, Logistics and Intelligent Manufacturing Systems and Applications, Cooperation management and its effective applications. Topics include RFID Applications, Economic Impacts in Logistics, ICT Support for Industry 4.0, Industrial and Smart Logistics, Intelligent Manufacturing Systems and Applications, and much more.

The Latest Linux Security Solutions This authoritative guide will help you secure your Linux network--whether you use Linux as a desktop OS, for Internet services, for telecommunications, or for wireless services. Completely rewritten the ISECOM way, Hacking Exposed Linux, Third Edition provides the most up-to-date coverage available from a large team of topic-focused experts. The book is based on the latest ISECOM security research and shows you, in full detail, how to lock out intruders and defend your Linux systems against catastrophic attacks. Secure Linux by using attacks and countermeasures from the latest OSSTMM research Follow attack techniques of PSTN, ISDN, and PSDN over Linux Harden VoIP, Bluetooth, RF, RFID, and IR devices on Linux Block Linux signal jamming, cloning, and eavesdropping attacks Apply Trusted Computing and cryptography tools for your best defense Fix vulnerabilities in DNS, SMTP, and Web 2.0 services Prevent SPAM, Trojan, phishing, DoS, and DDoS exploits Find and repair errors in C code with static analysis and Hoare Logic

This book introduces the technologies and techniques of large-scale RFID-enabled mobile computing systems. The discussion is set in the context of specific system case studies where RFID has been the core enabling technology in retail, metropolitan transportation, logistics and e-passport applications. RFID technology fundamentals are covered including operating principles, core system components and performance trade-offs involved in the selection of specific RFID platforms.

Short Essays by Method and Theme

RFID and the Internet of Things

Card Design

MIFARE and Contactless Smartcards in Application

5th International Conference, MobiCase 2013, Paris, France, November 7-8, 2013, Revised Selected Papers

Handbook of Signal Processing Systems

RFID Essentials

A cellular network or mobile network is a wireless network distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station. In a cellular network, each cell uses a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed bandwidth within each cell. When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission. Cellular networks offer a number of desirable features: More capacity than a single large transmitter, since the same frequency can be used for multiple links as long as they are in different cells Mobile devices use less power than with a single transmitter or satellite since the cell towers are closer Larger coverage area than a single terrestrial transmitter, since additional cell towers can be added indefinitely and are not limited by the horizon Major telecommunications providers have deployed voice and data cellular networks over most of the inhabited land area of the Earth. This allows mobile phones and mobile computing devices to be connected to the public switched telephone network and public Internet. Private cellular networks can be used for research or for large organizations and fleets, such as dispatch for local public safety agencies or a taxicab company.

This book constitutes the proceedings of the 20th International Conference on Selected Areas in Cryptography, SAC 2013, held in Burnaby, Canada, in August 2013. The 26 papers presented in this volume were carefully reviewed and selected from 98 submissions. They are organized in topical sections named: lattices; discrete logarithms; stream ciphers and authenticated encryption; post-quantum (hash-based and system solving); white box crypto; block ciphers; elliptic curves, pairings and RSA; hash functions and MACs; and side-channel attacks. The book also contains 3 full-length invited talks.

This book constitutes the proceedings of the International Conference on Trusted Systems, held in Beijing, China, in December 2010.The 23 contributed papers presented together with nine invited talks from a workshop, titled "Asian Lounge on Trust, Security and Privacy" were carefully selected from 66 submissions. The papers are organized in seven topical sections on implentation technology, security analysis, cryptographic aspects, mobile trusted systems, hardware security, attestation, and software protection.

With the onset of the computer and e-mail, it seems these days we are less likely to send a card by post. However, there is something very personal about receiving personal mail. 'Card Design' has chapters covering invitation cards and promotional cards, as well as several types of greeting cards looking at the aspects of why people would want to keep your card rather than treat as junk mail. Over 150 detailed examples are included all in full colour.

Selected Areas in Cryptography -- SAC 2013

Linux Security Secrets and Solutions

IoT Security

A guide to attacking embedded systems and protecting them against the most common hardware attacks

How to Avoid Security Problems the Right Way

Practical Hardware Pentesting

RFID Security and Privacy

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.

Learn to build human-interactive Android apps, starting withdevice sensors This book shows Android developers how to exploit the rich setof device sensors—locational, physical (temperature,pressure, light, acceleration, etc.), cameras, microphones, andspeech recognition—in order to build fully human-interactiveAndroid applications. Whether providing hands-free directions orchecking your blood pressure, Professional Android SensorProgramming shows how to turn possibility into reality. The authors provide techniques that bridge the gap betweenaccessing sensors and putting them to meaningful use in real-worldsituations. They not only show you how to use the sensor relatedAPIs effectively, they also describe how to use supporting AndroidOS components to build complete systems. Along the way, theyprovide solutions to problems that commonly occur when usingAndroid's sensors, with tested, real-world examples. Ultimately,this invaluable resource provides in-depth, runnable code examplesthat you can then adapt for your own applications. Shows experienced Android developers how to exploit the richset of Android smartphone sensors to build human-interactiveAndroid apps Explores Android locational and physical sensors (includingtemperature, pressure, light, acceleration, etc.), as well ascameras, microphones, and speech recognition Helps programmers use the Android sensor APIs, use Android OScomponents to build complete systems, and solve commonproblems Includes detailed, functional code that you can adapt and usefor your own applications Shows you how to successfully implement real-world solutionsusing each class of sensors for determining location, interpretingphysical sensors, handling images and audio, and recognizing andacting on speech Learn how to write programs for this fascinating aspect ofmobile app development with Professional Android SensorProgramming.

The revolution in information management, brought about in recent years by advances in computer science, has presented many challenges in the field of security and privacy technology.This book presents the proceedings of RFIDsec12 Asia, the 2012 workshop on radio frequency identification RFID and the internet of things IoT Security held in Taipei, Taiwan, in November 2012. RFIDsec12 Asia provides researchers, enterprises and governments with a platform to investigate, discuss and propose new solutions to security and privacy issues relating to RFID/IoT technologies and applications.Some of the topics covered in the nine

The International Conference on Field Programmable Logic and Applications (FPL) is the first and largest conference covering the rapidly growing area of field programmable logic During the past 26 years, many of the advances achieved in reconfigurable system architectures, applications, embedded processors, design automation methods (EDA) and tools have been first published in the proceedings of the FPL conference series FPL 2016 will offer the following five conference tracks Architectures and Technology, Applications and Benchmarks, Design Methods and Tools, Self aware and Adaptive Systems, Surveys, Trends and Education

4th EAI International Conference on Management of Manufacturing Systems

Building Secure Software

UHF RFID in Practice

The Compact Reader

Networked RFID

133 Gadgets, 8 Categories

2016 26th International Conference on Field Programmable Logic and Applications (FPL)

The European Commission adopted a comprehensive package of reforms to the EU merger control regime in conjunction with the accession of the new Member States in 2004. This constituted the most radical reform of the regime since the previous Merger Regulation was adopted in 1989, aimed at better adapting it to a globalizing market and enlarging an increasingly integrated European Union. The extensive reform to the regulation has provoked significant questions about the way in which the Commission treats major merger evaluations. EC Merger Control provides a comprehensive and insightful account of the many important procedural and substantive aspects of the reform process, with contributions from eminent specialists in the field of mergers, including lawyers, economists, and representatives of the European Commission, Court of First Instance, US Department of Justice, the World Bank and several competition authorities. The papers in this book are based on the proceedings of the 2002 EC Merger Control conference - organised jointly by the European Commission and the International Bar Association.

This book presents the latest trends in attacks and protection methods of Critical Infrastructures. It describes original research models and applied solutions for protecting major emerging threats in Critical Infrastructures and their underlying networks. It presents a number of emerging endeavors, from newly adopted technical expertise in industrial security to efficient modeling and implementation of attacks and relevant security measures in industrial control systems; including advancements in hardware and services security, interdependency networks, risk analysis, and control systems security along with their underlying protocols. Novel attacks against Critical Infrastructures (CI) demand novel security solutions. Simply adding more of what is done already (e.g. more thorough risk assessments, more expensive Intrusion Prevention/Detection Systems, more efficient firewalls, etc.) is simply not enough against threats and attacks that seem to have evolved beyond modern analyses and protection methods. The knowledge presented here will help Critical Infrastructure authorities, security officers, Industrial Control Systems (ICS) personnel and relevant researchers to (i) get acquainted with advancements in the field, (ii) integrate security research into their industrial or research work, (iii) evolve current practices in modeling and analyzing Critical Infrastructures, and (iv) moderate potential crises and emergencies influencing or emerging from Critical Infrastructures.

2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT 2017) will be held in Coimbatore, Tamil Nadu, India during 22 24, February 2017 Series of ICECCT has been started in the year 2015 and scheduled to be conducted once in every two years The ICECCT 2017 aims to offer a great opportunity to bring together professors, researchers and scholars around the globe a great platform to deliver the latest innovative research results and the most recent developments and trends in Electrical, Electronics and Computer Engineering and Technology fields The conference will feature invited talks from eminent personalities all around the world, pre conference tutorial workshops and referred paper presentations The vision of ICECCT 2017 is to promote foster communication among researchers and practitioners working in a wide variety of the above areas in Engineering and Technology

Tag Protocols; Protocol Terms and Concepts; How Tags Store Data; GS1 SGTIN Encoding; Find the header; Find the partition; Concatenate the header, filter value, and partition; Append the Company Prefix, Item Reference, and Serial Number; Calculate the CRC and append the EPC to it; Singulation and Anti-Collision Procedures; Slotted Aloha; Adaptive Binary Tree; Slotted Terminal Adaptive Collection (STAC); EPC UHF Class I Gen2; Tag memory; Inventory commands; The Select command; Access commands; Tag states; Tag Features for Security and Privacy; Destroying and Disabling Tags.

RFID Handbook

MMS 2019

Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication

2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT)

Vigilance and Visibility in Postmodern Life

The Hacker's Hardware Toolkit

Recommendations of the National Institute of Standards and Technology

State-of-the-Art Virtual Reality and Augmented Reality Knowhow is a compilation of recent advancements in digital technologies embracing a wide arena of disciplines. Amazingly, this book presents less business cases of these emerging technologies, but rather showcases the scientific use of VR/AR in healthcare, building industry and education. VR and AR are known to be resource intensive, namely, in terms of hardware and wearables - this is covered in a chapter on head-mounted display (HMD). The research work presented in this book is of excellent standard presented in a very pragmatic way; readers will appreciate the depth and breadth of the methodologies and discussions about the findings. We hope it serves as a springboard for future research and development in VR/AR and stands as a lighthouse for the scientific community.

This book explains how UHF tags and readers communicate wirelessly. It gives an understanding of what limits the read range of a tag, how to increase it (and why that might result in breaking the law), and the practical things that need to be addressed when designing and implementing RFID technology. Avoiding heavy math but giving breadth of coverage with the right amount of detail, it is an ideal introduction to radio communications for engineers who need insight into how tags and readers work. New to this edition: • Examples of near-metal antenna techniques • Discussion of the wakeup challenge for battery-assisted tags, with a BAT architecture example • Latest development of protocols: EPC Gen 1.2.0 • Update 18000-6 discussion with battery-assisted tags, sensor tags, Manchester tags and wakeup provisions Named a 2012 Notable

Computer Book for Computer Systems Organization by Computing Reviews The only book to give an understanding of radio communications, the underlying technology for radio frequency identification (RFID) Praised for its readability and clarity, it balances breadth and depth of coverage New edition includes latest developments in chip technology, antennas and protocols

Most organizations have a firewall, antivirus software, and intrusion detection systems, all of which are intended to keep attackers out. So why is computer security a bigger problem today than ever before? The answer is simple--bad software lies at the heart of all computer security problems. Traditional solutions simply treat the symptoms, not the problem, and usually do so in a reactive way. This book teaches you how to take a proactive approach to computer security. Building Secure Software cuts to the heart of computer security to help you get security right the first time. If you are serious about computer security, you need to read this book, which includes essential lessons for both security professionals who have come to realize that software is the problem, and software developers who intend to make their code behave. Written for anyone involved in software development and use—from managers to coders—this book is your first step toward building more secure software. Building Secure Software provides expert perspectives and techniques to help you ensure the security of essential software. If you consider threats and vulnerabilities early in the devel-opment cycle you can build security into your system. With this book you will learn how to determine an acceptable level of risk, develop security tests, and plug security holes before software is even shipped. Inside you'll find the ten guiding principles for software security, as well as detailed coverage of: Software risk management for security Selecting technologies to make your code more secure Security implications of open source and proprietary software How to audit software The dreaded buffer overflow Access control and password authentication Random number generation Applying cryptography Trust management and input Client-side security Dealing with firewalls Only by building secure software can you defend yourself against security breaches and gain the confidence that comes with knowing you won't have to play the "penetrate and patch" game anymore. Get it right the first time. Let these expert authors show you how to properly design your system; save time, money, and credibility; and preserve your customers' trust.

This book provides a broad overview of the many card systems and solutions that are in practical use today. This new edition adds content on RFIDs, embedded security, attacks and countermeasures, security evaluation, javacards, banking or payment cards, identity cards and passports, mobile systems security, and security management. A step-by-step approach educates the reader in card types, production, operating systems, commercial applications, new technologies, security design, attacks, application development, deployment and lifecycle management. By the end of the book the reader should be able to play an educated role in a smart card related project, even to programming a card application. This book is designed as a textbook for graduate level students in computer science. It is also as an invaluable post-graduate level reference for professionals and researchers. This volume offers insight into benefits and pitfalls of diverse industry, government, financial and logistics aspects while providing a sufficient level of technical detail to support technologists, information security specialists, engineers and researchers.

RFID Design Principles

Guide to Bluetooth Security

Systems, Software and Services

13th International Conference, Seoul, Korea, December 1-3, 2010, Revised Selected Papers

State of the Art Virtual Reality and Augmented Reality Knowhow

Second International Conference, INTRUST 2010, Beijing, China, December 13-15, 2010, Revised Selected Papers

RFID (Radio Frequency Identification) technology allows forautomatic identification of information contained in a tag byscanning and interrogation using radio frequency (RF) waves. An RFID tag contains an antenna and a microchip that allows it totransmit and receive. This technology is a possible alternative tothe use of barcodes, which are frequently inadequate in the face ofrapid growth in the scale and complexity of just-in-time inventoryrequirements, regional and international trade, and emerging newmethods of trade based on it. Use of RFID tags will likelyeventually become as widespread as barcodes today. This book describes the technologies used for implementation ofRFID: from hardware, communication protocols, cryptography, toapplications (including electronic product codes, or EPC) andmiddleware. The five parts of this book will provide the reader with a detaileddescription of all the elements that make up a RFID system today,including hot topics such as the privacy concerns, and the Internetof Things.

This revised edition of the Artech House bestseller, RFID Design Principles, serves as an up-to-date and comprehensive introduction to the subject. The second edition features numerous updates and brand new and expanded material on emerging topics such as the medical applications of RFID and new ethical challenges in the field. This practical book offers you a detailed understanding of RFID design essentials, key applications, and important management issues. The book explores the role of RFID technology in supply chain management, intelligent building design, transportation systems, military applications, and numerous other applications. It explains the design of RFID circuits, antennas, interfaces, data encoding schemes, and complete systems. Starting with the basics of RF and microwave propagation, you learn about major system components including tags and readers. This hands-on reference distills the latest RFID standards, and examines RFID at work in supply chain management, intelligent buildings, intelligent transportation systems, and tracking animals. RFID is controversial among privacy and consumer advocates, and this book looks at every angle concerning security, ethics, and protecting consumer data. From design detailsOC to applicationsOC to socio-cultural implications, this authoritative volume offers the knowledge you need to create an optimal RFID system and maximize its performance."

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.

This book constitutes the thoroughly refereed post-conference proceedings of the 5th International Conference on Mobile Computing, Applications, and Services (MobiCASE 2013) held in Paris, France, in November 2013. The 13 full, 5 short and 9 poster papers were carefully reviewed and selected from 64 submissions, and are presented together with 3 papers from the Workshop on Near Field Communication for Mobile Applications (NFS). The conference papers are covering mobile applications development, mobile social networking, novel user experience and interfaces, mobile services and platforms such as Android, iOS, BlackBerry OS, Windows phone, Bada, mobile software engineering and mobile Web, mobile payments and M2M infrastructure, mobile services such as novel hardware add-ons, energy aware services or tools, NFC-based services, authentication services.

EC Merger Control

Alarm and Electronic Security Systems

Hacking Exposed Linux

Information Security and Cryptology - ICISC 2010

7th International Workshop, RFIDsec 2011, Amherst, MA, USA, June 26-28, 2011, Revised Selected Papers

Smart Cards, Tokens, Security and Applications

Advances in Authentication