

Card Essentials Rfid Mifare Desfire Ev1

The most comprehensive book on state-of-the-art smart card technology available Updated with new international standards and specifications, this essential fourth edition now covers all aspects of smart card in a completely revised structure. Its enlarged coverage now includes smart cards for passports and ID cards, health care cards, smart cards for public transport, and Java Card 3.0. New sub-chapters cover near field communication (NFC), single wire protocol (SWP), and multi megabyte smart cards (microcontroller with NAND-Flash). There are also extensive revisions to chapters on smart card production, the security of smart cards (including coverage of new attacks and protection methods), and contactless card data transmission (ISO/IEC 10536, ISO/IEC 14443, ISO/IEC 15693). This edition also features: additional views to the future development of smart cards, such as USB, MMU, SWP, HCI, Flash memory and their usage; new internet technologies for smart cards; smart card web server, HTTP-Protocol, TCP/IP, SSL/TLS; integration of the new flash-based microcontrollers for smart cards (until now the usual ROM-based microcontrollers), and a completely revised glossary with explanations of all important smart card subjects (600 glossary terms). Smart Card Handbook is firmly established as the definitive reference to every aspect of smart card technology, proving an invaluable resource for security systems development engineers. Professionals and microchip designers working in the smart card industry will continue to benefit from this essential guide. This book is also ideal for newcomers to the field. The Fraunhofer Smart Card Award was presented to the authors for the Smart Card Handbook, Third Edition in 2008.

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

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.

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 to get 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 hoses 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.

Systems, Software and Services

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

Card Design

First European Workshop, ESAS 2004, Heidelberg, Germany, August 6, 2004, Revised Selected Papers

IoT Security

MIFARE and Contactless Smartcards in Application

80 Tales of Electronics Bygones

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

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.

Smart Card Developer's Kit is designed to provide the practical information you need to design and build applications that incorporate smart cards. Using a combination of detailed exposition, technical reference summaries, and extended examples, this book familiarizes you with the unique strengths and capabilities of this emerging computer technology. Increase your security from a one-factor security-a password-to a two-factor security-a smart card and its PIN. Use the smart card as a portable place to carry your personal preference information and your identity-establishing private signing key. In marketing applications, a smart card offers a much wider and more flexible set of customer benefits than a magnetic-strip card or a paper record card. A smart card can also carry secured information-such as medical records, licenses, subscriptions, and accreditations-that must be guarded against tampering.

This work presents a comprehensive treatment of the entire construction materials management process, examining the many cost tradeoffs between materials functions. It discusses how to manage construction materials efficiently by implementing measures such as data management, Total Quality Management, process control, electronic data interchange, and bar coding. This book delineates the real cost of materials management. It is intended for: cost, materials, construction, project, civil and industrial engineers, cost estimators and controllers, and upper-level undergraduate and graduate students in these disciplines.

Developer's Kit

Construction Materials Management

RFID Security and Privacy

RFID Handbook

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

Handbook of Signal Processing Systems

Trusted Systems

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 book constitutes the refereed proceedings of the 4th International Conference on Security Standardisation Research, SSR 2018, held in Darmstadt, Germany, in November 2018. The papers cover a range of topics in the field of security standardisation research, including cryptographic evaluation, standards development, analysis with formal methods, potential future areas of standardisation, and improving existing standards.

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.

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

The Hacker's Hardware Toolkit

Security in Ad-hoc and Sensor Networks

Smart Cards, Tokens, Security and Applications

2017 IEEE 7th Annual Computing and Communication Workshop and Conference : 09-11 January, 2017, Las Vegas, USA

RFID Design Principles

The Art and Science of NFC Programming

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

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 development 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.

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.

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 implementation technology, security analysis, cryptographic aspects, mobile trusted systems, hardware security, attestation, and software protection.

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.

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

The RF in RFID

4th EAI International Conference on Management of Manufacturing Systems

Radio Frequency Identification System Security

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

Networked RFID

4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings

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-netal 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

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 (MobCASE 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.

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.

UHF RFID in Practice

Advances in Authentication

133 Gadgets, 8 Categories

Mobile Computing, Applications, and Services

Architecture and Programmer's Guide

March 4-7, 2008, Barcelona, Spain

Proceedings of the Third International Conference on Availability, Security, and Reliability

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.

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. The Insider's Guide to Working with RFID is a collection of the most popular and informative articles and guides found at RFID Insider, the widely regarded trade publication of atlasRFIDstore. These selected compositions range from RFID basics to intermediate topics and cover RFID concepts to frequently asked questions.

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.

How to Avoid Security Problems the Right Way

RFID

Building Secure Software

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

Smart Card Handbook

Control of the Physical Environment

Selected Areas in Cryptography -- SAC 2013

This book constitutes the thoroughly refereed post-workshop 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 cryptology, on tag cryptography, securing RFID with physics, and protocol-level security.

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 network, and mobile device. The document also provides information on 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.

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, design tools and methodologies. This handbook is an essential tool for professionals in many fields and researchers of all levels.

Ad hoc and sensor networks are making their way from research to real-world deployments. Body and personal-area networks, intelligent homes, environmental monitoring or inter-vehicle communications: there is almost nothing left that is not going to be smart and networked. While a great amount of research has been devoted to the pure networking aspects, ad hoc and sensor networks have not been successfully deployed if security, dependability, and privacy issues are not addressed adequately. As the first book devoted to the topic, this volume constitutes the thoroughly refereed post-proceedings of the First European Workshop on Security in Ad-hoc and Sensor Networks, ESAS, 2004, held in Heidelberg, Germany in August 2004. The 17 revised full papers were carefully reviewed and selected from 48 submissions. Among the key topics addressed are key distribution and management, authentication, energy-aware cryptographic primitives, anonymity and pseudonymity, secure diffusion, secure peer-to-peer overlays, and RFIDs.

Retronics

Learning iOS Forensics

Development and Implementation of RFID Technology

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

Security of Ubiquitous Computing Systems

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

Proprietary Burglar Alarm Units and Systems, UL 1076

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."

If you are a digital forensics examiner daily involved in the acquisition and analysis of mobile devices and want to have a complete overview of how to perform your work on iOS devices, this book is definitely for you.

Tag Protocols; Protocol Terms and Concepts; How Tags Store Data; 6S1 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.

Intended for Java Card applet developers, platform implementers, and technical managers seeking an overall understanding of Java Card technology, this guide provides an introduction to the development of applications with Java Card technology based on Java Card version 2.1. Includes an introduction to the platform, an overview and discussion of the technology, a programming guide, and tips. Annotation copyrighted by Book News, Inc., Portland, OR

The Insider's Guide to Working with RFID

Java Card Technology for Smart Cards

Selected Topics

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

RFID Essentials

IEEE CCWC-2017

Smart Card