High Performance Computing

Secure IT Systems

Android Hacker's Handbook

Mobile Malware Attacks and Defense

Android Malware and Analysis

2016 IEEE WIC ACM International Conference on Web Intelligence Workshops (WIW)
The Mobile Application Hacker's Handbook

Safety of Web Applications

Android Malware and Analysis

Computer Network Security

Digital Forensic Investigation of Internet of Things (IoT) Devices

Cloud Data Centers and Cost Modeling

Android Malware

Proceedings of the 31st Annual Computer Security Applications Conference

Research in Attacks, Intrusions, and Defenses

Dissecting the Hack

Rootkits

The Art and Science of Analyzing Software Data

Risks and Security of Internet and Systems

Handbook on Securing Cyber-Physical Critical Infrastructure

Computer Security – ESORICS 2017

Learning Pentesting for Android Devices

Routing, Flow, and Capacity Design in Communication and Computer Networks

Service Science, Management, and Engineering:

Information Science and Applications

2017 Android Cookbook

Detection of Intrusions and Malware, and Vulnerability Assessment

iOS Hacker's Handbook

Android Malware Detection using Machine Learning

Adaptive Mobile Computing

Information Science and Applications

A Step Towards Society 5.0

Security and Privacy in Communication Networks

Malware Detection

CISSP Study Guide

E-Business and Telecommunications

Financial Cryptography and Data Security

Digital Forensic Investigation of Internet of Things (IoT) Devices

Android Forensics

High Performance Computing

This book constitutes the revised selected papers from the 13th International Conference on Risks and Security of Internet and Systems, CRiSIS 2018, held in Arcachon, France, in October 2018. The 12 full papers and 6 short papers presented in this volume were carefully reviewed and selected from 34 submissions. They cover diverse research themes that range from classic topics, such as vulnerability analysis and classification; apps security; access control and filtering; cloud security; cyber-insurance and cyber threat intelligence; human-centric security and trust; and risk analysis.

Secure IT Systems

Provides instruction on building Android apps, including solutions to working with web services, multitouch gestures, location awareness, and device features.

Android Hacker's Handbook

A guide to rootkits describes what they are, how they work, how to build them, and how to detect them.

Mobile Malware Attacks and Defense

The worldwide reach of the Internet allows malicious cyber criminals to coordinate and launch attacks on both cyber and cyber-physical infrastructure from anywhere in the world. This purpose of this handbook is to introduce the
theoretical foundations and practical solution techniques for securing critical cyber and physical infrastructures as well as their underlying computing and communication architectures and systems. Examples of such infrastructures include utility networks (e.g., electrical power grids), ground transportation systems (automotives, roads, bridges and tunnels), airports and air traffic control systems, wired and wireless communication and sensor networks, systems for storing and distributing water and food supplies, medical and healthcare delivery systems, as well as financial, banking and commercial transaction assets. The handbook focus mostly on the scientific foundations and engineering techniques – while also addressing the proper integration of policies and access control mechanisms, for example, how human-developed policies can be properly enforced by an automated system. Addresses the technical challenges facing design of secure infrastructures by providing examples of problems and solutions from a wide variety of internal and external attack scenarios. Includes contributions from leading researchers and practitioners in relevant application areas such as smart power grid, intelligent transportation systems, healthcare industry and so on. Loaded with examples of real world problems and pathways to solutions utilizing specific tools and techniques described in detail throughout.

Android Malware and Analysis The authors develop a malware fingerprinting framework to cover accurate android malware detection and family attribution in this book. The authors emphasize the following: (1) the scalability over a large malware corpus; (2) the resiliency to common obfuscation techniques; (3) the portability over different platforms and architectures. First, the authors propose an approximate fingerprinting technique for android packaging that captures the underlying static structure of the android applications in the context of bulk and offline detection at the app-market level. This book proposes a malware clustering framework to perform malware clustering by building and partitioning the similarity network of malicious applications on top of this fingerprinting technique.

Second, the authors propose an approximate fingerprinting technique that leverages dynamic analysis and natural language processing techniques to generate Android malware behavior reports. Based on this fingerprinting technique, the authors propose a portable malware detection framework employing machine learning classification. Third, the authors design an automatic framework to produce intelligence about the underlying malicious cyber-infrastructures of Android malware. The authors then leverage graph analysis techniques to generate relevant intelligence to identify the threat effects of malicious Internet activity associated with android malware. The authors elaborate on an effective android malware detection system, in the online detection context at the mobile device level. It is suitable for deployment on mobile devices, using machine learning classification on method call sequences. Also, it is resilient to common code obfuscation techniques and adaptive to operating systems and malware change overtime, using natural language processing and deep learning techniques. Researchers working in mobile and network security, machine learning and pattern recognition will find this book useful as a reference. Advanced-level students studying computer science within these topic areas will purchase this book as well.
2016 IEEE WIC ACM International Conference on Web Intelligence Workshops (WIW) Safety of Web Applications: Risks, Encryption and Handling Vulnerabilities with PHP explores many areas that can help computer science students and developers integrate security into their applications. The Internet is not secure, but it's very friendly as a tool for storing and manipulating data. Customer confidence in Internet software is based on its ability to prevent damage and attacks, but secure software is complicated, depending on several factors, including good risk estimation, good code architecture, cyphering, web server configuration, coding to prevent the most common attacks, and identification and rights allocation. Helps computer science students and developers integrate security into their applications. Includes sections on risk estimate, MVC modeling, the cyphering (certificates, bi-keys, https protocol).

The Mobile Application Hacker's Handbook This book constitutes the thoroughly refereed post-conference proceedings of the 20th International Conference on Financial Cryptography and Data Security, FC 2016, held in Christ church, Barbados, in February 2016. The 27 revised full papers and 9 short papers were carefully selected and reviewed from 137 full papers submissions. The papers are grouped in the following topical sections: fraud and deception; payments, auctions, and e-voting; multiparty computation; mobile malware; social interaction and policy; cryptanalysis; surveillance and anonymity; Web security and data privacy; Bitcoin mining; cryptographic protocols; payment use and abuse.

Safety of Web Applications The rapid growth and development of Android-based devices has resulted in a wealth of sensitive information on mobile devices that offer minimal malware protection. This has created an immediate need for security professionals that understand how to best approach the subject of Android malware threats and analysis. In Android Malware and Analysis, K

Android Malware and Analysis This book constitutes the refereed proceedings of the 6th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2012, held in St. Petersburg, Russia in October 2012. The 14 revised full papers and 8 revised short presentations were carefully reviewed and selected from a total of 44 submissions. The papers are organized in topical sections on applied cryptography and security protocols, access control and information protection, security policies, security event and information management, intrusion prevention, detection and response, anti-malware techniques, security modeling and cloud security.

Android Security Internals The Art and Science of Analyzing Software Data provides valuable information on analysis techniques often used to derive insight from software data. This book shares best practices in the field generated by leading data scientists, collected from their experience training software engineering students and practitioners to master data science. The book covers topics such as...
the analysis of security data, code reviews, app stores, log files, and user telemetry, among others. It covers a wide variety of techniques such as co-change analysis, text analysis, topic analysis, and concept analysis, as well as advanced topics such as release planning and generation of source code comments. It includes stories from the trenches from expert data scientists illustrating how to apply data analysis in industry and open source, present results to stakeholders, and drive decisions. Presents best practices, hints, and tips to analyze data and apply tools in data science projects. Presents research methods and case studies that have emerged over the past few years to further understanding of software data. Shares stories from the trenches of successful data science initiatives in industry.

Computer Network Security Cloud Data Centers and Cost Modeling establishes a framework for strategic decision-makers to facilitate the development of cloud data centers. Just as building a house requires a clear understanding of the blueprints, architecture, and costs of the project; building a cloud-based data center requires similar knowledge. The authors take a theoretical and practical approach, starting with the key questions to help uncover needs and clarify project scope. They then demonstrate probability tools to test and support decisions, and provide processes that resolve key issues. After laying a foundation of cloud concepts and definitions, the book addresses data center creation, infrastructure development, cost modeling, and simulations in decision-making, each part building on the previous. In this way the authors bridge technology, management, and infrastructure as a service, in one complete guide to data centers that facilitates educated decision making. Explains how to balance cloud computing functionality with data center efficiency. Covers key requirements for power management, cooling, server planning, virtualization, and storage management. Describes advanced methods for modeling cloud computing cost including Real Option Theory and Monte Carlo Simulations. Blends theoretical and practical discussions with insights for developers, consultants, and analysts considering data center development.

Digital Forensic Investigation of Internet of Things (IoT) Devices In network design, the gap between theory and practice is woefully broad. This book narrows it, comprehensively and critically examining current network design models and methods. You will learn where mathematical modeling and algorithmic optimization have been under-utilized. At the opposite extreme, you will learn where they tend to fail to contribute to the twin goals of network efficiency and cost-savings. Most of all, you will learn precisely how to tailor theoretical models to make them as useful as possible in practice. Throughout, the authors focus on the traffic demands encountered in the real world of network design. Their generic approach, however, allows problem formulations and solutions to be applied across the board to virtually any type of backbone communication or computer network. For beginners, this book is an excellent introduction. For seasoned professionals, it provides immediate solutions and a strong foundation for further advances in the use of mathematical modeling for network design. Written by leading researchers with a combined 40 years of industrial and academic network design.
experience. Considers the development of design models for different technologies, including TCP/IP, IDN, MPLS, ATM, SONET/SDH, and WDM. Discusses recent topics such as shortest path routing and fair bandwidth assignment in IP/MPLS networks. Addresses proper multi-layer modeling across network layers using different technologies—for example, IP over ATM over SONET, IP over WDM, and IDN over SONET. Covers restoration-oriented design methods that allow recovery from failures of large-capacity transport links and transit nodes. Presents, at the end of each chapter, exercises useful to both students and practitioners.

Cloud Data Centers and Cost Modeling This book contains selected papers from the 8th International Conference on Information Science and Applications (ICISA 2017) and provides a snapshot of the latest issues encountered in technical convergence and convergences of security technology. It explores how information science is core to most current research, industrial and commercial activities and consists of contributions covering topics including Ubiquitous Computing, Networks and Information Systems, Multimedia and Visualization, Middleware and Operating Systems, Security and Privacy, Data Mining and Artificial Intelligence, Software Engineering, and Web Technology. The proceedings introduce the most recent information technology and ideas, applications and problems related to technology convergence, illustrated through case studies, and reviews converging existing security techniques. Through this volume, readers will gain an understanding of the current state-of-the-art information strategies and technologies of convergence security. The intended readerships are researchers in academia, industry and other research institutes focusing on information science and technology.

Android Malware The first comprehensive guide to discovering and preventing attacks on the Android OS. As the Android operating system continues to increase its share of the smartphone market, smartphone hacking remains a growing threat. Written by experts who rank among the world's foremost Android security researchers, this book presents vulnerability discovery, analysis, and exploitation tools for the good guys. Following a detailed explanation of how the Android OS works and its overall security architecture, the authors examine how vulnerabilities can be discovered and exploits developed for various system components, preparing you to defend against them. If you are a mobile device administrator, security researcher, Android app developer, or consultant responsible for evaluating Android security, you will find this guide is essential to your toolbox. A crack team of leading Android security researchers explain Android security risks, security design and architecture, rooting, fuzz testing, and vulnerability analysis. Covers Android application building blocks and security as well as debugging and auditing Android apps. Prepares mobile device administrators, security researchers, Android app developers, and security consultants to defend Android systems against attack. Android Hacker's Handbook is the first comprehensive resource for IT professionals charged with smartphone security.
Proceedings of the 31st Annual Computer Security Applications Conference This book constitutes the refereed proceedings of the 12th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2015, held in Milan, Italy, in July 2015. The 17 revised full papers presented were carefully reviewed and selected from 75 submissions. The papers are organized in topical sections on attacks, attack detection, binary analysis and mobile malware protection, social networks and large-scale attacks, Web and mobile security, and provenance and data sharing.

Research in Attacks, Intrusions, and Defenses Discover all the security risks and exploits that can threaten iOS-based mobile devices. iOS is Apple’s mobile operating system for the iPhone and iPad. With the introduction of iOS 5, many security issues have come to light. This book explains and discusses them all. The award-winning author team, experts in Mac and iOS security, examines the vulnerabilities and the internals of iOS to show how attacks can be mitigated. The book explains how the operating system works, its overall security architecture, and the security risks associated with it, as well as exploits, rootkits, and other payloads developed for it. Covers iOS security architecture, vulnerability hunting, exploit writing, and how iOS jailbreaks work. Explores iOS enterprise and encryption, code signing and memory protection, sandboxing, iPhone fuzzing, exploitation, ROP payloads, and baseband attacks. Also examines kernel debugging and exploitation. Companion website includes source code and tools to facilitate your efforts. iOS Hacker’s Handbook arms you with the tools needed to identify, understand, and foil iOS attacks.

Dissecting the Hack Malware has gone mobile, and the security landscape is changing quickly with emerging attacks on cell phones, PDAs, and other mobile devices. This first book on the growing threat covers a wide range of malware targeting operating systems like Symbian and new devices like the iPhone. Examining code in past, current, and future risks, protect your banking, auctioning, and other activities performed on mobile devices. * Visual Payloads View attacks as visible to the end user, including notation of variants. * Timeline of Mobile Hoaxes and Threats Understand the history of major attacks and horizon for emerging threats. * Overview of Mobile Malware Families Identify and understand groups of mobile malicious code and their variations. * Taxonomy of Mobile Malware Bring order to known samples based on infection, distribution, and payload strategies. * Phishing, SMishing, and Vishing Attacks Detect and mitigate phone-based phishing (vishing) and SMS phishing (SMishing) techniques. * Operating System and Device Vulnerabilities Analyze unique OS security issues and examine offensive mobile device threats. * Analyze Mobile Malware Design a sandbox for dynamic software analysis and use MobileSandbox to analyze mobile malware. * Forensic Analysis of Mobile Malware Conduct forensic analysis of mobile devices and learn key differences in mobile forensics. * Debugging and Disassembling Mobile Malware Use IDA and other tools to reverse-engineer samples of malicious code for analysis. * Mobile Malware Mitigation Measures Qualify risk, understand threats to mobile assets, defend against attacks, and remediate incidents. * Understand the History and Threat Landscape of Rapidly
Emerging Mobile Attacks * Analyze Mobile Device/Platform Vulnerabilities and Exploits * Mitigate Current and Future Mobile Malware Threats

Rootkits Adaptive Mobile Computing: Advances in Processing Mobile Data Sets explores the latest advancements in producing, processing and securing mobile data sets. The book provides the elements needed to deepen understanding of this trend which, over the last decade, has seen exponential growth in the number and capabilities of mobile devices. The pervasiveness, sensing capabilities and computational power of mobile devices have turned them into a fundamental instrument in everyday life for a large part of the human population. This fact makes mobile devices an incredibly rich source of data about the dynamics of human behavior, a pervasive wireless sensors network with substantial computational power and an extremely appealing target for a new generation of threats. Offers a coherent and realistic image of today's architectures, techniques, protocols, components, orchestration, choreography and development related to mobile computing Explains state-of-the-art technological solutions for the main issues hindering the development of next-generation pervasive systems including: supporting components for collecting data intelligently, handling resource and data management, accounting for fault tolerance, security, monitoring and control, addressing the relation with the Internet of Things and Big Data and depicting applications for pervasive context-aware processing Presents the benefits of mobile computing and the development process of scientific and commercial applications and platforms to support them Familiarizes readers with the concepts and technologies that are successfully used in the implementation of pervasive/ubiquitous systems

The Art and Science of Analyzing Software Data This is an easy-to-follow guide, full of hands-on and real-world examples of applications. Each of the vulnerabilities discussed in the book is accompanied with the practical approach to the vulnerability, and the underlying security issue. This book is intended for all those who are looking to get started in Android security or Android application penetration testing. You don’t need to be an Android developer to learn from this book, but it is highly recommended that developers have some experience in order to learn how to create secure applications for Android.

Risks and Security of Internet and Systems CISSP Study Guide, Third Edition provides readers with information on the CISSP certification, the most prestigious, globally-recognized, vendor-neutral exam for information security professionals. With over 100,000 professionals certified worldwide, and many more joining their ranks, this new third edition presents everything a reader needs to know on the newest version of the exam's Common Body of Knowledge. The eight domains are covered completely and as concisely as possible, allowing users to ace the exam. Each domain has its own chapter that includes a specially-designed pedagogy to help users pass the exam, including clearly-stated exam objectives, unique terms and definitions, exam warnings, "learning by example" modules,
hands-on exercises, and chapter ending questions. Provides the most complete and effective study guide to prepare users for passing the CISSP exam, giving them exactly what they need to pass the test Authored by Eric Conrad who has prepared hundreds of professionals for passing the CISSP exam through SANS, a popular and well-known organization for information security professionals Covers all of the new information in the Common Body of Knowledge updated in January 2015, and also provides two exams, tiered end-of-chapter questions for a gradual learning curve, and a complete self-test appendix


Computer Security – ESORICS 2017 This book serves the need for developing an insight and understanding of the cutting-edge innovation in Cloud technology. It provides an understanding of cutting-edge innovations, paradigms, and security by using real-life applications, case studies, and examples. This book provides a holistic view of cloud technology theories, practices, and future applications with real-life examples. It comprehensively explains cloud technology, design principles, development trends, maintaining state-of-the-art cloud computing and software services. It describes how cloud technology can transform the operating contexts of business enterprises. It exemplifies the potential of cloud computing for next-generation computational excellence and the role it plays as a key driver for the 4th industrial revolution in Industrial Engineering and a key driver for manufacturing industries. Researchers, academicians, postgraduates, and industry specialists will find this book of interest.

Learning Pentesting for Android Devices This book provides a valuable reference for digital forensics practitioners and cyber security experts operating in various fields of law enforcement, incident response and commerce. It is also aimed at researchers seeking to obtain a more profound knowledge of Digital Forensics and Cybercrime. Furthermore, the book is an exceptional advanced text for PhD and Master degree programmes in Digital Forensics and Cyber Security. Each chapter of this book is written by an internationally-renowned expert who has extensive experience in law enforcement, industry and academia. The increasing popularity in the use of IoT devices for criminal activities means that there is a maturing discipline and industry around IoT forensics. As technology becomes cheaper and easier to deploy in an increased number of discrete, everyday objects, scope for the automated creation of personalised digital footprints becomes greater. Devices which are presently included within the Internet of Things (IoT) umbrella have a massive potential to enable and shape the way that humans interact and achieve objectives. These also forge a trail of data that can be used to triangulate and identify individuals and their actions. As such, interest and developments in autonomous vehicles, unmanned drones
and ‘smart’ home appliances are creating unprecedented opportunities for the research communities to investigate the production and evaluation of evidence through the discipline of digital forensics.

Routing, Flow, and Capacity Design in Communication and Computer Networks The rapid growth and development of Android-based devices has resulted in a wealth of sensitive information on mobile devices that offer minimal malware protection. This has created an immediate need for security professionals that understand how to best approach the subject of Android malware threats and analysis. In Android Malware and Analysis, Ken Dunham, renowned global malware expert and author, teams up with international experts to document the best tools and tactics available for analyzing Android malware. The book covers both methods of malware analysis: dynamic and static. This tactical and practical book shows you how to use to use dynamic malware analysis to check the behavior of an application/malware as it has been executed in the system. It also describes how you can apply static analysis to break apart the application/malware using reverse engineering tools and techniques to recreate the actual code and algorithms used. The book presents the insights of experts in the field, who have already sized up the best tools, tactics, and procedures for recognizing and analyzing Android malware threats quickly and effectively. You also get access to an online library of tools that supplies what you will need to begin your own analysis of Android malware threats. Tools available on the book’s site include updated information, tutorials, code, scripts, and author assistance. This is not a book on Android OS, fuzz testing, or social engineering. Instead, it is about the best ways to analyze and tear apart Android malware threats. After reading the book, you will be able to immediately implement the tools and tactics covered to identify and analyze the latest evolution of Android threats. Updated information, tutorials, a private forum, code, scripts, tools, and author assistance are available at AndroidRisk.com for first-time owners of the book.

Service Science, Management, and Engineering: This book constitutes the refereed proceedings of the 18th International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2015, held in Kyoto, Japan, in November 2015. The 28 full papers were carefully reviewed and selected from 119 submissions. This symposium brings together leading researchers and practitioners from academia, government, and industry to discuss novel security problems, solutions, and technologies related to intrusion detection, attacks, and defenses.

Information Science and Applications 2017 The open source nature of the platform has not only established a new direction for the industry, but enables a developer or forensic analyst to understand the device at the most fundamental level. Android Forensics covers an open source mobile device platform based on the Linux 2.6 kernel and managed by the Open Handset Alliance. The Android platform is a major source of digital forensic investigation and analysis. This book provides a thorough review of the Android platform including
supported hardware devices, the structure of the Android development project and implementation of core services (wireless communication, data storage and other low-level functions). Finally, it will focus on teaching readers how to apply actual forensic techniques to recover data. Ability to forensically acquire Android devices using the techniques outlined in the book Detailed information about Android applications needed for forensics investigations Important information about SQLite, a file based structured data storage relevant for both Android and many other platforms.

Android Cookbook This book constitutes the refereed proceedings of the 13th International Joint Conference on E-Business and Telecommunications, ICETE 2016, held in Lisbon, Portugal, in July 2016. ICETE is a joint international conference integrating four major areas of knowledge that are divided into six corresponding conferences: International Conference on Data Communication Networking, DCNET; International Conference on E-Business, ICE-B; International Conference on Optical Communication Systems, OPTICS; International Conference on Security and Cryptography, SECRYPT; International Conference on Signal Processing and Multimedia, SIGMAP; International Conference on Wireless Information Systems, WINSYS. The 20 full papers presented together with an invited paper in this volume were carefully reviewed and selected from 241 submissions. The papers cover the following key areas of e-business and telecommunications: data communication networking; e-business; optical communication systems; security and cryptography; signal processing and multimedia applications; wireless networks and mobile systems.

Detection of Intrusions and Malware, and Vulnerability Assessment High Performance Computing: Modern Systems and Practices is a fully comprehensive and easily accessible treatment of high performance computing, covering fundamental concepts and essential knowledge while also providing key skills training. With this book, domain scientists will learn how to use supercomputers as a key tool in their quest for new knowledge. In addition, practicing engineers will discover how supercomputers can employ HPC systems and methods to the design and simulation of innovative products, and students will begin their careers with an understanding of possible directions for future research and development in HPC. Those who maintain and administer commodity clusters will find this textbook provides essential coverage of not only what HPC systems do, but how they are used. Covers enabling technologies, system architectures and operating systems, parallel programming languages and algorithms, scientific visualization, correctness and performance debugging tools and methods, GPU accelerators and big data problems Provides numerous examples that explore the basics of supercomputing, while also providing practical training in the real use of high-end computers Helps users with informative and practical examples that build knowledge and skills through incremental steps Features sidebars of background and context to present a live history and culture of this unique field Includes online resources, such as recorded lectures from the authors’ HPC courses
iOS Hacker's Handbook This book constitutes the refereed proceedings of the 25th Nordic Conference on Secure IT Systems, NordSec 2020, which was organized by Linköping University, Sweden, and held online during November 23-24, 2020. The 15 papers presented in this volume were carefully reviewed and selected from 45 submissions. They were organized in topical sections named: malware and attacks; formal analysis; applied cryptography; security mechanisms and training; and applications and privacy.

Android Malware Detection using Machine Learning This book constitutes the thoroughly refereed post-conference proceedings of the 9th International ICST Conference on Security and Privacy in Communication Networks, held in Sydney, Australia, in September 2013. The 26 revised full papers presented were carefully reviewed and selected from 70 submissions. The papers are grouped in topical sections on: security and privacy in mobile, sensor and ad hoc networks; malware, botnets and distributed denial of service; security for emerging technologies: VoIP, peer-to-peer and cloud computing; encryption and key management; security in software and machine learning; network and system security model; security and privacy in pervasive and ubiquitous computing.

Adaptive Mobile Computing This book presents selected papers from the 10th International Conference on Information Science and Applications (ICISA 2019), held on December 16–18, 2019, in Seoul, Korea, and provides a snapshot of the latest issues regarding technical convergence and convergences of security technologies. It explores how information science is at the core of most current research as well as industrial and commercial activities. The respective chapters cover a broad range of topics, including ubiquitous computing, networks and information systems, multimedia and visualization, middleware and operating systems, security and privacy, data mining and artificial intelligence, software engineering and web technology, as well as applications and problems related to technology convergence, which are reviewed and illustrated with the aid of case studies. Researchers in academia, industry, and at institutes focusing on information science and technology will gain a deeper understanding of the current state of the art in information strategies and technologies for convergence security.

Information Science and Applications The Intelligent Systems Series comprises titles that present state of the art knowledge and the latest advances in intelligent systems. Its scope includes theoretical studies, design methods, and real-world implementations and applications. Service Science, Management, and Engineering presents the latest issues and development in service science. Both theory and applications issues are covered in this book, which integrates a variety of disciplines, including engineering, management, and information systems. These topics are each related to service science from various perspectives, and the book is supported throughout by applications and case studies that showcase best practice and provide insight and guidelines to assist in building successful service systems. Presents the latest research on service science, management and engineering, from both theory and applications perspectives.
Includes coverage of applications in high-growth sectors, along with real-world frameworks and design techniques. Applications and case studies showcase best practices and provide insights and guidelines to those building and managing service systems.

A Step Towards Society 5.0 The two-volume set, LNCS 10492 and LNCS 10493 constitutes the refereed proceedings of the 22nd European Symposium on Research in Computer Security, ESORICS 2017, held in Oslo, Norway, in September 2017. The 54 revised full papers presented were carefully reviewed and selected from 338 submissions. The papers address issues such as data protection; security protocols; systems; web and network security; privacy; threat modeling and detection; information flow; and security in emerging applications such as cryptocurrencies, the Internet of Things and automotive.

Security and Privacy in Communication Networks Mobile devices, such as smart phones, have achieved computing and networking capabilities comparable to traditional personal computers. Their successful consumerization has also become a source of pain for adopting users and organizations. In particular, the widespread presence of information-stealing applications and other types of mobile malware raises substantial security and privacy concerns. Android Malware presents a systematic view on state-of-the-art mobile malware that targets the popular Android mobile platform. Covering key topics like the Android malware history, malware behavior and classification, as well as, possible defense techniques.

Malware Detection There are more than one billion Android devices in use today, each one a potential target. Unfortunately, many fundamental Android security features have been little more than a black box to all but the most elite security professionals—until now. In Android Security Internals, top Android security expert Nikolay Elenkov takes us under the hood of the Android security system. Elenkov describes Android security architecture from the bottom up, delving into the implementation of major security-related components and subsystems, like Binder IPC, permissions, cryptographic providers, and device administration. You’ll learn: - How Android permissions are declared, used, and enforced - How Android manages application packages and employs code signing to verify their authenticity - How Android implements the Java Cryptography Architecture (JCA) and Java Secure Socket Extension (JSSE) frameworks - About Android’s credential storage system and APIs, which let applications store cryptographic keys securely - About the online account management framework and how Google accounts integrate with Android - About the implementation of verified boot, disk encryption, lockscreen, and other device security features - How Android’s bootloader and recovery OS are used to perform full system updates, and how to obtain root access. With its unprecedented level of depth and detail, Android Security Internals is a must-have for any security-minded Android developer.
CISSP Study Guide See your app through a hacker's eyes to find the real sources of vulnerability The Mobile Application Hacker's Handbook is a comprehensive guide to securing all mobile applications by approaching the issue from a hacker's point of view. Heavily practical, this book provides expert guidance toward discovering and exploiting flaws in mobile applications on the iOS, Android, Blackberry, and Windows Phone platforms. You will learn a proven methodology for approaching mobile application assessments, and the techniques used to prevent, disrupt, and remediate the various types of attacks. Coverage includes data storage, cryptography, transport layers, data leakage, injection attacks, runtime manipulation, security controls, and cross-platform apps, with vulnerabilities highlighted and detailed information on the methods hackers use to get around standard security. Mobile applications are widely used in the consumer and enterprise markets to process and/or store sensitive data. There is currently little published on the topic of mobile security, but with over a million apps in the Apple App Store alone, the attack surface is significant. This book helps you secure mobile apps by demonstrating the ways in which hackers exploit weak points and flaws to gain access to data. Understand the ways data can be stored, and how cryptography is defeated Set up an environment for identifying insecurities and the data leakages that arise Develop extensions to bypass security controls and perform injection attacks Learn the different attacks that apply specifically to cross-platform apps IT security breaches have made big headlines, with millions of consumers vulnerable as major corporations come under attack. Learning the tricks of the hacker's trade allows security professionals to lock the app up tight. For better mobile security and less vulnerable data, The Mobile Application Hacker's Handbook is a practical, comprehensive guide.

E-Business and Telecommunications This book provides a valuable reference for digital forensics practitioners and cyber security experts operating in various fields of law enforcement, incident response and commerce. It is also aimed at researchers seeking to obtain a more profound knowledge of Digital Forensics and Cybercrime. Furthermore, the book is an exceptional advanced text for PhD and Master degree programmes in Digital Forensics and Cyber Security. Each chapter of this book is written by an internationally-renowned expert who has extensive experience in law enforcement, industry and academia. The increasing popularity in the use of IoT devices for criminal activities means that there is a maturing discipline and industry around IoT forensics. As technology becomes cheaper and easier to deploy in an increased number of discrete, everyday objects, scope for the automated creation of personalised digital footprints becomes greater. Devices which are presently included within the Internet of Things (IoT) umbrella have a massive potential to enable and shape the way that humans interact and achieve objectives. These also forge a trail of data that can be used to triangulate and identify individuals and their actions. As such, interest and developments in autonomous vehicles, unmanned drones and 'smart' home appliances are creating unprecedented opportunities for the research communities to investigate the production and evaluation of evidence through the discipline of digital forensics.
Financial Cryptography and Data Security This book captures the state of the art research in the area of malicious code detection, prevention and mitigation. It contains cutting-edge behavior-based techniques to analyze and detect obfuscated malware. The book analyzes current trends in malware activity online, including botnets and malicious code for profit, and it proposes effective models for detection and prevention of attacks using. Furthermore, the book introduces novel techniques for creating services that protect their own integrity and safety, plus the data they manage.

Digital Forensic Investigation of Internet of Things (IoT) Devices As an important part of the conference, the workshop special session program will focus on new research challenges and initiatives The workshops may have special invited sessions organized by prominent researchers Each paper will be allocated 4 pages in the proceedings and all papers accepted for workshops will be included in the Workshop Proceedings published by the IEEE Computer Society Press that is indexed by EI, and will be available at the workshops

Android Forensics Dissecting the Hack: The V3rb0t3n Network ventures further into cutting-edge techniques and methods than its predecessor, Dissecting the Hack: The F0rb1dd3n Network. It forgoes the basics and delves straight into the action, as our heroes are chased around the world in a global race against the clock. The danger they face will forever reshape their lives and the price they pay for their actions will not only affect themselves, but could possibly shake the foundations of an entire nation. The book is divided into two parts. The first part, entitled "The V3rb0t3n Network," continues the fictional story of Bob and Leon, two hackers caught up in an adventure in which they learn the deadly consequence of digital actions. The second part, "Security Threats Are Real" (STAR), focuses on these real-world lessons and advanced techniques, as used by characters in the story. This gives the reader not only textbook knowledge, but real-world context around how cyber-attacks may manifest. "The V3rb0t3n Network" can be read as a stand-alone story or as an illustration of the issues described in STAR. Scattered throughout "The V3rb0t3n Network" are "Easter eggs"—references, hints, phrases, and more that will lead readers to insights into hacker culture. Drawing on "The V3rb0t3n Network," STAR explains the various aspects of reconnaissance; the scanning phase of an attack; the attacker’s search for network weaknesses and vulnerabilities to exploit; the various angles of attack used by the characters in the story; basic methods of erasing information and obscuring an attacker’s presence on a computer system; and the underlying hacking culture. All new volume of Dissecting the Hack by Jayson Street, with technical edit by Brian Martin Uses actual hacking and security tools in its story - helps to familiarize readers with the many devices and their code Features cool new hacks and social engineering techniques, in real life context for ease of learning

Copyright code: 12a3e10ee4b1a64330c311e6ccf31743