Byod Mobile Security Crowd Research Partners

The Oxford Handbook of Mobile Communication and Society
A Comprehensive Guide to 5G Security
Cloud Security and Privacy
Rapidly Deployable Mobile Security Solutions for the Military: Navy Cyber Policies and Threats, Security, Mobile Devices, Bring Your Own Device (BYOD), Risk Management, Android Application Program
Mobile Platform Security
Zero Trust Networks
Managing Risk and Information Security
The Implementation Challenges to Bring Your Own Device Concept (BYOD) in Relation to Information Assurance and Security
Bring Your Own Device (BYOD) to Work
Computer and Communication Engineering
Corporate Security Management
Challenges in Cybersecurity and Privacy - the European Research Landscape

Privacy-Preserving in Mobile Crowdsensing
New Technologies, Development and Application
Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution
Wireless and Mobile Device Security
Information Security
Guide to Bluetooth Security
Handbook of Research on Knowledge and Organization Systems in Library and Information Science
Mastering Defensive Security
Personalized Learning
Information Systems for Business and Beyond
Guidelines on Firewalls and Firewall Policy
Mobile Cloud Computing
Moodle for Mobile Learning
Proceedings of the International Conference on Computing and Communication Systems
Adaptive Mobile Computing
Negotiating Control
Growth Poles of the Global Economy: Emergence, Changes and Future Perspectives

The Internet of People, Things and Services
The Strategic Manager
Emerging Technologies in Data Mining and Information Security
Mobile Phone Security and Forensics
Study on Mobile Device Security
Mobile Learning
Mobile Security and Privacy
Hacking Exposed Mobile
Computational Science and Its Applications -- ICCSA 2015
Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security

Byod Mobile Security Crowd Research Partners

KENNY PORTER

The Oxford Handbook of Mobile Communication and Society Newnes " Millions of Americans currently use mobile devices-e.g., cellphones, smartphones, and tablet computers-on a daily basis to communicate, obtain Internet-based information, and share their own information, photographs, and videos. Given the extent of consumer reliance on mobile interactions, it is increasingly important that these devices be secured from expanding

threats to the confidentiality, integrity, and availability of the information they maintain and share. Accordingly, GAO was asked to determine (1) what common security threats and vulnerabilities affect mobile devices, (2) what security features and practices have been identified to mitigate the risks associated with these vulnerabilities, and (3) the extent to which government and private entities have been addressing the security vulnerabilities of mobile devices. To do so, GAO analyzed publically available mobile security reports, surveys related to consumer cybersecurity practices, as well as statutes, regulations, and agency policies; GAO also interviewed representatives from federal agencies and private companies with responsibilities in telecommunications and cybersecurity. "

A Comprehensive Guide to 5G Security

CRC Press

Mobile crowdsensing is a new sensing paradigm that utilizes the intelligence of a crowd of individuals to collect data for mobile purposes by using their portable devices, such as smartphones and wearable devices. Commonly, individuals are incentivized to collect data to fulfill a crowdsensing task released by a data requester. This “sensing as a service” elaborates our knowledge of the physical world by opening up a new door of data collection and analysis. However, with the expansion of mobile crowdsensing, privacy issues urgently need to be solved. In this book, we discuss the research background and current

research process of privacy protection in mobile crowdsensing. In the first chapter, the background, system model, and threat model of mobile crowdsensing are introduced. The second chapter discusses the current techniques to protect user privacy in mobile crowdsensing. Chapter three introduces the privacy-preserving content-based task allocation scheme. Chapter four further introduces the privacy-preserving location-based task scheme. Chapter five presents the scheme of privacy-preserving truth discovery with truth transparency. Chapter six proposes the scheme of privacy-preserving truth discovery with truth hiding. Chapter seven summarizes this monograph and proposes future research directions. In summary, this book introduces the following techniques in mobile crowdsensing: 1) describe a randomizable matrix-based task-matching method to protect task privacy and enable secure content-based task allocation; 2) describe a multi-clouds randomizable matrix-based task-matching method to protect location privacy and enable secure arbitrary range queries; and 3) describe privacy-preserving truth discovery methods to support efficient and secure truth discovery. These techniques are vital to the rapid development of privacy-preserving in mobile crowdsensing.

Cloud Security and Privacy "O'Reilly Media, Inc."

Proven security tactics for today's mobile apps, devices, and networks "A great overview of the new threats created by

mobile devices. ...The authors have heaps of experience in the topics and bring that to every chapter." -- Slashdot Hacking Exposed Mobile continues in the great tradition of the Hacking Exposed series, arming business leaders and technology practitioners with an in-depth understanding of the latest attacks and countermeasures--so they can leverage the power of mobile platforms while ensuring that security risks are contained." -- Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, VISA Identify and evade key threats across the expanding mobile risk landscape. Hacking Exposed Mobile: Security Secrets & Solutions covers the wide range of attacks to your mobile deployment alongside ready-to-use countermeasures. Find out how attackers compromise networks and devices, attack mobile services, and subvert mobile apps. Learn how to encrypt mobile data, fortify mobile platforms, and eradicate malware. This cutting-edge guide reveals secure mobile development guidelines, how to leverage mobile OS features and MDM to isolate apps and data, and the techniques the pros use to secure mobile payment systems. Tour the mobile risk ecosystem with expert guides to both attack and defense Learn how cellular network attacks compromise devices over-the-air See the latest Android and iOS attacks in action, and learn how to stop them Delve into mobile malware at the code level to understand how to write resilient apps Defend against server-side mobile attacks, including SQL

and XML injection Discover mobile web attacks, including abuse of custom URI schemes and JavaScript bridges Develop stronger mobile authentication routines using OAuth and SAML Get comprehensive mobile app development security guidance covering everything from threat modeling to iOS- and Android-specific tips Get started quickly using our mobile pen testing and consumer security checklists

Rapidly Deployable Mobile Security Solutions for the Military: Navy Cyber Policies and Threats, Security, Mobile Devices, Bring Your Own Device (BYOD), Risk Management, Android Application Program Routledge

Mobile Security and Privacy: Advances, Challenges and Future Research Directions provides the first truly holistic view of leading edge mobile security research from Dr. Man Ho Au and Dr. Raymond Choo—leading researchers in mobile security. Mobile devices and apps have become part of everyday life in both developed and developing countries. As with most evolving technologies, mobile devices and mobile apps can be used for criminal exploitation. Along with the increased use of mobile devices and apps to access and store sensitive, personally identifiable information (PII) has come an increasing need for the community to have a better understanding of the associated security and privacy risks. Drawing upon the expertise of world-renowned researchers and experts, this volume comprehensively discusses a

range of mobile security and privacy topics from research, applied, and international perspectives, while aligning technical security implementations with the most recent developments in government, legal, and international environments. The book does not focus on vendor-specific solutions, instead providing a complete presentation of forward-looking research in all areas of mobile security. The book will enable practitioners to learn about upcoming trends, scientists to share new directions in research, and government and industry decision-makers to prepare for major strategic decisions regarding implementation of mobile technology security and privacy. In addition to the state-of-the-art research advances, this book also discusses prospective future research topics and open challenges. Presents the most current and leading edge research on mobile security and privacy, featuring a panel of top experts in the field Provides a strategic and international overview of the security issues surrounding mobile technologies Covers key technical topics and provides readers with a complete understanding of the most current research findings along with future research directions and challenges Enables practitioners to learn about upcoming trends, scientists to share new directions in research, and government and industry decision-makers to prepare for major strategic decisions regarding the implementation of mobile technology security and privacy initiatives

Mobile Platform Security Springer

Recently, mobile security has garnered considerable interest in both the research community and industry due to the popularity of smartphones. The current smartphone platforms are open systems that allow application development, also for malicious parties. To protect the mobile device, its user, and other mobile ecosystem stakeholders such as network operators, application execution is controlled by a platform security architecture. This book explores how such mobile platform security architectures work. We present a generic model for mobile platform security architectures: the model illustrates commonly used security mechanisms and techniques in mobile devices and allows a systematic comparison of different platforms. We analyze several mobile platforms using the model. In addition, this book explains hardware-security mechanisms typically present in a mobile device. We also discuss enterprise security extensions for mobile platforms and survey recent research in the area of mobile platform security. The objective of this book is to provide a comprehensive overview of the current status of mobile platform security for students, researchers, and practitioners.

Zero Trust Networks John Wiley & Sons

The perimeter defenses guarding your network perhaps are not as secure as you think. Hosts behind the firewall have no defenses of their own, so when a host in the "trusted" zone is breached, access to your data center is not far behind. That’s an all-too-familiar scenario today.

With this practical book, you'll learn the principles behind zero trust architecture, along with details necessary to implement it. The Zero Trust Model treats all hosts as if they're internet-facing, and considers the entire network to be compromised and hostile. By taking this approach, you'll focus on building strong authentication, authorization, and encryption throughout, while providing compartmentalized access and better operational agility. Understand how perimeter-based defenses have evolved to become the broken model we use today Explore two case studies of zero trust in production networks on the client side (Google) and on the server side (PagerDuty) Get example configuration for open source tools that you can use to build a zero trust network Learn how to migrate from a perimeter-based network to a zero trust network in production

Managing Risk and Information Security
DIANE Publishing

This book constitutes refereed proceedings of the Third International Conference on Computer and Communication Engineering, CCCE 2023, held in Stockholm, Sweden, in March 2023. The 18 full papers presented were carefully reviewed and selected from 36 submissions. The papers are organized in the following topical sections: image analysis and method; network model and function analysis of mobile network; system security estimation and analysis of data network; and AI-based system model and algorithm.

The Implementation Challenges to Bring Your Own Device Concept (BYOD) in Relation to Information Assurance and Security IGI Global
There can be no doubt that mobile technologies are here to stay. Global mobile traffic grew 74 percent in 2015 alone, with 563 million devices and connections added -- most of them tablets and Smartphones. This growth has been 4000-fold in the past 10 years and 400 million-fold in the past 15 years (Cisco, 2016). Mobile technologies permeate the lives of 21st century citizens as mainstays of organizational and institutional day-to-day operations, commerce, and communication and as tools used to support individuals' personal, social, and career responsibilities. In both the corporate and educational worlds, e- and m-learning and marketing with mobile technologies are moving forward at breakneck speed with, in many cases, a blurring of traditional sector boundaries. As neither the technology nor the uses are static, exploring practices and policies that underpin this quickly shifting mobile technology context is crucial for ensuring its intelligent, purposeful, and equitable use. This edited book provides a venue for researchers to share their work on mobile learning with a focus on uses for mobiles in informal settings and PK-20 classrooms, language learning, mobile gaming, leadership and policy issues, and what mobile learning in the future may be. It assists researchers and educators to consider and answer

questions such as: What is “mobile learning” today? How can mobiles be used to enable learning? How is mobile learning crossing or connecting economic, social, and/or cultural sectors? How do specific cultural practices with media influence mobile learning (e.g., youth practices, educator practices, parent practices, community practices)? What are policy and leadership implications in supporting mobile learning? What policies, practices, and/or pedagogical approaches are necessary to move forward with mobiles in schools or universities? In what ways is mobile learning impacting education; including how students learn and teachers teach? What will/ should/might mobile learning look like in the future?

Bring Your Own Device (BYOD) to Work

Springer

An immersive learning experience enhanced with technical, hands-on labs to understand the concepts, methods, tools, platforms, and systems required to master the art of cybersecurity Key FeaturesGet hold of the best defensive security strategies and toolsDevelop a defensive security strategy at an enterprise levelGet hands-on with advanced cybersecurity threat detection, including XSS, SQL injections, brute forcing web applications, and moreBook Description Every organization has its own data and digital assets that need to be protected against an ever-growing threat landscape that compromises the availability, integrity, and confidentiality of crucial data. Therefore, it is important to train professionals in the latest

defensive security skills and tools to secure them. Mastering Defensive Security provides you with in-depth knowledge of the latest cybersecurity threats along with the best tools and techniques needed to keep your infrastructure secure. The book begins by establishing a strong foundation of cybersecurity concepts and advances to explore the latest security technologies such as Wireshark, Damn Vulnerable Web App (DVWA), Burp Suite, OpenVAS, and Nmap, hardware threats such as a weaponized Raspberry Pi, and hardening techniques for Unix, Windows, web applications, and cloud infrastructures. As you make progress through the chapters, you'll get to grips with several advanced techniques such as malware analysis, security automation, computer forensics, and vulnerability assessment, which will help you to leverage pentesting for security. By the end of this book, you'll have become familiar with creating your own defensive security tools using IoT devices and developed advanced defensive security skills. What you will learnBecome well versed with concepts related to defensive securityDiscover strategies and tools to secure the most vulnerable factor – the userGet hands-on experience using and configuring the best security toolsUnderstand how to apply hardening techniques in Windows and Unix environmentsLeverage malware analysis and forensics to enhance your security strategySecure Internet of Things (IoT) implementationsEnhance the security of

web applications and cloud deploymentsWho this book is for This book is for all IT professionals who want to take their first steps into the world of defensive security; from system admins and programmers to data analysts and data scientists with an interest in security. Experienced cybersecurity professionals working on broadening their knowledge and keeping up to date with the latest defensive developments will also find plenty of useful information in this book. You'll need a basic understanding of networking, IT, servers, virtualization, and cloud platforms before you get started with this book.

Computer and Communication Engineering Springer

Growth Poles of the Global Economy: Emergence, Changes and Future PerspectivesSpringer

Corporate Security Management DIANE Publishing

Security is a major consideration in the way that business and information technology systems are designed, built, operated, and managed. The need to be able to integrate security into those systems and the discussions with business functions and operations exists more than ever. This IBM® Redbooks® publication explores concerns that characterize security requirements of, and threats to, business and information technology (IT) systems. This book identifies many business drivers that illustrate these concerns, including managing risk and cost, and compliance to business policies and external regulations. This book shows how these

drivers can be translated into capabilities and security needs that can be represented in frameworks, such as the IBM Security Blueprint, to better enable enterprise security. To help organizations with their security challenges, IBM created a bridge to address the communication gap between the business and technical perspectives of security to enable simplification of thought and process. The IBM Security Framework can help you translate the business view, and the IBM Security Blueprint describes the technology landscape view. Together, they can help bring together the experiences that we gained from working with many clients to build a comprehensive view of security capabilities and needs. This book is intended to be a valuable resource for business leaders, security officers, and consultants who want to understand and implement enterprise security by considering a set of core security capabilities and services.

Challenges in Cybersecurity and Privacy - the European Research Landscape

Packt Publishing Ltd

The world of wireless and mobile devices is evolving day-to-day, with many individuals relying solely on their wireless devices in the workplace and in the home. The growing use of mobile devices demands that organizations become more educated in securing this growing technology and determining how to best protect their assets. Written by an industry expert, Wireless and Mobile Device Security explores the

evolution of wired networks to wireless networking and its impact on the corporate world. Using case studies and real-world events, it goes on to discuss risk assessments, threats, and vulnerabilities of wireless networks, as well as the security measures that should be put in place to mitigate breaches. The text closes with a look at the policies and procedures in place and a glimpse ahead at the future of wireless and mobile device security.

Privacy-Preserving in Mobile Crowdsensing Academic Press

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.

New Technologies, Development and Application Syngress

Strategy is a much-discussed, much-misunderstood topic among managers. In this new edition of The Strategic Manager, Harry Sminia continues to

focus on how strategy works in practice, questioning readers' existing expectations that strategy is a matter of strategic planning in order to help them to move into practicing strategy as an everyday activity. The book is based around six different strategy theories, individually presented and supplemented with useful lists of questions that encourage readers to become competent strategic thinkers. Bridging theory and practice, a range of real life case studies open a window into the real world of strategic management. Essential reading for postgraduate students and those in executive education, this text will also be a useful tool for managers trying to develop a better understanding of this easily confused subject.

Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution Oxford University Press, USA

Mobile communication has dramatically changed over the past decade with the diffusion of smartphones. Unlike the basic 2G mobile phones, which "merely" facilitated communication between individuals on the move, smartphones allow individuals to communicate, to entertain and inform themselves, to transact, to navigate, to take photos, and countless other things. Mobile communication has thus transformed society by allowing new forms of coordination, communication, consumption, social interaction, and access to news/entertainment. All of this is regardless of the space in which users

are immersed. Set in the context of the developed and the developing world, The Oxford Handbook of Mobile Communication and Society updates current scholarship surrounding mobile media and communication. The 43 chapters in this handbook examine mobile communication and its evolving impact on individuals, institutions, groups, societies, and businesses. Contributors examine the communal benefits, social consequences, theoretical perspectives, organizational potential, and future consequences of mobile communication. Topics covered include, among many other things, trends in the Global South, location-based services, and the "appification" of mobile communication and society.

Wireless and Mobile Device Security Springer Science & Business Media

This book contains the latest research work presented at the International Conference on Computing and Communication Systems (I3CS 2020) held at North-Eastern Hill University (NEHU), Shillong, India. The book presents original research results, new ideas and practical development experiences which concentrate on both theory and practices. It includes papers from all areas of information technology, computer science, electronics and communication engineering written by researchers, scientists, engineers and scholar students and experts from India and abroad.

Information Security Routledge

A guide with practical examples that gives you hands-on knowledge in

creating learning environments for Mobile devices using Moodle, while also empowering you to create your own effective mlearning course designs."Moodle for Mobile Learning" is primarily aimed at Moodle course practitioners – teachers, tutors, instructors, and learning and development professionals. It does not require you to have an in-depth knowledge about any mobile technologies. It is for anyone who has the desire to deliver great courses that allow their learners to interact using the devices in their pockets.

Guide to Bluetooth Security Springer Nature

April 2017 Mobile devices on the market today are some of the most complex and capable computing devices ever created. Although many can now match the capabilities of desktops and are being marketed as desktop replacements, they have features and capabilities not available to any desktop. They also sit in the broader mobile ecosystem giving them significantly more exposure. This means they share many of the same security threats as traditional desktop and laptop computers and are also exposed to more threats brought about by their mobility, complexity, and additional sensors. The impact of many of these threats can be magnified by the unique attributes of mobile devices. Why buy a book you can download for free? First you gotta find it and make sure it''s the latest version (not always easy). Then you gotta print it using a network printer you share with 100 other people -

and its outta paper - and the toner is low (take out the toner cartridge, shake it, then put it back). If it''s just 10 pages, no problem, but if it''s a 250-page book, you will need to punch 3 holes in all those pages and put it in a 3-ring binder. Takes at least an hour. An engineer that''s paid $75 an hour has to do this himself (who has assistant''s anymore?). If you are paid more than $10 an hour and use an ink jet printer, buying this book will save you money. It''s much more cost-effective to just order the latest version from Amazon.com This book is published by 4th Watch Books and includes copyright material. We publish compact, tightly-bound, full-size books (8 &#65533; by 11 inches), with glossy covers. 4th Watch Books is a Service Disabled Veteran-Owned Small Business (SDVOSB), and is not affiliated with the National Institute of Standards and Technology. For more titles published by 4th Watch Books, please visit: cybah.webplus.net A full copy of all the pertinent cybersecurity standards is available on DVD-ROM in the CyberSecurity Standards Library disc which is available at Amazon.com. NIST SP 500-299 NIST Cloud Computing Security Reference Architecture NIST SP 500-291 NIST Cloud Computing Standards Roadmap Version 2 NIST SP 500-293 US Government Cloud Computing Technology Roadmap Volume 1 & 2 NIST SP 500-293 US Government Cloud Computing Technology Roadmap Volume 3 DRAFT NIST SP 1800-8 Securing Wireless Infusion Pumps NISTIR 7497 Security Architecture Design Process for Health

Information Exchanges (HIEs) NIST SP 800-66 Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule NIST SP 1800-1 Securing Electronic Health Records on Mobile Devices NIST SP 800-177 Trustworthy Email NIST SP 800-184 Guide for Cybersecurity Event Recovery NIST SP 800-190 Application Container Security Guide NIST SP 800-193 Platform Firmware Resiliency Guidelines NIST SP 1800-1 Securing Electronic Health Records on Mobile Devices NIST SP 1800-2 Identity and Access Management for Electric Utilities NIST SP 1800-5 IT Asset Management: Financial Services NIST SP 1800-6 Domain Name Systems-Based Electronic Mail Security NIST SP 1800-7 Situational Awareness for Electric Utilities NIST SP 500-288 Specification for WS-Biometric Devices (WS-BD) NIST SP 500-304 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information NIST SP 800-32 Public Key Technology and the Federal PKI Infrastructure NIST SP 800-63-3 Digital Identity Guidelines NIST SP 800-63a Digital Identity Guidelines - Enrollment and Identity Proofing NIST SP 800-63b Digital Identity Guidelines - Authentication and Lifecycle Management NIST SP 800-63c Digital Identity Guidelines NIST SP 800-178 Comparison of Attribute Based Access Control (ABAC) Standards

Handbook of Research on Knowledge and Organization Systems in Library and Information Science Packt Publishing Ltd

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
Mastering Defensive Security GRIN Verlag
The fast-food worker finds refuge in a bathroom stall to respond to her boyfriend's fifth message in an hour. The human resources manager sees a colleague sending a stream of text messages during a meeting and quickly grabs her mobile to make sure she's also multitasking. These scenarios are common, but unique to the 21st century. Until the early 2000s, workplaces provided most of the computers and portable devices that employees used to perform their jobs and communicate with others. Today, people bring their own mobile devices to work and create new norms for how communication occurs in the workplace. Managers and organizations respond by setting and enforcing new policies that are intended to help them navigate the ever-changing mobile-communication environment. In Negotiating Control: Organizations and Mobile Communication, Keri K. Stephens responds to the struggles of employees, organizations, and even friends and family, as they try to understand new norms for connectedness in the workplace. Drawing on over two decades of her own research and fieldwork, , representing people in over 35 different types of jobs, Stephens claims that though people assume mobile communication is a uniform practice, there are underlying -- and often hidden -- issues of control and power at play,

which shape how people are permitted and expected to use mobiles to communicate while working. The accounts Stephens offers reveal the many ways that these portable tools are actually used across work environments today, integrating information, communication, and data, and connecting people in expected and often conflicting ways.