Delivering Security And Privacy For E Business

ASHER LEVY

Enhancing Security and Privacy for Mobile Systems John Wiley & Sons
This book presents an in-depth overview of recent work related to the safety, security, and privacy of cyber-physical systems (CPSs). It brings together contributions from leading researchers in networked control systems and closely related fields to discuss overarching aspects of safety, security, and privacy; characterization of attacks; and solutions to detecting and mitigating such attacks. The book begins by providing an insightful taxonomy of problems, challenges and techniques related to safety, security, and privacy for CPSs. It then moves through a thorough discussion of various control-based solutions to these challenges, including cooperative fault-tolerant and resilient control and estimation, detection of attacks and security metrics, watermarking and encrypted control, privacy and a novel defense approach based on deception. The book concludes by discussing risk management and cyber-insurance challenges in CPSs, and by presenting the future outlook for this area of research as a whole. Its wide-ranging collection of varied works in the emerging fields of security and privacy in networked control systems makes this book a benefit to both academic researchers and advanced practitioners interested in implementing diverse applications in the fields of IoT, cooperative autonomous vehicles and the smart cities of the future.
Handbook of Research on High Performance and Cloud Computing in Scientific Research and Education OECD Publishing
Cloud computing has quickly become the next big step in security development for companies and institutions all over the world. With the technology changing so rapidly, it is important that businesses carefully consider the available advancements and opportunities before implementing cloud computing in their organizations. The Handbook of Research on Security Considerations in Cloud Computing brings together discussion on current approaches to cloud-based technologies and assesses the possibilities for future advancements in this field. Highlighting the need for consumers to understand the unique nature of cloud-delivered security and to evaluate the different aspects of this service to verify if it will meet their needs, this book is an essential reference source for researchers, scholars, postgraduate students, and developers of cloud security systems.
Hearing Before a Subcommittee of the Committee on Government Operations, House of Representatives, Ninety-eighth Congress, Second Session, March 18, 1984 Commonwealth Secretariat
With the ever-increasing demands of people's social interactions, traditional online social networking applications are being shifted to the mobile ones, enabling users' social networking and interactions anywhere anytime. Due to the portability and pervasiveness of mobile devices, such as smartphones, wearable devices and tablets, Mobile Social Network (MSN), as a promising social network platform, has become increasingly popular

and brought immense benefits. In MSN, users can easily discover and chat with social friends in the vicinity even without the Internet; vehicle drivers and passengers can exchange traffic information, videos or images with other vehicles on the road; customers in a shopping mall can share sale information and recommend it to their friends. With MSNs, massive opportunities are created to facilitate people's social interactions and enlarge the inherent social circle. However, the flourish of MSNs also hinges upon fully understanding and managing the challenges, such as security threats and privacy leakage. Security and privacy concerns rise as the boom of MSN applications comes up, but few users have paid adequate attentions to protect their privacy-sensitive information from disclosing. First of all, to initiate social interactions, users sometimes exchange their social interests or preferences with each other (including strangers in the vicinity) without sufficient protections. As such, some private information may be inferred from the exchanged social interests by attackers and untrusted users. Secondly, some malicious attackers might forge fake identities or false contents, such as spam and advertisements, to disrupt MSNs or mislead other users. These attackers could even collude and launch a series of security threats to MSNs. In addition, massive social network data are usually stored in untrusted cloud servers, where data confidentiality, authentication, access control and privacy are of paramount importance. Last but not least, the trade-off between data availability and privacy should be taken into account when the data are stored, queried and processed for various MSN applications. Therefore, novel security and privacy techniques become essential for MSN to provide sufficient and adjustable protections. In this thesis, we focus on security and privacy for MSNs. Based on the MSN architecture and emerging applications, we first investigate security and privacy requirements for MSNs and introduce several challenging issues, i.e., spam, misbehaviors and privacy leakage. To tackle these problems, we propose efficient security and privacy preservation schemes for MSNs. Specifically, the main contributions of this thesis can be three-fold. Firstly, to address the issues of spam in autonomous MSNs, we propose a personalized fine-grained spam filtering scheme (PIF), which exploits social characteristics during data delivery. The PIF allows users to create personalized filters according to their social interests, and enables social friends to hold these filters, discarding the unwanted data before delivery. We also design privacy-preserving coarse-grained and fine-grained filtering mechanisms in the PIF to not only enable the filtering but also prevent users' private information included in the filters from disclosing to untrusted entities. Secondly, to detect misbehaviors during MSN data sharing, we propose a social-based mobile Sybil detection scheme (SMSD). The SMSD detects Sybil attackers by differentiating the abnormal pseudonym changing and contact behaviors, since Sybil attackers frequently or rapidly change their pseudonyms to cheat legitimate users. As the volume of contact data from users keeps increasing, the SMSD utilizes local cloud servers to store and process the users' contact data such that the burden of mobile users is alleviated. The SMSD also detects the collusion attacks and prevents user's data from malicious modification when employing the untrusted local cloud server for the detection. Thirdly, to achieve the trade-off between privacy and data availability, we investigate a centralized social network application, which exploits social network to enhance human-to-human infection analysis. We integrate social network data and health data to jointly analyze the instantaneous infectivity during human-to-human contact, and propose a novel privacy-preserving infection analysis approach (PIA). The PIA enables the collaboration among different cloud servers (i.e., social network cloud server and health cloud server). It employs a privacy-preserving data query method based on conditional oblivious transfer to enable data sharing and prevent data from disclosing to untrusted entities. A privacy-preserving classification-based infection analysis method is also proposed to enable the health cloud server to infer infection spread but preserve privacy simultaneously. Finally, we summarize the thesis and share several open research directions in MSNs. The developed security solutions and research results in this thesis should provide a useful step towards better understanding and implementing secure and privacy-preserving MSNs.

Big Data Technologies and Applications IGI Global

INTERNET OF HEALTHCARE THINGS The book addresses privacy and security issues providing solutions through authentication and authorization mechanisms, blockchain, fog computing, machine learning algorithms, so that machine learning-enabled IoT devices can deliver information concealed in data for fast, computerized responses and enhanced decision-making. The main objective of this book is to motivate healthcare providers to use telemedicine facilities for monitoring patients in urban and rural areas and gather clinical data for further research. To this end, it provides an overview of the Internet of Healthcare Things (IoHT) and discusses one of the major threats posed by it, which is the data security and data privacy of health records. Another major threat is the combination of numerous devices and protocols, precision time, data overloading, etc. In the IoHT, multiple devices are connected and communicate through certain protocols. Therefore, the application of emerging technologies to mitigate these threats and provide secure data communication over the network is discussed. This book also discusses the integration of machine learning with the IoHT for analyzing huge amounts of data for predicting diseases more accurately. Case studies are also given to verify the concepts presented in the book. Audience Researchers and industry engineers in computer science, artificial intelligence, healthcare sector, IT professionals, network administrators, cybersecurity experts.

Case Studies in Secure Computing John Wiley & Sons

The communication field is evolving rapidly in order to keep up with society’s demands. As such, it becomes imperative to research and report recent advancements in computational intelligence as it applies to communication networks. The Handbook of Research on Recent Developments in Intelligent Communication Application is a pivotal reference source for the latest developments on emerging data communication applications. Featuring extensive coverage across a range of relevant perspectives and topics, such as satellite communication, cognitive radio networks, and wireless sensor networks, this book is ideally designed for engineers, professionals, practitioners, upper-level students, and academics seeking current information on emerging communication networking trends.

International Conferences, SecTech and DRBC 2010, Held as Part of the Future Generation Information Technology Conference, FGIT 2010, Jeju Island, Korea, December 13-15, 2010. Proceedings Elsevier

Improvements in health services require continual attention and dedication to ensure proper care and treatment for citizens. To support this endeavor, professionals rely more and more on the application of information systems and technologies to promote the overall quality of modern healthcare. Maximizing Healthcare Delivery and Management through Technology Integration is an authoritative reference source for the latest scholarly research on the integration of ICT within the health services sector. Featuring comprehensive coverage on a range of topics from technical and non-technical perspectives, this book is an essential reference source for IT specialists, professionals, managers, and students seeking current research on the growing relationship between technology and healthcare.

Security and Privacy for Mobile Healthcare Networks John Wiley & Sons

The auditor's guide to ensuring correct security and privacy practices in a cloud computing environment Many organizations are reporting or projecting a significant cost savings through the use of cloud computing—utilizing shared computing resources to provide ubiquitous access for organizations and end users. Just as many organizations, however, are expressing concern with security and privacy issues for their organization's data in the "cloud." Auditing Cloud Computing provides necessary guidance to build a proper audit to ensure operational integrity and customer data protection, among other aspects, are addressed for cloud based resources. Provides necessary guidance to ensure auditors address security and privacy aspects that through a proper audit can provide a specified level of assurance for an organization's resources Reveals effective methods for evaluating the security and privacy practices of cloud services A cloud computing reference for auditors and IT security professionals, as well as those preparing for certification credentials, such as Certified Information Systems Auditor (CISA) Timely and practical, Auditing Cloud Computing expertly provides information to assist in preparing for an audit addressing cloud computing security and privacy for both businesses and cloud based service providers.

Internet of Healthcare Things IET

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.

Information Security Theory and Practice. Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems Springer

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 initiatives. 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

Data Security and Privacy Third Edition Syngress

It is essential for an organization to know before involving themselves in cloud computing and big data, what are the key security requirements for applications and data processing. Big data and cloud computing are integrated together in practice. Cloud computing offers massive storage, high computation power, and distributed capability to support processing of big data. In such an integrated environment the security and privacy concerns involved in both technologies become combined. This book discusses these security and privacy issues in detail and provides necessary insights into cloud computing and big data integration. It will be useful in enhancing the body of knowledge concerning innovative technologies offered by the research community in the area of cloud computing and big data. Readers can get a better understanding of the basics of cloud computing, big data, and security mitigation techniques to deal with current challenges as well as future research opportunities.

Handbook of Research on Recent Developments in Intelligent Communication Application Springer

Abstract: With the growing trend of mobile device utilization and recent exploitation of both security and privacy, there is a growing need to ensure that the security and privacy controls of these devices are sound. Standard controls that are provided as part of the operating system do not allow the level of control to let the user decide not only if an application can access their data, but what other operations can the application perform with their data. Solutions to this problem have been researched with a focus primarily on providing a custom operating system by rooting/jailbreaking a device. However this approach is not sustainable as each minor update to the operating system requires a new modified OS and the user to install the custom OS. Additionally a user jailbreaking or rooting the device requires the user to know how to perform the operation correctly and they can lose the inherent trust provided by the OS. In this dissertation research, we focus on solving the problem of providing enhanced security and privacy controls for mobile operating systems without requiring modification to the operating system. Through this research our contributions are as follows: 1) We provide a security and privacy enhanced framework that provides the user with fine grained control of security and privacy of their mobile device. 2) We provide a formal ontology for describing the policy, knowledge and activity used to enforce the policy, and describe their relationships. 3) We provide a web based proxy solution that can be utilized to effectively enforce the policies described in the aforementioned ontology without requiring modification to the operating system or application. From our contributions, we provide sustainable solutions to the problem of providing fine grained security and privacy controls for mobile devices without compromising the experience and exhausting the resources that exist on a mobile device.

Networked RFID Systems and Lightweight Cryptography Springer Nature

You may regard cloud computing as an ideal way for your company to control IT costs, but do you know how private and secure this service really is? Not many people do. With Cloud Security and Privacy, you'll learn what's at stake when you trust your data to the cloud, and what you can do to keep your virtual infrastructure and web applications secure. Ideal for IT staffers, information security and privacy practitioners, business managers, service providers, and investors alike, this book offers you sound advice from three well-known authorities in the tech security world. You'll learn detailed information on cloud computing security that-until now-has been sorely lacking. Review the current state of data security and storage in the cloud, including confidentiality, integrity, and availability Learn about the identity and access management (IAM) practice for authentication, authorization, and auditing of the users accessing cloud services Discover which security management frameworks and standards are relevant for the cloud Understand the privacy aspects you need to consider in the cloud, including how they compare with traditional computing models Learn the importance of audit and compliance functions within the cloud, and the various standards and frameworks to consider Examine security delivered as a service-a different facet of cloud security

7th International Conference, ICISS 2011, Kolkata, India, December 15-19, 2011, Proceedings Springer

This volume constitutes the refereed proceedings of the 6th IFIP WG 11.2 International Workshop on Information Security Theory and Practice: Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems, WISTP 2012, held in Egham, UK, in June 2012. The 9 revised full papers and 8 short papers presented together with three keynote speeches were carefully reviewed and selected from numerous submissions. They are organized in topical sections on protocols, privacy, policy and access control, multi-party computation, cryptography, and mobile security.

Achievements and Trends IGI Global

This book examines state-of-art research on designing healthcare applications with the consideration of security and privacy. It explains the Mobile Healthcare Network (MHN) architecture and its diverse applications, and reviews the existing works on security and privacy for MHNs. Critical future challenges and research problems are also identified. Using a Quality-of-Protection perspective, the authors provide valuable insights on security and privacy preservation for MHNs. Some promising solutions are proposed to accommodate the issues of secure health data transmission, misbehavior detection, health data processing with privacy preservation and access control in MHNs. Specifically, the secure health data aggregation explores social spots to help forward health data and enable users to select the optimal relay according to their social ties and health data priority. The secure aggregation achieves the desirable delivery ratio with reasonable communication costs and lower delay for the data in different priorities. A proposed misbehavior detection scheme distinguishes Sybil attackers from normal users by comparing their mobile contacts and pseudonym changing behaviors. The detection accuracy is high enough to resist various Sybil attacks including forgery. In addition, the health data processing scheme can analyze the encrypted health data and preserve user’s privacy at the same time. Attribute based access control can achieve fine-grained acces s control with user-defined access policy in MHNs. Security and Privacy for Mobile Healthcare Networks is designed for researchers and advanced-level students interested in healthcare security and secure data transmission.

Machine Learning for Security and Privacy Springer

"This encyclopedia is a research reference work documenting the past, present, and possible future directions of knowledge management"--Provided by publisher.

The Canadian Experience of Public Sector Management Reform (1995-2002). Springer

As information systems used for research and educational purposes have become more complex, there has been an increase in the need for new computing architecture. High performance and cloud computing provide reliable and cost-effective information technology infrastructure that enhances research and educational processes. Handbook of Research on High Performance and Cloud Computing in Scientific Research and Education presents the applications of cloud computing in various settings, such as scientific research, education, e-learning, ubiquitous learning, and social computing. Providing various examples, practical solutions, and applications of high performance and cloud computing; this book is a useful reference for professionals and researchers discovering the applications of information and communication technologies in science and education, as well as scholars seeking insight on how modern technologies support scientific research.

Security and Privacy Trends in Cloud Computing and Big Data IGI Global

This book provides a thorough treatment of privacy and security issues for researchers in the fields of smart grids, engineering, and computer science. It presents comprehensive insight to understanding the big picture of privacy and security challenges in both physical and information aspects of smart grids. The authors utilize an advanced interdisciplinary approach to address the existing security and privacy issues and propose legitimate countermeasures for each of them in the standpoint of both computing and electrical engineering. The proposed methods are theoretically proofed by mathematical tools and illustrated by real-world examples.

Safety, Security and Privacy for Cyber-Physical Systems Springer Publishing Company

This book consists of a collection of works on utilizing the automatic identification technology provided by Radio Frequency Identification (RFID) to address the problems of global counterfeiting of goods. The book presents current research, directed to securing supply chains against the efforts of counterfeit operators, carried out at the Auto-ID Labs around the globe. It assumes very little knowledge on the part of the reader on Networked RFID systems as the material provided in the introduction familiarizes the reader with concepts, underlying principles and vulnerabilities of modern RFID systems.

Information Security and Cryptology - ICISC 2010 IGI Global

This book constitutes the refereed proceedings of the 7th International Conference on Information Systems Security, ICISS 2011, held in Kolkata, India, in December 2011. The 20 revised full papers presented together with 4 short papers and 4 invited papers were carefully reviewed and selected from 105 submissions. The papers are organized in topical sections on access control and authorization, malwares and anomaly detection, crypto and steganographic systems, verification and analysis, wireless and mobile systems security, Web and network security.

Trust, Security and Privacy for Big Data IGI Global

This book presents chapters from diverse range of authors on different aspects of how Blockchain and IoT are converging and the impacts of these developments. The book provides an extensive cross-sectional and multi-disciplinary look into this trend and how it affects artificial intelligence, cyber-physical systems, and robotics with a look at applications in aerospace, agriculture, automotive, critical infrastructures, healthcare, manufacturing, retail, smart transport systems, smart cities, and smart healthcare. Cases include the impact of Blockchain for IoT Security; decentralized access control systems in IoT; Blockchain architecture for scalable access management in IoT; smart and sustainable IoT applications incorporating Blockchain, and more. The book presents contributions from international academics, researchers, and practitioners from diverse perspectives. Presents how Blockchain and IoT are converging and the impacts of these developments on technology and its application; Discusses IoT and Blockchain from cross-sectional and multi-disciplinary perspectives; Includes contributions from researchers, academics, and professionals from around the world.

Related with Delivering Security And Privacy For E Business:

• Graveyard Keeper Autopsy Guide : click here