Byod Le Security Crowd Research Partners

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics XII describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: Themes and Issues, Mobile Device Forensics, Network Forensics, Cloud Forensics, Social Media Forensics, Image Forensics, Forensic Techniques, and Forensic Tools. This book is the twelfth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of twenty edited papers from the Twelfth Annual IFIP WG 11.9 International Conference on Digital Forensics, held in New Delhi, India in the winter of 2016. Advances in Digital Forensics XII is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in

research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson, Chair, IFIP WG 11.9 on Digital Forensics, is a Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.

Similar to unraveling a math word problem, Security Intelligence: A Practitioner's Guide to Solving Enterprise Security Challenges guides you through a deciphering process that translates each security goal into a set of security variables, substitutes each variable with a specific security technology domain, formulates the equation that is the deployment strategy, then verifies the solution against the original problem by analyzing security incidents and mining hidden breaches, ultimately refines the security formula iteratively in a perpetual cycle. You will learn about: Secure proxies – the necessary extension of the endpoints Application identification and control – visualize the threats Malnets – where is the source of infection and who are the pathogens Identify the security breach – who was the victim and what was the lure Security in Mobile computing – SNAFU With this book, you will be able to: Identify the relevant solutions to secure the infrastructure Construct policies that provide flexibility to the users so to ensure productivity Deploy effective defenses against the ever evolving web threats Implement solutions that are compliant to relevant rules and regulations Offer insight to developers who are building new security solutions and products

Healthcare Information Management Systems, 4th edition, is a comprehensive volume addressing the technical, organizational and management issues confronted by healthcare professionals in the selection, implementation and management of healthcare information

systems. With contributions from experts in the field, this book focuses on topics such as strategic planning, turning a plan into reality, implementation, patient-centered technologies, privacy, the new culture of patient safety and the future of technologies in progress. With the addition of many new chapters, the 4th Edition is also richly peppered with case studies of implementation. The case studies are evidence that information technology can be implemented efficiently to yield results, yet they do not overlook pitfalls, hurdles, and other challenges that are encountered. Designed for use by physicians, nurses, nursing and medical directors, department heads, CEOs, CFOs, CIOs, COOs, and healthcare informaticians, the book aims to be a indispensible reference.

This professional guide and reference examines the challenges of assessing security vulnerabilities in computing infrastructure. Various aspects of vulnerability assessment are covered in detail, including recent advancements in reducing the requirement for expert knowledge through novel applications of artificial intelligence. The work also offers a series of case studies on how to develop and perform vulnerability assessment techniques using start-of-the-art intelligent mechanisms. Topics and features: provides tutorial activities and thought-provoking questions in each chapter, together with numerous case studies; introduces the fundamentals of vulnerability assessment, and reviews the state of the art of research in this area; discusses vulnerability assessment frameworks, including frameworks for industrial control and cloud systems; examines a range of applications that make use of artificial intelligence to enhance the vulnerability assessment processes; presents visualisation techniques that can be used to assist the vulnerability assessment process. In addition to serving the needs of security practitioners and researchers, this accessible volume is also ideal

for students and instructors seeking a primer on artificial intelligence for vulnerability assessment, or a supplementary text for courses on computer security, networking, and artificial intelligence.

The increasing use of mobile devices in work contexts has the potential to alter our work and learning practices. This is particularly true for knowledge workers. In addressing the implications of this transformation the book offers a multi-faceted collection of different concepts and cases of mobile learning in work environments from international contexts. The contributions are centred on the question of how individual users and organisations can harness mobile devices for learning and education. The range of examples presented in this book demonstrates that mobile devices foster situated approaches to learning in and across work contexts. The book is targeted at both practitioners - trainers or managers in charge of in-company training - and researchers, who are interested in designing, implementing or evaluating work-based mobile learning.

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

This book provides the most current and comprehensive overview available today of the critical role of information systems in emergency response and preparedness. It includes contributions from leading scholars, practitioners, and industry researchers, and covers all phases of disaster management - mitigation, preparedness, response, and recovery. 'Foundational' chapters provide a design framework and review ethical issues. 'Context' chapters describe the characteristics of individuals and organizations in which EMIS are designed and studied. 'Case Study' chapters include systems for distributed microbiology laboratory diagnostics to detect possible epidemics or bioterrorism, humanitarian MIS, and response coordination systems.

'Systems Design and Technology' chapters cover simulation, geocollaborative systems, global disaster impact analysis, and environmental risk analysis. Throughout the book, the editors and contributors give special emphasis to the importance of assessing the practical usefulness of new information systems for supporting emergency preparedness and response, rather than drawing conclusions from a theoretical understanding of the potential benefits of new technologies.

Modern critical infrastructures comprise of many interconnected cyber and physical assets, and as such are large scale cyber-physical systems. Hence, the conventional approach of securing these infrastructures by addressing cyber security and physical security separately is no longer effective. Rather more integrated approaches that address the security of cyber and physical assets at the same time are required. This book presents integrated (i.e. cyber and physical) security approaches and technologies for the critical infrastructures that underpin our societies. Specifically, it introduces advanced techniques for threat detection, risk assessment and security information sharing, based on leading edge technologies like machine learning, security knowledge modelling, IoT security and distributed ledger infrastructures. Likewise, it presets how established security technologies like Security Information and Event Management (SIEM), pen-testing, vulnerability assessment and security data analytics can be used in the context of integrated Critical Infrastructure Protection. The novel methods and techniques of the book are exemplified in case studies involving critical infrastructures in four industrial sectors, namely finance, healthcare, energy and communications. The peculiarities of critical infrastructure protection in each one of these sectors is discussed and addressed based on sector-specific solutions. The advent of the fourth industrial revolution (Industry 4.0) is

expected to increase the cyber-physical nature of critical infrastructures as well as their interconnection in the scope of sectorial and cross-sector value chains. Therefore, the demand for solutions that foster the interplay between cyber and physical security, and enable Cyber-Physical Threat Intelligence is likely to explode. In this book, we have shed light on the structure of such integrated security systems, as well as on the technologies that will underpin their operation. We hope that Security and Critical Infrastructure Protection stakeholders will find the book useful when planning their future security strategies.

Iot Security IssuesWalter de Gruyter GmbH & Co KG

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.

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

This book "provides managers with an awareness of the issues involved in managing change, moving them beyond "one-best way" approaches and providing them with access to multiple perspectives that they can draw upon in order to enhance their success in producing organizational change. These multiple perspectives provide a theme for the text as well as a framework for the way each chapter outlines different options open to managers in helping them to identify, in a reflective way, the actions and choices open to them."--Cover.

Modernizing Learning: Building the Future Learning Ecosystem is an implementation blueprint for connecting learning experiences across time and space. This co-created plan represents an advancement of how and where learning will occur in the future. Extensive learning and technological research has been conducted across the myriad disciplines and communities needed to develop this holistic maturation of the learning continuum. These advancements have created the opportunity for formal and informal learning experiences to be accessible anywhere, anytime, and to be personalized to individual needs. However, for full implementation and maximal benefits for learners of all ages and within all communities to be achieved, it is necessary to centralize and coordinate the required connections across technology, learning science, and the greater supporting structures. Accordingly, the ADL Initiative has taken the lead in this

coordination process, connecting Government, Military, Academia, Industry, and K-12 teachers, instructors, technologists, researchers, and implementers to create and execute a coordinated transition process. Input was included from stakeholders, communities, and supporting entities which will be involved in this advancement of the life-long learning ecosystem.

Evolve your traditional intranet platform into a next-generation digital workspace with this comprehensive book. Through in-depth coverage of strategies, methods, and case studies, you will learn how to design and build an employee experience platform (EXP) for improved employee productivity, engagement, and collaboration. In Build a Next-Generation Digital Workplace, author Shailesh Kumar Shivakumar takes you through the advantages of EXPs and shows you how to successfully implement one in your organization. This book provides extensive coverage of topics such as EXP design, user experience, content strategy, integration, EXP development, collaboration, and EXP governance. Real-world case studies are also presented to explore practical applications. Employee experience platforms play a vital role in engaging, empowering, and retaining the employees of an organization. Next-generation workplaces demand constant innovation and responsiveness, and this book readies you to fulfill that need with an employee experience platform. You will: Understand key design elements of EXP, including the visual design, EXP strategy, EXP transformation themes, information architecture, and navigation design. Gain insights into end-to-end EXP

topics needed to successfully design, implement, and maintain next-generation digital workplace platforms. Study methods used in the EXP lifecycle, such as requirements and design, development, governance, and maintenance Execute the main steps involved in digital transformation of legacy intranet platforms to EXP. Discover emerging trends in digital workplace such as gamification, machine-led operations model and maintenance model, employee-centric design (including persona based design and employee journey mapping), cloud transformation, and design transformation. Comprehend proven methods for legacy Intranet modernization, collaboration, solution validation, migration, and more. Who This Book Is For Digital enthusiasts, web developers, digital architects, program managers, and more.

This book presents original contributions on the theories and practices of emerging Internet, Data and Web technologies and their applications in businesses, engineering and academia. As a key feature, it addresses advances in the life-cycle exploitation of data generated by digital ecosystem technologies. The Internet has become the most proliferative platform for emerging large-scale computing paradigms. Among these, Data and Web technologies are two of the most prominent paradigms, manifesting in a variety of forms such as Data Centers, Cloud Computing, Mobile Cloud, Mobile Web Services, and so on. These technologies altogether create a digital ecosystem whose cornerstone is the data cycle, from capturing to processing, analysis and visualization. The need to investigate various research and development issues in this digital

ecosystem has been made even more pressing by the ever-increasing demands of real-life applications, which are based on storing and processing large amounts of data. Given its scope, the book offers a valuable asset for all researchers, software developers, practitioners and students interested in the field of Data and Web technologies.

GSV's aspirational vision for how to address society's greatest challenge...ensuring that everyone has equal opportunity to participate in the future.

Minimize Power Consumption and Enhance User ExperienceEssential for high-speed fifth-generation mobile networks, mobile cloud computing (MCC) integrates the power of cloud data centers with the portability of mobile computing devices. Mobile Cloud Computing: Architectures, Algorithms and Applications covers the latest technological and architectura

This handbook provides an overview of the research on the changing nature of work and workers by marshalling interdisciplinary research to summarize the empirical evidence and provide documentation of what has actually changed. Connections are explored between the changing nature of work and macro-level trends in technological change, income inequality, global labor markets, labor unions, organizational forms, and skill polarization, among others. This edited volume also reviews evidence for changes in workers, including generational change (or lack thereof), that has accumulated across domains. Based on documented changes in work and worker behavior, the handbook derives implications for a range of management functions, such as selection, performance management, leadership, workplace ethics, and employee well-being. This evaluation of the extent of changes and their impact

gives guidance on what best practices should be put in place to harness these developments to achieve success.

IoT Security Issues looks at the burgeoning growth of devices of all kinds controlled over the Internet of all varieties, where product comes first and security second. In this case, security trails badly. This book examines the issues surrounding these problems, vulnerabilities, what can be done to solve the problem, investigating the stack for the roots of the problems and how programming and attention to good security practice can combat the problems today that are a result of lax security processes on the Internet of Things. This book is for people interested in understanding the vulnerabilities on the Internet of Things, such as programmers who have not yet been focusing on the IoT, security professionals and a wide array of interested hackers and makers. This book assumes little experience or knowledge of the Internet of Things. To fully appreciate the book, limited programming background would be helpful for some of the chapters later in the book, though the basic content is explained. The author, Alasdair Gilchrist, has spent 25 years as a company director in the fields of IT, Data Communications, Mobile Telecoms and latterly Cloud/SDN/NFV technologies, as a professional technician, support manager, network and security architect. He has project-managed both agile SDLC software development as well as technical network architecture design. He has experience in the deployment and integration of systems in enterprise, cloud, fixed/mobile telecoms, and service provider networks. He is therefore knowledgeable in a wide range of technologies and has written a number of books in related fields.

The seventh edition of Spanish banking group BBVA's annual series is dedicated to unveiling the new digital business models for twenty-first century companies. Esteemed experts from

BBVA, "The Economist," Harvard University, Columbia Business School, Geoffrey Moore Consulting and more, contribute texts in accessible language.

The five-volume set LNCS 12932-12936 constitutes the proceedings of the 18th IFIP TC 13 International Conference on Human-Computer Interaction, INTERACT 2021, held in Bari, Italy, in August/September 2021. The total of 105 full papers presented together with 72 short papers and 70 other papers in these books was carefully reviewed and selected from 680 submissions. The contributions are organized in topical sections named: Part I: affective computing; assistive technology for cognition and neurodevelopment disorders; assistive technology for mobility and rehabilitation; assistive technology for visually impaired; augmented reality; computer supported cooperative work. Part II: COVID-19 & HCI; croudsourcing methods in HCI; design for automotive interfaces; design methods; designing for smart devices & IoT; designing for the elderly and accessibility; education and HCI; experiencing sound and music technologies; explainable AI. Part III: games and gamification; gesture interaction; human-centered AI; human-centered development of sustainable technology; human-robot interaction; information visualization; interactive design and cultural development. Part IV: interaction techniques; interaction with conversational agents; interaction with mobile devices; methods for user studies; personalization and recommender systems; social networks and social media; tangible interaction; usable security. Part V: user studies; virtual reality; courses; industrial experiences; interactive demos; panels; posters; workshops. The chapter ‘Stress Out: Translating Real-World Stressors into Audio-Visual Stress Cues in VR for Police Training’ is open access under a CC BY 4.0 license at link.springer.com. The chapter ‘WhatsApp in Politics?! Collaborative Tools Shifting Boundaries’ is open access under a CC BY 4.0 license

at link.springer.com.

This book constitutes the refereed proceedings of the IFIP WG 8.6 International Working Conference "Creating Value for All Through IT" on Transfer and Diffusion of IT, TDIT 2014, held in Aalborg, Denmark, in June 2014. The 18 revised full papers presented together with 5 research-in-progress papers, 2 experience reports and a panel were carefully reviewed and selected from 37 submissions. The full papers are organized in the following topical sections: creating value; creating value through software development; and creating value through applications.

Technological change is ridden with conflicts, bifurcations and unexpected developments. Neurocapitalism takes us on an extraordinarily original journey through the effects that cutting-edge technology has on cultural, anthropological, socio-economic and political dynamics. Today, neurocapitalism shapes the technological production of the commons, transforming them into tools for commercialization, automatic control, and crisis management. But all is not lost: in highlighting the growing role of General Intellect's autonomous and cooperative production through the development of the commons and alternative and antagonistic uses of new technologies, Giorgio Griziotti proposes new ideas for the organization of the multitudes of the new millennium.

As more and more devices become interconnected through the Internet of Things (IoT), there is an even greater need for this book,which explains the technology, the internetworking, and applications that are making IoT an everyday reality. The book begins with a discussion of IoT "ecosystems" and the technology that enables them, which includes: Wireless Infrastructure and Service Discovery Protocols Integration Technologies and Tools Application and Analytics

Enablement Platforms A chapter on next-generation cloud infrastructure explains hosting IoT platforms and applications. A chapter on data analytics throws light on IoT data collection, storage, translation, real-time processing, mining, and analysis, all of which can yield actionable insights from the data collected by IoT applications. There is also a chapter on edge/fog computing. The second half of the book presents various IoT ecosystem use cases. One chapter discusses smart airports and highlights the role of IoT integration. It explains how mobile devices, mobile technology, wearables, RFID sensors, and beacons work together as the core technologies of a smart airport. Integrating these components into the airport ecosystem is examined in detail, and use cases and real-life examples illustrate this IoT ecosystem in operation. Another in-depth look is on envisioning smart healthcare systems in a connected world. This chapter focuses on the requirements, promising applications, and roles of cloud computing and data analytics. The book also examines smart homes, smart cities, and smart governments. The book concludes with a chapter on IoT security and privacy. This chapter examines the emerging security and privacy requirements of IoT environments. The security issues and an assortment of surmounting techniques and best practices are also discussed in this chapter.

Actionable guidance and expert perspective for real-world cybersecurity The Cyber Risk Handbook is the practitioner's guide to implementing, measuring and improving the counter-cyber capabilities of the modern enterprise. The first resource of its kind, this book provides authoritative guidance for real-world situations, and cross-functional solutions for enterprise-wide improvement.

Beginning with an overview of counter-cyber evolution, the discussion quickly turns practical with design and implementation guidance for the range of capabilities expected of a robust cyber risk management system that is integrated with the enterprise risk management (ERM) system. Expert contributors from around the globe weigh in on specialized topics with tools and techniques to help any type or size of organization create a robust system tailored to its needs. Chapter summaries of required capabilities are aggregated to provide a new cyber risk maturity model used to benchmark capabilities and to road-map gap-improvement. Cyber risk is a fast-growing enterprise risk, not just an IT risk. Yet seldom is guidance provided as to what this means. This book is the first to tackle in detail those enterprise-wide capabilities expected by Board, CEO and Internal Audit, of the diverse executive management functions that need to team up with the Information Security function in order to provide integrated solutions. Learn how cyber risk management can be integrated to better protect your enterprise Design and benchmark new and improved practical counter-cyber capabilities Examine planning and implementation approaches, models, methods, and more Adopt a new cyber risk maturity model tailored to your enterprise needs The need to manage cyber risk across the enterprise—inclusive of the IT operations—is a growing concern as massive data

breaches make the news on an alarmingly frequent basis. With a cyber risk management system now a business-necessary requirement, practitioners need to assess the effectiveness of their current system, and measure its gap-improvement over time in response to a dynamic and fast-moving threat landscape. The Cyber Risk Handbook brings the world's best thinking to bear on aligning that system to the enterprise and vice-a-versa. Every functional head of any organization must have a copy at-hand to understand their role in achieving that alignment.

Management Information Systems provides comprehensive and integrative coverage of essential new technologies, information system applications, and their impact on business models and managerial decision-making in an exciting and interactive manner. The twelfth edition focuses on the major changes that have been made in information technology over the past two years, and includes new opening, closing, and Interactive Session cases.

Learn the ins and outs of the IT security field and efficiently prepare for the CompTIA Security+ Exam SY0-601 with one easy-to-follow resource CompTIA Security+ Review Guide: Exam SY0-601, Fifth Edition helps you to efficiently review for the leading IT security certification—CompTIA Security+ SY0-601. Accomplished author and security expert James Michael Stewart covers each

domain in a straightforward and practical way, ensuring that you grasp and understand the objectives as quickly as possible. Whether you're refreshing your knowledge or doing a last-minute review right before taking the exam, this guide includes access to a companion online test bank that offers hundreds of practice questions, flashcards, and glossary terms. Covering all five domains tested by Exam SY0-601, this guide reviews: Attacks, Threats, and Vulnerabilities Architecture and Design Implementation Operations and Incident Response Governance, Risk, and Compliance This newly updated Fifth Edition of CompTIA Security+ Review Guide: Exam SY0-601 is not just perfect for anyone hoping to take the SY0-601 Exam, but it is also an excellent resource for those wondering about entering the IT security field.

This book was prepared as the Final Publication of COST Action IC0703 "Data Traffic Monitoring and Analysis: theory, techniques, tools and applications for the future networks". It contains 14 chapters which demonstrate the results, quality,and the impact of European research in the field of TMA in line with the scientific objective of the Action. The book is structured into three parts: network and topology measurement and modelling, traffic classification and anomaly detection, quality of experience.

This book covers many aspects of cyberspace, emphasizing not only its possible

‘negative’ challenge as a threat to security, but also its positive influence as an efficient tool for defense as well as a welcome new factor for economic and industrial production. Cyberspace is analyzed from quite different and interdisciplinary perspectives, such as: conceptual and legal, military and socio-civil, psychological, commercial, cyber delinquency, cyber intelligence applied to public and private institutions, as well as the nuclear governance.

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics XI describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: Themes and Issues Internet Crime Investigations Forensic

Techniques Mobile Device Forensics Cloud Forensics Forensic Tools This book is the eleventh volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and prac tice in digital forensics. The book contains a selection of twenty edited papers from the Eleventh Annual IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida in the winter of 2015. Advances in Digital Forensics XI is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson, Chair, IFIP WG 11.9 on Digital Forensics, is a Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.

The two-volume set LNICST 169 and 170 constitutes the thoroughly refereed post-conference proceedings of the Second International Internet of Things Summit, IoT 360° 2015, held in Rome, Italy, in October 2015. The IoT 360° is an

event bringing a 360 degree perspective on IoT-related projects in important sectors such as mobility, security, healthcare and urban spaces. The conference also aims to coach involved people on the whole path between research to innovation and the way through to commercialization in the IoT domain. This volume contains 62 revised full papers at the following four conferences: The International Conference on Safety and Security in Internet of Things, SaSeIoT, the International Conference on Smart Objects and Technologies for Social Good, GOODTECHS, the International Conference on Cloud, Networking for IoT systems, CN4IoT, and the International Conference on IoT Technologies for HealthCare, HealthyIoT.

A Clear Outline of Current Methods for Designing and Implementing Automotive Systems Highlighting requirements, technologies, and business models, the Automotive Embedded Systems Handbook provides a comprehensive overview of existing and future automotive electronic systems. It presents state-of-the-art methodological and technical solutions in the areas of in-vehicle architectures, multipartner development processes, software engineering methods, embedded communications, and safety and dependability assessment. Divided into four parts, the book begins with an introduction to the design constraints of automotive-embedded systems. It also examines AUTOSAR as the emerging de

facto standard and looks at how key technologies, such as sensors and wireless networks, will facilitate the conception of partially and fully autonomous vehicles. The next section focuses on networks and protocols, including CAN, LIN, FlexRay, and TTCAN. The third part explores the design processes of electronic embedded systems, along with new design methodologies, such as the virtual platform. The final section presents validation and verification techniques relating to safety issues. Providing domain-specific solutions to various technical challenges, this handbook serves as a reliable, complete, and well-documented source of information on automotive embedded systems.

This book constitutes the thoroughly refereed proceedings of the First International Conference on HCI for Cybersecurity, Privacy and Trust, HCI-CPT 2019, which was held as part of the 21st HCI International Conference, HCII 2019, in Orlando, FL, USA, in July 2019. The total of 1275 papers and 209 posters included in the 35 HCII 2019 proceedings volumes were carefully reviewed and selected from 5029 submissions. HCI-CPT 2019 includes a total of 32 papers; they were organized in topical sections named: Authentication; cybersecurity awareness and behavior; security and usability; and privacy and trust.

This is Volume 42 of the Educational Media and Technology Yearbook. For the

past 40 years, our Yearbook has contributed to the field of Educational Technology in presenting contemporary topics, ideas, and developments regarding diverse technology tools for educational purposes. Our Yearbook has inspired researchers, practitioners, and teachers to consider how to develop technological designs and develop curricula and instruction integrating technology to enhance student learning, teach diverse populations across levels with effective technology integration, and apply technology in interactive ways to motivate students to engage in course content. In addition, Volume 42 features the Virtual Reality (VR) and Augmented Reality (AR) research and educational use cases, organized and coordinated by Vivienne and David. This section provides evidence that the affordances of AR, VR, and mixed reality, defined as an immersive multi-platform experience reality (XR), have begun to make indelible changes in teaching and learning in the United States. XR's recent developments stimulated the editors to propose a special edition to mark the interoperability of immersive technology to push the boundaries of human curiosity, creativity, and problem solving. After years of incremental development, XR has reached a critical level of investment, infrastructure, and emerging production. The chapters included in this section illustrate how XR can push user inquiry, engagement, learning, and interactivity to new levels within physical and

digital contexts.

This open access book presents theoretical and practical research relating to the vast, publicly financed program for the construction of new schools and the reorganization of existing educational buildings in Italy. This transformative process aims to give old buildings a fresh identity, to ensure that facilities are compliant with the new educational and teaching models, and to improve both energy efficiency and structural safety with respect to seismic activity. The book is divided into three sections, the first of which focuses on the social role of the school as a civic building that can serve the needs of the community. Innovations in both design and construction processes are then analyzed, paying special attention to the Building Information Modeling (BIM) strategy as a tool for the integration of different disciplines. The final section is devoted to the built heritage and tools, technologies, and approaches for the upgrading of existing buildings so that they meet the new regulations on building performance. The book will be of interest to all who wish to learn about the latest insights into the challenges posed by, and the opportunities afforded by, a comprehensive school building and renovation program.

Surveys the online social habits of American teens and analyzes the role technology and social media plays in their lives, examining common

misconceptions about such topics as identity, privacy, danger, and bullying.
This book constitutes the refereed post-conference proceedings of the 5th International Conference on Future Access Enablers for Ubiquitous and Intelligent Infrastructures, FABULOUS 2021, held in May 2021. Due to COVID-19 pandemic the conference was held virtually. This year's conference topic covers security of innovative services and infrastructure in traffic, transport and logistic ecosystems. The 30 revised full papers were carefully reviewed and selected from 60 submissions. The papers are organized in thematic sessions on: Internet of things and smart city; smart environment applications; information and communications technology; smart health applications; sustainable communications and computing infrastructures.
This edited book investigates the lack of interoperability in the IoT realm, including innovative research as well as technical solutions to interoperability, integration, and interconnection of heterogeneous IoT systems, at any level. It also explores issues caused by lack of interoperability such as impossibility to plug non-interoperable IoT devices into heterogeneous IoT platforms, impossibility to develop IoT applications exploiting multiple platforms in homogeneous and/or cross domains, slowness of IoT technology introduction at large-scale: discouragement in adopting IoT technology, increase of costs;

scarce reusability of technical solutions and difficulty in meeting user satisfaction. This book offers a concise summary of cutting-edge research and practical implications about employee engagement. The author presents a clear perspective on the meaning of employee engagement, its antecedents and consequences are presented with evidences. Based on latest research results, the book discusses organizational practices which enhance people engagement focusing on the new trends of the HRM domain such as well-being practices, e-HRM systems and social volunteering initiatives. The detailed analysis also takes the recent complaints about the HR function into account. This book emphasizes that modern organizations require passionate people to thriving in a rapidly changing world, and it is important to understand why, despite the growing relevance of employee engagement, disengaged persists.