The Architecture Of Privacy On Engineering Technologies That Can Deliver Trustworthy Safeguards

This book grew out of the First Symposium on the Personal Web, co-located with CASCON 2010 in Markham, Ontario, Canada. The purpose of the symposium was to bring together prominent researchers and practitioners from a diverse range of research areas relevant to the advancement of science and practice relating to the Personal Web. Research on the Personal Web is an outgrowth of the Smart Internet initiative, which seeks to extend and transform the web to be centred on the user, with the web as a calm platform ubiquitously providing cognitive support to its user and his or her tasks. As with the preceding SITCON workshop (held at CASCON 2009), this symposium involved a multi-disciplinary effort that brought together researchers and practitioners in data integration; web services modelling and architecture; human-computer interaction; predictive analytics; cloud infrastructure; semantics and ontology; and industrial application domains such as health care and finance. The discussions during the symposium dealt with different aspects of the architecture and functionality needed to make the Personal Web a reality. After the symposium the authors reworked their presentations into draft chapters that were submitted for peer evaluation and review. Every chapter went through two rounds of reviewing by at least two independent expert reviewers, and accepted chapters were then revised and are presented in this book.

The International Conference on E-commerce and Web Technologies (EC-Web) is a mature and well-established forum for researchers working in the area of electronic commerce and web technologies. These are the proceedings of the ninth conference in the series, which, like previous EC-Web conferences, was co-located with DEXA, the International Conference on Database and Expert Systems Applications, which, this year, took place in Turin, Italy. One key feature of EC-Web is its two-fold nature: it brings together both papers proposing technological solutions for e-commerce and the World Wide Web, and papers concerning the management of e-commerce, such as web marketing, the impact of e-commerce on business processes and organizations, the analysis of case studies, as well as social aspects of e-commerce (to understand the impact of e-commerce solutions on day-to-day life and the new opportunities that these behaviors open). The technical program included 12 reviewed papers and two invited papers. Each paper was reviewed by five reviewers, in order to select only the best quality papers. The program included five sessions: “Security in E-Commerce” (with two papers), “Social Aspects of E-Commerce” (with two papers), “Business Process and EC Inf- structures” (with three papers), “Recommender Systems and E-Negotiations” (with four papers) and “Web Marketing and User Profiling” (with three papers). We found the program interesting and we hope participants and readers feel the same. Furthermore, we hope the attendees enjoyed the conference and Turin. June 2008 Giuseppe Psaila Roland R. Wagner

In the beginning of 2003, I found a short article about the privacy implications of RFID technology in a newspaper. It raised my interest, and after reading some early research papers on the topic, I thought: “There must exist better solutions. ” I c- cerned myself with the topic in my spare time. After having developed my rst - lutions, I asked my supervisor, Prof. Dr. Paul Muller ? , whether I could write a paper about my results. As the topic did not t into any running project or at least the overall research directions of his group, he could have answered no. But instead, he encouraged me to do it. The paper became a success, and many other papers about new concepts and solutions followed. Now the answer is obvious: There exist better solutions. I have dealt with the topic over the past years. Now I want to share the basics as well as current research results with the reader. This book is surely not a bedside reading. But with all the presented concepts, it can broaden the mind of the reader concerning security,privacy, and RFIDsystems. Iwishthe reader many new insights. There are many people I would like to thank. First of all, my thanks go to my ? supervisor, Prof. Dr. Paul Muller. He gave me room for creativity and plenty of rope to work on my own.

Due to the continuously stream of security breaches two security architects in the Netherlands started a project to harvest good practices for better and faster creating architecture and privacy solution designs. This project resulted in a reference architecture that is aimed to help all security architects and designers worldwide. All kinds of topics that help creating a security or privacy solution architecture are outlined, such as: security and privacy principles, common attack vectors, threat models while in-depth guidelines are also given to evaluate the use of Open Source security and privacy application in various use cases.

This book looks at the different approaches to privacy through the centuries, and at how labour-saving devices have transformed the home.

This book describes how to architect and design Internet of Things (IoT) solutions that provide end-to-end security and privacy at scale. It is unique in its detailed coverage of threat analysis, protocol analysis, secure design principles, intelligent IoT's impact on privacy, and the effect of usability on security. The book also unveils the impact of digital currency and the dark web on the IoT-security economy. It's both informative and entertaining. "Filled with practical and relevant examples based on years of experience ... with lively discussions and storytelling related to IoT security design flaws and architectural issues."— Dr. James F. Ransome, Senior Director of Security Development Lifecycle (SOL) Engineering, Intel 'There is an absolute treasure trove of information within this book that will benefit anyone, not just the engineering community. This book has earned a permanent spot on my office bookshelf."— Erv Comer, Fellow of Engineering, Office of Chief Architect Zebra Technologies 'The importance of this work goes well beyond the engineer and architect. The IoT Architect's Guide to Attainable Security & Privacy is a crucial resource for every executive who delivers connected products to the market or uses connected products to run their business."— Kurt Lee, VP Sales and Strategic Alliances at PWNIE Express "If we collectively fail to follow the advice described here regarding IoT security and Privacy, we will continue to add to our mounting pile of exploitable computing devices. The attackers are having a field day. Read this book, now."— Brook S.E. Schoenfield, Director of Advisory Services at IOActive, previously Master Security Architect at McAfee, and author of Securing Systems

Towns are imagined, lived and experienced, as much as they are conceived and constructed. They reflect cultural and intellectual currents, prevailing economic climates and unresolved tensions. They are physical entities, shaped by topography, time and technology, as well as social and spatial constructs. They are also always gendered and contested spaces. This volume, the last from the Gender in the European Town (GENETON) project, approaches life in the European town over time and across class and national boundaries. Through contextualized case studies, it provides scholars and students with new research—snapshots—of contemporary physical and built environments that explores how contemporary urban residents experienced and deployed gendered urban spaces over an important period of

modernization.
Technology’s influence on privacy not only concerns consumers, political leaders, and advocacy groups, but also the software architects who design new products. In this practical guide, experts in data analytics, software engineering, security, and privacy policy describe how software teams can make privacy-protective features a core part of product functionality, rather than add them late in the development process. Ideal for software engineers new to privacy, this book helps you examine privacy-protective information management architectures and their foundational components—building blocks that you can combine in many ways. Policymakers, academics, students, and advocates unfamiliar with the technical terrain will learn how these tools can help drive policies to maximize privacy protection. Restrict access to data through a variety of application-level controls Use security architectures to avoid creating a single point of trust in your systems Explore federated architectures that let users retrieve and view data without compromising data security Maintain and analyze audit logs as part of comprehensive system oversight Examine case studies to learn how these building blocks help solve real problems Understand the role and responsibilities of a Privacy Engineer for maintaining your privacy architecture
The aim of this book is to provide the latest research findings, innovative research results, methods and development techniques from both theoretical and practical perspectives related to intelligent social networks and collaborative systems, intelligent networking systems, mobile collaborative systems, secure intelligent cloud systems, etc., and to reveal synergies among various paradigms in the multi-disciplinary field of intelligent collaborative systems. It presents the Proceedings of the 9th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2017), held on August 24–26, 2017 in Toronto, Canada. With the rapid evolution of the Internet, we are currently experiencing a shift from the traditional sharing of information and applications as the main purpose of the Web to an emergent paradigm that puts people at the very centre of networks and exploits the value of people’s connections, relations and collaborations. Social networks are also pla ying a major role in the dynamics and structure of intelligent Web-based networking and collaborative systems. Virtual campuses, virtual communities and organizations effectively leverage intelligent networking and collaborative systems by tapping into a broad range of formal and informal electronic relations, such as business-to-business, peer-to-peer and many types of online collaborative learning interactions, including the emerging e-learning systems. This has resulted in entangled systems that need to be managed efficiently and autonomously. In addition, the latest and powerful technologies based on Grid and wireless infrastructure as well as Cloud computing are now greatly enhancing collaborative and networking applications, but are also facing new issues and challenges. The principal objective of the research and development community is to stimulate research that leads to the creation of responsive environments for networking and, in the longer-term, the developmen t of adaptive, secure, mobile, and intuitive intelligent systems for collaborative work and learning.
?Privacy is a burden for most organizations, the more complex and wider an organization is, the harder to manage and enforce privacy is. GDPR and other regulations on privacy impose strict constraints that must be coherently enforced, considering also privacy needs of organization and their users. Furthermore, organizations should allow their users to express their privacy needs easily, even when the process that manages users' data is complex and involves multiple organizations. Many research work consider the problem using simplistic examples, with solutions proposed that never actually touch pragmatic problems of real, large organizations, with thousands of users and terabytes of personal and sensitive data. This book faces the privacy management problem targeting actual large organizations, such as public administrations, including stakeholders in the process of definition of the solution and evaluating the results with its actual integration in four large organizations. The contribution of this book is twofold: a privacy platform that can be customized and used to manage privacy in large organizations; and the process for the design of such a platform, from a state-of-the-art survey on privacy regulations, through the definition of its requirements, its design and its architecture, until the evaluation of the platform.
This book constitutes the refereed proceedings of the 7th International Conference on Cloud Computing, Security, Privacy in New Computing Environments, CloudComp 2016, and the First EAI International Conference SPNCE 2016, both held in Guangzhou, China, in November and December 2016.The proceedings contain 10 full papers selected from 27 submissions and presented at CloudComp 2016 and 12 full papers selected from 69 submissions and presented at SPNCE 2016. CloudComp 2016 presents recent advances and experiences in clouds, cloud computing and related ecosystems and business support. SPNCE 2016 focuses on security and privacy aspects of new computing environments including mobile computing, big data, cloud computing and other large-scale environments.
This SpringerBrief covers the security and privacy challenges in fog computing, and proposes a new secure and privacy-preserving mechanisms to resolve these challenges for securing fog-assisted IoT applications. Chapter 1 introduces the architecture of fog-assisted IoT applications and the security and privacy challenges in fog computing. Chapter 2 reviews several promising privacy-enhancing techniques and illustrates examples on how to leverage these techniques to enhance the privacy of users in fog computing. Specifically, the authors divide the existing privacy-enhancing techniques into three categories: identity-hidden techniques, location privacy protection and data privacy enhancing techniques. The research is of great importance since security and privacy problems faced by fog computing impede the healthy development of its enabled IoT applications. With the advanced privacy-enhancing techniques, the authors propose three secure and privacy-preserving protocols for fog computing applications, including smart parking navigation, mobile crowdsensing and smart grid. Chapter 3 introduces identity privacy leakage in smart parking navigation systems, and proposes a privacy-preserving smart parking navigation system to prevent identity privacy exposure and support efficient parking guidance retrieval through road-side units (fogs) with high retrieving probability and security guarantees. Chapter 4 presents the location privacy leakage, during task allocation in mobile crowdsensing, and propose a strong privacy-

preserving task allocation scheme that enables location-based task allocation and reputation-based report selection without exposing knowledge about the location and reputation for participators in mobile crowdsensing. Chapter 5 introduces the data privacy leakage in smart grid, and proposes an efficient and privacy-preserving smart metering protocol to allow collectors (fogs) to achieve real-time measurement collection with privacy-enhanced data aggregation. Finally, conclusions and future research directions are given in Chapter 6. This brief validates the significant feature extension and efficiency improvement of IoT devices without sacrificing the security and privacy of users against dishonest fog nodes. It also provides valuable insights on the security and privacy protection for fog-enabled IoT applications. Researchers and professionals who carry out research on security and privacy in wireless communication will want to purchase this SpringerBrief. Also, advanced level students, whose main research area is mobile network security will also be interested in this SpringerBrief.

"Originally published as Foundations and trends in human-computer interaction, volume 1, issue 1 (2007), ISSN: 1551-3955"--P. [4] of cover.

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.

This book presents a comprehensive framework for IoT, including its architectures, security, privacy, network communications, and protocols. The book starts by providing an overview of the aforementioned research topics, future directions and open challenges that face the IoT development. The authors then discuss the main architectures in the field, which include Three- and Five-Layer Architectures, Cloud and Fog Based Architectures, a Social IoT Application Architecture. In the security chapter, the authors outline threats and attacks, privacy preservation, trust and authentication, IoT data security, and social awareness. The final chapter presents case studies including smart home, wearables, connected cars, industrial Internet, smart cities, IoT in agriculture, smart retail, energy engagement, IoT in healthcare, and IoT in poultry and farming. Discusses ongoing research into the connection of the physical and virtual worlds; Includes the architecture, security, privacy, communications, and protocols of IoT; Presents a variety of case studies in IoT including wearables, smart cities, and energy management.

This volume constitutes the refereed proceedings of the following 9 international workshops: OTM Academy, OTM Industry Case Studies Program, Cloud and Trusted Computing, C&TC, Enterprise Integration, Interoperability, and Networking, EI2N, Industrial and Business Applications of Semantic Web Technologies, INBAST, Information Systems, om Distributed Environment, ISDE, Methods, Evaluation, Tools and Applications for the Creation and Consumption of Structured Data for the e-Society, META4eS, Mobile and Social Computing for collaborative interactions, MSC, and Ontology Content, OnToContent 2014. These workshops were held as associated events at OTM 2014, the federated conferences "On The Move Towards Meaningful Internet Systems and Ubiquitous Computing", in Amantea, Italy, in October 2014. The 56 full papers presented together with 8 short papers, 6 posters and 5 keynotes were carefully reviewed and selected from a total of 96 submissions. The focus of the workshops were on the following subjects models for interoperable infrastructures, applications, privacy and access control, reliability and performance, cloud and configuration management, interoperability in (System-of-)Systems, distributed information systems applications, architecture and process in distributed information system, distributed information system development and operational environment, ontology is use for eSociety, knowledge management and applications for eSociety, social networks and social services, social and mobile intelligence, and multimodal interaction and collaboration.

The idea that 'home' is a special place, a separate place, a place where we can be our true selves, is so obvious to us today that we barely pause to think about it. But, as Judith Flanders shows in this revealing book, 'home' is a relatively new concept. When in 1900 Dorothy assured the citizens of Oz that 'There is no place like home', she was expressing a view that was a culmination of 300 years of economic, physical and emotional change. In The Making of Home, Flanders traces the evolution of the house across northern Europe and America from the sixteenth to the early twentieth century, and paints a striking picture of how the homes we know today differ from homes through history. The transformation of houses into homes, she argues, was not a private matter, but an essential ingredient in the rise of capitalism and the birth of the Industrial Revolution. Without 'home', the modern world as we know it would not exist, and as Flanders charts the development of ordinary household objects - from cutlery, chairs and curtains, to fitted kitchens, plumbing and windows - she also peels back the myths that surround some of our most basic assumptions, including our entire notion of what it is that makes a family. As full of fascinating detail as her previous bestsellers, The Making of Home is also a book teeming with original and provocative ideas.

This book provides the state-of-the-art development on security and privacy for fog/edge computing, together with their system architectural support and applications. This book is organized into five parts with a total of 15 chapters. Each area corresponds to an important snapshot. The first part of this book presents an overview of fog/edge computing, focusing on its relationship with cloud technology and the future with the use of 5G communication. Several applications of edge computing are discussed. The second part of this book considers several security issues in fog/edge computing, including the secure storage and search services, collaborative intrusion detection method on IoT-fog computing, and the feasibility of deploying Byzantine agreement protocols in untrusted environments. The third part of this book studies the privacy issues in fog/edge computing. It first investigates the unique privacy challenges in fog/edge computing, and then discusses a privacy-preserving framework for the edge-based video analysis, a popular machine learning application on fog/edge. This book also covers the security architectural design of fog/edge computing, including a comprehensive overview of vulnerabilities in fog/edge computing within multiple architectural levels, the security and intelligent management, the implementation of network-function-virtualization-enabled multicasting in part four. It explains how to use the blockchain to realize security services. The last part of this book surveys applications of fog/edge computing, including the fog/edge computing in Industrial IoT, edge-based augmented reality, data streaming in fog/edge computing, and the blockchain-based application for edge-IoT. This book is designed for academics, researchers and government officials, working in the field of fog/edge computing and cloud computing. Practitioners, and business organizations (e.g., executives, system designers, and marketing professionals), who conduct teaching, research, decision making, and designing fog/edge technology will also benefit from this book The content of this book will be particularly useful for advanced-level students studying computer science, computer technology, and information systems, but also applies to students in business, education, and economics, who would benefit from the information, models, and case studies therein.

Before wireless commerce, or even wireless access to the corporate network can really take off, organizations are going to have to improve their efforts in wireless security. Wireless Security and Privacy presents a complete methodology for security professionals and wireless developers to coordinate their efforts, establish wireless security best practices, and establish security measures that keep pace with development. The material shows how to develop a risk model, and shows how to implement it through the lifecycle of a system. Coverage includes the essentials on cryptography and privacy issues. In order to design appropriate security applications, the authors teach the limitations inherent in wireless devices as well as best methods for developing secure software for them. The authors combine the right amount of technological background in conjunction with a defined process for assessing wireless security.

Security and privacy protection within computer networks can be a challenge. By examining the current problems and challenges this domain is facing, more efficient strategies can be established to safeguard personal information against invasive pressures. Security and Privacy in Smart Sensor Networks is a critical scholarly resource that examines recent developments and emerging trends in smart sensor security and privacy by providing new models, practical solutions, and technological advances related to security. Featuring coverage on a broad range of topics such as cloud security, encryption, and intrusion detection systems, this book is geared towards academicians, engineers, IT specialists, researchers, and students seeking current research on authentication and intrusion detection.

This book on privacy and data protection offers readers conceptual analysis as well as thoughtful discussion of issues, practices, and solutions. It features results of the seventh annual International Conference on Computers, Privacy, and Data Protection, CPDP 2014, held in Brussels January 2014. The book first examines profiling, a persistent core issue of data protection and privacy. It covers the emergence of profiling technologies, on-line behavioral tracking, and the impact of profiling on fundamental rights and values. Next, the book looks at preventing privacy risks and harms through impact assessments. It contains discussions on the tools and methodologies for impact assessments as well as case studies. The book then goes on to cover the purported trade-off between privacy and security, ways to support privacy and data protection, and the controversial right to be forgotten, which offers individuals a means to oppose the often persistent digital memory of the web. Written during the process of the fundamental revision of the current EU data protection law by the Data Protection Package proposed by the European Commission, this interdisciplinary book presents both daring and prospective approaches. It will serve as an insightful resource for readers with an interest in privacy and data protection.

Since its original publication in 1999, this foundational book has become a classic in its field. This second edition, Code Version 2.0, updates the work and was prepared in part through a wiki, a web site allowing readers to edit the text, making this the first reader-edited revision of a popular book. Code counters the common belief that cyberspace cannot be controlled or censored. To the contrary, under the influence of commerce, cyberspace is becoming a highly regulable world where behavior will be much more tightly controlled than in real space. We can - we must - choose what kind of cyberspace we want and what freedoms it will guarantee. These choices are all about architecture: what kind of code will govern cyberspace, and who will control it. In this realm, code is the most significant form of law and it is up to lawyers, policymakers, and especially average citizens to decide what values that code embodies.

Organizations of all kinds are recognizing the crucial importance of protecting privacy. Their customers, employees, and other stakeholders demand it. Today, failures to safeguard privacy can destroy organizational reputations – and even the organizations themselves. But implementing effective privacy protection is difficult, and there are few comprehensive resources for those tasked with doing so. In Information Privacy Engineering and Privacy by Design, renowned information technology author William Stallings brings together the comprehensive and practical guidance you need to succeed. Stallings shows how to apply today’s consensus best practices and widely-accepted standards documents in your environment, leveraging policy, procedures, and technology to meet legal and regulatory requirements and protect

everyone who depends on you. Like Stallings' other award-winning texts, this guide is designed to help readers quickly find the information and gain the mastery needed to implement effective privacy. Coverage includes: Planning for privacy: Approaches for managing and controlling the privacy control function; how to define your IT environment's requirements; and how to develop appropriate policies and procedures for it Privacy threats: Understanding and identifying the full range of threats to privacy in information collection, storage, processing, access, and dissemination Information privacy technology: Satisfying the privacy requirements you've defined by using technical controls, privacy policies, employee awareness, acceptable use policies, and other techniques Legal and regulatory requirements: Understanding GDPR as well as the current spectrum of U.S. privacy regulations, with insight for mapping regulatory requirements to IT actions
This volume, the 36th issue of Transactions on Large-Scale Data- and Knowledge-Centered Systems, contains eight revised, extended papers selected from the 3rd International Conference on Future Data and Security Engineering, FDSE 2016, and the 10th International Conference on Advanced Computing and Applications, ACOMP 2016, which were held in Can Tho City, Vietnam, in November 2016. Topics covered include big data analytics, massive dataset mining, security and privacy, cryptography, access control, deep learning, crowd sourcing, database watermarking, and query processing and optimization.
The Architecture of PrivacyOn Engineering Technologies that Can Deliver Trustworthy Safeguards"O'Reilly Media, Inc."
This book contains a range of keynote papers and submitted papers presented at the 7th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6 International Summer School, held in Nijmegen, The Netherlands, in June 2013. The 13 revised full papers and 6 keynote papers included in this volume were carefully selected from a total of 30 presentations and 11 keynote talks and were subject to a two-step review process. The keynote papers cover the dramatic global changes, including legislative developments that society is facing today. Privacy and identity management are explored in specific settings, such as the corporate context, civic society, and education and using particular technologies such as cloud computing. The regular papers examine the challenges to privacy, security and identity; ways of preserving privacy; identity and identity management and the particular challenges presented by social media.
Privacy and Publicity boldly questions certain ideological assumptions underlying the received view of modern architecture and reconsiders the methodology of architectural criticism itself. Where conventional criticism portrays modern architecture as a high artistic practice in opposition to mass culture, Colomina sees the emerging systems of communication that have come to define twentieth-century culture -the mass media - as the true site within which modern architecture was produced. She considers architectural discourse as the intersection of a number of systems of representation such as drawings, models, photographs, books, films, and advertisements. This does not mean abandoning the architectural object, the building, but rather looking at it in a different way. The building is understood here in the same way as all the media that frame it, as a mechanism of representation in its own right.
The volume includes a set of selected papers extended and revised from the I2009 Pacific-Asia Conference on Knowledge Engineering and Software Engineering (KESE 2009) was held on December 19~ 20, 2009, Shenzhen, China. Volume 2 is to provide a forum for researchers, educators, engineers, and government officials involved in the general areas of Knowledge Engineering and Communication Technology to disseminate their latest research results and exchange views on the future research directions of these fields. 135 high-quality papers are included in the volume. Each paper has been peer-reviewed by at least 2 program committee members and selected by the volume editor Prof.Yanwen Wu. On behalf of the this volume, we would like to express our sincere appreciation to all of authors and referees for their efforts reviewing the papers. Hoping you can find lots of profound research ideas and results on the related fields of Knowledge Engineering and Communication Technology.