



River Publishers

River Publishers Book Catalogue

Series in Security and Digital Forensics

River Publishers Series in Security and Digital Forensics

Cryptocurrency and Blockchains

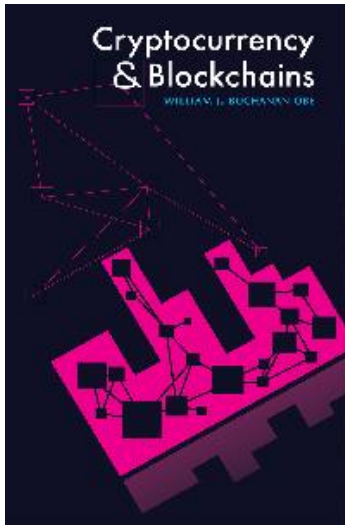
Author: William J. Buchanan, OBE, Edinburgh Napier University, UK

ISBN: 9788793609327

e-ISBN: 9788793609310

Available From: August 2019

Price: € 60.00



Description:

Cryptocurrency and Blockchains outlines many of the key developments in building a more trustworthy world. It includes a background within the main methods used within creating data infrastructure which use Blockchain methods, and how these will change existing methods of authentication and identity provision. This will include a discussion of a range of application areas including with health care, law, finance and government services, and how smart contracts can be used to make transactions more trustworthy.

Within the cryptocurrency part, the book outlines the trust infrastructure within the main cryptocurrency methods and around the usage of electronic tokens to transfer credits.

An important element of the book is to look forwards a world where every transaction is made trustworthy, and were privacy requirements are respected.

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customer@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

The Humanized Internet Dignity, Digital Identity and Democracy

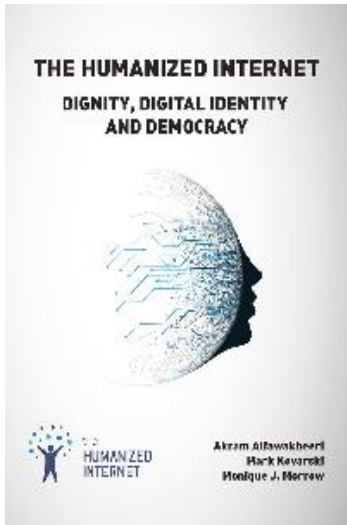
Authors:

Akram Alfawakheeri, The Humanized Internet Institute, Germany
Mark Kovarski, The Humanized Internet Institute, Canada
Monique J. Morrow, The Humanized Internet Institute, Switzerland

Contributors :

Ann Greenberg, Entertainment AITM, USA
Daniel Gasteiger and Adithya Pradeep Kumar, Procvivis, Switzerland
Frances Hughes, The University of Sydney, Australia

ISBN: 9788770220323



Description:

In reading this book, there are key themes that are constant such as the notion of identity and identity sets; e-sovereignty and privacy and most importantly the function of an Internet that is inclusive, not "controlled" by a few organizations for their own profitability. Certainly, "enterprising" the Internet has been a process over these past years and there is no intent to set judgement here but rather pause for a moment and reflect on the impact of these technologies to individuals.

Yes, this is *The Humanized Internet*.

These tenets may sound libertarian but in fact we are speaking about core principles to guide the development and perhaps the return of the Internet to the people especially those who are underserved .

"Do No Evil" should not be a company motto but rather foundational to the development of any technologies that do impact us as individual consumers of these technologies and corresponding products. Indeed there is a polarity between an Internet that is used for mass empowerment and one that can be used for mass destruction. Privacy, security and the management of your digital footprint should be done by you.

With the progression of Human and Machine interaction due to advances in Biotech and Brain/Computer interface Cloud, Virtual and Mixed Reality, we need to understand the impact of these technologies to identity overall. Do we require a new definition of identity? What is e-Sovereignty and its application moving forward if we posit that the institutions that exist today may indeed no longer be relevant in their current structure. We have read about the abuses when your data falls into the hands of other entities, intentionally or not.

The Humanized Internet is therefore a call to action, your action.

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customercare@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

Visual Communication for Cybersecurity Beyond Awareness to Advocacy

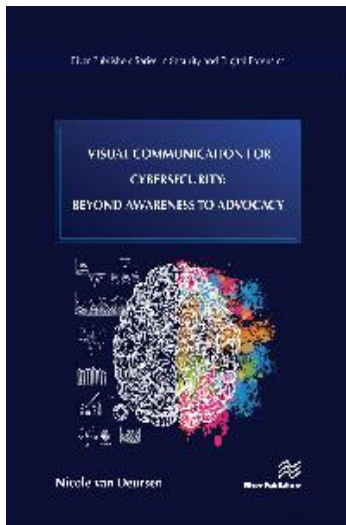
Author: Nicole van Deursen, Consultant, the Netherlands

ISBN: 9788770220903

e-ISBN: 9788770220897

Available From: August 2019

Price: € 75.00



Description:

Cybersecurity needs a change in communication. It is time to show the world that cybersecurity is an exciting and diverse field to work in. Cybersecurity is not only about hackers and technical gobbledygook. It is a diverse field of work with a lot of collaboration with other disciplines. Over the years, security professionals have tried different awareness strategies to promote their work and to improve the knowledge of their audience but without much success. Communication problems are holding back advances in the field.

Visual Communication for Cybersecurity explores the possibilities of visual communication as a tool to improve the communication about cybersecurity and to better connect with non-experts. Visual communication is useful to explain complex topics and to solve complex problems. Visual tools are easy to share through social media and have the possibility to reach a wide audience. When applied strategically, visual communication can contribute to a people-centric approach to security, where employees are encouraged to actively engage in security activities rather than simply complying with the policies.

Cybersecurity education does not usually include communication theory or creative skills. Many experts think that it is not part of their job and is best left to the communication department or they think that they lack any creative talent. This book introduces communication theories and models, gives practical tips, and shows many examples. The book can support students in cybersecurity education and professionals searching for alternatives to bullet-point presentations and textual reports. On top of that, if this book succeeds in inspiring the reader to start creating visuals, it may also give the reader the pleasure of seeing new possibilities and improving their performance.

The book is divided into different parts for readers with different interests. There is no need to read the book from cover to cover; the chapters are organized thematically. Readers that are interested in how to apply communication theory to cybersecurity will enjoy the chapters about learning, the context in which communication takes place, and how people are persuaded. Readers that are looking for inspiration and examples of how to use visuals in their daily tasks go straight to the third section of the book. The last section is a workbook that will help the reader to take the first steps towards using visual communication at work.

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customer@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

Blockchain Technology and Applications

Author: Ahmed Banafa, San Jose State University, USA and Stanford University, USA

ISBN: 9788770221061

e-ISBN: 9788770221054

Available From: August 2019

Price: € 90.00



Description:

Blockchain is an emerging technology that can radically improve security in transaction networks, it provides the basis for a dynamic distributed ledger that can be applied to save time when recording transactions between parties, remove costs associated with intermediaries, and reduce risks of fraud and tampering. This book explores the fundamentals and applications of Blockchain technology; the transparent, secure, immutable and distributed database used currently as the underlying technology for Cryptocurrency. Decentralized peer-to-peer network, distributed ledger and the trust model that defines Blockchain technology will be explained. Components of Blockchain, its operations, underlying algorithms, and essentials of trust will be defined. Types of Blockchain networks including private and public Blockchain networks will be introduced. Concepts of smart contracts, proof of work and proof of stack will be clarified. The relationship between Blockchain technology, Internet of Things (IoT), Artificial Intelligence (AI), Cybersecurity and Digital Transformation will be explored in this book. Myths about Blockchain will be exposed and a look at the future of Blockchain will be presented.

Topics will be covered in this book: Blockchain technology, Smart contracts, Hashing, SHA-256 Hash, Verification, Validation, Consensus models, Digital Mining, Hard fork, Soft fork, Bitcoin, Ethereum, Proof of work, Proof of stack, Myths about Blockchain, Decentralized peer-to-peer network, Types of Blockchain networks, Hot and Cold Wallets, Double Spend, Decentralized Applications, Transaction networks, Sidechains, 51% attack, Cryptocurrency, Digital transformation, Internet of Things (IoT), Artificial Intelligence (AI), Cybersecurity and the Future of Blockchain.

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customer@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

Cyber Resilience

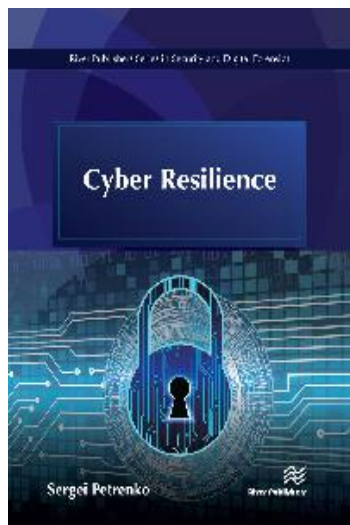
Author: Sergei Petrenko, Innopolis University, Russia

ISBN: 9788770221160

e-ISBN: 9788770221153

Available From: August 2019

Price: € 95.00



Description:

Modern cyber systems acquire more emergent system properties, as far as their complexity increases: cyber resilience, controllability, self-organization, proactive cyber security and adaptability. Each of the listed properties is the subject of the cybernetics research and each subsequent feature makes sense only if there is a previous one.

Cyber resilience is the most important feature of any cyber system, especially during the transition to the sixth technological stage and related Industry 4.0 technologies: Artificial Intelligence (AI), Cloud and foggy computing, 5G +, IoT/IloT, Big Data and ETL, Q-computing, Blockchain, VR/AR, etc. We should even consider the cyber resilience as a primary one, because the mentioned systems cannot exist without it. Indeed, without the sustainable formation made of the interconnected components of the critical information infrastructure, it does not make sense to discuss the existence of 4.0 Industry cyber-systems. In case when the cyber security of these systems is mainly focused on the assessment of the incidents' probability and prevention of possible security threats, the cyber resilience is mainly aimed at preserving the targeted behavior and cyber systems' performance under the conditions of known (about 45 %) as well as unknown (the remaining 55 %) cyber attacks.

This monograph shows that modern Industry 4.0. Cyber systems do not have the required cyber resilience for targeted performance under heterogeneous mass intruder cyber-attacks. The main reasons include a high cyber system structural and functional complexity, a potential danger of existing vulnerabilities and "sleep" hardware and software tabs, as well as an inadequate efficiency of modern models, methods, and tools to ensure cyber security, reliability, response and recovery. A new formulation of the cyber resilience problem under heterogeneous mass cyber-attacks is proposed, in which the cyber system performance recovery in destructive software impacts prevents significant or catastrophic consequences. Here, the idea of ensuring the cyber resilience is to give the cyber systems the ability to develop immunity to disturbances of the computational processes under destructive influences, by analogy with the immune system protecting a living organism.

The book contains three chapters, devoted to the following topics:

- Development of the Cyber Resilience Management Concept of modern technological platforms and cyber-systems of 4.0 Industry;
- Development of a corporate cyber risk management methodology;
- Technical implementation of the corporate program of business sustainability management based on the best practices (standards).

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customercare@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

Cyber Security Innovation for the Digital Economy **A Case Study of the Russian Federation**

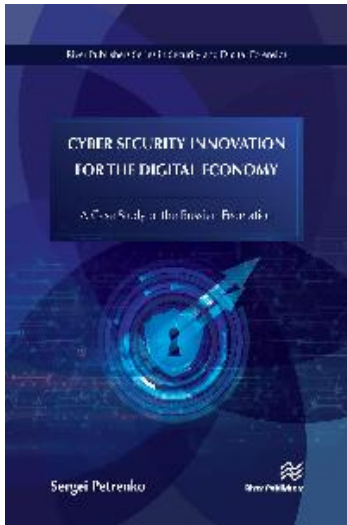
Author: Sergei Petrenko, Innopolis University, Russia

ISBN: 9788770220224

e-ISBN: 9788770220217

Available From: December 2018

Price: € 90.00



Description:

Cyber Security Innovation for the Digital Economy considers possible solutions to the relatively new scientific-technical problem of developing innovative solutions in the field of cyber security for the Digital Economy. The solutions proposed are based on the results of exploratory studies conducted by the author in the areas of Big Data acquisition, cognitive information technologies (cogno-technologies), new methods of analytical verification of digital ecosystems on the basis of similarity invariants and dimensions, and "computational cognitivism," involving a number of existing models and methods.

In practice, this successfully allowed the creation of new entities - the required safe and trusted digital ecosystems - on the basis of the development of digital and cyber security technologies, and the resulting changes in their behavioral preferences. Here, the ecosystem is understood as a certain system of organizations, created around a certain Technological Platform that use its services to make the best offers to customers and access to them to meet the ultimate needs of clients - legal entities and individuals. The basis of such ecosystems is a certain technological platform, created on advanced innovative developments, including the open interfaces and code, machine learning, cloud technologies, Big Data collection and processing, artificial intelligence technologies, etc. The mentioned Technological Platform allows creating the best offer for the client both from own goods and services and from the offers of external service providers in real time.

This book contains four chapters devoted to the following subjects:

- Relevance of the given scientific-technical problems in the cybersecurity of Digital Economy
- Determination of the limiting capabilities
- Possible scientific and technical solutions
- Organization of perspective research studies in the area of Digital Economy cyber security in Russia.

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customercare@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

Practical LTE Based Security Forces PMR Networks

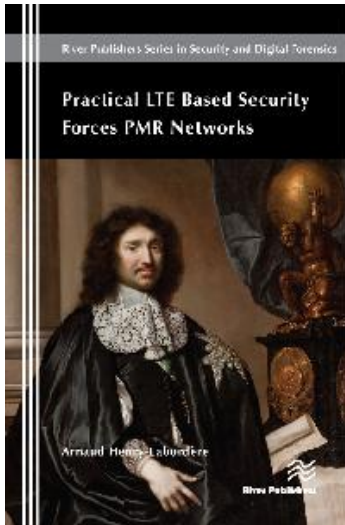
Author: Arnaud Henry-Labordère, Ecole Nationale des Ponts et Chaussées & Halys, France

ISBN: 9788793609792

e-ISBN: 9788793609785

Available From: September 2018

Price: € 90.00



Description:

Security forces PMR networks are moving from proprietary technologies for their "Mission Critical Push-To-Talk" basic service, and their data services which must provide large bandwidth real-time access, to the databases. LTE Based is adopted with backup access to public MNOs to complement their own radio coverage. Specific technologies such as multicasting of video are required so the MCPTT works within a restricted bandwidth. The need to be able to change the main MNOs to provide resilient coverage requires specific choices of SIM cards, with OTAA security domains.

Practical LTE Based Security Forces PMR Networks assumes that the reader has a basic knowledge of the 4G network architecture and services, and the book focusses on the specific features and choices required to fulfill the need of security forces PMR networks. These include tactical and centralized, including LTE based voice services VoLTE and IMS. It can be used as a reference or textbook, with many detailed call flows and traces being included.

The author, who has also a long teaching career in Operations Research, provides mathematical models for the optimization of tactical network federations, multicast coverage and allocation of preemptive priorities to PMR group members. He is a pioneer in the area of Virtual Roaming, an application of graph theory and telecommunications to provide roaming without direct relations, having previously published books on SMS Hubs, SS7 Hubs, Diameter Hubs, GTP Hubs. The use of M2M (monitoring devices) for security forces with mobility is covered in detail in the book, including the new LoRa virtual roaming which goes beyond the scope of PMR.

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customer@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

Internet of Things Security: Fundamentals, Techniques and Applications

Editors:

Shishir K. Shandilya, Vellore Institute of Technology, VIT Bhopal University, India

Soon Ae Chun, City University of New York, USA

Smita Shandilya, Sagar Institute of Research, Technology and Science, India

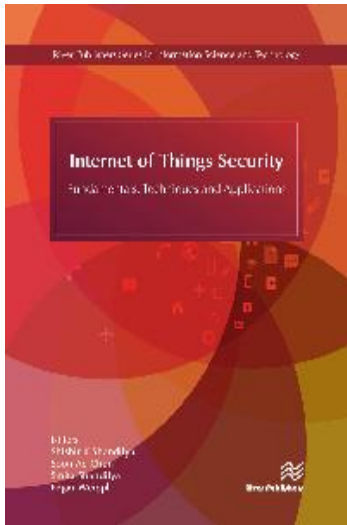
Edgar Weippl, SBA Research, Austria

ISBN: 9788793609532

e-ISBN: 9788793609525

Available From: August 2018

Price: € 90.00



Description:

Internet of Things (IoT) security deals with safeguarding the devices and communications of IoT systems, by implementing protective measures and avoiding procedures which can lead to intrusions and attacks. However, security was never the prime focus during the development of the IoT, hence vendors have sold IoT solutions without thorough preventive measures. The idea of incorporating networking appliances in IoT systems is relatively new, and hence IoT security has not always been considered in the product design.

To improve security, an IoT device that needs to be directly accessible over the Internet should be segmented into its own network, and have general network access restricted. The network segment should be monitored to identify potential anomalous traffic, and action should be taken if a problem arises. This has generated an altogether new area of research, which seeks possible solutions for securing the devices, and communication amongst them.

Internet of Things Security: Fundamentals, Techniques and Applications provides a comprehensive overview of the overall scenario of IoT Security whilst highlighting recent research and applications in the field. Technical topics discussed in the book include:

- Machine-to-Machine Communications
- IoT Architecture
- Identity of Things
- Block Chain
- Parametric Cryptosystem
- Software and Cloud Components

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customercare@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

GDPR and Cyber Security for Business Information Systems

Authors:

Antoni Gobeo, Edinburgh Napier University, UK
Connor Fowler, Edinburgh Napier University, UK
William J. Buchanan, Edinburgh Napier University, UK

ISBN: 9788793609136

e-ISBN: 9788770220798

Available From: August 2018

Price: € 60.00



Description:

The General Data Protection Regulation is the latest, and one of the most stringent, regulations regarding Data Protection to be passed into law by the European Union. Fundamentally, it aims to protect the Rights and Freedoms of all the individuals included under its terms; ultimately the privacy and security of all our personal data. This requirement for protection extends globally, to all organisations, public and private, wherever personal data is held, processed, or transmitted concerning any EU citizen.

Cyber Security is at the core of data protection and there is a heavy emphasis on the application of encryption and state of the art technology within the articles of the GDPR. This is considered to be a primary method in achieving compliance with the law. Understanding the overall use and scope of Cyber Security principles and tools allows for greater efficiency and more cost effective management of Information systems.

GDPR and Cyber Security for Business Information Systems is designed to present specific and practical information on the key areas of compliance to the GDPR relevant to Business Information Systems in a global context.

Key areas covered include:

- Principles and Rights within the GDPR
- Information Security
- Data Protection by Design and Default
- Implementation Procedures
- Encryption methods
- Incident Response and Management
- Data Breaches

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customer@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

Cryptography

Author: William J. Buchanan, OBE, Edinburgh Napier University, UK

ISBN: 9788793379107

e-ISBN: 9788793609143

Available From: September 2017

Price: € 57.00



Description:

Cryptography has proven to be one of the most contentious areas in modern society. For some it protects the rights of individuals to privacy and security, while for others it puts up barriers against the protection of our society. This book aims to develop a deep understanding of cryptography, and provide a way of understanding how privacy, identity provision and integrity can be enhanced with the usage of encryption.

The book has many novel features including:

- full provision of Web-based material on almost every topic covered
- provision of additional on-line material, such as videos, source code, and labs
- coverage of emerging areas such as Blockchain, Light-weight Cryptography and Zero-knowledge Proofs (ZKPs)

Key areas covered include:

- Fundamentals of Encryption
- Public Key Encryption
- Symmetric Key Encryption
- Hashing Methods
- Key Exchange Methods
- Digital Certificates and Authentication
- Tunneling
- Crypto Cracking
- Light-weight Cryptography
- Blockchain
- Zero-knowledge Proofs

This book provides extensive support through the associated website of: <http://asecuritysite.com/encryption>

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customer@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

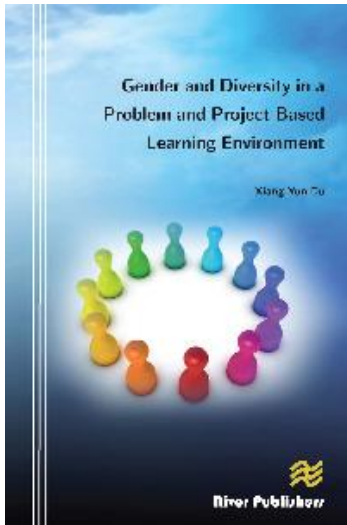
Gender and Diversity in a Problem and Project Based Learning Environment

Author: Xiangyun Du, Associate Professor, Department of Learning and Philosophy, Aalborg University

ISBN: 9788792329844

Available From: December 2011

Price: € 75.00



Description:

Problem and Project Based Learning (PBL) has been well used as an educational philosophy and methodology in the construction of student centered and contextualized learning environment. PBL is also regarded as an effective method in producing engineering graduates who can not only meet the needs of professional competences, but also are prepared for new challenges in the globalized and technological context. However, can PBL be a solution to the challenge of a general lack of university students studying engineering and technology in many countries? The book reports an ethnographical study on the learning experiences of engineering students in the PBL environment in Denmark. This book also attempts to question the issue of diversity in engineering education via the exploration of whether or in which ways the PBL environment is friendly to diverse groups of learners such as women.

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customer@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

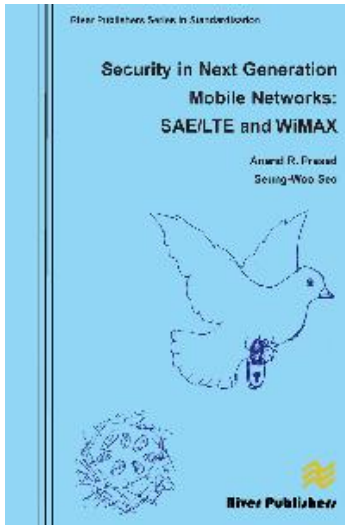
Security in Next Generation Mobile Networks: SAE/LTE and WiMAX

Author: Anand R. Prasad, NEC Corporation, Japan and Seung-Woo Seo, Seoul National University, South Korea

ISBN: 9788792329639

Available From: August 2011

Price: € 85.00



Description:

Starting from voice services with simple terminals, today a mobile device is nothing sort of a small PC in the form of smart-phones. The result has been a huge increase in data-services giving mobile communication access to critical aspects of human society / life. This has led to standardization of SAE/LTE (System Architecture Evolution / Long Term Evolution) by 3GPP and IEEE 802.16e / WiMAX. Together with penetration of mobile communications and new standardization come new security issues and thus the need for new security solutions. This book provides a fresh look at those security aspects, with main focus on the latest security developments of 3GPP SAE/LTE and WiMAX. SAE/LTE is also known as Evolved Packet System (EPS).

The intended audience for this book is mobile network and device architects, designers, researchers and students. The goal of the authors, who have a combined experience of more than 25 years in mobile security standardization, architecture, research, and education, is to provide the book's readers with a fresh and up-to-date look at the architecture and challenges of EPS and WiMAX security. This book includes 6 chapters, where the first 3 chapters are intended to be introductory ones, and the remaining 3 chapters provide more in-depth discussions. The book starts with Chapter 1 where we give a background of Next Generation Mobile Networks (NGMN) activity and requirements. Following explanation of NGMN, Chapter 2 provides an overview of security, telecommunication systems and their requirements. Chapter 3 provides some background on standardization. Chapter 4 discusses the EPS (or SAE/LTE) security architecture developed by 3GPP. In particular, this chapter covers the authentication and key agreement method for SAE/LTE together with newly defined key hierarchy. This chapter also addresses the challenging aspects of SAE/LTE interworking and mobility with UMTS together with the necessary key-exchange technologies. The focus of Chapter 5 is WiMAX (IEEE 802.16) security. Chapter 5 provides an in-depth discussion of the WiMAX security requirements, the authentication aspects of PKMv2, and the overall WiMAX network security aspects. In Chapter 6 we briefly cover security for (i) Home(evolved)NodeB (H(e)NB) is the Femto solution from 3GPP), (ii) Machine-to-Machine (M2M) security and (iii) Multimedia Broadcast and Multicast Service (MBMS) and Group Key Management.

Contents:

Preface;

- Introduction to next generation mobile networks (NGMN) and security requirements;
- Security basics;
- Standardization process in 3GPP and IEEE/WiMAX;
- SAE/LTE Security;
- Security in IEEE 802.16e / WiMAX;
- Security for other systems like M2M and 3GPP Femto; Abbreviations; Index.

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customercare@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

Future Trends and Challenges for ICT Standardization

Editor: Ramjee Prasad, Founding Chairman of GISFI & Director CTIF, Denmark

ISBN: 9788792329387

Available From: February 2010

Price: € 70.00



Description:

This book comes in response to the Future Trends and Challenges for ICT Standardization. The technological areas covered are:

- the need, importance and management of radio spectrum,
- the development of future radio access technologies,
- the convergence of telecommunications and broadcasting,
- the possibilities and challenges brought by the Internet of Things (IoT),
- the environment sustainability through the use of Green ICT,

The book aims at identifying the importance of ICT standardization for strengthening the Indian industrial and business sector through Global ICT Standardization Forum for India (GISFI-www.gisfi.org). Further, it outlines the major challenges and trends in the ICT development worldwide, while mapping the Indian efforts on the background of the overall progress.

The motivation behind this book is that a more informed context is made available to ensure sustainable scientific and economic growth.

Finally, the book puts forward the best research roadmaps, strategies and challenges contributed by engineers from the industry, academia, and Government. It addresses the benefits to the entire society resulting from standardization.

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customer@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

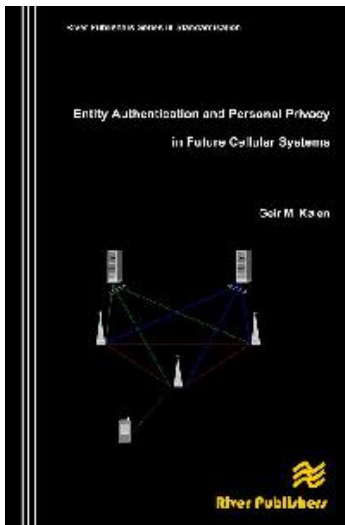
Entity Authentication and Personal Privacy in Future Cellular Systems

Editor: Dr. Geir M. Koien, Telenor R&I, Norway and University of Agder, Norway

ISBN: 9788792329325

Available From: September 2009

Price: € 85.00



Description:

There are now (Q1 2009) more than 4 billion cellular subscribers in the world and this number is constantly growing. With this in mind it should be clear that use of mobile communication has already become both pervasive and ubiquitous. It has become a global commodity really. Entity Authentication and Personal Privacy in Future Cellular Systems aims at explaining and examining access security as it is found in mobile/cellular systems. A thorough investigation of how access security and personal privacy is handled in the 3GPP system is conducted. This includes both the 2G systems GSM/GPRS and the 3G system UMTS. The emerging fourth generation LTE architecture is also examined. The first part of the book deals exclusively with presenting access security as found in the 3GPP system. Particular attention is given to the authentication and key agreement procedures. The 3GPP systems have evolved and the access security architecture in LTE is substantially more advanced and mature than what you would find in GSM/GPRS, but even the LTE security architecture has its limitations. In part two of the book we go on to examine what is missing from the current cellular access security architectures. Some of the shortcomings found in GSM/GPRS and later UMTS have been partially addressed in LTE, but the burden of backwards compatibility has meant that many issues could not easily be resolved. Free from those restrictions, we shall see that one can provide substantially improved subscriber privacy and enhanced entity authentication, while also avoiding the delegated authentication control that all 3GPP systems have.

The design of authentication protocols is discussed in depth, and this would also include looking into the role of formal verification in the design of security protocols.

Errata

ERRATA SECTION 3.3.8

[Download](#)

ERRATA SECTION 3.3.8 notes

[Download](#)

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customercare@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers Series in Security and Digital Forensics

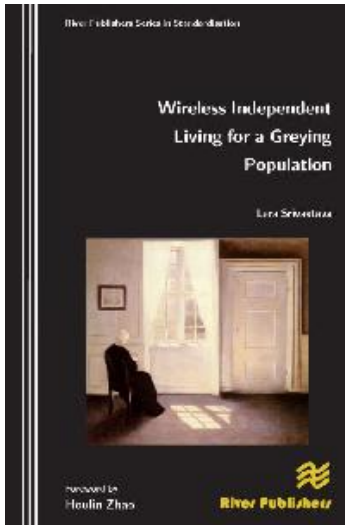
Wireless Independent Living for a Greying Population

Author: Lara Srivastava, CtiF, Aalborg University/International Telecommunications Union

ISBN: 9788792329226

Available From: April 2009

Price: € 85.00



Description:

It is widely known today that not only are the aged ageing, or the old getting older, but they are also increasing in number the world over. At the same time, proper care and support for our aged is increasingly at risk. Without some form of support, the quantitative extension of life cannot be matched by a qualitative one. This may mean that the opportunity provided by a longer life is squandered, and life itself, of course, is nothing if not opportunity. Societies find that self-sufficiency and independence not only contribute to individual well-being, but are also economically desirable due to the resultant increase in productivity.

The challenges of daily living for a growing population of the aged form the basis of the independent living platform, the AGE@HOME platform, which is described in this book. The platform combines both existing and emerging technologies suitable for the home. Its use and application is considered in the wider context of Web 2.0, the internet of things, and other elements of the burgeoning digital world. It is time that a holistic and multi-disciplinary approach to this constantly enlarging area of human existence is taken.

This book is written for researchers and designers of wireless tools, analog and digital circuits as well as academics who are active in the various fields of Human Sciences.

Foreword

"This book appears at the right moment when several developments have made age and its consequences an important element of human existence. It makes for informative reading, being based on considerations related to independence for the aged and the application of emerging technologies to enhance this independence....."

From the foreword by:

Houlin Zhao

*Deputy Secretary-General of the
International Telecommunication Union*

Contact River Publishers

Phone: +13-176899634 , +31-(0)-6-46573673
Email: customercare@riverpublishers.com
www.riverpublishers.com

The Netherlands Office

Lange Geer 44,
2611 PW Delft
The Netherlands

Denmark Office

Alsbjergvej 10
9260 Gistrup
Denmark