IEEE COMMUNICATIONS SOCIETY

Published on *IEEE Communications Society* (http://www.comsoc.org)

Best Readings in Communications and Information Systems Security

Best Readings is a collection of Books, Journals, Special Issues, articles and papers on a featured topic. This Best Readings is on Communications and Information Systems Security (CIS). For questions or comment click here.
Issued September 2013

Evaluation Committee:
Erol Gelenbe, Guangjie Han, Neeli Prasad, Peng He, Peter Stavroulakis, Pierangela Samarati, Shui Yu, Stamatios Kartalopoulos, Zheng Yan, Amitav Mukherjee, Chau Yuen, Jun He, K. P. Subbalakshmi, Maode Ma, Narisa Chu, Niki Pissinou, Raullen Chai, Roberto Di Pietro, Sushmita Ruj, Peter Mueller, Kejie Lu, Xiaodong Lin, Yi Qian.

Topics on Security

- Ad-hoc Networks
- Routing
- Integrity
- Internet of Things (IoT)
- Anonymity
- Voice over IP (VoIP)
- WiMAX (IEEE 802.16)
- RFID
- Cryptographic Procedures
- Cloud
- Security Management
- Smartphone

Special Issues

Peter Stavroulakis, "Special Issue on Multimedia Information Security", InderSience, International Journal of Multimedia Intelligence and Security, Vol. 1 No. 4, 2010.
Five years after the appearance of the first publications on CIS in International technical Journals and the creation of the IEEE TC-CIS, the multimedia field was open for a revisit from the security point of view. Cloud computing security thus became the main new research challenge. An attempt has been made to fill this void by this special issue. Advanced techniques such as fuzzy logic, Hidden Marcov Models, the zero knowledge principle and chaotic techniques are presented to show that Multimedia Information Security can be dealt with as an integral part of CIS.

Journals

Hsiao-Hwa Chen (Ed.), "Security and Communication Networks", Wiley, ISSN 1939-0122.
Security and Communication Networks is an international journal publishing original research and review papers on security and cryptographic mechanisms applied to all types of information and communication networks, including wired, wireless and optical transmission platforms. The journal provides a prestigious forum for the R&D community in academia and industry working at the inter-disciplinary nexus of next generation communications technologies with physical and upper layer network security implementations. Answering the highly practical and commercial importance of network security R&D, submissions of applications-oriented papers describing case studies and simulations are encouraged as well as research analysis-type papers.

Sabu M. Thampi (Ed.), "International Journal of Trust Management in Computing and Communications", InderScience, ISSN 2048-8378.
The volatile growth of the internet and globalization that influences every facet of life are fuelled by the rapid acceleration of computing/communication technologies. Although security is a major concern, we must also protect ourselves from false/misleading information provided by some

information/service providers. Traditional security mechanisms cannot protect against this type of threat. Trust management mechanisms on the other hand can provide protection. IJTMCC provides a forum for discussion on theoretical and practical aspects of the latest developments in this area.

Books

Stamatios Kartalopoulos, "Security of Information and Communication Networks", IEEE/Wiley, 2009, ISBN 978-0470290255.
This CHOICE awarded book provides a complete conceptual treatment of securing information and transporting it over a secure network in a manner that does not require a strong mathematical background. It stresses why information security is important, what is being done about it, how it applies to networks, and an overview of its key issues. It is written for anyone who needs to understand these important topics at a conceptual rather than a technical level.

Anestis Karasaridis, "DNS Security", Amazon (KDP), 2012.
The objective of this book is to give the reader an in-depth understanding of how the Domain Name System (DNS) works, its security vulnerabilities, how to monitor and detect security related events and how to prevent and mitigate attacks. After reading the book, the reader will be able to recognize the major issues around DNS security, and know the best practices to setup, operate, and protect DNS service. The book also explores active areas of research and development in anomaly detection, authentication, and attack mitigation. Sections of the book can be used in academic courses as assigned readings.

Mohssen Mohammed and Al-Sakib Khan Pathan, "Automatic Defense against Zero-day Polymorphic Worms in Communication Networks", CRC Press, Taylor & Francis Group, 2013, ISBN 978-1466557277.
Able to propagate quickly and change their payload with each infection, polymorphic worms have been able to evade even the most advanced intrusion detection systems. And, because zero-day worms require only seconds to launch flooding attacks on your servers, using traditional methods such as manually creating and storing signatures to defend against these threats is just too slow. Bringing together critical knowledge and research on the subject, this book details a new approach for generating automated signatures for unknown polymorphic worms. It presents experimental results on a new method for polymorphic worm detection and examines signature-generation algorithms and double-honeynet systems.

Shafiullah Khan and Al-Sakib Khan Pathan, "Wireless Networks and Security: Issues, Challenges and Research Trends", Springer Series: Signals and Communication Technology, 2013, ISBN 978-3-642-36168-5.
Wireless Networks and Security provides a broad coverage of wireless security issues including cryptographic coprocessors, encryption, authentication, key management, attacks and countermeasures, secure routing, secure medium access control, intrusion detection, epidemics, security performance analysis, security issues in applications. The contributions identify various vulnerabilities in the physical layer, MAC layer, network layer, transport layer, and application

layer, and focus on ways of strengthening security mechanisms and services throughout the layers. This carefully edited monograph is targeting for researchers, post-graduate students in universities, academics, and industry practitioners or professionals.

Al-Sakib Khan Pathan, "Security of Self-Organizing Networks: MANET, WSN, WMN, VANET", Auerbach Publications, CRC Press, Taylor & Francis Group, 2010, ISBN 978-1-4398-1919-7.
Reflecting recent advancements, Security of Self-Organizing Networks: MANET, WSN, WMN, VANET explores wireless network security from all angles. It begins with a review of fundamental security topics and often-used terms to set the foundation for the following chapters. Examining critical security issues in a range of wireless networks, the book proposes specific solutions to security threats. Ideal for those with a basic understanding of network security, the text provides a clear examination of the key aspects of security in self-organizing networks and other networks that use wireless technology for communications.

Tansu Alpcan and Tamer Ba?ar, "Network Security: A Decision and Game Theoretic Approach", Cambridge University Press, 2010, ISBN 978-0521119320.
Covering attack detection, malware response, algorithm and mechanism design, privacy, and risk management, this comprehensive work applies unique quantitative models derived from decision, control, and game theories to understanding diverse network security problems. It provides the reader with a system-level theoretical understanding of network security, and is essential reading for researchers interested in a quantitative approach to key incentive and resource allocation issues in the field. It also provides practitioners with an analytical foundation that is useful for formalizing decision-making processes in network security.

Andrei Gurtov, "Host Identity Protocol (HIP): Towards the Secure Mobile Internet", Wiley, 2008, ISBN 978-0-470-99790-1.
One of the challenges facing the current Internet architecture is the incorporation of mobile and multi-homed terminals (hosts), and an overall lack of protection against Denial-of-Service attacks and identity spoofing. The Host Identity Protocol (HIP) is being developed by the Internet Engineering Task Force (IETF) as an integrated solution to these problems. The book presents a well-structured, readable and compact overview of the core protocol with relevant extensions to the Internet architecture and infrastructure. The covered topics include IPsec, Overlay Routable Cryptographic Hash Identifiers, extensions to the Domain Name System, IPv4 and IPv6 interoperability, and support for legacy applications.

Lynn Batten, "Public Key Cryptography: Applications and Attacks", IEEE/Wiley, 2013, ISBN 978-1118317129.
This book describes in depth all major public-key cryptosystems in current use, including ElGamal, RSA, Elliptic Curve, and digital signature schemes. It explains the underlying mathematics needed to build these schemes, and examines the most common techniques used in attacking them. The book includes many examples, and it provides a solid foundation for professionals in government, service providers, and large enterprises that use public-key systems to secure their data.

Peter Stavroulakis and Mark Stamp (Eds.), "Handbook of Information and Communication Security", Springer, 2010, ISBN 978-3-642-04117-4.

This Handbook covers for the first time in a compact and integral form all the latest advances in fundamentals, cryptography ,intrusion detection, access control, networking, software, forensics including extensive sections on optics as well as legal issues and thus setting the conceptual definition of the field of CIS. In addition the topics covered are highly relevant to the real world practice of information security which makes it a valuable resource for working IT professionals as well as academics and active researchers.

Peter Stavroulakis (Ed.), "TErrestrial Trunked RAdio - TETRAA Global Security Tool ", Springer, 2007, ISBN 978-3-540-71190-2.
Terrestrial Trunked Radio (TETRA) until recently was considered as a medium for only public safety applications. In the book new advances in in Channel assignment and multiple access techniques , video transmission, wireless LAN integration, and the establishment of multiple wireless mesh networks are examined from the security point of view and is shown that TETRA can be used for large scale systems security such as Olympic Games and thus become the vehicle for a Global Security tool.

Peter Stavroulakis (Ed.), "Chaos Applications in Telecommunications", CRC Taylor and Francis, 2006, ISBN 8493-3832-8.
Up until this book was published, Chaos was not considered as a technique that enhances greatly security. Besides showing how classical transmission and reception methods can be put on a more secure framework by using chaotic techniques, it is shown that it even outperforms the other classical method for security which is based on spread spectrum. This volume provides the essential information for those who wish to have an integrated view on how an established concept such as chaos can open new roads in the CIS field.

Xiali Hei and Xiaojiang Du, "Security in Wireless Implantable Medical Devices", Springer, 2013, ISBN 978-1-4614-7152-3.
In the treatment of chronic diseases, wireless Implantable Medical Devices (IMDs) are commonly used to communicate with an outside programmer (reader). Such communication raises serious security concerns, such as the ability for hackers to gain access to a patient's medical records. This book provides an overview of such attacks and the new security challenges, defenses, design issues, modeling and performance evaluation in wireless IMDs.

Yang Xiao, Xuemin Shen and Dingzhu Du, "Wireless Network Security", Series: Signals and Communication Technology, Springer, 2007, ISSN 0387280405.
This timely volume, Wireless Network Security, provides broad coverage of wireless security issues including cryptographic coprocessors, encryption, authentication, key management, attacks and countermeasures, secure routing, secure medium access control, intrusion detection, epidemics, security performance analysis, security issues in applications, and much more. The contributions identify various vulnerabilities in the physical layer, MAC layer, IP layer, transport layer, and application layer, and focus on ways for strengthening security mechanisms and services throughout the layers.

Seok-Yee Tang, Peter Mueller and Hamid R. Sharif (Eds.), "WiMAX Security and Quality of Service", Wiley and Sons, 2010, ISBN 978-1-119-95620-4.
WiMAX is the first standard technology to deliver true broadband mobility at speeds that enable

powerful multimedia applications such as Voice over Internet Protocol (VoIP), online gaming, mobile TV, and personalized infotainment. WiMAX Security and Quality of Service, focuses on the interdisciplinary subject of advanced Security and Quality of Service (QoS) in WiMAX wireless telecommunication systems including its models, standards, implementations, and applications. Split into 4 parts, Part A of the book is an end-to-end overview of the WiMAX architecture, protocol, and system requirements. Security is an essential element in the wireless world and Part B is fully dedicated to this topic. Part C provides an in depth analysis of QoS, including mobility management in WiMAX. Finally, Part D introduces the reader to advanced and future topics.

Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis and Sabrina De Capitani di Vimercati (Eds.), "Digital Privacy: Theory, Technologies and Practices", Auerbach Publications, Taylor & Francis, 2007, ISBN 978-1420052176.
Throughout recent years, a continuously increasing amount of personal data has been made available through different Web sites around the world. Although the availability of personal information has created several advantages, it can be easily misused and may lead to violations of privacy. Privacy, as a fundamental human right, must be protected. With growing interest in this area, Digital Privacy: Theory, Technologies, and Practices addresses this timely issue, providing information on state-of-the-art technologies, best practices, and research results, as well as legal, regulatory, and ethical issues. This book features contributions from top experts in academia, industry, and government.

H. Mouratidis (Ed.), "Software Engineering for Secure Systems: Industrial and Research Perspectives", IGI Global, 2011, ISBN 978-1615208371.
Software Engineering for Secure Systems: Industrial and Research Perspectives presents the most recent and innovative lines of research and industrial practice related to secure software engineering. The book provides coverage of recent advances in the area of secure software engineering that address the various stages of the development process from requirements to design to testing to implementation. Contributions offer a comprehensive understanding secure software engineering, inspire and motivate further research and development, and bridge the gap between academic research and industrial practice.

Matthieu Bloch and João Barros, "Physical-Layer Security: From Information Theory to Security Engineering ", Cambridge University Press, 2011, ISBN 978-0521516501.
This complete guide to physical-layer security presents the theoretical foundations, practical implementation, challenges and benefits of a groundbreaking new model for secure communication. Using a bottom-up approach, it provides essential practical tools that enable graduate students, industry professionals and researchers to build more secure systems by exploiting the noise inherent to communications channels. The book begins with a self-contained explanation of the information-theoretic limits of secure communications at the physical layer. It then goes on to develop practical coding schemes, enabling readers to understand the challenges and opportunities related to the design of physical layer security schemes.

Source URL: http://www.comsoc.org/best-readings/communications-and-information-systems-security