

Handbook on Securing Cyber-Physical Critical Infrastructure: Foundations and Challenges

Sajal K. Das, Krishna Kant, Nan Zhang
Elsevier | Morgan Kaufmann

Book review by Katina Michael, School of Information Systems and Technology, University of Wollongong, Australia
Phone: +61242213937; Fax: +61242214045; katina@uow.edu.au

Das, Kant and Zhang have done a brilliant job editing *Securing Cyber-Physical Critical Infrastructure*, bringing together a who's who list of researchers and practitioners. Das is a University distinguished Scholar Professor of Computer Science and Engineering at the University of Texas Arlington with more than 500 published papers, three books and the editorship at Elsevier's *Pervasive and Mobile Computing* journal. Kant is a research professor at the Center for Secure Information Systems at George Mason University, Fairfax, VA. Kant comes equipped with many years of academic experience and industry exposure at Bell Labs, Telcordia and Intel, as well as government positions including at the National Science Foundation (NSF). Finally, Zhang, the third book's editor, was an assistant professor of Computer Science and Engineering at the University of Texas at Arlington from 2006-2008 and is currently researching databases and information security/privacy. Zhang received the prestigious NSF CAREER award in 2008.

This 800+ page handbook is divided into eight parts and contains thirty chapters, ideal for either an advanced undergraduate or graduate course in security. At the heart of this handbook is how we might go about managing both physical and cyber infrastructures, as they continue to become embedded and enmeshed, through advanced control systems, and new computing and communications paradigms.

Part I provides theoretical foundations in the area of control theory, game theory and epidemic theory as applied to cyber-physical infrastructure management. Part II focuses on security for wireless mobile networks. Robert Brammer who wrote the foreword of the handbook, emphasized the successes of the New York City Wireless Network (NYCWIn), motivated partly by the events of 9/11. NYCWiN became operational in 2009 and its cyber-physical systems architecture has addressed issues in the control of transport, public health, environmental quality and communications during critical emergencies. Part III covers security for sensor networks which are fast becoming integral for monitoring and controlling cyber-physical systems. These systems provide much of the feedback mechanism, forewarning or alerting to subsystems when things go wrong. As we increasingly become reliant on sensor networks, we need to ensure that they are as secure and reliable.

Parts IV and V position the importance of platform security, and address cloud computing and data security. The section on platform security includes chapters on traditional hardware and software vulnerabilities and presents solutions that could be employed to make it even more difficult for large-scale systems to be penetrated. The section on cloud computing makes sure to emphasize how systems are changing in terms of outsourcing to companies whose core competency is information technology infrastructure, platforms and services. The

cloud, mobile devices, and online social networks are particularly creating opportunities for hackers toward data breaches, and this is discussed in detail.

Part VI and VII are on event monitoring and situation awareness, as well as policy issues in security management. These chapters provide approaches to systems monitoring, discovery and tracking patterns of interest in security data streams, discontinuous clustering, sequencing, geo-spatial temporal correlations and other event detections mechanisms. For those seeking examples of how such systems monitoring occur, there are equations, algorithms, proofs, process flows, physical infrastructure layout maps, pictorial evidence, graphs, tables, and example simulation outputs to spend hours and hours exploring further. Finally, policies, access control and formal analysis methods for overseeing security in cyber-physical critical infrastructure are also shown.

The biggest highlight for me personally was the coming together of Parts I-VII in the security issues in real-world systems presented in Part VIII which brings home the relevance and timeliness of this handbook today. Chapters 25-30 could have been a book in their own right for their depth of insight into emerging smart infrastructures- including smart grids, automotive information technology, mobile health care systems, internet infrastructure, emergency vehicular networks, and more broadly unified telecommunications infrastructure using Voice over Internet Protocol (VoIP). It is not too difficult to see the complexities of these big systems needing to interact with each other and the security and privacy concerns this might raise.

As noted by the authors, the handbook could be used to cover courses on security and robustness of computer networks, the security in physical infrastructure, or even the security in cyber infrastructure. Today, we are witnessing a paradigm shift toward autonomous systems, and despite most physical infrastructure being considered legacy, even the old wires and cables are becoming “switched onto” the cyber. An understanding of both these elements is crucial in engineering and maintaining better working and resilient systems for the future.