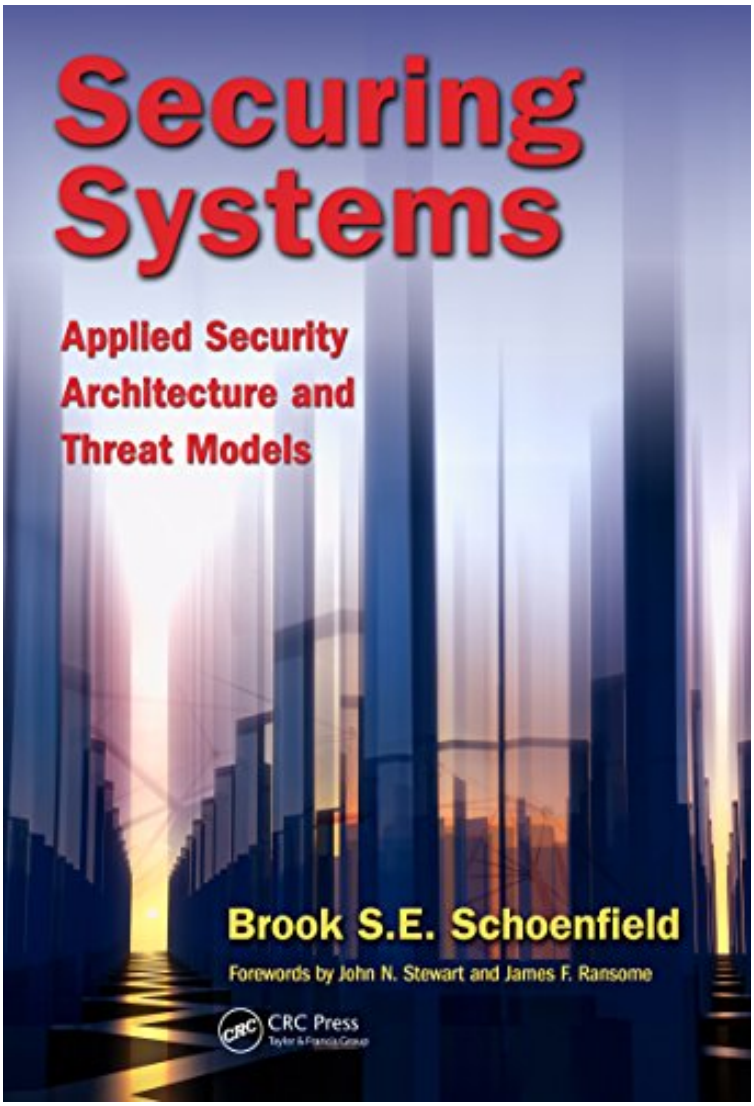
[Read free] Securing Systems: Applied Security Architecture and Threat Models

Securing Systems: Applied Security Architecture and Threat Models

Brook S. E. Schoenfield
*audiobook | *ebooks | Download PDF | ePub | DOC*



Download Read Online

#286933 in eBooks 2015-05-20 2015-05-20File Name: B00XKX1FK8 | File size: 20.Mb

Brook S. E. Schoenfield : Securing Systems: Applied Security Architecture and Threat Models before purchasing it in order to gage whether or not it would be worth my time, and all praised Securing Systems: Applied Security Architecture and Threat Models:

1 of 2 people found the following review helpful. A must read book for software security architecture and threat modelingBy Robert HurlbutThis is a solid entry in the list of "must read books" for software security architecture and threat modeling. Brook Schoenfield's writing is clear and concise - it is always a pleasure for me to read his writing. For a great introduction to Brook's writing, also read his chapter "Applying the SDL Framework to the Real World" in

Core Software Security Core Software Security: Security at the Source, another highly recommended book.In this book, Brook helps you understand aspects of security architecture and introduces his recommendations for running a security assessment. It is the security assessment part (i.e. threat modeling) that drew me to the book and for which the book shines. Brook talks about applying the threat modeling pedagogy ATASM which stands for:ATASM Architecture Threats Attack Surfaces MitigationsUsing these tools, a software or security architect is able to decompose the system (understand the architecture), enumerate the threats, expose what attack surfaces are present in the architecture, and finally determine the best ways to mitigate the threats and attack surfaces with sufficient security controls. Brook gives several examples of applying ATASM to sample systems such as an eCommerce Website, a mobile security system, a Cloud-based Software as a Service (SaaS) system, and several others.I thoroughly enjoyed this book and I have been recommending it to all my clients in my own threat modeling practice.2 of 3 people found the following review helpful. One of the best books on software securityBy Matt ParsonsI felt like I was having a riveting conversation with Brook. His book is one of the best and most exciting software security books I have ever read. Brook is a great guy and knows his security architecture. Awesome book, five stars!!!9 of 11 people found the following review helpful. Easily the Best Security Architecture Book in Print - IMHOP the Seminal Tutorial and HandBook.By Mr. Bookish, Mild and MeekEasily the Best Security Architecture Book in Print - IMHOP the Seminal Tutorial and HandBook.The SABSA book: http://www..com/Enterprise-Security-Architecture-Business-Driven-Approach/dp/157820318X/ref=sr_1_2?s=booksie=UTF8qid=1437060092sr=1-2 has been the de facto Security Architecture handbook book for most security professionals and for I myself as a Security Architect. But it was published around 2005 and whilst very methodical, risk- and business-focussed and originally near-comprehensive it has in the last few years begun to show its age and indeed to lose its practical relevance in a dynamic Threat, Security, IT and Business ecosystem with key business, risk and technology forces such as OutSourcing and Third-Party Access, Privacy Concerns, Advanced Persistent Threats (APT), increasing relevance of Web Application Security, Mobile and Cloud Technologies, etc. That book is crying for a new edition to bring the content and case studies up to date. I am supposing the Authors' SABSA courses are probably more up-to-date. (I have not attended any of them, but I have read and do refer to the book often).This, Mr. Schonfield's book is not nearly as methodical or comprehensive but in my view it is definitely a much better book and more suited to contemporary Security Architecture forces and practice. It is quite concise, immensely readable, up-to-date, pragmatic and accurately reflects how expert Information Security Architects go about their job and what they do or how they should be doing it. It also discusses issues such as effective stakeholder liaison and several other practical considerations in Security Architecture formulation and review. It is also admirable how the author makes it all readable, pragmatic, yet quite concise and quite comprehensive. It is many years expert Security Architecture and Strategy experience synthesized brilliantly into about 400 pages. The case studies are very well done, useful and cover several contemporary security challenges. In my humble opinion it is a MUST read for every Security Architecture professional - beginner to expert - and student. I would even dare say all Security professionals, Enterprise, Application, Data and Infrastructure/Network Architects who work on IT projects that require Security and whose Designs will be reviewed by Security Consultants must read it. Chief Information Security Officers, in particular, need to read this book to help them get the right perspective for formulating Enterprise Security Strategies, Architectures and Programmes.I think this is the best Security Architecture book around; but the following book does better when looking at Security technologies: http://www..com/Enterprise-Cybersecurity-Successful-Cyberdefense-Advanced/dp/1430260823/ref=pd_sim_sbs_14_3?ie=UTF8refRID=1F93ZP91W6JFJ6MD92M6 It is another excellent, modern Security Architecture book and one should also read that book to round up one's knowldge and skills. For methodology, and risk and business drivers orientation none beats the SABSA book; which I believe still remains relevant; but one neeeds to tailor it's the SABSA methodolgy to one's organisational or project circumatsnaces as for most situations it could be overkill.

Internet attack on computer systems is pervasive. It can take from less than a minute to as much as eight hours for an unprotected machine connected to the Internet to be completely compromised. It is the information security architectrsquo;s job to prevent attacks by securing computer systems. This book describes both the process and the practice of assessing a computer systemrsquo;s existing information security posture. Detailing the time-tested practices of experienced security architects, it explains how to deliver the right security at the right time in the implementation lifecycle.Securing Systems: Applied Security Architecture and Threat Models covers all types of systems, from the simplest applications to complex, enterprise-grade, hybrid cloud architectures. It describes the many factors and prerequisite information that can influence an assessment. The book covers the following key aspects of security analysis:When should the security architect begin the analysis?At what points can a security architect add the most value?What are the activities the architect must execute?How are these activities delivered?What is the set of knowledge domains applied to the analysis?What are the outputs?What are the tips and tricks that make security architecture risk assessment easier?To help you build skill in assessing architectures for security, the book presents six sample assessments. Each assessment examines a different type of system architecture and introduces at least one new

pattern for security analysis. The goal is that after yoursquo;ve seen a sufficient diversity of architectures, yoursquo;ll be able to understand varied architectures and can better see the attack surfaces and prescribe security solutions.

"Brook Schoenfield has distilled a tremendous amount of practical experience and critical thinking about security architecture into a resource that should be extremely helpful to practitioners." Jack Jones, Originator of The Open Group Standard, Factor Analysis for Information Risk (FAIR) "Five stars for Brook Schoenfield who has created a one-stop resource for both the security strategist/technologist and the executive suite, sounding the lsquo;proactiversquo; klaxon. The reader is given substantive exemplars on the practicality of architecting security solutions into the mix from the get-go, and obviating the tendency to lsquo;bolt onrsquo; security at a later date. Securing Systems should be on every CSOrsquo;s and CISOrsquo;s desk, and referenced often as teams are built and security solutions architected." Christopher Burgess, CEO, Prevendra Inc, Author of Secrets Stolen, Fortunes Lost and Protecting Intellectual Property "Brook Schoenfieldrsquo;s approach to securing systems addresses the entire enterprise, not only its digital systems, as well as the processes and people who will interact, design, and build the systems. This book fills a significant gap in the literature and is appropriate for use as a resource for both aspiring and seasoned security architects alike." Dr. James F. Ransome, CISSP, CISM, Senior Director of Product Security at Intel Security Group and Co-Author of Core Software Security "It is not good enough just to build something and try and secure it, it must be architected from the bottom up with security in it, by professionally trained and skilled security architects, checked and validated by regular assessments for weakness, and through a learning system that learns from today to inform tomorrow. We must succeed." John N. Stewart, SVP Chief Security Officer, Cisco Security and Trust Organization and Winner of the CSO 40 Silver Award for the 2014 Chief Security Officer of the Year "This book describes well why some companies are successful and some are not in the area of software security. Brook writes this book out of his own experiences from many years in the trade. I doubt that you can find many who have more years of great achievements in his field. By reading this book, you will get a fast track to build competence in a very advanced area. The possibilities to take the wrong route are much wider than you can imagine. Please do like me read it and think how I can improve my daily business from what I have learned." Per-Olof Persson, Head of Software Security, Sony MobileAbout the AuthorBrook S.E. Schoenfield is Director of Product Security Architecture at Intel Security Group. He is the senior technical leader for software security across the divisionrsquo;s broad product portfolio. He has held leadership security architecture positions at high-tech companies for many years. Brook has presented at conferences such as RSA, BSIMM, and SANS What Works Summits on subjects within security architecture, including architecture risk assessment and threat models, information security risk, SaaS/Cloud security, and Agile security. He has been published by CRC Press, SANS, Cisco, and the IEEE.