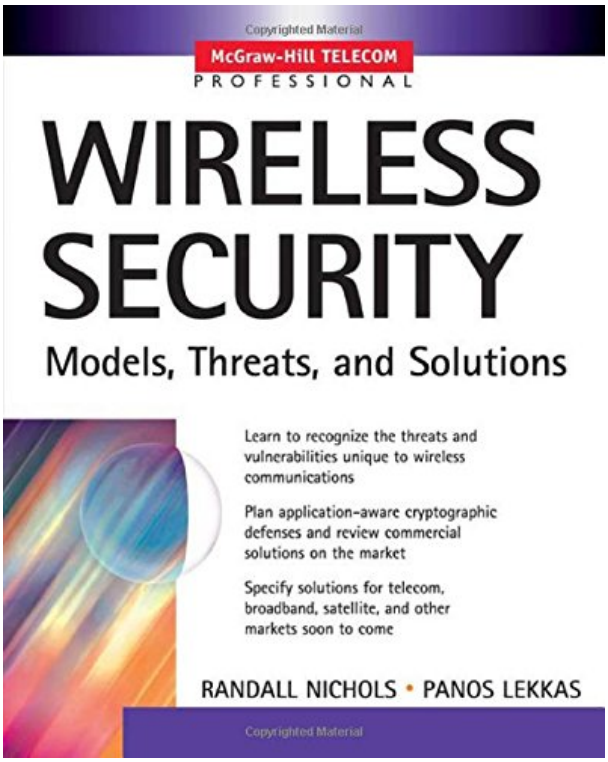
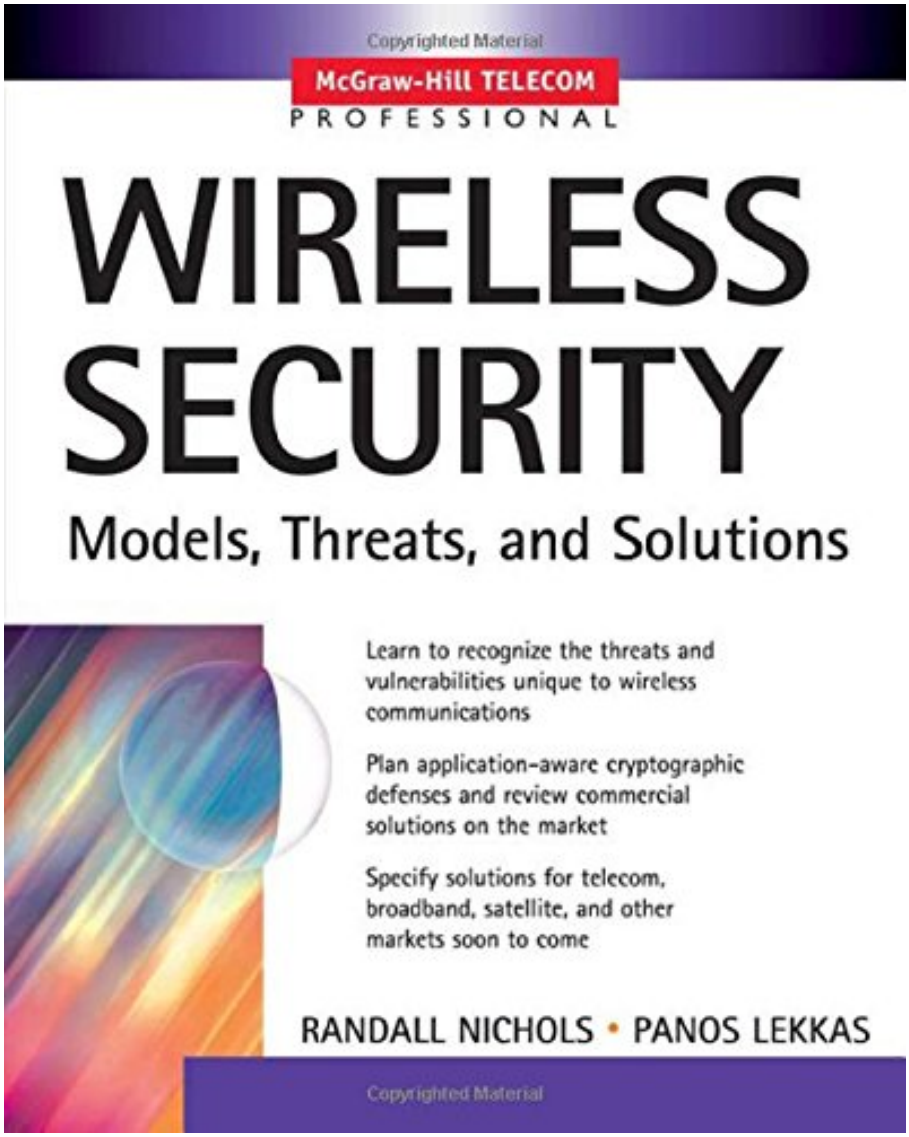
WIRELESS SECURITY: MODELS, THREATS, AND SOLUTIONS BY RANDALL K. NICHOLS, PANOS C. LEKKAS





WIRELESS SECURITY: MODELS, THREATS, AND SOLUTIONS BY RANDALL K. NICHOLS, PANOS C. LEKKAS PDF

Get the perks of checking out habit for your life style. Reserve Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas message will always associate with the life. The real life, knowledge, science, health, religious beliefs, enjoyment, as well as a lot more can be located in composed e-books. Many writers offer their encounter, science, research study, as well as all points to share with you. One of them is through this Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas This e-book Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas will certainly supply the needed of message and declaration of the life. Life will be finished if you understand more points through reading books.

Review

J.M. (Mike) McConnell, Vice Admiral, USN (Ret), Vice President, Booz, Allen & Hamilton, Inc. and former Director of the National Security Agency (NSA), 1992-1996, sets the stage for this timely book with a perceptive Foreword that states the problem in his first sentence: "The safeguarding of information traveling over wireless technology has quickly become one of the most important and contentious challenges facing today's technology innovators."

With their book, Nichols and Lekkas pick up the gauntlet and provide a comprehensive guide for managers and policy makers involved with wireless communications. They explain the vulnerabilities, response options, and real-world costs associated with wireless platforms and applications, plus information needed to help develop the background and skills required to: Recognize new and established threats to wireless systems; Close gaps that threaten privacy, profits, and customer loyalty; Replace temporary, fragmented, and partial solutions with more robust and durable answers; Weigh platforms against characteristic attacks and protections; Apply clear guidelines for the best solutions now and going forward; Prepare for the boom in m-business; Assess today's protocol options and compensate for documented shortcomings.

This book is also an encyclopedic guide to the state of the art with: Encryption algorithms you can use now, End-to-end hardware solutions and field programmable gate arrays, An extensive guide to speech cryptology, Authentication strategies and security protocols for wireless systems, Infosec and infowar experience, Adding satellites to your security mix and much more. The book is another blockbuster... (The Cryptogram, Journal of the American Cryptogram Association 2002-03-01)

From the Back Cover
REAL-WORLD WIRELESS SECURITY

This comprehensive guide catalogs and explains the full range of the security challenges involved in wireless communications. Experts Randall K. Nichols and Panos C. Lekkas lay out the vulnerabilities, response

options, and real-world costs connected with wireless platforms and applications. Read this book to develop the background and skills to--

* Recognize new and established threats to wireless systems
* Close gaps that threaten privary, profits, and customer loyalty
* Replace temporary, fragmented, and partial solutions with more robust and durable answers
* Prepare for the boom in m-business
* Weigh platforms against characteristic attacks and protections
* Apply clear guidelines for the best solutions now and going forward
* Assess today's protocol options and compensate for documented shortcomings

A COMPREHENSIVE GUIDE TO THE STATE OF THE ART

* Encryption algorithms you can use now
* End-to-end hardware solutions and field programmable gate arrays
* Speech cryptology
* Authentication strategies and security protocols for wireless systems
* Infosec and infowar experience
* Adding satellites to your security mix

About the Author

RANDALL NICHOLS is Vice President of Cryptography for TeleHubLink Corporation, where he directs development of embedded security solutions. He is Professor of Information Security at George Washington University and the author of four books on communications security, including McGraw-Hill's ICSA Guide to Cryptography.

PANOS LEKKAS is Chief Technology Officer and General Manager of Technology for TeleHubLink. Originally a VLSI designer, Mr. Lekkas worked for many years for IBM, where he was instrumental in the introduction of RISC architecture. Before joining TeleHubLink, he was President and CEO of wirelessEncryption.com, where he invented and developed telecom security.

WIRELESS SECURITY: MODELS, THREATS, AND SOLUTIONS BY RANDALL K. NICHOLS, PANOS C. LEKKAS PDF

Tips in picking the most effective book **Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas** to read this day can be obtained by reading this web page. You can locate the very best book Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas that is offered in this world. Not only had the books released from this nation, yet additionally the various other nations. And now, we intend you to read Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas as one of the reading materials. This is only one of the most effective books to collect in this site. Take a look at the page and browse guides Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas You can locate lots of titles of the books given.

Obtaining guides *Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas* now is not kind of hard method. You could not only going with e-book shop or library or borrowing from your good friends to read them. This is a really straightforward means to precisely get the book by on-line. This on the internet book Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas could be one of the choices to accompany you when having leisure. It will not squander your time. Believe me, the publication will certainly reveal you new thing to check out. Merely spend little time to open this on the internet publication Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas and also review them anywhere you are now.

Sooner you get guide Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas, sooner you can take pleasure in reading guide. It will certainly be your rely on keep downloading and install guide Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas in given web link. This way, you could truly choose that is served to obtain your personal e-book online. Right here, be the first to obtain the book entitled Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas and be the initial to recognize just how the author suggests the message as well as understanding for you.

WIRELESS SECURITY: MODELS, THREATS, AND SOLUTIONS BY RANDALL K. NICHOLS, PANOS C. LEKKAS PDF

This comprehensive guide catalogues and explains the full range of the security challenges involved in wireless communications. Experts Randall K. Nichols and Panos C. Lekkas lay out the vulnerabilities, response options, and real-world costs connected with wireless platforms and applications. Read this book to develop the background and skills to: recognize new and established threats to wireless systems; close gaps that threaten privacy, profits, and customer loyalty; replace temporary, fragmented, and partial solutions with more robust and durable answers; prepare for the boom in m-business; weigh platforms against characteristic attacks and protections; apply clear guidelines for the best solutions now and going forward; and assess today's protocol options and compensate for documented shortcomings. It is a comprehensive guide to the states-of-the-art. It includes: encryption algorithms you can use now; end-to-end hardware solutions and field programmable gate arrays; speech cryptology; authentication strategies and security protocols for wireless systems; infosec and infowar experience; and adding satellites to your security mix.

- Sales Rank: #511406 in Books
- Brand: Brand: McGraw-Hill Professional
- Published on: 2001-12-13
- Original language: English
- Number of items: 1
- Dimensions: 9.20" h x 1.67" w x 7.30" l, 3.04 pounds
- Binding: Paperback
- 657 pages

Features

- Used Book in Good Condition

Review

J.M. (Mike) McConnell, Vice Admiral, USN (Ret), Vice President, Booz, Allen & Hamilton, Inc. and former Director of the National Security Agency (NSA), 1992-1996, sets the stage for this timely book with a perceptive Foreword that states the problem in his first sentence: "The safeguarding of information traveling over wireless technology has quickly become one of the most important and contentious challenges facing today's technology innovators."

With their book, Nichols and Lekkas pick up the gauntlet and provide a comprehensive guide for managers and policy makers involved with wireless communications. They explain the vulnerabilities, response options, and real-world costs associated with wireless platforms and applications, plus information needed to help develop the background and skills required to: Recognize new and established threats to wireless systems; Close gaps that threaten privacy, profits, and customer loyalty; Replace temporary, fragmented, and partial solutions with more robust and durable answers; Weigh platforms against characteristic attacks and protections; Apply clear guidelines for the best solutions now and going forward; Prepare for the boom in m-

business; Assess today's protocol options and compensate for documented shortcomings.

This book is also an encyclopedic guide to the state of the art with: Encryption algorithms you can use now, End-to-end hardware solutions and field programmable gate arrays, An extensive guide to speech cryptology, Authentication strategies and security protocols for wireless systems, Infosec and infowar experience, Adding satellites to your security mix and much more. The book is another blockbuster... (The Cryptogram, Journal of the American Cryptogram Association 2002-03-01)

From the Back Cover
REAL-WORLD WIRELESS SECURITY

This comprehensive guide catalogs and explains the full range of the security challenges involved in wireless communications. Experts Randall K. Nichols and Panos C. Lekkas lay out the vulnerabilities, response options, and real-world costs connected with wireless platforms and applications. Read this book to develop the background and skills to--

* Recognize new and established threats to wireless systems
* Close gaps that threaten privary, profits, and customer loyalty
* Replace temporary, fragmented, and partial solutions with more robust and durable answers
* Prepare for the boom in m-business
* Weigh platforms against characteristic attacks and protections
* Apply clear guidelines for the best solutions now and going forward
* Assess today's protocol options and compensate for documented shortcomings

A COMPREHENSIVE GUIDE TO THE STATE OF THE ART

* Encryption algorithms you can use now
* End-to-end hardware solutions and field programmable gate arrays
* Speech cryptology
* Authentication strategies and security protocols for wireless systems
* Infosec and infowar experience
* Adding satellites to your security mix

About the Author
RANDALL NICHOLS is Vice President of Cryptography for TeleHubLink Corporation, where he directs development of embedded security solutions. He is Professor of Information Security at George Washington University and the author of four books on communications security, including McGraw-Hill's ICSA Guide to Cryptography.

PANOS LEKKAS is Chief Technology Officer and General Manager of Technology for TeleHubLink. Originally a VLSI designer, Mr. Lekkas worked for many years for IBM, where he was instrumental in the introduction of RISC architecture. Before joining TeleHubLink, he was President and CEO of wirelessEncryption.com, where he invented and developed telecom security.

Most helpful customer reviews

10 of 10 people found the following review helpful.
Impressive work on a very hard-to-define subject!

By A Customer
The subject of security in the wireless field is a rather confusing one. It relies on an intricate web of multiple and tightly interweaved technical and scientific disciplines way beyond what the average Berkeley "kid" will ever dream to hack. One is usually not an expert in all of these areas. The field has therefore been and pretty much remains the domain of a few top-notch pros.
To master the subject however does not mean that one has suddenly come up with an all-encompassing solution or a magic checklist. It rather means that one has acquired a broad and dense set of knowledge from communications theory to cryptography and from electrical engineering to network design that will allow one to apply discernment as to what may go wrong in a project and what options there are to address the issues, what may work and what may not work and above all why. Before you cook you must know what a kitchen is and what utensils are needed for what purpose.
WIRELESS SECURITY is not a cookbook. It is a massive and scholary exposition of lots of inter-related material much of which cannot be easily found elsewhere and even that which can be found elsewhere will require time and money until one produces it on one's desk, like the material on stream ciphers, on voice processing, or on embedded end-to-end secure systems that transcend vocoders and network infrasrtuctures.
Besides themselves, the authors have put together an impressive list of individual contributors to this book that reads like a Who's Who list from the government military and intelligence communications field and this brings an extra aura of authority and competence to this book. Many books these days are written by a self-appointed expert, usually a fly-by-night quasi-consultant, whose academic credentials at best span an evening class at a local community college and whose major technical accomplishment is that they can safely....start a C-language compiler from the command line, yet they portray themselves as undisputed experts on a cutting-edge subject.
Well WIRELESS SECURITY is not one of those books. It is a heavy-duty impressive textbook that has been clearly written by professionals for readers with a broad thirst and a deep desire to understand the multiple dimensions of the problem of wireless security. It does not give answers to all your questions, in fact it will generate many more questions in your head, but it will help you form a clear idea of contexts, possibilities, ramifications and implications, and more importantly it will steer you to the right direction for subsequent research on a subject. Isn't that however what a good textbook is supposed to be all about?
The book makes the reader sensitive about issues that many people (even professionals) today are simply not even aware about. It covers lots and lots of material from many relevant and seemingly remote areas, spanning from cryptography and voice processing all the way to integrated systems design, and from high-power eavesdropping techniques in the era of CDMA to weaknesses in the set up of wireless LANs.
Of course, if one is looking for a crytography-fundamentals book there are others that are much better suited to the subject. Or if one is looking for a How-To-set-up-your-LAN-by-grilling-your-vendors type of book full of checklists, then this is not for you. There are several other books on certain aspects of wireless security in the market, that are much less scholarly, and certainly less pricey than this one.
If one however wants to take a thorough and comprehensive look over the field of Wireless Security at large, then there should be no doubt that THIS is and by far THE book on the subject. There are no subfields in the area that it does not cover and the authors manage to do it in a nicely flowing style that never becomes boring, no matter how esoteric the subject is.
It is extremely well documented with lots of references and useful footonotes. The care of the authors and their passion about the subject is manifest all over the book. The only small weakness of this book is it has some annoying typos in a couple of places (however nothing critical in terms of overall correctness of text) including some of the earlier figures. If it goes to a 2nd edition the publisher had better address these with a competent copy editor as they do injustice to an overall superb effort.
I am working in the area of advanced DSP-based wireless communications security and in short, I find this book very useful. I refer to it very often during my work. I strongly recommend WIRELESS SECURITY to anyone seriously interested in the subject.

9 of 9 people found the following review helpful.
The most comprehensive all around
By Marco De Vivo
The Approach:
You can find elsewhere any of the issues covered by this book. But only in this book, they are presented all together in detail. Every wireless security related field is discussed and the correspondent defensive and preventive countermeasures are proposed.
The Book:
657+ pages, well structured into 13 chapters. Literally, hundreds of useful references, and plenty of figures, tables, and photos.
The contents:
- Wireless Basics
- Wireless Information Warfare
- Telephone System Vulnerabilities
- Satellite Communications
- Cryptographic Security
- Speech Cryptology
- WLAN
- WAP
- WTLS
- Bluetooth
- Voice Over IP
- E2E Wireless Security
- Optimizing Wireless Security with ASICs and FPGAs
- Extensive Bibliography
The Bottom Line:
As a researcher and professor of Computer Networks Security, I consider this book as a very useful reference for my students. Even if they use the book mostly to learn about WLAN, WAP, WTLS, and Bluetooth security issues, many of them (the students) have been exploring the rest of the book to improve their knowledge. As far as I know, they use particularly: the cryptographic chapters to complement the regular (Dr. Stallings) textbook, and the Wireless Information Warfare chapter to improve their general background.
A unique in its kind book.

5 of 5 people found the following review helpful.
Extremely Useful!
By Shunysuke Takahara
I'm an active systems architect from Sweden working with multiple types of wireless communications devices(cellular, Bluetooth, etc.). I have been looking for a comprehensive coverage of security aspects in RF transmissions for quite some time. A colleague of mine recommended this book to me.
My first reaction was surprise due to the breadth of its coverage. It gives a well-rounded view of the subject in a very scholarly fashion. It is very meticulously written, clearly by people who know what they are talking about, and it includes some interesting issues like voice processing and cryptography without ever becoming boring. It provides a great deal of references so one can pursue further and deeper study of the subjects that one is interested in. Lots of footnotes and explanations show the authors' attention and care about detail.
My interest happens to be in implementing embedded integrated systems and this book provided me with ample food for thought with its original coverage of issues related to cipher synchronization in real-time wireless communications protocol stacks. To my knowledge, the subject is not covered anywhere else.
Besides a couple of typos probably due to the publisher's rush to bring the book to the market, I strongly recommend this book to anyone who is interested in the area of wireless communications security.

See all 13 customer reviews...

WIRELESS SECURITY: MODELS, THREATS, AND SOLUTIONS BY RANDALL K. NICHOLS, PANOS C. LEKKAS PDF

It will certainly have no uncertainty when you are visiting select this publication. This impressive **Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas** book can be reviewed entirely in certain time depending upon exactly how typically you open up as well as review them. One to bear in mind is that every publication has their very own production to obtain by each visitor. So, be the good reader and also be a much better individual after reviewing this book Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas

Review

J.M. (Mike) McConnell, Vice Admiral, USN (Ret), Vice President, Booz, Allen & Hamilton, Inc. and former Director of the National Security Agency (NSA), 1992-1996, sets the stage for this timely book with a perceptive Foreword that states the problem in his first sentence: "The safeguarding of information traveling over wireless technology has quickly become one of the most important and contentious challenges facing today's technology innovators."

With their book, Nichols and Lekkas pick up the gauntlet and provide a comprehensive guide for managers and policy makers involved with wireless communications. They explain the vulnerabilities, response options, and real-world costs associated with wireless platforms and applications, plus information needed to help develop the background and skills required to: Recognize new and established threats to wireless systems; Close gaps that threaten privacy, profits, and customer loyalty; Replace temporary, fragmented, and partial solutions with more robust and durable answers; Weigh platforms against characteristic attacks and protections; Apply clear guidelines for the best solutions now and going forward; Prepare for the boom in m-business; Assess today's protocol options and compensate for documented shortcomings.

This book is also an encyclopedic guide to the state of the art with: Encryption algorithms you can use now, End-to-end hardware solutions and field programmable gate arrays, An extensive guide to speech cryptology, Authentication strategies and security protocols for wireless systems, Infosec and infowar experience, Adding satellites to your security mix and much more. The book is another blockbuster... (The Cryptogram, Journal of the American Cryptogram Association 2002-03-01)

From the Back Cover
REAL-WORLD WIRELESS SECURITY

This comprehensive guide catalogs and explains the full range of the security challenges involved in wireless communications. Experts Randall K. Nichols and Panos C. Lekkas lay out the vulnerabilities, response options, and real-world costs connected with wireless platforms and applications. Read this book to develop the background and skills to--

* Recognize new and established threats to wireless systems
* Close gaps that threaten privary, profits, and customer loyalty

* Replace temporary, fragmented, and partial solutions with more robust and durable answers
* Prepare for the boom in m-business
* Weigh platforms against characteristic attacks and protections
* Apply clear guidelines for the best solutions now and going forward
* Assess today's protocol options and compensate for documented shortcomings

A COMPREHENSIVE GUIDE TO THE STATE OF THE ART

* Encryption algorithms you can use now
* End-to-end hardware solutions and field programmable gate arrays
* Speech cryptology
* Authentication strategies and security protocols for wireless systems
* Infosec and infowar experience
* Adding satellites to your security mix

About the Author
RANDALL NICHOLS is Vice President of Cryptography for TeleHubLink Corporation, where he directs development of embedded security solutions. He is Professor of Information Security at George Washington University and the author of four books on communications security, including McGraw-Hill's ICSA Guide to Cryptography.

PANOS LEKKAS is Chief Technology Officer and General Manager of Technology for TeleHubLink. Originally a VLSI designer, Mr. Lekkas worked for many years for IBM, where he was instrumental in the introduction of RISC architecture. Before joining TeleHubLink, he was President and CEO of wirelessEncryption.com, where he invented and developed telecom security.

Get the perks of checking out habit for your life style. Reserve Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas message will always associate with the life. The real life, knowledge, science, health, religious beliefs, enjoyment, as well as a lot more can be located in composed e-books. Many writers offer their encounter, science, research study, as well as all points to share with you. One of them is through this Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas This e-book Wireless Security: Models, Threats, And Solutions By Randall K. Nichols, Panos C. Lekkas will certainly supply the needed of message and declaration of the life. Life will be finished if you understand more points through reading books.