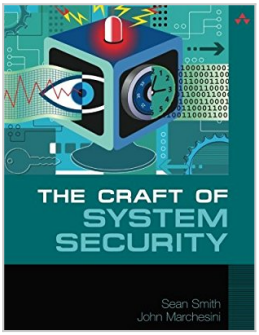

The Craft of System Security

By Sean Smith, John Marchesini

The Craft of System Security By Sean Smith, John Marchesini

"I believe The Craft of System Security *is one of the best software security books on the market today. It has not only breadth, but depth, covering topics ranging from cryptography, networking, and operating systems--to the Web, computer-human interaction, and how to improve the security of software systems by improving hardware. Bottom line, this book should be required reading for all who plan to call themselves security practitioners, and an invaluable part of every university's computer science curriculum."*
--Edward Bonver, CISSP, Senior Software QA Engineer, Product Security, Symantec Corporation

"Here's to a fun, exciting read: a unique book chock-full of practical examples of the uses and the misuses of computer security. I expect that it will motivate a good number of college students to want to learn more about the field, at the same time that it will satisfy the more experienced professional."
--L. Felipe Perrone, Department of Computer Science, Bucknell University

Whether you're a security practitioner, developer, manager, or administrator, this book will give you the deep understanding necessary to meet today's security challenges--and anticipate tomorrow's. Unlike most books, ***The Craft of System Security*** doesn't just review the modern security practitioner's toolkit: It explains why each tool exists, and discusses how to use it to solve real problems.

After quickly reviewing the history of computer security, the authors move on to discuss the modern landscape, showing how security challenges and responses have evolved, and offering a coherent framework for understanding today's systems and vulnerabilities. Next, they systematically introduce the basic building blocks for securing contemporary systems, apply those building blocks to today's applications, and consider important emerging trends such as hardware-based security.

After reading this book, you will be able to

- Understand the classic Orange Book approach to security, and its limitations
- Use operating system security tools and structures--with examples from Windows, Linux, BSD, and Solaris
- Learn how networking, the Web, and wireless technologies affect security

- Identify software security defects, from buffer overflows to development process flaws
- Understand cryptographic primitives and their use in secure systems
- Use best practice techniques for authenticating people and computer systems in diverse settings
- Use validation, standards, and testing to enhance confidence in a system's security
- Discover the security, privacy, and trust issues arising from desktop productivity tools
- Understand digital rights management, watermarking, information hiding, and policy expression
- Learn principles of human-computer interaction (HCI) design for improved security
- Understand the potential of emerging work in hardware-based security and trusted computing

The Craft of System Security

By Sean Smith, John Marchesini

The Craft of System Security By Sean Smith, John Marchesini

"I believe The Craft of System Security *is one of the best software security books on the market today. It has not only breadth, but depth, covering topics ranging from cryptography, networking, and operating systems--to the Web, computer-human interaction, and how to improve the security of software systems by improving hardware. Bottom line, this book should be required reading for all who plan to call themselves security practitioners, and an invaluable part of every university's computer science curriculum."*
--Edward Bonver, CISSP, Senior Software QA Engineer, Product Security, Symantec Corporation

"Here's to a fun, exciting read: a unique book chock-full of practical examples of the uses and the misuses of computer security. I expect that it will motivate a good number of college students to want to learn more about the field, at the same time that it will satisfy the more experienced professional."
--L. Felipe Perrone, Department of Computer Science, Bucknell University

Whether you're a security practitioner, developer, manager, or administrator, this book will give you the deep understanding necessary to meet today's security challenges--and anticipate tomorrow's. Unlike most books, ***The Craft of System Security*** doesn't just review the modern security practitioner's toolkit: It explains why each tool exists, and discusses how to use it to solve real problems.

After quickly reviewing the history of computer security, the authors move on to discuss the modern landscape, showing how security challenges and responses have evolved, and offering a coherent framework for understanding today's systems and vulnerabilities. Next, they systematically introduce the basic building blocks for securing contemporary systems, apply those building blocks to today's applications, and consider important emerging trends such as hardware-based security.

After reading this book, you will be able to

- Understand the classic Orange Book approach to security, and its limitations
- Use operating system security tools and structures--with examples from Windows, Linux, BSD, and Solaris
- Learn how networking, the Web, and wireless technologies affect security
- Identify software security defects, from buffer overflows to development process flaws
- Understand cryptographic primitives and their use in secure systems
- Use best practice techniques for authenticating people and computer systems in diverse settings
- Use validation, standards, and testing to enhance confidence in a system's security
- Discover the security, privacy, and trust issues arising from desktop productivity tools
- Understand digital rights management, watermarking, information hiding, and policy expression
- Learn principles of human-computer interaction (HCI) design for improved security
- Understand the potential of emerging work in hardware-based security and trusted computing

The Craft of System Security By Sean Smith, John Marchesini Bibliography

- Rank: #184340 in Books

- Published on: 2007-12-01
- Released on: 2007-11-21
- Ingredients: Example Ingredients
- Original language: English
- Number of items: 1
- Dimensions: 8.90" h x 1.20" w x 6.90" l, 1.87 pounds
- Binding: Paperback
- 592 pages

Editorial Review

From the Back Cover

""I believe" The Craft of System Security "is one of the best software security books on the market today. It has not only breadth, but depth, covering topics ranging from cryptography, networking, and operating systems--to the Web, computer-human interaction, and how to improve the security of software systems by improving hardware. Bottom line, this book should be required reading for all who plan to call themselves security practitioners, and an invaluable part of every university's computer science curriculum.""
--Edward Bonver, CISSP, Senior Software QA Engineer, Product Security, Symantec Corporation

""Here's to a fun, exciting read: a unique book chock-full of practical examples of the uses and the misuses of computer security. I expect that it will motivate a good number of college students to want to learn more about the field, at the same time that it will satisfy the more experienced professional.""
--L. Felipe Perrone, Department of Computer Science, Bucknell University

Whether you're a security practitioner, developer, manager, or administrator, this book will give you the deep understanding necessary to meet today's security challenges--and anticipate tomorrow's. Unlike most books, "The Craft of System Security" doesn't just review the modern security practitioner's toolkit: It explains why each tool exists, and discusses how to use it to solve real problems.

After quickly reviewing the history of computer security, the authors move on to discuss the modern landscape, showing how security challenges and responses have evolved, and offering a coherent framework for understanding today's systems and vulnerabilities. Next, they systematically introduce the basic building blocks for securing contemporary systems, apply those building blocks to today's applications, and consider important emerging trends such as hardware-based security.

After reading this book, you will be able toUnderstand the classic Orange Book approach to security, and its limitations Use operating system security tools and structures--with examples from Windows, Linux, BSD, and SolarisLearn how networking, the Web, and wireless technologies affect securityIdentify software security defects, from buffer overflows to development process flawsUnderstand cryptographic primitives and their use in secure systemsUse best practice techniques for authenticating people and computer systems in diverse settingsUse validation, standards, and testing to enhance confidence in a system's securityDiscover the security, privacy, and trust issues arising from desktop productivity toolsUnderstand digital rights management, watermarking, information hiding, and policy expressionLearn principles of human-computer interaction (HCI) design for improved securityUnderstand the potential of emerging work in hardware-based security and trusted computing

About the Author

Professor Sean Smith has been working in information security--attacks and defenses, for industry and government--since before there was a Web. As a post-doc and staff member at Los Alamos National Laboratory, he performed security reviews, designs, analyses, and briefings for a wide variety of public-sector clients; at IBM T.J. Watson Research Center, he designed the security architecture for (and helped code and test) the IBM 4758 secure coprocessor, and then led the formal modeling and verification work that earned it the world's first FIPS 140-1 Level 4 security validation. In July 2000, Sean left IBM for Dartmouth, since he was convinced that the academic education and research environment is a better venue for changing the world. His current work, as PI of the Dartmouth PKI/Trust Lab, investigates how to build trustworthy systems in the real world. Sean was educated at Princeton (A.B., Math) and CMU (M.S., Ph.D., Computer

Science), and is a member of Phi Beta Kappa and Sigma Xi.

Dr. John Marchesini received a B.S. in Computer Science from the University of Houston in 1999 and, after spending some time developing security software for BindView, headed to Dartmouth to pursue a Ph.D. There, he worked under Professor Sean Smith in the PKI/Trust lab designing, building, and breaking systems. John received his Ph.D. in Computer Science from Dartmouth in 2005 and returned to BindView, this time working in BindView's RAZOR security research group. He conducted numerous application penetration tests and worked closely with architects and developers to design and build secure systems. In 2006, BindView was acquired by Symantec and he became a member of Symantec's Product Security Group, where his role remained largely unchanged. John recently left Symantec and is now the Principal Security Architect at EminentWare LLC.

Computer security, once the arcane concern of specialists, is becoming everyone's problem in society. Because so many aspects of society now depend on computing, coaxing or tricking a computer into misbehaving can have serious consequences. Attempts to grasp the nuances of this problem are bedeviled by its sheer complexity--in the individual components and computer hardware, in the operating systems that make this hardware useful, in the application programs, in the network protocols--and in the human processes that use and maintain these systems.

Since security is everyone's problem, a natural question is how to give each cybercitizen the knowledge and perspective needed to reason about these issues. In navigating their careers as software engineers, managers, lawyers, or anything else, students and practitioners need to be exposed to not only the breadth of the space of this security challenge but also what trends and principles to look out for.

Too many existing texts seem to focus on hacks-du-jour or system administration or cryptographic specialists or the OrangeBook/NSA criteria. The computer science student or computer security practitioner can easily find books detailing particular tools that can be used to assess the security of a system but not books that take the reader into the deeper world of why these tools exist or explain how and when to apply the appropriate tool to a particular problem. Furthermore, many of the popular texts fail to aid one who is trying to build a system; many of the tool catalogs out there are geared toward the auditor, not the artisan.

We wrote this book to be that missing doorway. This book presents the modern security practitioner's toolkit; more important, this book also explains why these tools exist and how to use them in order to solve real problems. We want to give students enough practical knowledge to be useful and to give practitioners enough of the fundamentals to foster a deep understanding of the issues. Such mastery of the toolkit is necessary to understand the craft of system security.

How does one get such a security education? One could read through a bookshelf of material or access a large set of CD-ROMs to get the necessary depth, but most people do not have that time. Furthermore, much of that material may pertain to fine details of current systems and is thus doomed to a short shelf life. The material will likely be stale by the time the reader finishes reading it all.

This book itself grew out of a college course the first author developed (and then the second author helped with) to solve just this problem: to provide the right security education to students who may only ever take one security course and then move on toward a wide range of professional careers. We wanted to arm these students with a deep understanding of what they need to know in order to meet today's and tomorrow's security challenges. In the course, and throughout this book, we draw on our experience as security practitioners and try to relay some of the lessons we have learned.

One of us had the good fortune to be working in a government security laboratory at the dawn of the Web--

when the very first forward-thinking government agencies started considering using this new medium for service delivery to wide populations. [1] This experience provided some important lessons to frame what has followed. Computing technology will keep changing explosively, in ways that affect everyone, not only computer scientists--compare the state of home or office computing and of the Web in 1994 to today. However, security must be viewed in the context of the social impact of the systems. If one is going to build, deploy, work with, manage, or perhaps simply use the systems that keep flooding society, one needs to understand these issues.

The other author has spent time working in the security software industry, shipping security products to such institutions as banks, airlines, and government agencies. This experience has made it clear why vendors deal with security by shipping patches on a regular schedule. Software vendors are under continual pressure to release products that are loaded with new features and must get these releases out as quickly as possible. At every stage of the development cycle, security is at odds with this goal. The requirement phase tends to favor features--and thus complexity--over robustness; the design phase typically favors elegance and reuse over durability; the implementation phase usually favors speed over safety; the quality assurance phase traditionally focuses on feature testing rather than crash testing. The result is that many companies ship software that is neither robust, durable, nor safe and that has not been tested to see how well it holds up against malicious users. An essentially infinite list of BugTraq identifiers is just waiting to get assigned to such products. If one hopes to build systems that break this mold, one needs to understand these types of issues as well.

The dynamic nature of the security game makes it different from other types of engineering, such as building a bridge or building a safe. When building a bridge, one calculates the strength required, buys the appropriate materials, and constructs the bridge according to the specification. In security, the building blocks age quickly--sometimes faster than predicted and sometimes dramatically faster. Staying on top of this situation requires continued vigilance, as well as a solid grasp of the fundamentals. That's why we wrote this book.

Structure of the Book

We begin by presenting the historical background of computer security (Part I). We then describe the modern computing landscape (Part II), present the basic building blocks for securing systems (Part III), apply these blocks to modern computing applications (Part IV), and consider emerging tools and trends that will change the future landscape of system security (Part V).

History

Part I looks at history. Today, computers permeate nearly every aspect of life. Decades ago, however, the migration of computation from laboratory toys to real world applications was just beginning. Military and defense provided many of these early applications, as well as significant funding. These domains traditionally featured real adversaries interested in such matters as espionage, sabotage, and war fighting. The move into computerized settings brought along these concerns. These early days of computing gave rise to much thinking about new problems of computer security. Some in our field regard this thinking as gospel, never to be challenged or extended; others dismiss it out of hand. We believe that the truth lies somewhere in between.

Introduction. We use these roots as the foundation for our journey. Our discussion of computer system security starts out in Chapter 1 with discussions of the terms security and system. We consider the standard notion of "system" as a computer providing simple information applications and "security" as the standard confidentiality, integrity, and availability (CIA) rubric. We also introduce the basics of access control/protection--subjects, domains, and objects--and the matrix that describes who can do what to whom when. We finish by talking about the theoretical implications and practical instantiations of this matrix.

The Old Testament. A subset of the security community believes that all computer security problems were solved a few decades ago, in the body of *Department of Defense (DoD)*-sponsored work popularly identified with the *Orange Book*. When Roger Schell espoused this view at a December 2001 talk, a curmudgeon in the audience characterized him as the Old Testament prophet Jeremiah, castigating the community for turning

away from the true path. It is important to understand Schell's point of view, whether or not one accepts it. In Chapter 2, we present this point of view.

Old Principles, New World. In Chapter 3, we discuss how the "ancient history" from Chapters 1 and 2 applies--and fails to apply--to modern computing scenarios. We look at how the confidentiality-integrity-availability rubric can, when applied carelessly, miss important aspects of system security, and we present an alternative characterization in terms of *correctness* against adversaries. We also look at the difficulty of establishing the system boundary. We critique the Orange Book--what works now and what doesn't. We close by reviewing some other system design principles and discuss how they still apply to this new world.

Landscape

After studying the history, we examine where that history has taken us. In Part II, we look at the security of the elements used to build applications.

OS Security. In the cyber infrastructure, the *operating system (OS)* lies between a user's computing experience and the rest of the world. The OS provides the first line of defense between the user and external adversaries and, since it shapes and confines the user's computing experience, also provides the first line of defense against internal adversaries. Chapter 4 presents the basic structures and tools the OS brings to the security battle. We present the basic principles and discuss how they are manifested in common Windows systems and the UNIX family (e.g., OS X, Linux, BSD, Solaris).

Network Security. Funny things happen when one lets computers talk to each other. In Chapter 5, we present some of the basic pieces of networking and highlight some of the principal areas of concern for security practitioners. We also focus on the emerging networking technology of wireless. Rare four years ago, wireless technology is now standard on new laptops. For hotels, industrial campuses, and universities, not offering wireless almost seems as backward as not offering electricity. However, the new technology also comes with risks. As we have personally seen, information practices that were safe with a tethered network become rather dangerous when migrated to wireless; one can enliven boring conferences by discovering and browsing the Bluetooth-equipped devices in range that have accidentally been left open to the world.

Implementation Security. Abstractions are all well and good, but computing eventually consists of real code executing on real machines. A longtime source of computer security problems consists of basic flaws in these implementations. In Chapter 6, we survey these flaws--both common blunders, such as buffer overflow, lack of argument validation, escape sequences, and time-of-check/time-of-use, and more subtle problems, such as development process, tool-chain issues, and hardware issues. For each, we present real examples and general principles and discuss defensive coding practices and other counter measures. We also discuss how programming language techniques and software development processes can impact security--and what we can do about it.

Building Blocks for Secure Systems

In Part III, we survey the basic building blocks critical to designing, building, and deploying secure systems today.

Using Cryptography. Cryptographic primitives are a fundamental building block for secure systems today. Computer professionals need to have a good working understanding of what these primitives are and how to use them in larger applications. Chapter 7 introduces the standard primitives (public key, symmetric block ciphers, and so on) and the standard ways of using them (hashing functions, padding algorithms, hybrid cryptography, and MACs, and so on). In our teaching experience, we have encountered too many students who have "learned RSA" but have not known about all the steps involved in constructing digital signatures.

Subverting Cryptography. Humans like to deal with simple abstractions. However, dangers have often lurked in the messy details of realizing cryptographic primitives in real systems. These dangers can break a system that seemed safe when examined as clean abstractions. As with cryptographic primitives, computer professionals need to have a good working understanding of the types of issues that can arise in practice. Chapter 8 considers problem areas and real-world case studies in order to help cultivate a healthy wariness.

Authentication. Talking about "secure systems" makes sense only when there's a possibility of more than one player being involved. Chapter 9 covers the basics of authentication, as well as techniques when authenticating humans and systems in various settings: direct machine access, over an untrusted network, or over an untrusted network through an untrusted client. We also discuss the difference between authentication and authorization.

Public Key Infrastructure. By removing the need for sharing secrets a priori, public key cryptography enables trusted communication across boundaries of space, time, and organizations. However, the infrastructure necessary to realize the public key vision is still emerging; some dissidents even feel that the whole approach is fundamentally flawed. In Chapter 10, we look at the problem space, the main approaches, the issues that complicate deployment and progress in this space, and the dissenting points of view.

Validation, Standards, and Testing. Why should one believe that a given system is secure? Whether one is a vendor, an implementer, an administrator, or a customer, this question is fundamental. In Chapter 11, we talk about penetration testing, validation, and standards: how they can work to help achieve security and privacy and what their limitations are. We draw on our own experience in validation an testing and provide some suggestions to guide the reader through the cloud of emerging standards.

Applications

We have examined the history and the building blocks. In Part IV, we now apply these principles and tools to principal ways in which our society uses computing.

The Web and Security. Created by physicists too lazy to go to the library, the Web is now the central medium for electronic services in our society. We review how the Web works and then present the various security and privacy threats it faces--and the principal solutions. In Chapter 12, we cover both the standard material (e.g., SSL and cookies) and more subtle material.

We also discuss recent case studies of how institutions that should have known better ended up inadvertently disclosing information via Web-based services. For example, had editorial writers read this chapter, they would not have condemned the business school applicants for "hacking" the Apply Yourself site to learn application decisions prematurely; had the schools in question read this chapter, they might have disciplined the IT staff who approved that site, rather than summarily reject the applicants.

Office Tools and Security. Productivity tools, such as the Microsoft Office suite, Lotus 1-2-3, and rich graphical HTML email, etc., have become standard in nearly all settings. However, the richness and the complexity of these tools have continually led to interesting security and privacy issues. Since these tools work with electronic objects that look like familiar paper objects and provide manipulation functions that feel like familiar paper manipulation, users tend to assume that electronic objects behave like their paper counterparts and proceed to make trust decisions based on this assumption. However, this assumption is incorrect, and often, so are the resulting trust decisions. Chapter 13 explores these issues.

Money, Time, Property. Bits are not paper. Our social systems rest on the properties of paper, which we've had millennia to understand. In Chapter 14, we discuss some problems--and some tools--in making bits act like paper money and notarized documents. Another important distinction between bits and paper is that we have evolved techniques for traditional media--books, magazines, and even recordings--that make it easy to

enforce notions of intellectual property. Bits provide no such natural physical reinforcement; the area of *digital rights management (DRM)* and associated areas, such as watermarking, information hiding, and policy expression, are attempts to design and build secure systems that enforce certain types of "good" states despite certain types of malicious behavior.

Tools

In this book, we aim to equip the reader with the knowledge necessary to navigate the security field not only now but also in the future. In Part V, we look at computer security techniques and tools that promise to play an increasingly important role in this future. Consequently, some of these chapters are "lighter" than the previous material. The topics of Chapters 15 and 17 are full-fledged fields in their own right but often fall outside the view of the security artisan. Chapter 18 surveys a field that didn't even exist until recently.

Formal Methods and Security. One of the main challenges in ensuring secure behavior of contemporary computing systems and applications is managing their ever-increasing complexity. If the system is too complex to understand, how can any stakeholder--let alone the designers and implementers--have any confidence that it works securely?

Industrial-strength formal methods are emerging as potent weapons in the security and privacy arsenal. Holzmann's SPIN even won the ACM Systems Award in 2002. The computer professional should be aware that, if one formally specifies what one's system does and what it means for a state to preserve "security" and "privacy," semiautomatic methods exist to verify whether the system, as modeled, has these properties. Chapter 15 surveys these tools.

Hardware-Based Security. Research on computer security and privacy typically focuses on computation. However, since computation ultimately requires computer hardware at its base, the structure and behavior of this hardware can fundamentally shape properties of the computation it hosts. A subset of the computer security community, including at least one of the authors, has long advocated and explored using hardware-based techniques to improve security. In recent times, with e-commerce creating a market for cryptographic accelerators, with enterprise authentication creating a market for user hardware tokens, and with the computing industry advancing TCPA/TCG hardware, we see the feasibility of such techniques increasing. Chapter 16 presents the state of the art in research into the design, use, and evaluation of hardware techniques to achieve security and privacy properties in higher-level computation.

In Search of the Evil Bit. The field of artificial intelligence provides a grab bag of learning and recognition techniques that can be valuable tools in the security arsenal. (For example, it led to a Los Alamos research project that made a profit.) In Chapter 17, we survey these tools and how they can be applied in security to look for known bad patterns as well as unusual patterns and to look at not only system and network intrusion but also higher-level application data.

Human Issues. For the most part, security and privacy are issues in computing systems only because these systems are used by humans for things that are important to humans. The area of human/computer interaction (HCI) has studied how humans interact with devices: the principles that guide this interaction and how bad design can lead to amusing annoyance or major disaster. In Chapter 18, we look at the field of HCI-security (HCISEC) and at some fundamental design principles--nicely expressed in Norman's book *The Design of Everyday Things*--and their implications in computing security. We also look at the increasing attention that security researchers are paying to this human angle.

End Materials

We conclude the book with a final wrap-up chapter, and an appendix containing some background from theoretical computer science to shed more light on some of the topics covered in the main text. The

bibliography takes the reader further into the primary sources and cutting-edge research--which should be in a reference book but, for the most part, wasn't until this one was published.

1. In 2006, this same author renewed his amateur radio license and carried out the entire process via the FCC Web site. It's amazing to think how far e-government has come in these 12 years.

Users Review

From reader reviews:

Marilyn Daniels:

In this 21st century, people become competitive in most way. By being competitive at this point, people have do something to make these survives, being in the middle of the particular crowded place and notice simply by surrounding. One thing that often many people have underestimated that for a while is reading. Sure, by reading a publication your ability to survive raise then having chance to endure than other is high. In your case who want to start reading the book, we give you this kind of The Craft of System Security book as basic and daily reading reserve. Why, because this book is more than just a book.

Douglas Barlow:

Playing with family within a park, coming to see the sea world or hanging out with pals is thing that usually you have done when you have spare time, after that why you don't try point that really opposite from that. One activity that make you not experiencing tired but still relaxing, trilling like on roller coaster you already been ride on and with addition details. Even you love The Craft of System Security, you may enjoy both. It is fine combination right, you still want to miss it? What kind of hang type is it? Oh can occur its mind hangout people. What? Still don't buy it, oh come on its known as reading friends.

Lowell Seymour:

Reading a book to get new life style in this calendar year; every people loves to go through a book. When you read a book you can get a large amount of benefit. When you read guides, you can improve your knowledge, simply because book has a lot of information into it. The information that you will get depend on what sorts of book that you have read. If you want to get information about your analysis, you can read education books, but if you want to entertain yourself read a fiction books, this kind of us novel, comics, in addition to soon. The The Craft of System Security provide you with a new experience in reading a book.

Dwight Hancock:

Many people said that they feel uninterested when they reading a reserve. They are directly felt it when they get a half elements of the book. You can choose the book The Craft of System Security to make your own

reading is interesting. Your skill of reading proficiency is developing when you similar to reading. Try to choose very simple book to make you enjoy to read it and mingle the idea about book and studying especially. It is to be very first opinion for you to like to wide open a book and learn it. Beside that the book The Craft of System Security can to be your friend when you're truly feel alone and confuse in what must you're doing of the time.

Read The Craft of System Security By Sean Smith, John Marchesini for online ebook

The Craft of System Security By Sean Smith, John Marchesini Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read The Craft of System Security By Sean Smith, John Marchesini books to read online.

Online The Craft of System Security By Sean Smith, John Marchesini ebook PDF download

The Craft of System Security By Sean Smith, John Marchesini Doc

The Craft of System Security By Sean Smith, John Marchesini Mobipocket

The Craft of System Security By Sean Smith, John Marchesini EPub