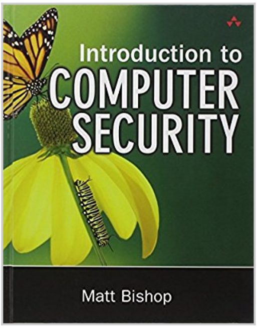

Introduction to Computer Security

By Matt Bishop

Introduction to Computer Security By Matt Bishop

In this authoritative book, widely respected practitioner and teacher Matt Bishop presents a clear and useful introduction to the art and science of information security. Bishop's insights and realistic examples will help any practitioner or student understand the crucial links between security theory and the day-to-day security challenges of IT environments.

Bishop explains the fundamentals of security: the different types of widely used policies, the mechanisms that implement these policies, the principles underlying both policies and mechanisms, and how attackers can subvert these tools--as well as how to defend against attackers. A practicum demonstrates how to apply these ideas and mechanisms to a realistic company.

Coverage includes

- Confidentiality, integrity, and availability
- Operational issues, cost-benefit and risk analyses, legal and human factors
- Planning and implementing effective access control
- Defining security, confidentiality, and integrity policies
- Using cryptography and public-key systems, and recognizing their limits
- Understanding and using authentication: from passwords to biometrics
- Security design principles: least-privilege, fail-safe defaults, open design, economy of mechanism, and more
- Controlling information flow through systems and networks
- Assuring security throughout the system lifecycle
- Malicious logic: Trojan horses, viruses, boot sector and executable infectors, rabbits, bacteria, logic bombs--and defenses against them
- Vulnerability analysis, penetration studies, auditing, and intrusion detection and prevention
- Applying security principles to networks, systems, users, and programs

Introduction to Computer Security is adapted from Bishop's comprehensive and widely praised book, *Computer Security: Art and Science*. This shorter version of the original work omits much mathematical formalism, making it more accessible for professionals and students who have a less formal mathematical background, or for readers with a more practical than theoretical interest.

Introduction to Computer Security

By Matt Bishop

Introduction to Computer Security By Matt Bishop

In this authoritative book, widely respected practitioner and teacher Matt Bishop presents a clear and useful introduction to the art and science of information security. Bishop's insights and realistic examples will help any practitioner or student understand the crucial links between security theory and the day-to-day security challenges of IT environments.

Bishop explains the fundamentals of security: the different types of widely used policies, the mechanisms that implement these policies, the principles underlying both policies and mechanisms, and how attackers can subvert these tools--as well as how to defend against attackers. A practicum demonstrates how to apply these ideas and mechanisms to a realistic company.

Coverage includes

- Confidentiality, integrity, and availability
- Operational issues, cost-benefit and risk analyses, legal and human factors
- Planning and implementing effective access control
- Defining security, confidentiality, and integrity policies
- Using cryptography and public-key systems, and recognizing their limits
- Understanding and using authentication: from passwords to biometrics
- Security design principles: least-privilege, fail-safe defaults, open design, economy of mechanism, and more
- Controlling information flow through systems and networks
- Assuring security throughout the system lifecycle
- Malicious logic: Trojan horses, viruses, boot sector and executable infectors, rabbits, bacteria, logic bombs--and defenses against them
- Vulnerability analysis, penetration studies, auditing, and intrusion detection and prevention
- Applying security principles to networks, systems, users, and programs

Introduction to Computer Security is adapted from Bishop's comprehensive and widely praised book, *Computer Security: Art and Science.* This shorter version of the original work omits much mathematical formalism, making it more accessible for professionals and students who have a less formal mathematical background, or for readers with a more practical than theoretical interest.

Introduction to Computer Security By Matt Bishop Bibliography

- Sales Rank: #776579 in Books
- Published on: 2004-11-05
- Original language: English

- Number of items: 1
- Dimensions: 9.40" h x 1.30" w x 7.60" l, 3.00 pounds
- Binding: Hardcover
- 784 pages

Editorial Review

From the Back Cover

In this authoritative book, widely respected practitioner and teacher Matt Bishop presents a clear and useful introduction to the art and science of information security. Bishop's insights and realistic examples will help any practitioner or student understand the crucial links between security theory and the day-to-day security challenges of IT environments.

Bishop explains the fundamentals of security: the different types of widely used policies, the mechanisms that implement these policies, the principles underlying both policies and mechanisms, and how attackers can subvert these tools--as well as how to defend against attackers. A practicum demonstrates how to apply these ideas and mechanisms to a realistic company.

Coverage includes

- Confidentiality, integrity, and availability
- Operational issues, cost-benefit and risk analyses, legal and human factors
- Planning and implementing effective access control
- Defining security, confidentiality, and integrity policies
- Using cryptography and public-key systems, and recognizing their limits
- Understanding and using authentication: from passwords to biometrics
- Security design principles: least-privilege, fail-safe defaults, open design, economy of mechanism, and more
- Controlling information flow through systems and networks
- Assuring security throughout the system lifecycle
- Malicious logic: Trojan horses, viruses, boot sector and executable infectors, rabbits, bacteria, logic bombs--and defenses against them
- Vulnerability analysis, penetration studies, auditing, and intrusion detection and prevention
- Applying security principles to networks, systems, users, and programs

Introduction to Computer Security is adapted from Bishop's comprehensive and widely praised book, *Computer Security: Art and Science.* This shorter version of the original work omits much mathematical formalism, making it more accessible for professionals and students who have a less formal mathematical background, or for readers with a more practical than theoretical interest.

About the Author

Matt Bishop is a professor in the Department of Computer Science at the University of California at Davis. A recognized expert in vulnerability analysis, secure systems/software design, network security, access control, authentication, and UNIX security, Bishop also works to improve computer security instruction.

Hortensio: Madam, before you touch the instrument
To learn the order of my fingering,
I must begin with rudiments of art
To teach you gamouth in a briefer sort,
More pleasant, pithy and effectual,
Than hath been taught by any of my trade;
And there it is in writing, fairly drawn.
The Taming of the Shrew, III, i, 62-68.

On September 11, 2001, terrorists seized control of four airplanes. Three were flown into buildings, and a fourth crashed, with catastrophic loss of life. In the aftermath, the security and reliability of many aspects of society drew renewed scrutiny. One of these aspects was the widespread use of computers and their interconnecting networks.

The issue is not new. In 1988, approximately 5,000 computers throughout the Internet were rendered unusable within 4 hours by a program called a worm. While the spread, and the effects, of this program alarmed computer scientists, most people were not worried because the worm did not affect their lives or their ability to do their jobs. In 1993, more users of computer systems were alerted to such dangers when a set of programs called sniffers were placed on many computers run by network service providers and recorded login names and passwords.

After an attack on Tsutomu Shimomura's computer system, and the fascinating way Shimomura followed the attacker's trail, which led to his arrest, the public's interest and apprehension were finally aroused. Computers were now vulnerable. Their once reassuring protections were now viewed as flimsy.

Several films explored these concerns. Movies such as *War Games* and *Hackers* provided images of people who can, at will, wander throughout computers and networks, maliciously or frivolously corrupting or destroying information it may have taken millions of dollars to amass. (Reality intruded on Hackers when the World Wide Web page set up by MGM/United Artists was quickly altered to present an irreverent commentary on the movie and to suggest that viewers see *The Net* instead. Paramount Pictures denied doing this.) Another film, *Sneakers*, presented a picture of those who test the security of computer (and other) systems for their owners and for the government.

Goals

This book has three goals. The first is to show the importance of theory to practice and of practice to theory. All too often, practitioners regard theory as irrelevant and theoreticians think of practice as trivial. In reality, theory and practice are symbiotic. For example, the theory of covert channels, in which the goal is to limit the ability of processes to communicate through shared resources, provides a mechanism for evaluating the effectiveness of mechanisms that confine processes, such as sandboxes and firewalls. Similarly, business practices in the commercial world led to the development of several security policy models such as the Clark-Wilson model and the Chinese Wall model. These models in turn help the designers of security policies better understand and evaluate the mechanisms and procedures needed to secure their sites.

The second goal is to emphasize that computer security and cryptography are different. Although cryptography is an essential component of computer security, it is by no means the only component. Cryptography provides a mechanism for performing specific functions, such as preventing unauthorized people from reading and altering messages on a network. However, unless developers understand the context in which they are using cryptography, and unless the assumptions underlying the protocol and the cryptographic mechanisms apply to the context, the cryptography may not add to the security of the system. The canonical example is the use of cryptography to secure communications between two low-security systems. If only trusted users can access the two systems, cryptography protects messages in transit. But if untrusted users can access either system (through authorized accounts or, more likely, by breaking in), the cryptography is not sufficient to protect the messages. The attackers can read the messages at either endpoint.

The third goal is to demonstrate that computer security is not just a science but also an art. It is an art because no system can be considered secure without an examination of how it is to be used. The definition of a "secure computer" necessitates a statement of requirements and an expression of those requirements in the form of authorized actions and authorized users. (A computer engaged in work at a university may be considered "secure" for the purposes of the work done at the university. When moved to a military installation, that same system may not provide sufficient control to be deemed "secure" for the purposes of the work done at that installation.) How will people, as well as other computers, interact with the computer system? How clear and restrictive an interface can a designer create without rendering the system unusable while trying to prevent unauthorized use or access to the data or resources on the system?

Just as an artist paints his view of the world onto canvas, so does a designer of security features articulate his view of the world of human/machine interaction in the security policy and mechanisms of the system. Two designers may use entirely different designs to achieve the same creation, just as two artists may use different subjects to achieve the same concept.

Computer security is also a science. Its theory is based on mathematical constructions, analyses, and proofs. Its systems are built in accordance with the accepted practices of engineering. It uses inductive and deductive reasoning to examine the security of systems from key axioms and to discover underlying principles. These scientific principles can then be applied to untraditional situations and new theories, policies, and mechanisms.

Philosophy

Key to understanding the problems that exist in computer security is a recognition that the problems are not new. They are old problems, dating from the beginning of computer security (and, in fact, arising from parallel problems in the noncomputer world). But the locus has changed as the field of computing has changed. Before the mid-1980s, mainframe and mid-level computers dominated the market, and computer security problems and solutions were phrased in terms of securing files or processes on a single system. With the rise of networking and the Internet, the arena has changed. Workstations and servers, and the networking infrastructure that connects them, now dominate the market. Computer security problems and solutions now focus on a networked environment. However, if the workstations and servers, and the supporting network infrastructure, are viewed as a single system, the models, theories, and problem statements developed for systems before the mid-1980s apply equally well to current systems.

As an example, consider the issue of assurance. In the early period, assurance arose in several ways: formal methods and proofs of correctness, validation of policy to requirements, and acquisition of data and programs from trusted sources, to name a few. Those providing assurance analyzed a single system, the code on it, and the sources (vendors and users) from which the code could be acquired to ensure that either the sources could be trusted or the programs could be confined adequately to do minimal damage. In the later period, the same basic principles and techniques apply, except that the scope of some has been greatly expanded (from a single system and a small set of vendors to the world-wide Internet). The work on proof-carrying code, an exciting development in which the proof that a downloadable program module satisfies a stated policy is incorporated into the program itself, is an example of this expansion. It extends the notion of a proof of consistency with a stated policy. It advances the technology of the earlier period into the later period. But in order to understand it properly, one must understand the ideas underlying the concept of proof-carrying code, and these ideas lie in the earlier period.

As another example, consider Saltzer and Schroeder's principles of secure design. Enunciated in 1975, they promote simplicity, confinement, and understanding. When security mechanisms grow too complex, attackers can evade or bypass them. Many programmers and vendors are learning this when attackers break into their systems and servers. The argument that the principles are old, and somehow outdated, rings hollow when the result of their violation is a nonsecure system.

The work from the earlier period is sometimes cast in terms of systems that no longer exist and that differ in many ways from modern systems. This does not vitiate the ideas and concepts, which also underlie the work done today. Once these ideas and concepts are properly understood, applying them in a multiplicity of environments becomes possible. Furthermore, the current mechanisms and technologies will become obsolete and of historical interest themselves as new forms of computing arise, but the underlying principles will live on, to underlie the next generation--indeed the next era--of computing.

The philosophy of this book is that certain key concepts underlie all of computer security, and that the study of all parts of computer security enriches the understanding of all parts. Moreover, critical to an understanding of the applications of security-related technologies and methodologies is an understanding of the theory underlying those applications.

Advances in the theory of computer protection have illuminated the foundations of security systems. Issues of abstract modeling, and modeling to meet specific environments, lead to systems designed to achieve a specific and rewarding goal. Theorems about the undecidability of the general security question have indicated the limits of what can be done.

Application of these results has improved the quality of the security of the systems being protected. However, the issue is how compatibly the assumptions of the model (and theory) conform to the environment to which the theory is applied. Although our knowledge of how to apply these abstractions is continually increasing, we still have difficulty correctly transposing the relevant information from a realistic setting to one in which analyses can then proceed. Such abstraction often eliminates vital information. The omitted data may pertain to security in nonobvious ways. Without this information, the analysis is flawed.

Unfortunately, no single work can cover all aspects of computer security, so this book focuses on those parts that are, in the author's opinion, most fundamental and most pervasive. The mechanisms exemplify the applications of these principles.

Organization

The organization of this book reflects its philosophy. It begins with fundamentals and principles that provide boundaries within which security can be modeled and analyzed effectively. This provides a framework for expressing and analyzing the requirements of the security of a system. These policies constrain what is allowed and what is not allowed. Mechanisms provide the ability to implement these policies. The degree to which the mechanisms correctly implement the policies, and indeed the degree to which the policies themselves meet the requirements of the organizations using the system, are questions of assurance. Exploiting failures in policy, in implementation, and in assurance comes next, as well as mechanisms for providing information on the attack. The book concludes with the applications of both theory and policy focused on realistic situations. This natural progression emphasizes the development and application of the principles existent in computer security.

The first chapter describes what computer security is all about and explores the problems and challenges to be faced. It sets the context for the remainder of the book.

Chapters 2 and 3 deal with basic questions such as how "security" can be clearly and functionally defined, whether or not it is realistic, and whether or not it is decidable.

Chapters 4 through 7 probe the relationship between policy and security. The definition of "security" depends on policy. We examine several types of policies, including the ever-present fundamental questions of trust, analysis of policies, and the use of policies to constrain operations and transitions.Chapters 9 through 12 discuss cryptography and its role in security, focusing on applications and issues such as key management, key distribution, and how cryptosystems are used in networks. A quick study of authentication completes this part.

Chapters 13 through 16 consider how to implement the requirements imposed by policies using system-oriented techniques. Certain design principles are fundamental to effective security mechanisms. Policies define who can act and how they can act, and so identity is a critical aspect of implementation. Mechanisms implementing access control and flow control enforce various aspects of policies.

Chapters 17 and 18 present concepts and standards used to ascertain how well a system, or a product, meets its goals.

Chapters 19 through 22 discuss some miscellaneous aspects of computer security. Malicious logic thwarts many mechanisms. Despite our best efforts at high assurance, systems today are replete with vulnerabilities. Why? How can a system be analyzed to detect vulnerabilities? What models might help us improve the state of the art? Given these security holes, how can we detect attackers who exploit them? A discussion of auditing flows naturally into a discussion of intrusion detection--a detection method for such attacks.

Chapters 23 through 26 present examples of how to apply the principles discussed throughout the book. They begin with networks and proceed to systems, users, and programs. Each chapter states a desired policy and shows how to translate that policy into a set of mechanisms and procedures that support the policy. This part tries to demonstrate that the material covered elsewhere can be, and should be, used in practice.

Each chapter in this book ends with a summary and some suggestions for further reading. The summary highlights the important ideas in the chapter. Interested readers who wish to pursue the topics in any chapter in more depth can go to some of the suggested readings. They expand on the material in the chapter or present other interesting avenues.

Differences Between this Book and *Computer Security: Art and Science*

The differences between this book and *Computer Security: Art and Science* result from the different intended audiences. This book is a shorter version of the latter, omitting much of the mathematical formalism. It is suited for computer security professionals, students, and prospective readers who have a less formal mathematical background, or who are not interested in the mathematical formalisms and would only be distracted by them, or for courses with a more practical than theoretical focus.

The foundations and policy sections of this book do not present results involving formal modeling or derivations of limits on the decidability of security (although it does present the central result, that the generic safety problem is undecidable). Some policies, significant in the history of the development of policy models but no longer used widely, have been omitted, as has discussion of the notions of nondeducibility and noninterference. Further, the section on assurance omits the presentation of formal methods and the detailed discussion of designing and building secure systems. It preserves the exposition of the basic concepts and ideas, especially those related to reference monitors, and discusses commonly encountered evaluation criteria.

The reasons for these differences come from the different backgrounds expected of readers. This book is intended for readers who may not be familiar with highly mathematical concepts, or for classes in which the instructor does not intend to expound upon formalisms, such as those required for the development of high assurance systems, but wants students to be exposed to the ideas underlying a "high assurance system." These situations most often arise in classes in which students' backgrounds may not include classes that provide the understanding needed to assimilate the mathematical details of the work. As a consequence, students are often intimidated by the formalism even if the instructor skips it. The original version of this book is intended for classes where the instructor wishes to explain, or allow the students to explore on their own, the rich mathematical background and formalisms of computer security.

Some students learn best by an informal description of a subject. What is the intuition underlying the ideas and principles of the field? How does the practitioner apply these to improve the state of the art? For these students, this version of the book is more appropriate. Other students are most comfortable with intuition augmented by a formal mathematical exposition of the underlying concepts. How does one make the intuition formal? How does one apply the ideas rigorously to assure a secure system (for an appropriate definition of security)? For these students, the original book, *Computer Security: Art and Science*, would be more appropriate.

Practitioners who are less interested in mathematical expositions of the theories underlying computer security will find this version more to their liking. This version keeps the intuitive, non-mathematical exposition of the underlying principles, but does so using a small amount of formal mathematics. Practitioners will find this version shorter and, most likely, easier to read because they will not be distracted by material they would find irrelevant.

Special Acknowledgment

Elisabeth Sullivan contributed the assurance part of this book. She wrote several drafts, all of which reflect her extensive knowledge and experience in that aspect of computer security. I am particularly grateful to her for contributing her real-world knowledge of how assurance is managed. Too often, books recount the mathematics of assurance without recognizing that other aspects are equally important and more widely used. These other aspects shine through in the assurance section, thanks to Liz. As if that were not enough, she made several suggestions that improved the policy part of this book. I will always be grateful for her contribution, her humor, and especially her friendship.

Users Review

From reader reviews:

Madeline Edwards:

Do you have favorite book? If you have, what is your favorite's book? Reserve is very important thing for us to find out everything in the world. Each e-book has different aim or maybe goal; it means that e-book has different type. Some people feel enjoy to spend their the perfect time to read a book. These are reading whatever they get because their hobby is usually reading a book. Consider the person who don't like reading through a book? Sometime, person feel need book if they found difficult problem or perhaps exercise. Well, probably you should have this Introduction to Computer Security.

Kelly Breedlove:

Playing with family inside a park, coming to see the ocean world or hanging out with good friends is thing that usually you have done when you have spare time, subsequently why you don't try factor that really opposite from that. 1 activity that make you not sensation tired but still relaxing, trilling like on roller coaster you are ride on and with addition of knowledge. Even you love Introduction to Computer Security, it is possible to enjoy both. It is good combination right, you still would like to miss it? What kind of hangout type is it? Oh can occur its mind hangout fellas. What? Still don't have it, oh come on its referred to as reading friends.

Homer Gardner:

Beside this particular Introduction to Computer Security in your phone, it could give you a way to get nearer to the new knowledge or facts. The information and the knowledge you might got here is fresh in the oven so don't become worry if you feel like an outdated people live in narrow town. It is good thing to have Introduction to Computer Security because this book offers for your requirements readable information. Do you sometimes have book but you don't get what it's about. Oh come on, that will not happen if you have this inside your hand. The Enjoyable arrangement here cannot be questionable, just like treasuring beautiful island. Techniques you still want to miss this? Find this book in addition to read it from now!

James Stevens:

As we know that book is very important thing to add our understanding for everything. By a book we can know everything we really wish for. A book is a pair of written, printed, illustrated or perhaps blank sheet. Every year ended up being exactly added. This publication Introduction to Computer Security was filled regarding science. Spend your free time to add your knowledge about your science competence. Some people has different feel when they reading a new book. If you know how big selling point of a book, you can feel enjoy to read a book. In the modern era like today, many ways to get book that you just wanted.

Read Introduction to Computer Security By Matt Bishop for online ebook

Introduction to Computer Security By Matt Bishop 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 Introduction to Computer Security By Matt Bishop books to read online.

Online Introduction to Computer Security By Matt Bishop ebook PDF download

Introduction to Computer Security By Matt Bishop Doc

Introduction to Computer Security By Matt Bishop Mobipocket

Introduction to Computer Security By Matt Bishop EPub

MIFNTGY2BUL: Introduction to Computer Security By Matt Bishop