国外优秀信息科学与技术系列教学用书

计算机安全原理

（影印版）

PRINCIPLES OF COMPUTER SECURITY: SECURITY+™ AND BEYOND

■ Wm. Arthur Conklin
Gregory B. White
Chuck Cothren
Dwayne Williams
Roger L. Davis

Mc Graw Hill Education

高等教育出版社
Higher Education Press

国外优秀信息科学与技术系列教学用书

计算机安全原理

（影印版）

PRINCIPLES OF COMPUTER SECURITY:

Security +^{TM} and Beyond

Wm. Arthur Conklin, Gregory B. White,
Chuck Cothren, Dwayne Williams, Roger L. Davis

高等教育出版社
HIGHER EDUCATION PRESS

图字:01 -2004 -6716 号

Principles of Computer Security: Security +^{TM} and Beyond
Wm. Arthur Conklin, Gregory B. White, Chuck Cothren, Dwayne Williams, Roger L. Davis
原版 ISBN:0-07-225509-9

图书在版编目（CIP）数据

计算机安全原理 = Principles of Computer Security:
Security +（TM）and Beyond/（美）康克林（Conk
lin, W. A.）. —影印版. —北京：高等教育出版社，
2005. 6
ISBN 7-04-016775-1

Ⅰ.计... Ⅱ.康... Ⅲ.电子计算机—安全技术—
高等学校—教材—英文 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2005)第000019号

出版发行	高等教育出版社	**购书热线**	010-58581118
社　　址	北京市西城区德外大街4号	**免费咨询**	800-810-0598
邮政编码	100011	**网　　址**	http://www.hep.edu.cn
总　　机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
			http://www.landraco.com.cn
经　　销	北京蓝色畅想图书发行有限公司		
印　　刷	北京民族印刷厂		
开　　本	787×1092　1/16	**版　　次**	2005年6月第1版
印　　张	43	**印　　次**	2005年6月第1次印刷
字　　数	950 000	**定　　价**	49.50元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号 16775-00

出 版 说 明

20世纪末，以计算机和通信技术为代表的信息科学和技术对世界经济、科技、军事、教育和文化等产生了深刻影响。信息科学技术的迅速普及和应用，带动了世界范围信息产业的蓬勃发展，为许多国家带来了丰厚的回报。

进入21世纪，尤其随着我国加入WTO，信息产业的国际竞争将更加激烈。我国信息产业虽然在20世纪末取得了迅猛发展，但与发达国家相比，甚至与印度、爱尔兰等国家相比，还有很大差距。国家信息化的发展速度和信息产业的国际竞争能力，最终都将取决于信息科学技术人才的质量和数量。引进国外信息科学和技术优秀教材，在有条件的学校推动开展英语授课或双语教学，是教育部为加快培养大批高质量的信息技术人才采取的一项重要举措。

为此，教育部要求由高等教育出版社首先开展信息科学和技术教材的引进试点工作。同时提出了两点要求，一是要高水平，二是要低价格。在高等教育出版社和信息科学技术引进教材专家组的努力下，经过比较短的时间，第一批由教育部高等教育司推荐的20多种引进教材已经陆续出版。这套教材出版后受到了广泛的好评，其中有不少是世界信息科学技术领域著名专家、教授的经典之作和反映信息科学技术最新进展的优秀作品，代表了目前世界信息科学技术教育的一流水平，而且价格也是最优惠的，与国内同类自编教材相当。这套教材基本覆盖了计算机科学与技术专业的课程体系，体现了权威性、系统性、先进性和经济性等特点。

目前，教育部正在全国35所高校推动示范性软件学院的建设，这也是加快培养信息科学技术人才的重要举措之一。为配合软件学院的教学工作，结合各软件学院的教学计划和课程设置，高等教育出版社近期聘请有关专家和软件学院的教师遴选推荐了一批相应的原版教学用书，正陆续组织出版，以方便各软件学院开展双语教学。

我们希望这些教学用书的引进出版，对于提高我国高等学校信息科学技术的教学水平，缩小与国际先进水平的差距，加快培养一大批具有国际竞争力的高质量信息技术人才，起到积极的推动作用。同时我们也欢迎广大教师和专家们对我们的教材引进工作提出宝贵的意见和建议。联系方式：hep.cs@263.net。

高等教育出版社
二〇〇二年九月

This book is dedicated to the many
security professionals who daily work
to ensure the safety of our nation's
critical infrastructures.

We want to recognize the thousands
of dedicated individuals who strive
to protect our national assets but who
seldom receive praise and often are
only noticed when an incident occurs.

To you we say thank you for a job well done!

ABOUT THE AUTHORS

Wm. Arthur Conklin is a Senior Lecturer in the College of Business at The University of Texas at San Antonio and a Research Scientist at the Center for Infrastructure Assurance and Security. He is currently working on a Ph.D. specializing in Information Systems/Information Assurance. Mr. Conklin has an MBA from UTSA, and two graduate degrees in electrical engineering from the Naval Postgraduate School in Monterey, California. His current research interests are in the areas of steganography and in security implications of distributed computing. Mr. Conklin is a 10-year veteran of the U.S. Navy, serving as a surface warfare officer and engineering duty officer, and has over 10 years experience in software engineering and project management. He is a co-author of McGraw Hill's *Security+ Certification All-in-One Exam Guide*.

Dr. Gregory White has been involved in computer and network security since 1986. He spent 19 years on active duty with the United States Air Force and is currently in the Air Force Reserves assigned to the Air Force Information Warfare Center. He obtained his Ph.D. in computer science from Texas A&M University in 1995. His dissertation topic was in the area of computer network intrusion detection, and he continues to conduct research in this area today. He is currently the Interim Executive Director and Technical Director for the Center for Infrastructure Assurance and Security (CIAS) and is an associate professor of information systems at the University of Texas at San Antonio (UTSA). Dr. White has written and presented numerous articles and conference papers on security. He is also the coauthor for four other textbooks on computer and network security and has written chapters for two other security books. Dr. White continues to be active in security research. His current research initiatives include efforts in high-speed intrusion detection, infrastructure protection, and methods to calculate a return on investment and the total cost of ownership from security products.

Chuck Cothren, CISSP, is a research scientist at UTSA CIAS, and currently serves on the Information Systems Security Association (ISSA)'s Alamo Chapter Board of Directors. Mr. Cothren has a wide array of security experience including performing controlled penetration testing, network security policies, computer intrusion forensics, and computer security training. He is also well versed in wireless networking and wireless security assessments. Mr. Cothren joined UTSA CIAS in February 2003. He was previously employed as a senior network security engineer working with Fortune 100 clients to provide them with vulnerability assessments and other security services. Prior to that he was employed as a network administrator, and also as a trainer for an information technology firm. Mr. Cothren is a certified information systems security professional (CISSP) and has coauthored *Voice and Data Security* as well as *Security+ Certification All-in-One Exam Guide.* Mr. Cothren also holds a B.S. in industrial distribution from Texas A&M University.

Dwayne Williams, CISSP, joined the UTSA CIAS in 2002 as a senior researcher and has over ten years' experience in information systems and network security. Mr. Williams' experience includes six years of commissioned military service as a communications computer information systems officer in the United States Air Force specializing in network security, corporate information protection, intrusion detection systems, incident response, and VPN technology. Prior to joining the CIAS, he served as director of consulting for SecureLogix Corporation where he directed and provided security assessment and integration services to Fortune 100, government, public utility, oil and gas, financial, and technology clients. Mr. Williams graduated in May 1993 from Baylor University with a bachelor of arts in computer science. Mr. Williams is a certified information systems security professional (CISSP) and coauthor of *Voice and Data Security* and *Security+ Certification All-in-One Exam Guide.*

Roger L. Davis, CISSP, CISM, CISA, is senior internal audit manager at Nu Skin Enterprises, evaluating global business operations in over 35 countries. He has served as president of the Utah chapter of the Information Systems Security Association (ISSA) and various board positions for the Utah chapter of the Information Systems Audit and Control Association (ISACA). He is a retired Air Force lieutenant colonel with over 20 years of military and information security experience. Mr. Davis served on the faculty of Brigham Young University and the Air Force Institute of Technology. He coauthored McGraw-Hill's *Security+ Certification All-in-One Exam Guide* and *Voice and Data Security,* which was also translated into Chinese. He holds a master's degree in computer science from George Washington University, a bachelor's degree in computer science from Brigham Young University, and performed post-graduate studies in electrical engineering and computer science at the University of Colorado.

ABOUT THE SERIES EDITOR

Corey D. Schou, Ph.D., is the University Professor of Informatics and the Associate Dean of the College of Business at Idaho State University. He has been involved in establishing computer security and information assurance training and standards for 25 years. His research interests include information assurance, ethics, privacy, and collaborative decision making. He was responsible for compiling and editing computer security standards and training materials for the Committee on National Security Systems (CNSS).

Throughout his career, Dr. Schou has remained an active classroom teacher despite his research and service commitments. He is the founding director of the Informatics Research Institute and the National Information Assurance Training and Education Center (NIATEC), which was designated the National Center of Excellence in Information Assurance Education.

In 1996, his research center was cited by the Information Systems Security Association (ISSA) for Outstanding Contributions to the Security Profession and he was selected as the Educator of the Year by the Federal Information Systems Security Educators Association (FISSEA). In 1997, the Masie Institute and TechLearn Consortium recognized his contributions to distance education. In 2001, Dr. Schou was honored by the International Information Systems Security Certification Consortium [(ISC)^2] with the Tipton award for his work in professionalization of computer security and his development of the generally accepted common body of knowledge (CBK) used in the certification of information assurance professionals.

Dr. Schou serves as the chair of the Colloquium for Information Systems Security Education (CISSE). Under his leadership, the Colloquium creates an environment for exchange and dialogue among leaders in government, industry, and academia concerning information security and information assurance education. In addition, he is the editor of *Information Systems Security* and serves on the board of several professional organizations.

ABOUT THE TECHNICAL EDITORS

Steven C. Bale, JD, CISSP, is a Professor of Computer Technology at Truckee Meadows Community College in Reno, Nevada. Steve has more than 25 years in system design, implementation and network administration as well as network security in both the private and public sector, including having worked with various state and federal agencies. He is currently the program director for the Microsoft IT Academy and the MCSE program at Truckee Meadows Community College. In addition to being a Certified Information Systems Security Professional, he holds a variety of other industry certifications including, MCSA (2000 & 2003), MCSE (2000 & 2003), MCSAS, MCSES, MCSAM, MCDBA, MCT, CCNA, CCDA, A+, Network+, Security+, Server+, CTT+, and CNA. In addition to his law degree, he holds a MPA from the Graduate School of Management at Brigham Young University and is finishing a Ph.D. in public administration and public policy at the University of Nevada Reno.

ACKNOWLEDGMENTS

We, the authors of *Principles of Computer Security: Security+ and Beyond,* have so many individuals that we need to acknowledge—individuals without whom this effort would not have been successful.

The list needs to start with those folks at McGraw-Hill who worked tirelessly with the project's multiple authors to lead us successfully through the minefield that is a schedule, who took our rough chapters and drawings and turned them into a final, professional product we can be proud of: Chris Johnson, Laura Stone, Julie Smith, and Jean Butterfield. We also thank the copy editor Mike McGee; the proofreader, Susie Elkind; and the indexer, Valerie Perry for all their attention to detail that made this a finer work after they finished with it.

We also need to acknowledge our current employers who, to our great delight, have seen fit to pay us to work in a career field that we all find exciting and rewarding. There is never a dull moment in security because it is constantly changing.

We would like to thank Dr. James Frost and Dr. John Springer for their contributions to the Instructor's Resource Kit.

Finally, we would each like to individually thank those people who—on a personal basis—have provided the core support for us individually. Without these special people in our lives, none of us could have put this work together.

To Susan, my muse and inspiration–I send my thanks, my love, and my deepest appreciation.

Wm. Arthur Conklin

I would like to thank my wife, Charlan. No matter how many times I have sworn that I'll never get involved with another book project, only to return within months to yet another, you have always remained supportive and my constant source of inspiration.

I would also like to thank all of the individuals at the Center for Infrastructure Assurance and Security at UTSA for their dedication and tremendous work. You make it worth coming back each day to fight the bureaucracy that seems to constantly be placed in our way. Thanks to all of you for all that you do.

Gregory B. White, Ph.D.

Josie, thank you for all love and support you have given me, you make the things I do possible.

Chuck Cothren

I would like to thank my wife Leah and my family for all the support and love they've shown me on this and every other project I've undertaken.

Dwayne E. Williams

Special thanks to my wife and best friend, Geena, for her unfailing support and to my kids, Angee, Adam, and Reed.

Roger L. Davis

FOREWORD

About the McGraw-Hill Information Security Series

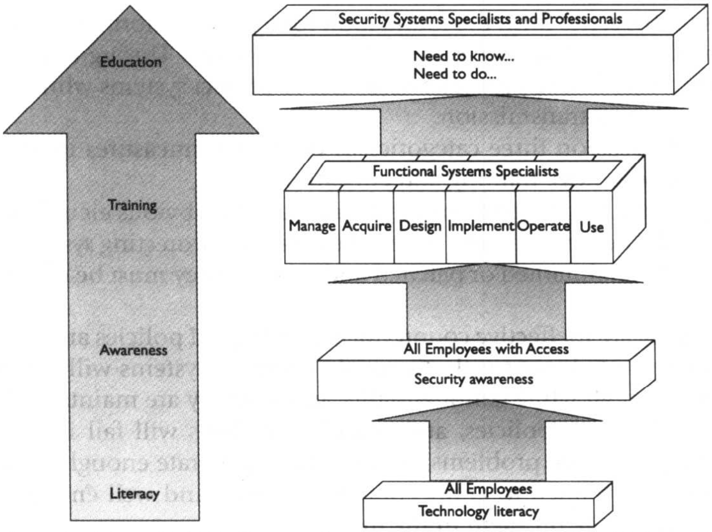
A new century—a new set of problems and a new curriculum. In the past four years, our awareness of critical information infrastructure and the importance of these systems in our lives has increased. Colleges and universities world wide have been challenged to increase course offerings in computer security, information systems, and information assurance. The stumbling block has been a lack of trained faculty and of suitable teaching materials to provide literacy, awareness, training and education at all levels.

Welcome to the McGraw Hill series on Information Assurance. It will provide material to support an integrated curriculum in information assurance for both technical and non technical programs. The texts in this series support all aspects of the Committee on National Security Standards (CNSS) (http://www.nstissc.gov/html/library.html) as well as many of the national and international certification standards.

A stable technological economy demands a general populace who are at least aware and literate in information security and assurance.

The texts in this series are based on more than fifteen years of international progress across academia, government, and industry in the developing cognitive and pedagogic models for teaching information security and assurance. Collectively the series deals with the defense in depth model that relies on technology, operations, and finally literacy, awareness, training, and education.

Literacy, awareness, training, and education are the most cost-effective means of protecting organizational information assets. The following illustration shows the relationship among these countermeasures.



Based on a figure in Schou, C., W. V. Maconachy, et al. (1993). "Organizational Information Security: Awareness, Training, and Education to Maintain System Integrity." Proceedings of the 9th International Computer Security Symposium, Toronto, Canada, IFIP.

To learn about information assurance, one must first be literate in information technology. The second step in the process is making the learner aware. Awareness is frequently a passive activity that focuses on short-term memory and may be a component of other classes.

The training is the next step of the process. It requires active participation and focus more on long-term memory, job skills, tasks and methods. In eDACUM studies (http://www.nsa.gov/isso/programs/nietp/edacum.htm) performed throughout the '90s information assurance experts established a series of KSAs (knowledge, skill, and Ability) and determined that functional security specialists used their KSAs in at least five major areas, management, acquisition, design, implementation, operation, and testing of secure systems. Depending on the functions performed individual need different combinations and amounts of training in each of these areas. Of course, every functional specialist is ultimately a user and needs specific training.

The final stage in the learning pyramid is education. It focuses on internalization and accommodation of the KSAs through research, analysis, evaluation, and judgment. Pedagogically these KSAs fall into two major categories - things you need to know and things you need to do.

Information Assurance

Information assurance is a combination of both art and science. It is an interdisciplinary activity that protects the most complex organizational asset—its data and the ability to provide information. Most organizations profess an interest in some aspects of information security. All organizations should view this effort as a planned integrative systematic objective at the highest level.

The books in this series form the foundation for teaching information assurance - the combination of availability, integrity, and confidentiality. Throughout the series students are lead to examine appropriate measures to protect systems while data are being processed, stored or in transmission.

The texts will focus on three categories of the countermeasures triad—technology, operations, and awareness, training and education.

Hardware and the associated technology are the most obvious elements of the countermeasures triad. They are the most expensive means of protecting systems. At best they must be constantly maintained or patched and at worst they must be recapitalized if severely compromised.

In any case, they are ineffective countermeasures if good policies are not in place and the systems are operated incorrectly. Correctly operated systems will insure that availability will remain high while confidentiality and integrity are maintained.

Hardware, technology, policies, and sound operations will fail if the humans involved are not aware of the problems, technologically literate enough to communicate about the problems, trained to apply countermeasures, and well enough educated to think about avoiding the problem in the future.

Principles of Computer Security Security+ and Beyond

The hard work and dedication of the authors have created a book that shows the importance of developing a professional approach to computer security and information assurance. The book is unique in that it deals with both certification and academic issues at the same time. They make an excellence balance between technological and managerial issues.

The overall writing style and tone make the book readable and thorough.. The examples are sufficiently clear that a true beginner can rapidly learn the essentials while the more experienced will be able to find examples for practical use. The authors challenge the learner to learn more.

On a regular basis I teach computer security related courses at both the graduate and undergraduate level. My students constantly ask about preparation for certifications. This book can be used to teach a thorough fundamentals of information security and assurance at the sophomore level in technical courses. In the upper division, the text is suitable for survey and introductory courses. As a bonus, the book covers the learning requirements for several certifications including the ComTIA Security Plus (http://comptia.com/) and (ISC)^2 SSCP examination (https://www.isc2.org/cgi/content.cgi?category=20). In addition, it is a teaching resource for major portions of the contents of NSTISSC 4011.

This outstanding team of authors has created a unique text that makes it clear to the reader that information security is a process not just manipulation of tools. It covers a broad spectrum of materials for security specialist.s

This book and the entire series can be summed up by the motto of my research center:

> Awareness—Training—Education
>
> There is no patch for ignorance.

Corey D. Schou, PhD
University Professor of Informatics
Professor of Computer Information Systems
Director of the National Information Assurance Training and Education Center

PREFACE

Information and computer security has moved from the confines of academia to mainstream America in the last decade. The Slammer and SoBig attacks were heavily covered in the media and broadcast into the average American's home. It has increasingly become obvious to everybody that something needs to be done in order to secure not only our nation's critical infrastructure but the businesses we deal with on a daily basis. The question is, "Where do we begin?" What can the average information technology professional do in order to secure the systems that they are hired to maintain? One immediate answer is education and training. If we want to secure our computer systems and networks, our IT professionals need to know how to do this, and what security entails. Computer security education is an essential foundational element for today's computer science and information systems professionals.

Complacency is not an option in today's hostile network environment. While we once considered the insider to be the major threat to corporate networks, and the "script kiddie" to be the standard external threat (often thought of as only a nuisance), the highly interconnected network world of today is a much different place. The U.S. government identified eight critical infrastructures a few years ago that were thought to be so critical to the nation's daily operation that if one were to be lost, it would have a catastrophic impact on the nation. To this original set of eight sectors, more have recently been added. A common thread throughout all of these, however, is technology—especially technology related to computers and communication. Thus, if an individual, organization, or nation wanted to cause damage to this nation, it could attack it not just with traditional weapons but with computers through the Internet. It is not surprising to hear that among the other information seized in raids on terrorist organizations, computers and information about the Internet are present. While the insider can certainly still do tremendous damage to an organization, the external threat is again becoming the chief concern among many. While many may argue the source and credibility of specific threats, the fact remains that computer security plays an essential role in reducing risk to our national economy and way of life.

So, where do you, the IT professional seeking more knowledge on security, start your studies? The IT world is overflowing with certifications that can be obtained by those attempting to learn more about their chosen profession. The security sector is no different, and the Security+ exam offers a basic level of certification for security. In the pages of this introductory text on computer security can be found not only material that can help you build a solid foundation in computer security, but also prepare for taking the Security+ examination. The basic information that you will need in order to understand the issues involved in securing our computer systems and networks today will act as a foundational element in your education as a computer science or information systems professional. In no way is this textbook the final source you will need in order to learn all about protecting your organization's systems, but it serves as a point from which to launch your security studies and career.

One thing is certainly true about this field of study—it never gets boring. It constantly changes as technology itself advances. Something else you will find as you progress in your security studies is that no matter how much technology advances and no matter how many new security devices are developed, at its most basic level, the human is still the weak link in the security chain. If you are looking for an exciting area to delve into, then you have certainly chosen wisely. Security offers a challenging blend of technology and people issues. We, the authors of this textbook, wish you luck as you embark on an exciting and challenging career path.

Wm. Arthur Conklin
Gregory B. White, Ph.D.
Chuck Cothren
Dwayne Williams
Roger L. Davis

INTRODUCTION

Computer security is becoming increasingly important today as the number of security incidents steadily climbs. Many corporations are now spending significant portions of their budget on security hardware, software, services, and personnel. They are spending this money not because it increases sales or enhances the product they provide, but because of the possible consequences should they not take protective actions.

Why Focus on Security?

Security is not something that we want to have to pay for, it would be nice if we didn't have to worry about protecting our data from disclosure, modification, or destruction from unauthorized individuals, but that is not the environment that we find ourselves in. Instead, we have seen the cost of recovering from security incidents steadily rise along with the rise in the number of incidents themselves. Since September 11, 2001 this has taken on an even greater sense of urgency as we now face securing our systems not just from attack by disgruntled employees, juvenile hackers, organized crime, or competitors. We now have to also consider the possibility of attacks on our systems from terrorist organizations. If nothing else, the events of September 11, 2001 showed that anybody is a potential target, you do not have to be part of the government or a government contractor, being an American is sufficient reason to make you a target to some and with the global nature of the Internet, collateral damage from cyber attacks on one organization could have a worldwide impact.

A Growing Need for Security Specialists

In order to protect our computer systems and networks, we will need a significant number of new security professionals trained in the many aspects of computer and network security. This is not an easy task for the systems we connect to the Internet are becoming increasingly complex with software whose lines of codes number in the millions. It is not hard to understand why this is such a difficult problem to solve if one considers just how many errors might be present in a piece of software that is several million lines long. When you add the additional factor of how fast software is being developed, out of necessity as the market is constantly moving, it is easy to understand how errors occur.

Not every "bug" in the software will result in a security hole, but it doesn't take many to have a drastic affect on the Internet community. We can't just blame the vendors for this situation, because they are reacting to the demands of government and industry. Most vendors are fairly adept at developing patches for flaws found in their software and patches are constantly issued to protect systems from bugs that may introduce security problems. This introduces a whole new problem for managers and administrators to be concerned with—patch management. How important this has become is easily illustrated by how many of the most recent security events have been as a result of a security bug that had been discovered months prior to the security incident, and for which a patch has been available, but the community has not correctly installed the patch making the incident possible. One of the reasons for this is that many of the individuals who would be responsible for installing the patches are not trained to understand the security implications surrounding the hole or the ramifications of not installing the patch. Many of these individuals simply lack the necessary training.

Security training has become a foundation element of a complete education in information systems and computer science. As such, measurement of a new graduate's computer security knowledge and ability is of interest to many employers. It is for this reason, the need for an increasing number of security professionals who are trained to some minimum level of understanding, that certifications such as the Security+ certification have been developed. Prospective employers want to know that the individual they are considering hiring knows what to do in terms of security. The prospective employees in turn want to have a way to demonstrate their level of understanding, which can enhance their chances of being hired. The community as a whole just wants more trained security professionals. This book is designed not only to serve as an introductory textbook, but to give the students the necessary material to pass the Security+ exam at the completion of the course. When you pass it, you will demonstrate that you have that basic understanding of security that employers are looking for. Passing this certification exam will not be an easy task for there are many things that you will need to learn to acquire that basic understanding of computer and network security.

How This Book is Organized

The book is divided into chapters to cover essential aspects of computer security and cover the objectives of the Security+ exam. Some of the chapters are more technical than others—reflecting the nature of the security environment where you will be forced to deal with not only technical details but other issues such as security policies and procedures as well as training and education. While there are many individuals involved in computer and network security that have advanced degrees in math, computer science, information systems, or computer or electrical engineering, you do not need to be this technical to effectively address security in your organization. For example, you do not need to develop your own cryptographic algorithm—you simply need to be able to understand how cryptography is used along with its strengths and weaknesses. As you progress in your studies, you will learn that many of the problems in security are a result of the human element. The best technology in the world still ends up being placed in an environment where humans have the opportunity to foul things up—and they all too often do.

This book begins with an introduction of some of the basic elements of security. This begins with the Introduction (Chapter 1) then General Security Concepts (Chapter 2), then an introduction to operational concepts (Chapter 3) and finishes with the role of people in computer security (Chapter 4). It is recommended that these chapters be used in order in all classes as they are foundational to other elements in the book.

Chapters 5 through 9 represent various technical elements of a computer security class. The order of presentation is somewhat arbitrary, although it would be best to have cryptography (Chapter 5) prior to public key infrastructure (Chapter 6).