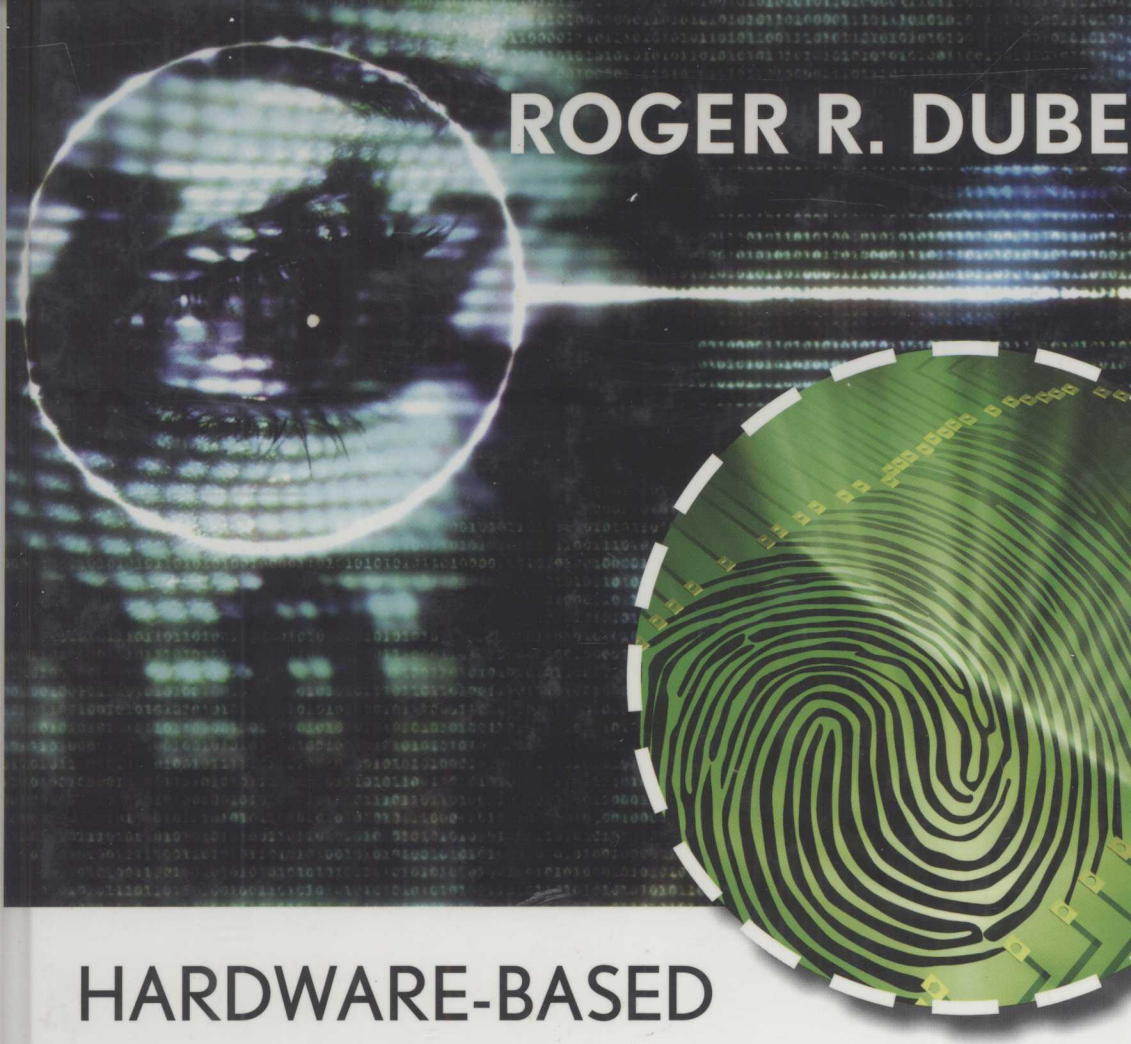

ROGER R. DUBE

HARDWARE-BASED COMPUTER SECURITY TECHNIQUES TO DEFEAT HACKERS

From Biometrics to Quantum Cryptography

WILEY

Hardware-Based Computer Security Techniques to Defeat Hackers

From Biometrics to Quantum Cryptography

Roger Dube

WILEY

E2008001449

A JOHN WILEY & SONS, INC., PUBLICATION

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data is available.

ISBN 978-0-470-19339-6

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Hardware-Based Computer Security Techniques to Defeat Hackers

This book is dedicated to my wife, Jeri, whose undying support and love have given me the courage to chart new directions in my life. The book is also dedicated to my children—Dawn, Danielle, Laura, and Jordan—and their wonderful children as well. The thrill of seeing each of them grow to find their talents, passions and partners in art, science, animal care and writing continues to make life fulfilling. I am very proud of them all.

Finally, the dedication would be incomplete without my deepest thanks to my mom and dad who created and maintained a nurturing environment through easy and hard times alike.

ACKNOWLEDGMENTS

I would like to express sincere appreciation to a number of professional colleagues who aided in my education as a physicist and my immersive education in the computer security field. The Experimental General Relativity Group at Princeton provided an environment in which a young physicist could learn fundamental approaches to difficult weak signal detection problems. Bill Wickes, the late Dave Wilkinson, Jim Peebles, and Ed Groth provided engaging and challenging discussions on various aspects of differential and phase sensitive detection. My years at IBM Research provided first hand management experience of technology development and commercialization projects, giving me an appreciation of the need to integrate technology and science with product schedules. Omesh Sahni was instrumental in helping me grow as a manager, carefully guiding me through progressively more difficult management situations. At DAT, Rick Morgenstern, Mary Ann Voreck, Peter Patsis, John Burdick, Bill Kazis, and Mukesh Kumar have provided support, companionship and boundless energy as the team worked to develop, refine, and deliver military grade authentication technology to various governmental organizations.

The fine folks at the United States Joint Forces Command, especially the Joint Experimentation Lab headed by Tony Cerri, were helpful, instructive, and patient as our technology was exposed to demanding attacks and attempts to break the hardware-based authentication system that we had developed. Lt. Col. Dave Robinson and Brad Mabe at SAIC invested countless hours helping us test, debug, and refine the technology.

I would like to thank Paul Petralia, senior editor at Wiley, for supporting the concept of the book. Finally, I would like to express my sincerest thanks to Lt. Col. Dave Robinson, who patiently read drafts and offered valuable suggestions, corrections, and refinements even through the height of Michigan football season.

ABOUT THE AUTHOR

Roger Dube received his bachelor's degree in physics and math from Cornell University and his Ph.D. in experimental physics from Princeton University. He completed a post-doctoral position at Kitt Peak National Observatory in Tucson, where he continued his work on using weak signal detection techniques to tackle problems in experimental general relativity. Over the next few years he held various academic positions at Caltech/Jet Propulsion Laboratory, the University of Michigan, and the University of Arizona. He joined IBM's Research Division in Yorktown Heights, NY after developing a system to store real time data in photorefractive crystals using holography. Dr. Dube rose through management levels at IBM while maintaining an adjunct professorship at nearby Yale University, where he mentored graduate students as well as lectured on device physics and technology commercialization.

Dr. Dube left IBM in 1996 to become president of Gate Technologies International, Inc. (later named Digital Authentication Technologies, Inc.) based in Boca Raton, FL. Gate provided advanced technology search services for leading technology companies in a variety of industries through the year 2000. During those years, it became apparent to Dr. Dube that there was a strong need for a computer security and authentication technology that employed an unalterable physical process as a source of randomness for cryptographic keys. During 2000 and early 2001, Dr. Dube invented the fundamental patents for a physics-based location aware security and authentication technology. Over the course of the next few years, the company received numerous contracts and research grants for the technology to examine how it might be applied to problems of securing information sharing, wireless communication, and control of critical infrastructure.

Dr. Dube currently holds a joint position as president and chief scientist of Digital Authentication Technologies, Inc. and as a professor of imaging science at Rochester Institute of Technology (RIT).

PREFACE

Advances in computer security technologies are occurring at a fast pace. As a result, defenses (over time) are dynamic and forever evolving. As new protective measures appear, new attacks are developed to defeat them, leading to corrective improvements in the protective measures, new attacks, and so on. Hacker organizations, often formed with the intent of forcing developers to improve and harden the security features of their products, meet frequently to discuss new security technologies as well as new attack tools. Challenges and contests in which participants try to break security products or operating systems are mounted frequently and the results published broadly, often to the consternation of the product developer. As more applications migrate to open source, the opportunity for deeper testing of security features is enhanced.

By its very nature, any book on the topic of computer security will be a snapshot of current protection technologies and common attack approaches. For example, even as this book goes to press, new articles are appearing on a possible vulnerability of quantum cryptography, which to date has been considered unbreakable by the intelligence community. Of course, the assertion will be studied and tested by countless groups around the world, and will likely result in an improvement.

With this dynamic quality in mind, readers should review each of the technologies discussed in this book periodically to determine if enhancements or fundamental changes have been made since the time of publishing. New technologies will appear as well, and they need to be subjected to careful analysis and testing before being deployed on mission critical systems. That having been said, the basic physics, mathematics, and electronics that are used to build these technologies do not change, and so the core principles remain the same. The specific implementations are usually the elements that evolve.

The book has been designed to present each security technology from a fundamental principles perspective first, so that the reader can understand the issue that motivated the creation of the technology. With this in mind, the subsequent analysis of the technology's ability to meet those goals and withstand attacks is generally easier to accomplish. Perhaps as important, such an understanding will help a user appreciate the need to implement each technology properly so that the intent of the developers is preserved. Otherwise, additional vulnerabilities due to mismatching interdependencies may be introduced that compromise a specific implementation.

Dependencies are another important aspect of security elements in an information processing environment. No single product is developed without attention to other components or critical processes upon which it depends. Failure of IT administrators to understand such dependencies can undermine a security rollout.

INTRODUCTION

Since ancient times, mankind has had a need to communicate with complete privacy and authenticity. Signatures, trusted couriers, secret passwords, and sealing wax were all elements of early systems that sought to authenticate or otherwise protect messages between two parties. As wars between nations became fiercer, the need for secure communication increased. Over time we have witnessed the development of increasingly complex ciphers, cryptography, and even the introduction of the Enigma machine.

With the advent of electronic computers, there has been an explosion of activity in the creation of new cryptographic algorithms. Many of these systems required the use of random numbers in some aspect of their operation, but John von Neumann, who is regarded as the father of computer science, strongly cautioned people against the use of any form of software algorithm to generate random numbers (see Chapter 1, page 12 of this book). Von Neumann recognized that only a physical process can produce a truly random, unpredictable number. The output of a mathematical algorithm, by its very nature, can be predicted if the algorithm is returned to the initial condition of a previous time. Moreover, as explained in Chapter 3, there are fundamental concerns with the distribution or sharing of keys. Against this setting, the exponential growth of processing power has enhanced the ability of hackers to break algorithms and keys. So how do we move security forward?

Hardware devices can tie a computer system and its user to the physical world. Proper protection of such devices against tampering can further strengthen the system. The use of person-specific information that can only be obtained in person (such as biometrics) can add credibility to the authentication process. New technologies that employ location-specific signatures can be used to place such an authenticated person at an authenticated location, provided that the technology cannot be spoofed or defeated.

With this backdrop in mind, this book presents computer security from the perspective of employing hardware-based security technologies to construct systems that cannot be broken by hackers. Armed with a review of basic computer security concepts and analysis techniques, the book quickly moves into the realm of hardware-based security technologies. Such technologies span a wide range of topics, including physics-based random number generators, biometric devices, trusted computing systems, location awareness, and quantum cryptography.

Each of these technologies is examined with an eye toward possible attack avenues. By following the types of approaches currently being employed by hackers to defeat hardware-based security devices, the reader should develop an understanding of the means by which security technologies can be evaluated for

Moreover, as specific security technology elements are broken, awareness of the impact on other elements within a deployment must be evaluated immediately to determine if the entire system is now compromised.

Security administrators must establish early on which priorities override others. For example, in high security organizational systems, control of access or knowledge of employee activities may override privacy of employees. It is important that policy governing these priorities be established early and communicated broadly throughout the organization so that implementations meet the requirements and that employee expectations are not misplaced.

Implementations, interdependencies, specific (existing and new) security technologies and organizational security goals should be revisited annually to assure that mission critical systems continue to be protected to the highest level possible. A fresh review and audit of the choices available and made (as described in Chapter 14 of this book) should be completed by a knowledgeable committee of internal and external auditors annually, and a summary of the current or recommended security implementation should be presented to executive management annually as well. This process need not be expensive nor time consuming, but the benefit will be measurable as new attacks appear and new technologies surface.

Finally, technology must not become a smokescreen for what is happening within the core of a security product. Security is an essential element of an information technology environment, and as such, must be chosen with care. A deep understanding of the processes might require some additional education in a specific field (such as optics, electronics, or even introductory quantum theory), but the benefit of such an understanding is that no marketing material will succeed in obscuring the true limitations and capabilities of a technology from someone who has taken time to master its basic principles. To quote Francis Bacon, "knowledge is power."

Roger R. Dube
Rochester, NY

possible use in any given security system. With an understanding of the security goals of a system, any technology device can be analyzed for possible vulnerabilities if used in that system.

CONTENTS