Wireless Networks

Series Editor

Xuemin Sherman Shen
University of Waterloo
Waterloo, ON, Canada

The purpose of Springer's new Wireless Networks book series is to establish the state of the art and set the course for future research and development in wireless communication networks. The scope of this series includes not only all aspects of wireless networks (including cellular networks, WiFi, sensor networks, and vehicular networks), but related areas such as cloud computing and big data. The series serves as a central source of references for wireless networks research and development. It aims to publish thorough and cohesive overviews on specific topics in wireless networks, as well as works that are larger in scope than survey articles and that contain more detailed background information. The series also provides coverage of advanced and timely topics worthy of monographs, contributed volumes, textbooks and handbooks.

More information about this series at http://www.springer.com/series/14180

Jiangxing Wu

Cyberspace Mimic Defense

Generalized Robust Control and Endogenous Security

Springer

Jiangxing Wu
National Digital Switching System Engineering
& Technological R & D Center
Zhengzhou, Henan, China

ISSN 2366-1186 ISSN 2366-1445 (electronic)
Wireless Networks
ISBN 978-3-030-29843-2 ISBN 978-3-030-29844-9 (eBook)
https://doi.org/10.1007/978-3-030-29844-9

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

While human beings enter in high spirits the era of network-based digital economy and enjoy to their hearts' content the wonderful material and cultural life delivered by science and technology, they encounter the problem of cyberspace security, which haunts, like a ghost, in both the physical and virtual worlds of the Internet of Everything, constituting the "Achilles' heel" of the network information society and the digital economy. This is due to of the four theoretical and engineering security problems arising from the related original sources which are difficult to break through:

1. Loopholes: Loopholes result from the hardware and software defects that are unavoidable in the current stage of science development, though hardware and software are the bedrock of the information era.
2. Backdoors and Trojans: They are usually planted on the hardware during the making or supply process and are impossible to be eradicated due to the totally open ecosystem—the global value chain characterized by division of labor across countries, industries, and even within a product.
3. Lack of theoretical and technical means to thoroughly examine the complicated information system or control the hardware/software code configuration of devices in the foreseeable future.
4. Backdoors and loopholes polluting the cyberspace from the source. This is due to the above-mentioned causes, which lead to ineffective quality assurance and supervision during the design, production, maintenance, application, and management processes.

As the human society has been speeding up the informatization, cyber security technologies are not developing synchronously at the same level. On the contrary, the ever-increasing technology gap is forcing people to take the opportunistic trend that "the informatization is the first priority," thus opening the Pandora's box in the cyberspace. In addition, there exist too many interest temptations in cyberspace in the digital economy, alluring individuals, enterprises, entities, organizations, or even states or government organs to launch network attacks for self-interests and even take the pursuit for the unrestricted control of the fifth space and absolute

freedom in cyberspace as the national strategy. The pan-cyber terrorism is a serious impediment to the continuous prosperity of the modern society, causing people to live in unprecedented anxiety and prolonging darkness.

Human beings have never given up their efforts to address the rigorous cyber security issue. With the emergence of various security technologies, e.g., intrusion detection, intrusion prevention, intrusion tolerance, and encryption and authentication, especially the introduction of big data, artificial intelligence, blockchain, and other analytic techniques and means in recent years, we no longer have to trace the sources only after the occurrence of security problems. In other words, we take proactive measures for prevention, detection, and response rather than mend the fold after a sheep is lost. For example, it is possible to find the vulnerability or suspicious functions of file codes early by software and hardware gene mapping analysis; massive problem scene data can be collected and analyzed via big data for the detection and early warning of hidden attacks; AI can be employed to optimize the state explosion problem in the vulnerability analysis process; and the tamper-resistant technology can be provided through the blockchain consensus mechanism and the timestamp-based chain relations. In addition, in order to offset the advantage of the "single attack" launched by the attacker at the static, certain, and similar vulnerabilities of the target system, we can introduce multilevel defense techniques such as dynamicity, randomness, diversity, trusted computing, and trusted custom space, in the hope of reversing the unbalanced cyber attack and defense game where the defender is all the time in an unbalanced and declining position.

Unfortunately, these defensive measures, whether they are passive models based on various a priori knowledge or behavioral feature or active models using big data intelligence analysis or randomly changing address, data, and instruction, whether they are the sandbox technology for online real-time perception or the intelligent analysis method for offline/background screening, and whether they are the behavior perception technology using trusted computing or the data tampering-resistant technology using blockchain, are, in essence, the "attached" perimeter defense technologies, irrelevant to the functions and structure of the protected object. There exists the lack of necessary feedback control mechanisms or operation just runs like a "black box." Although they have achieved good application results in preventing or reducing the availability or exploitability of security defects in the target object (without considering performance overhead), they do not perform remarkably or fail completely in suppressing "coordinated internal and external" attacks based on the hidden or built-in backdoor functions of the target object or in addressing the attacks based on "side-channel effects" and hardware construction defects (such as CPU's Meltdown and Spectre). To make matters worse, in most cases, these attached perimeter defenses cannot even guarantee the service credibility of their own security functions. For example, the bottom-line defense device for encryption and authentication cannot give any convincing proof on whether it is possible to be "bypassed" by the host system or even has any backdoors or Trojans. It even cannot provide any convincing quantitative and measurable indicators on the security of its ontological service functions when the host cannot guarantee its credibility.

It should be emphasized that in the era of network-based digital economy, it has become a national strategy for defending cyber sovereignty and protecting data resources. All major jurisdictions in the world now regard it as their national strategy to seek a prioritized position in cyberspace, sparing no effort to mobilize national resources and even exploiting market forces and trade protection regulations to compete for cyberspace rights and information control. In particular, with the help of the first mover technical advantage, the market monopoly status, and the control or influence on the design, manufacturing, supply, and maintenance sections across the industrial chain, "hidden loopholes, built-in backdoors, and implanted Trojans" will become indispensable strategic resources for the so-called active defense, which can be almost freely used without the constraints of the current legal systems, ethics, or cyber codes of conduct. They can even be combined with conventional firepower weapons to gain an overwhelming strategic edge. This means that known unknown risks or unknown unknown security threats will pervade the entire industrial chain environment like a horrible plague, polluting and poisoning the entire cyberspace. It will not only pose severe challenges to the ultimate human ideal of "an intelligent and connected world" but also fundamentally shake the basic order and the principle of good faith on which the human society depends for survival and development in the age of digital economy and network information.

In view of the fact that the underlying conditions on which the traditional perimeter defense theory relies are constantly blurring and collapsing, coupled with the promotion and application of the "Zero Trust Architecture" supporting new business models such as mobile office, the perimeter defense software/hardware facilities are not only unable to guarantee their own service reliability but also fail to effectively deal with coordinated internal and external backdoor attacks or attacks exploiting other dark features of the target object of the "Zero Trust Architecture." Both the science and industrial communities must transform the traditional cyber security concepts, mindsets, and technological development models by abandoning the illusion of pursuing utopian "sterile, virus-free" cyberspace. In the "global, open, and shared" digital economy and ecology, we strive to innovate the endogenous security theories and methods. As the software/hardware component design chain, tool chain, production chain, supply chain, and service chain cannot guarantee their credibility, we are now developing disruptive theories and techniques based on system engineering to dispel the attack theories and methods targeted at software/hardware code problems at the structural level of the systems. Without relying on (but with access to) attached security measures or means, we can endow the "structure-determined security" functions in the target system (including the defense facilities) through the innovative software/hardware structural technology.

I remember that when I was studying the variable structure high-performance computer system 11 years ago, I occasionally watched a video showing the striped octopus (also known as the mimic octopus) on an NGC program and was deeply fascinated by the unique features of the magical marine creature. While admiring the greatness of the creator, I came up with an exciting idea: Is it possible to construct a collaborative computing and processing device with a variable structure similar to the mimic function of the octopus, so that the device can change its own

structure, operation mechanism, and processing scenario synergistically against different computing models, processing procedures, and resource conditions? Unlike the classic computing and processing model put forward by Von Neumann, the "structure for computer service"—a software/hardware computing method—can not only greatly improve the performance of the area-specific computing processing system but also make the parasitic backdoors in the system lose the stability of their apparent functions and characteristics due to uncertain changes in the structure. The device can, on the one hand, achieve joint optimization and coordinated management in effectiveness, performance, and security, and on the other hand, it makes it much more difficult to create effective and reliable attack chains. In my mind, the mimic computing system should be able to handle diverse, dynamic, and random processing scenarios through its active cognition and coordinated management functions. The nondeterministic relations between its task function, performance goal, and algorithm structure can just make up for the security flaws of staticity, certainty, and similarity in conventional information processing systems when addressing backdoor attacks. I have named the two types of applications based on software and hardware variable structure coordinated computing as "Mimic Structure Calculation" (MSC) and "Mimic Structure Defense" (MSD), respectively. However, the prerequisite for MSC and MSD to make coordinated variable structure reactions is the accurate perception or timely recognition of the on-site environment. Fortunately, MSC only needs to obtain the current running scene or posture data to implement structural transformation or scene migration according to the preset fitting rules, while MSD must judge whether there is a security threat. This may be acceptable when the a priori knowledge or the behavioral characteristics of the attacker are available or even the known unknown threats are perceptible, but for unknown threats lacking behavioral characteristics, there are philosophical cognition contradictions and technical feasibility challenges to conquer before a timely and reasonable judgment can be made.

Obviously, if we can propose an endogenous security function based on the system structure effect and "quantifiable design" and invent an "identification of friend or foe (IFF)" mechanism with controllable credibility, we can conditionally convert unknown unknown events into known unknown events and then into events that can be quantified and represented by probability based on such robustness control mechanisms as measurement awareness, error recognition, and feedback iteration. Namely, man-made attacks based on individual software/hardware backdoors can be normalized to general uncertain disturbances of the target object's heterogeneous redundant structure, so that mature reliability and robust control theories and methods can be used to handle traditional and nontraditional security issues in a unified manner and no longer stay in the period of thinking experiments. Cyber mimic defense is the outcome of theoretical exploration and engineering practice of this vision that "simplicity is the ultimate sophistication."

From the perspective of the defender, whether it is an incidental failure of the information system or control device or a man-made backdoor attack, it is generally an unknown event in nature, where the former is a known unknown event that can be expressed by probability in most cases, while the latter is often an unknown

unknown event that belongs to the uncertain problems and cannot be expressed by probability. Nevertheless, in the scientific sense, being "unknown" is always strongly correlated to cognitive scenarios and perceptual means. As our science and technology evolves, we may change these scenarios and means, and the "unknown" may be transformed into the "known." For instance, humans had thought that the Earth was the center of the solar system before the telescope was invented, while life and death were the will of god or devil before the invention of the microscope.

In fact, in the field of reliability engineering, the dissimilarity redundancy structure (DRS) has been able to, by means of the heterogeneous redundancy scenarios and multimode consensus mechanisms under functionally equivalent conditions (referred to herein as the "relatively correct" axioms), convert the unknown disturbances caused by uncertain physical elements or logic design defects of the random nature of a single device in the target system into an "abnormal event" that can be perceived by the multimode voting mechanism of the heterogeneous redundant architecture and obtain stability robustness and quality robustness through the heterogeneous redundant structure, which are measurable and verifiable. However, if it is directly used to deal with nonrandom man-made attacks featuring "one-way transparency" or "insider-outsider collaboration," there are security flaws in the mechanism such as staticity, certainty, and similarity, especially when the type and amount of heterogeneous redundant bodies are limited (relative to large-scale redundancy scenarios upon the blockchain consensus mechanism). In theory, an attacker mastering certain "common-mode" attack resources can still invalidate the dissimilarity redundancy mechanism for "majority ruling or 51% consensus" by using the "one fatal hit," trial and error, exclusion, and other violent attack methods. In other words, the structure of DRS does not possess stable robustness when dealing with deliberate attacks based on vulnerabilities and backdoors. Therefore, based on the dissimilarity redundancy structure, the author proposes a multi-dimensional reconfigurable "DHR" structure with a strategic decision-making, strategic scheduling, and negative feedback control mechanism, which allows the functionally equivalent "uncertain scenario" effect even in the small-scale space of heterogeneous redundancy. Under the premise of unchanged apparent service functions, any brute-force attacks, whether they are "trial and error" or "coordinated or non-coordinated," against the intra-architecture service elements will be "blocked without being perceived" or "made the attack results difficult to sustain" as long as it can be perceived by the multimode ruling segment. Changes in the ruling status or control policies will give rise to changes of variables in the feedback control functions, leading to changes in the combination of executors in the DHR architecture or changes in the executor's own structure. The basic premise of unchanged background conditions will no longer exist for trial-and-error or common-mode attacks.

It should be emphasized that the mimic defense discussed herein does not include the trial-and-error attacks that aim at an unrecoverable "downtime," or DDoS to block the target object's service chain, or cyber attacks that utilize communication protocols, procedures, specifications, and other design loopholes and backdoors.

You may easily find out that the cyber mimic defense essentially adopts a unique general robust control architecture that integrates high reliability, high credibility,

and high availability. Such a defense architecture, supported by the theory of bio-mimic camouflage, can produce an uncertain effect for attackers. This endows the target object with an endogenous security function that is independent from (but can naturally converge with) the effectiveness of attached defense measures. It has seven features: First, in the small-scale space, a man-made apparent uncertain attack against the individual loopholes of the target object's heterogeneous redundant body can be converted into an event with uncertain effects at the system functional level. Second, the event with uncertain effects can be further transformed into a reliability event with controllable probability. Third, the strategic decision-making, strategic scheduling, and multi-dimensional reconfigurable feedback control mechanism can prevent any form of trial-and-error attack based on its designable, quantifiable, verifiable, and measurable endogenous security effects through mimic camouflage Fourth, the coordinated expression based on the relatively correct axiom or consensus mechanism makes it possible to offer the IFF feature with controllable credibility and without relying on the attacker's a priori information or behavioral characteristics, thereby creating a prerequisite for the application of the traditional security defense technology based on the "detection-perception-removal" mechanism. Fifth, it can normalize non-conventional security threats into robust control problems under the framework of classical reliability theories and auto-control theories, which can then be handled through mature security defense measures. Sixth, despite of the uncertain attack effects on the backdoors above the mimic domain (such as those exploiting undetected design flaws or deep-planted backdoors in network protocols), all random failure disturbances and man-made attack disturbances within the mimic domain can be managed or suppressed by the general robust control structure, and the defense effectiveness is subject to quantitative design and verifiable metrics. Last but not least, the "difficulty of dynamic multi-target coordinated attacks under the non-cooperative conditions" provided by the mimic structure will fundamentally turn over the attack theories and methods based on the defects in the hardware/software codes of the target object.

We are excited to see that as the practical network information systems and control device products based on the mimic structure get entry to various application fields in recent years, the rule-changing mimic defense principle and its endogenous security mechanism are constantly revealing its revolutionary vitality. It is expected that in the globalized ecosystem where the credibility of the component supply chain or even the industry chain of the target product cannot be guaranteed, the innovative DHR architecture can blaze a new trail to address the dilemma of hardware/software component security and credibility from the origin of the product.

The author is deeply convinced that with the rapid evolution of the "open-source, diverse, and multiple" industrial and technological ecology in cyberspace, as well as the ceaseless improvement of the mimic defense theory and the continuous innovation of the applied technologies, the mimic structure system can, by naturally integrating or accepting the existing or coming information and security technology outcomes, achieve significant nonlinear defense gains (as the addition of the relevant security elements increases the heterogeneity in the mimic brackets). The strategic landscape of cyberspace, which is "easy to attack but hard to defend," is

expected to be reversed from the source of hardware/software products, and the unity of "security and openness," "superiority and maturity," and "independent controllability and security and credibility" will greatly reduce the severe negative impacts of non-tariff barriers (e.g., the reasons involving national security) on global free trade and the open industrial ecology at the engineering level. With the incremental deployment and upgrading of the new generation of information systems, industrial control devices, network infrastructure, terminal equipment, and even basic software and hardware components with the mimic structure and endogenous security functions, the basic order and behavioral code of conducts for cyberspace will be reshaped, and the sharp confrontation between the informatization development and the standardization of cyberspace security order will be relieved, or there even exists the possibility of eliminating it.

At that point, it will no longer be an impossible mission for us to reclose the "Pandora's box" in cyberspace and eradicate the "Achilles' heel" of IT products in the original sources, nor is it a wish difficult to be realized in the thinking experiments.

When the book was about to be published, the first permanently online and globally open Network Endogens Security Testbed (NEST) founded by the Purple Mountain Laboratory for Internet Communication and Security started the acceptance of online public testing on June 26 and welcomed challenges from individuals and organizations around the world. The readers of this book are also welcome to participate in the experience and challenges!

https://nest.ichunqiu.com/

Zhengzhou, Henan, China Jiangxing Wu
July 2019

Author's Profile

Jiangxing Wu was born in Jiaxing, Zhejiang, in 1953 with his parental native place in Jinzhai, Anhui, China. He is a Professor and the Director of the China National Digital Switching System Engineering and Technological Research Center (NDSC). In 2003, he became an Academician of China Academy of Engineering through strict selection. During the period from the Eighth Five-year Plan, the Ninth Five-year Plan, the Tenth Five-year Plan to the Eleventh Five-year Plan, he served as an Expert and the Deputy Director of the Group for the Communication Technology Theme and of the Information Domain Experts Group for the National Hi-Tech Development Program (863 Program) and as the General Director of the Experts Board for such national major dedicated projects as "High-Speed Information Demo Network," "China's High-Performance Broadband Information Network (3Tnet)," "China's Next-Generation Broadcast (NGB) Television Network," and "New Concept High-Efficiency Computer System Architecture Research and Development" and was in charge of the organizing group for the dedicated projects like the "New-Generation High Trustworthy Network" and the "Reconfigurable Flexible Network." He also served as the Director of the Verification Committee of the National Mobile Communication Major Projects and as the First Deputy Director for the "National Tri-network Convergence Experts Group." In the mid-1980s of the last century, he successfully developed such core switching technologies as software-defined functions, duplicate-T digital switching network, and the hierarchical distributed control architecture. In the following decade, he presided over the successful development of China's first large capacity digital SPC switch—HJD04—with NDSC's own intellectual property rights, which promoted the growth

of China's communication high-tech industry in the world. At the beginning of this century, he invented such network technologies as the full IP mobile communication, the indefinite long packet asynchronous switching network, the reconfigurable flexible network architecture, and the IPTV based on router selected broadcasting mechanisms. He also took charge of the successful development of information and communication network core equipment like the complex mobile communication system CMT based on full IP, China's first high-speed core router and the world's first large-scale tandem access router ACR. In 2010, he came up with the high-efficiency oriented mimic computing architecture (the multi-dimensional reconfigurable software and hardware cooperative computing architecture). In 2013, his high-efficiency computing prototype system based on the mimic computing came into being in the world for the first time and passed the national acceptance test, which was selected on the list of China's top ten S&T developments for the year 2013 by China's Academy of Sciences and China's Academy of Engineering. In the same year, he set up the cyberspace mimic defense theory. In 2016, the principle verification system was completed and passed the national test and assessment. In December 2017, he published his book *An Introduction to the Cyberspace Mimic Defense Principles*. On the above basis, he made further modifications and improvements and had his book reprinted, entitled *Cyberspace Mimic Defense Principles: General Robustness Control and Endogenous Security*. He won the First Prize for the National Science and Technological Progress for three times and the Second Prize for the National Science and Technological Progress for four times. He was granted the Science and Technological Progress Award and the Science and Technological Accomplishments Award from the Ho Leung Ho Lee Foundation in 1995 and 2015, respectively. In the same year, the network and switching research team headed by him was awarded the Innovation Team Prize for the National Science and Technology Progress.

Brief Introduction (Abstract)

This book, focusing on the most challenging and difficult problem of uncertain security threats in cyberspace and starting from the current technological limitations in the era, summarizes four basic security issues and three important inferences and comes up with the conjecture that the information system can successfully deal with uncertain threats from unknown sources if it possesses non-specific and specific immune functions like vertebrates. From the axiom perspective of structure-determined security, it elaborates on the formation of the concepts and theorem, original intention and vision, principles and methods, implementation basis and engineering cost, and other theories and methods which remain to be improved regarding the "cyberspace mimic defense" which can change the game rules. Various kinds of materials and contents including the system application examples, the authoritative testing reports, and the principle verification have proved both in theory and practice that the effect of indeterminacy generated by the innovative dynamic heterogeneous redundant architecture and mimic guise mechanisms enables the mimic software and hardware to possess the designable, quantifiable, verifiable, and measurable endogenous security efficacy. Without relying on a priori knowledge and behavioral characteristics of attackers and other attached defense methods except for integration, this approach can properly suppress, manage, and control in time general uncertain disturbances caused by attacks from dark functions based on software/hardware object vulnerabilities and backdoors or occasional failures within the mimic boundary and provides a "simplified and normalized" solution to the problem of conventional security reliability and unconventional cyber security threats through innovative robust control mechanisms. As a new enabling technology, it enables IT, ICT, and CPS software/hardware products to have endogenous security functions. This book has put forward the model of mimic architecture and provides a preliminary quantitative analysis and conclusions regarding the cyber reliability and anti-attack effects.

The book is designed to be used for scientists, researchers, and engineers in such areas as information technology, cybersecurity, and industrial control as well as for college faculty and postgraduates.

Preface

The human society is ushering in an era of digital economy at an unprecedented speed. The information network technology driven by the digital revolution has penetrated into every corner of the human society, creating a cyberspace which expands explosively to interconnect all things. A digital space associating both the real world and the virtual world is profoundly changing the ability of human beings to understand and transform the nature. Unfortunately, however, the security of cyberspace is increasingly becoming one of the most serious challenges in the information age or the digital economy era. It is the greediness of man and the periodical attributes in the development of science and technology that prevent the virtual world created by mankind from becoming a pure land beyond the real human society. The world today has its "Achilles' heel," for example, unscrupulously spying on personal privacy and stealing other people's sensitive information, arbitrarily trampling on the common codes of conduct of the human society and the security of cyberspace, and seeking illegitimate interests or illegal controls.

Despite the variety of cyberspace security risks, the attackers' means and goals are changing with each passing day, imposing unprecedented and far-reaching threats to human life and production. The basic technical reasons, though, can be simply summarized as the following five aspects. First, the existing scientific and technological capabilities of human beings cannot completely get rid of the loopholes caused by defects in software/hardware design. Second, the backdoor problem derived from the ecological context of economic globalization cannot be expected to be fundamentally eliminated in a certain period of time. Third, the current scientific theories and technical methods are generally not yet able to effectively check out the "dark features," such as loopholes and backdoors in the software/hardware systems. Fourth, the abovementioned reasons lead to the lack of effective safety and quality control measures for hardware/software products in terms of design, production, maintenance, and use management, where the cyber world gets severely polluted by the loopholes of technical products as the digital economy or social informatization accelerates, even heading toward annihilation. Fifth, the technical threshold for cyber attacks is relatively low in view of the defensive cost of the remedy. It seems that any individual or organization with cyber knowledge or the

ability to detect and exploit the hardware/software vulnerabilities of the target system can become a "hacker" to trample on the guidelines on cyberspace morals or behavior wantonly.

With such a cost disparity in attack-defense asymmetry and such a large interest temptation, it is difficult to believe that cyberspace technology pioneers or market monopolies will not deliberately take advantage of the opportunities arising from globalization, for instance, division of labor across countries, inside an industry and even among product components, to apply strategic control methods, such as hidden loopholes, preserved backdoors, and implanted Trojans. Then, they can obtain improper or illegal benefits other than the direct product profits in the market through the user data and sensitive information under their control. As a super threat or terrorist force that can affect individuals, businesses, countries, regions, and even the global community, dark features such as cyberspace loopholes have become a strategic resource, which are not only coveted and exploited by many unscrupulous individuals, organized criminal gangs, and terrorist forces but also undoubtedly used by stakeholder governments to build up their armed forces and operations for the purpose of seeking cyberspace/information supremacy. In fact, cyberspace has long been a normalized battlefield, where all parties concerned are trying to outplay others. Nowadays, however, the cyberspace is still vulnerable to attacks and yet not resilient to defend itself.

The majority of the current active/passive defense theories and methods are based on precise threat perception and perimeter defense theory and model characterized by threat perception, cognitive decision-making, and problem removal. In fact, in the current situation where intelligent handset or terminal-based mobile offices or e-commerce have become the main application mode, as for the target object or the attached protection facilities, neither the intranet-based regional defense nor the comprehensive ID certification measures based on the "Zero Trust Architecture" can completely eliminate negative effects caused by the loopholes or backdoors. Thus, in view of the "known unknown" security risks or "unknown unknown" security threats, the perimeter defense is not only outdated at the theoretical and technological level but also unable to provide suitable engineering means in practice for quantifiable defense effects. More seriously, so far, we have not found any ideas about the new threat perception that does not rely on attack attributes or behavioral information or any new defense methods that are technically effective, economically affordable, and universally applicable. The various dynamic defense technologies represented by "Moving Target Defense" (MTD, proposed by an American) have really achieved good results in reliably disturbing or crumbling the attack chains that make use of the vulnerabilities of the target object. However, in dealing with dark features hidden in the target system or unknown attacks through the hardware/software backdoors, there still exists the problem of ineffective mechanisms. Even if the underlying defense measures and mechanisms such as encrypted authentication are used, the risks of bypass, short circuit, or reverse encryption brought by dark functions from the internal vulnerabilities/backdoors of the host object cannot be completely avoided. The WannaCry, a Windows vulnerability-based ransomware, discovered in 2017 is a typical case of reverse encryption. In

fact, the technical system based on the perimeter defense theory and qualitative description has encountered more severe challenges in supporting either the new "cloud-network-terminal" application model or the zero trust security framework deployment.

Research results in biological immunology tell us that a specific antibody will be generated only upon multiple stimulations by the antigen and specific elimination can be performed only when the same antigen reinvades the body. This is very similar to the existing cyberspace defense model, and we may analogize it as "point defense." At the same time, we also notice that a variety of other organisms with different shapes, functions, and roles, including biological antigens known as scientifically harmful, coexist in the world of vertebrates. However, there is no dominant specific immunity in healthy organisms, which means the absolute majority of the invading antigens have been removed or killed by the innate non-specific selection mechanism. The magic ability obtained through the innate genetic mechanism is named non-specific immunity by biologists, and we might as well compare it to "surface defense." Biological findings also reveal that specific immunity is always based on non-specific immunity, with the latter triggering or activating the former, while the former's antibody can only be obtained through acquired effects. Besides, since there are qualitative and quantitative differences between biological individuals, no genetic evidence for specific immunity has been found to date. At this point, we know that vertebrates acquire the ability to resist the invasion of known or unknown antigens due to their point-facet and interdependent dual-immune mechanisms. What frustrates us is that humans have not created such a "non-specific immune mechanism with clean-sweep properties" in cyberspace; instead, we always try to address the task of coping with surface threats in a point defense manner. The contrast between rational expectation and harsh reality proves that "failure in blocking loopholes" is an inevitable outcome, and it is impossible to strategically get out of the dilemma of dealing with them passively.

The key factor causing this embarrassing situation is that the scientific community has not yet figured out how non-specific immunity can accurately "identify friend or foe." According to common sense, it is impossible for the biological genes, which cannot even carry the effective information generated from biological specific immunity, to possess all the antigenic information against bacteria, viruses, and chlamydia that may invade in the future. Just as the various vulnerability/attack information libraries in cyberspace based on behavioral features of the identified backdoors or Trojans, it is impossible for today's library information to include the attributes of backdoors or Trojans that may be discovered tomorrow, not to mention the information on the form of future attack characteristics. The purpose of our questioning is not to find out how the creator can endow vertebrate organisms with the non-specific selection ability to remove unknown invading antigens (the author believes that with the restraint of operational capability of the biological immune cells, the method of coarse-granule "fingerprint comparison" may be used based on their own genes and all the invading antigens not in conformity with the genes will be wiped out. As an inevitable cost, there exists a low probability of some "missing alarms, false alarms, or error alarms" in the coarse-granule fingerprint comparison.

Otherwise, vertebrate biological beings will not fall ill or suffer from cancers. And it would be unnecessary for extraordinary immune powers to exist. The comparison of own credibility and reliability is a prerequisite for the efficacy of the comparison mechanism but with an unavoidable risk.) but to know whether there is a similar identification friend or foe (IFF) mechanism in cyberspace, and whether there is a control structure that can effectively suppress general uncertain disturbances, including known unknown risks and unknown unknown threats, to obtain endogenous security effects not relying on (but naturally converging with) the effectiveness of any attached defense techniques. With such mechanisms, structures, and effects, the attack events based on vulnerability backdoors or virus Trojans can be normalized to conventional reliability issues. In accordance with the mature robust control and reliability theories and methods, the information systems or control devices can obtain both stability robustness and quality robustness to manage and control the impact of hardware/software failures and man-made attacks. In other words, it is necessary to find a single solution to address the reliability and credibility issues at both the theoretical and methodological level.

First, the four basic security problems in cyberspace are generally regarded as the restrictive conditions because the basic security problems will not change when the system host or the attached or parasitic organizational forms change or when system service functions alter. Hence, we can come up with three important conclusions: security measures may be bypassed in the target system with shared resource structure and graded operational mechanisms; attached defense cannot block the backdoor function in the target object; and defense measures based on a priori knowledge and behavior information and features cannot prevent uncertain threats from unknown vulnerabilities and backdoors in a timely manner.

Second, the challenge to be conquered is how to perceive unknown unknown threats, i.e., how to achieve the IFF function at low rates of false and missing alarms without relying on the a priori knowledge of attackers or the characteristics of attack behaviors. In fact, there is no absolute or unquestionable certainty in the philosophical sense. Being “unknown” or “uncertain” is always relative or bounded and is strongly correlated to cognitive space and perceptual means. For example, a common sense goes like this: “everyone has one shortcoming or another, but it is most improbable that they make the same mistake simultaneously in the same place when performing the same task independently” (the author calls it a “relatively correct” axiom, and the profession also has a wording of the consensus mechanism), which gives an enlightening interpretation of the cognitive relationship of “unknown or uncertain” relativity. An equivalent logic representation of the relatively correct axiom—the heterogeneous redundant structure and the multimode consensus mechanism—can transform an unknown problem scene in a single space into a perceptible scenario under the consensus mechanism in a functionally equivalent multi-dimensional heterogeneous redundant space and the uncertainty problem into a reliability problem subject to probability expression and transfer the uncertain behavior cognition based on individuals to the relative judgment of the behavior of a group (or a set of elements). In turn, the cognitive or consensus results of the majority are used as the relatively correct criteria for reliability (this is also the

cornerstone of democracy in human society). It should be emphasized that as long as a relative judgment is made, there must be a "Schrödinger's cat" effect like the superposition state in quantum theory. "Right" and "wrong" always exist at the same time, while the probability is different. The successful application of a relatively correct axiom in the field of reliability engineering dates back to the 1970s, when the first dissimilarity redundancy structure was proposed in flight controller design. For a target system based on this structure under certain preconditions, even if its software/hardware components have diversely distributed random failures or statistically uncertain failures caused by unknown design defects, they can be transformed by the multimode voting mechanism into reliability events that can be expressed with probabilities, enabling us to not only enhance system reliability by improving component quality but also significantly enhance the reliability and credibility of the system through innovative structural technology. In the face of uncertain threats exploiting the backdoors of the software/hardware system (or man-made attacks lacking in a priori knowledge), the dissimilarity redundancy structure also has the same or similar effect as the IFF. Although the attack effect of uncertain threats is usually not a probability problem for heterogeneous redundant individuals, the reflection of these attacks at the group level often depends on whether the attacker can coordinately express consensus on the space-time dimension of multimode output vectors, which is a typical matter of probability. However, in a small-scale space and a certain time, a target object based on the dissimilarity redundancy structure can suppress general uncertain disturbances, including unknown man-made attacks, and has the quality robustness of designable calibration and verification metrics. However, the genetic defects of the structure, such as staticity, similarity, and certainty, mean that its own backdoors are still available to some extent, where trial and error, exclusion, common model coordination, and other attack measures often corrupt the stability robustness of the target object.

Third, if viewed from the perspective of robust control, the majority of cyberspace security incidents can be considered as general uncertain disturbances arising from attacks targeted at the backdoors or other vulnerabilities of target objects. In other words, since humans are not yet able to control or suppress the dark features of hardware/software products, the security and quality problems, which originally arise from the design or manufacturing process, are "forced to overflow" as the top security pollution in cyberspace due to "the unconquerable technical bottleneck." Therefore, where a manufacturer refuses to promise the safety and quality of its software/hardware products, or is not held accountable for the possible consequences caused thereby, seems that it has a good reason to justify its behavior by the "universal dilemma." In the era of economic and technological globalization, to restore the sacred promise of product quality and the basic order of commodity economy and fundamentally rectify the maliciously polluted cyberspace ecology, we need to create a new type of robust control structure that can effectively manage and control the trial-and-error attacks and the uncertain effect generated by the feedback control mechanism driven by the bio-mimic camouflage strategy, providing the hardware/software system with stability robustness and quality robustness against general uncertain disturbances.

Furthermore, even if we can't expect the endogenous security effects of the general robust control structure and the mimic camouflage mechanism to solve all cyberspace security problems or even all the security problems of the target object, we still expect the innovative general robust structure to naturally converge with or accept advances in existing or coming information and security technologies. Whether the technology elements introduced is static or dynamic defense, active or passive defense, the target object's defense ability should be enhanced exponentially so as to achieve the integrated economic and technological goal of "service-providing, trusted defense, and robustness control."

In order to help the readers better understand the principles of cyberspace mimic defense, the author has summarized its key theoretical points into the following: one revolving premise (unknown vulnerabilities and backdoors in cyberspace can lead to uncertain threats); one theory-based axiom (conditional awareness of uncertain threats can be provided); discovery of one mechanism (with the self-adaptable mechanism of "non-decreasing initial information entropy," uncertain threats can be stably prevented); invention of one architecture (the dynamical heterogeneous redundant architecture DHR with the general robust control performance has been invented); introduction of one mechanism (mimic guise mechanism); creation of one effect (difficult to detect accurately); achievement of one function (endogenous security function); normalization of dealing with two problems simultaneously (making it possible to provide an integrated solution to the problems of conventional reliability and non-conventional cyber security); and production of one nonlinear defense gain (introduction of any security technology can exponentially promote defense effects within the architecture.)

Finally, it is necessary to complete the full-process engineering practice through the combination of theory and application, covering architecture design, common technology development, theoretical verification, application piloting, and industry-wide demonstration.

"Cyberspace mimic defense" is just what comes out from the iterative development and the unremitting exploration of the abovementioned ideas.

Commissioned by the MOST in January 2016, the STCSM organized more than 100 experts from a dozen authoritative evaluation agencies and research institutes across the country to conduct a crowd test verification and technology evaluation of the "mimic defense principle verification system." The test lasted for more than 4 months and proved that "the tested system fully meets the theoretical expectations and the theorem is universally applicable."

In December 2017, *An Introduction to Cyberspace Mimic Defense* was published by the Science Press. The book was renamed as *The Principle of Cyberspace Mimic Defense: General Robust Control and Endogenous Security* and republished after modification and supplementation in October 2018.

In January 2018, the world's first mimic domain name server was put into operation in the network of China Unicom Henan Branch; in April 2018, a variety of network devices based on the mimic structure, including web servers, routing/switching systems, cloud service platforms and firewalls, etc., was systematically deployed at the Henan-based Gianet to provide online services; in May 2018, a

complete set of information and communication network equipment based on the mimic structure was selected as the target facility of the "human-machine war" in the first session of the "Cyber Power" International Mimic Defense Championship held in Nanjing, China, where it underwent high-intensity confrontational tests under new rules. The challengers came from the top 20 domestic teams and 10 world-class foreign teams. A large number of live network operation data and man-machine battle logs persuasively interpret the scientific mechanism of the endogenous security effects generated by the general robust control structure and prove the significance of the unprecedented innovation of the mimic defense technology with trinity features of high reliability, high availability, and high credibility. In May of the same year, nearly 100 domestic research institutes and industrial pioneers co-initiated the "Mimetic Technology and Industrial Innovation Alliance," embarking on a new chapter in the history of the cyber information technology and security industry.

To help readers better understand the principles of mimic defense, the book is made with 14 chapters and 2 volumes. Chapter 1 "Security Threats Oncoming from Vulnerabilities and Backdoors" is compiled by Wei Qiang, which begins with an analysis of the unavoidable backdoors, with a focus on the dilemma of backdoor/vulnerability prevention and control, pointing out that the majority of the information security incidents in cyberspace are triggered by attackers exploiting the hardware/software backdoors and vulnerabilities. The original intention of transforming the defense philosophy was put forward through perception and thinking of these details. Chapter 2 "Formal Description of Cyber Attacks" is compiled by Li Guangsong, Zeng Junjie, and Wu Chengrong. It provides an overview and attempt to summarize the formal description methods of typical network attacks for the time being and proposes a method of formal analysis of cyber attacks targeted at complex cyber environments featuring dynamic heterogeneous redundancy. Chapter 3 "A Brief Analysis of Conventional Defense Technologies" is compiled by Liu Shengli and Guang Yan. It analyzes three current cyberspace defense methods from different angles, pointing out the four problems of the conventional cyber security framework model, especially the defect in the target object and the defense system: a lack of precautions against security threats such as possible backdoors. Chapter 4 "New Defense Technologies and Ideas" and Chap. 5 "Diversity, Randomness, and Dynamicity Analysis" are compiled by Cheng Guozhen and Wu Qi. The two chapters provide a brief introduction to new security defense technologies and ideas such as trusted computing, custom trusted space, mobile target defense, and blockchain and point out the major problems concerned. They give out a basic analysis of the effects and significance of diversity, randomness, and dynamicity of basic defense methods on destroying the stability attack chain and put forward the main technical challenges. Chapter 6 "Revelation of the Heterogeneous Redundancy Architecture" is co-produced by Si Xueming, He Lei, Wang Wei, Yang Benchao, Li Guangsong, and Ren Quan, outlining the mechanisms of suppressing the impacts of uncertain faults on the reliability of the target system based on heterogeneous redundancy techniques and indicating that the heterogeneous redundancy architecture is equivalent to the logical expression of the "relatively correct" axiom and has an intrinsic

attribute of transforming an uncertain problem into a controllable event of probability. The qualitative and quantitative methods are used to analyze the intrusion tolerance properties of the dissimilarity redundancy structure and the challenges of at least five aspects, assuming that the introduction of dynamicity or randomness in this structure can improve its intrusion tolerance. Chapter 7 "General Robust Control and Dynamic Heterogeneous Redundancy Architecture" is co-compiled by Liu Caixia, Si Xueming, He Lei, Wang Wei, and Ren Quan, proposing a general robust control architecture, called "dynamic heterogeneous redundancy," for the information system and proving through quantitative analysis methods that the endogenous defense mechanisms based on the architecture can, without relying on any characteristic information of the attacker, force unknown attack behaviors based on unknown backdoors of the target object to face the challenge of "dynamic multi-target coordinated attack in non-cooperating conditions." Chapter 8 "Original Intention and Vision of Cyberspace Mimic Defense" is written by Zhao Bo et al. It aims to apply the biological mimic camouflage mechanism to the feedback control loops of the dynamic heterogeneous redundancy architecture to form uncertain effects. It is expected that the attacker will be trapped in the cognitive dilemma of the defense environment (including the dark functions such as backdoors) within the mimic border, so that the cross-domain plural dynamic target coordinated attack will be much more difficult. Chapter 9 "Principles of Cyberspace Mimic Defense," Chap. 10 "Implementation of Cyberspace Mimic Defense Projects," and Chap. 11 "Bases and Costs of Cyberspace Mimic Defense" are co-compiled by He Lei, Hu Yuxiang, Li Junfei, and Ren Quan. The three chapters systematically describe the basic principles, methodologies, structures, and operating mechanisms of mimic defense, with a preliminary exploration of the engineering implementation of mimic defense, a discussion on the technical basis and application costs of mimic defense, and an outlook to some urgent scientific and technical concerns. Chapter 12 "Application Examples of the Mimic Defense Principle" is co-written by Ma Hailong, Guo Yudong, and Zhang Zheng, respectively briefing on the verification application examples of the mimic defense principle in the route switching system, the web server, and the network storage system. Chapter 13 "Testing and Evaluation of the Mimic Principle Verification System" is co-compiled by Yi Peng, Zhang Jianhui, Zhang Zheng, and Pang Jianmin, respectively introducing the verification of the mimic principle in the router scenario and the web server scenario. Chapter 14 "Application Demonstration and Current Network Testing of Mimic Defense" introduces the usage and tests of the mimic structure products, such as routers/switches, web servers, and domain name servers, in the current networks.

The readers can easily find the logic of the book: point out that the backdoors and vulnerabilities are the core of cyberspace security threats, analyze the genetic defects of existing defense theories and methods in dealing with uncertain threats, exploit the dissimilarity redundancy structure based on the relative correct axiom to get enlightenment of converting random failures to probability-controllable reliability events without a priori knowledge, propose the dynamic heterogeneous redundancy architecture based on multi-model ruling strategy scheduling and the negative feedback control of multi-dimensional dynamic reconstruction, propose to introduce

a mimic camouflage mechanism on the basis of this structure to form uncertain effects from the attacker's perspective, and discover that the general robust control architecture, which is similar to the dual mechanism of non-specific and specific immunity across vertebrates, has an endogenous security function and unparallelled defense effect as well as the expected target function, which can independently deal with known unknown security risks or unknown unknown security threats through the backdoors within the mimic border, as well as the impacts of conventional uncertain disturbances, systematically expounded. The principles, methodologies, bases, and engineering costs of cyberspace mimic defense provide the online pilot application cases with principle verification and give out the testing and evaluation results of the principle verification system. In conclusion, it describes the pilot operation of several mimic structure products in the real networks and demos.

Undoubtedly, the DHR-based cyberspace mimic defense will inevitably increase the design cost, volume power consumption, and operation and maintenance overhead along with its unique technical advantages. Similar to the "cost-efficiency" rule of all security defense technologies, where "protection efficiency and defense cost are proportional to the degree of closeness to the target object," the mimic defense is no exception. However, any defense technology is costly and cannot be applied ubiquitously. That's why "deployment in the gateway and defense at the core site" becomes a golden rule in military textbooks. The preliminary application practice in information communication networks shows that the increased cost of applying the mimic defense technology is far from enough to hinder its wide application when compared to the overall life-cycle benefit of the target system. In addition, the continued progress in microelectronics, definable software, reconfigurable hardware, virtualization, and other technologies and development tools, the widespread use of open source community models, and the irreversible globalization trend have made the market price of the target product highly correlated to the application scale only but relatively decoupled from its complexity. The "breaking a butterfly on the wheel" approach and the modular integration have become the preferred mode for market-leading engineers. Moreover, with the continuous sublimation of the "green, efficiency, safety, and credibility" concept, so while pursuing higher performance and more flexible functions of information systems or control devices, people are placing more emphasis on the cost-effectiveness of applications and the credibility of services, shifting from the traditional cost and investment concept to the concept of comprehensive investment and application efficiency of the system throughout its life cycle (including security protection, etc.). As a result, the author believes that with continuous progress made in the theorem and methodology of cyberspace mimic defense, the game rules in cyberspace are about to undergo profound changes. A new generation of hardware and software products with "designable," verifiable, and quantified endogenous security functions and efficacy is on their way, and a carnival of innovation in the mimic defense technology is around the corner.

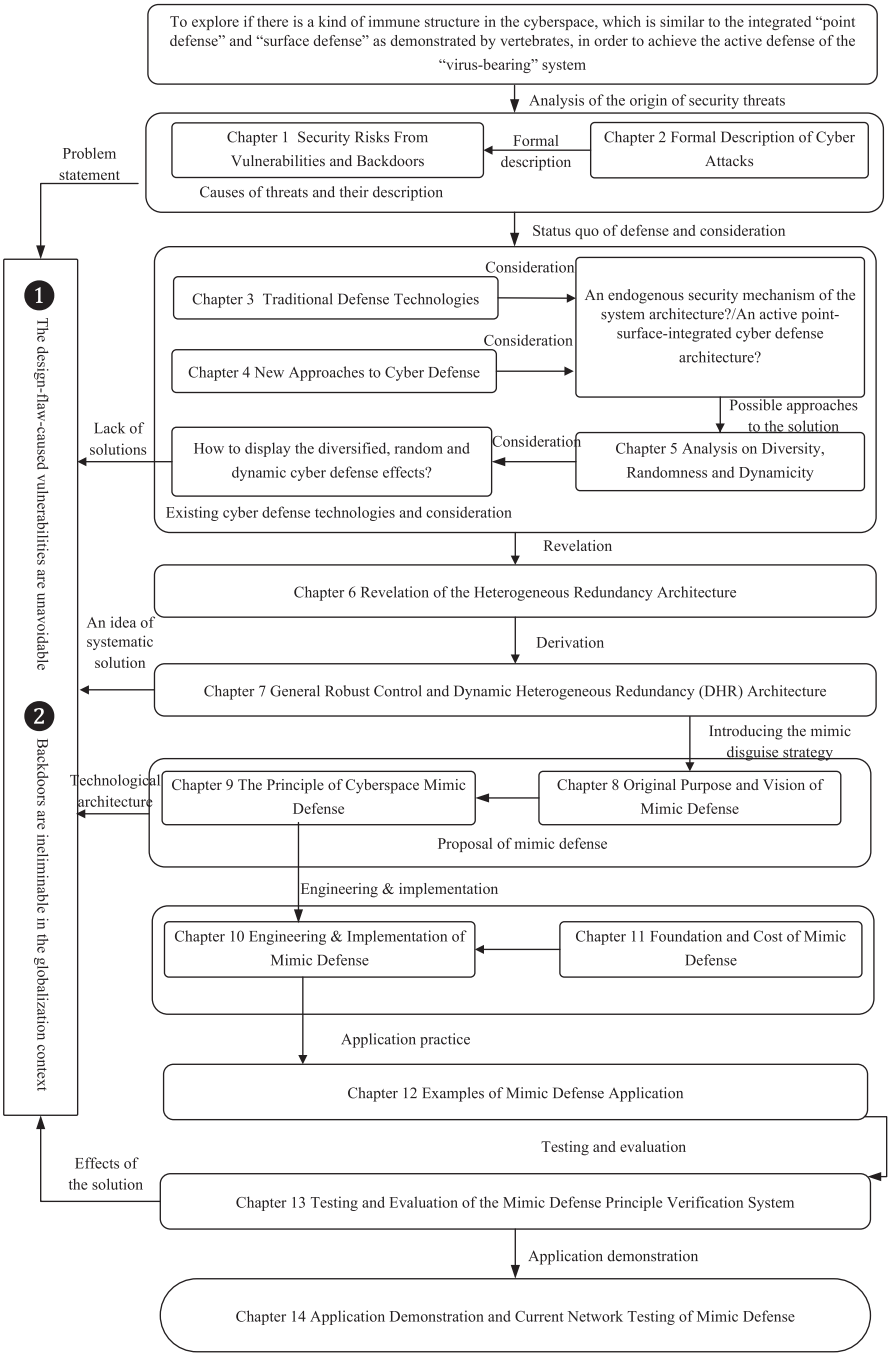
At present, the mimic defense theory has undergone the phases of logic self-consistency, principle verification, and common technology breakthroughs. The targeted application research and development are being carried out according to the

relevant industry characteristics. Valuable engineering experience has been acquired, and significant progress has been made in some pilot and demonstration application projects. New theories and technologies are often incomplete, immature, or not refined. And mistakes are unavoidable. The same is undoubtedly true of this book, for some technical principles are not fully segregated from the "thought experiment" stage, so the immature and rough expressions are inevitable. In addition, the book also lists some scientific and technical problems that need urgent studying and solution in theory and practice. However, the author is convinced that any theory or technology cannot grow to its maturity only in the study or laboratory, especially the cross-domain, game-changing, and subversive theories and techniques, such as mimic defense and general robust control, which are strongly related to application scenarios, engineering implementation, hierarchical protection, industrial policies, etc., and have to undergo rigorous practical testing and extensive application before they can produce positive outcomes. As a saying goes, he who casts a brick aims to attract jade. This book is just like a brick, the publication of which is intended to "attract" better cyber security theories and solutions and maximize the outcome through collective efforts. We sincerely appreciate all forms of theoretical analyses and technical discussions on our WeChat public account (Mimic Defense) and the mimic defense website (http://mimictech.cn). And we wholeheartedly hope that the theory and basic methods of mimic defense can bring revolutionary changes to the strategic landscape of today's "easy to attack yet hard to defend" cyberspace and that the general robust control structure and its endogenous security mechanism characterized by "structure-determined security," quantifiable design, and test validation can bring about strong innovation vitality and thriving replacement demand for the new generation of IT/ICT/CPS technology and the related industries.

This book can be treated as a textbook for postgraduates major in cyber security disciplines or a reference book for the related disciplines. It also serves as an introductory guide for researchers interested in practicing innovation in mimic defense applications or intended to perfect the mimic defense theories and methods. To give the readers a full picture of the connection between the chapters thereof and make it easier for professionals to read selectively, we attach a "chapter-specific relation map" to the contents.

Zhengzhou, Henan, China Jiangxing Wu
March 2019

The Chapter Relationships Chart



Acknowledgments

I am very grateful to all my colleagues who have contributed to the publication of this book. In particular, I would like to express my sincere gratitude to those who directly or indirectly engaged in the writing, revising, or supplementary work. In addition to the colleagues mentioned in the preface to the reprint of this book, who were responsible for or coauthored in the relevant chapters, I also extend my heartfelt thanks to the following people: Liu Xiaolong from the compilation team of Chap. 1, who summarized the related materials of the mitigation mechanism for vulnerability exploitation, and Ma Rongkuan, Song Xiaobin, and Geng Yangyang from the same team, who collected the types of vulnerabilities and made statistical analysis of the cases; He Kang, Pan Yan, and Li Ding from the compilation team of Chap. 3, who were responsible for the collection of the related materials, and Yin Xiaokang from the same team, who was responsible for the adjustment and modification of the entire format of the chapter; Wang Tao and Lin Jian from the compilation team of Chapters 4 and 5, who collected and compiled massive information on new defense types; Liu Qinrang from the compilation team of Chap. 8, who participated in the preparation of the relevant content; and Zhang Jiexin from the compilation team of Chapters 12 and 13, who participated in the writing of the verifying application cases of the web server and the theoretic verification test of web server scenarios. I would also like to thank the organizations engaged in the writing of the related content in Chap. 14, including China Unicom and Gianet (Henan), RuneStone and TopSec (Beijing), ZTE (Shenzhen), FiberHome (Wuhan), Maipu (Chengdu), etc. In addition, Qi Jianping revised the English version of the book and compiled the abbreviations. Ji Xinsheng participated in the planning, writing texture design, and revision of the book; Zhu Yuefei, Chen Fucai, and Hu Hongchao gave valuable suggestions for the writing and the arrangements of some contents; while Chen Fucai and Hu Hongchao, together with Liu Wenyan, Huo Shumin, Liang Hao, and Peng Jianhua, participated in the review of the book.

My special thanks go to Directors General Feng Jichun and Qin Yong, Deputy Director General Yang Xianwu, and Division Heads Qiang Xiaozhe and Wen Bin of the Department of High and New Technology Development and Industrialization under the Ministry of Science and Technology (MOST); Director Shou Ziqi, Deputy

Directors Chen Kehong and Gan Pin, Division Heads Miao Wenjing and Nie Chunni, and Deputy Division Head Xiao Jing of the Science and Technology Commission of Shanghai Municipality (STCSM); Deputy Director Wang Xiujun of the Office of the Central Cybersecurity and Informatization Leading Group (CCILG); Former Deputy Director General Huang Guoyong of the PLA-GSD Department of Communications and Information Technology; etc. They have provided ever-lasting support for the research program.

I would like to sincerely thank the National High-Tech Research and Development Program (863 Program), Zhejiang Lab, the National Natural Science Foundation of China, the Chinese Academy of Engineering, and the STCSM for their long-term funding of this research work.

To conclude, I wish to wholeheartedly thank all my colleagues at the National Digital Switching System Engineering and Technological Research Center (NDSC) and my wife, Chen Hongxing, for their constant contribution to and consistent engagement in this research over the years.

Contents

Abbreviations

ABC	artificial bee colony
ACK	acknowledgment
ACL	access control list
ADR	attack disturbance rate
AnC	ASLRCache
AP	availability probabilities
API	application programming interfaces
APT	Advanced Persistent Threat
AS	attack surface
ASD	all shielding
ASIC	application-specific integrated circuit
ASLR	Address Space Layout Randomization
ASMP	asynchronous symmetric multiprocessor
ASR	address space randomization
AST	attack surface theory
ATA	average time of attack
ATD	average time of defense
AV	access vector
AWGN	additive white Gaussian noise
BGP	Border Gateway Protocol
BIOS	basic input/output system
BNF	Backus-Naur form
BV	backward verification
BVI	backward verification information
C&R	cleaning and recovery
CA	central authentication
CAC	complexity of attack chain
CAICT	China Academy of Information and Communications Technology (hereinafter referred to as the CAICT)
CDN	content delivery network
CERNET	China Education and Research Network

CERT	Computer Emergency Readiness Team
CMD	cyberspace mimic defense
CMDA	CMD Architecture
CMED	common mode events defend
CMF	common mode failure
CNCERT	National Internet Emergency Center
CNNVD	China National Vulnerability Database of Information Security
CNVD	China National Vulnerability Database
CPU	central processing unit
CR	cleaning and recover
CRTM	core root of trust for measurement
CTMC	continuous-time Markov chain
CUHB	China Unicom Henan Branch (hereinafter referred to as CUHB)
CVE	common vulnerabilities and exposures
CVSS	common vulnerability scoring system
DAPAR	Defense Advanced Research Projects Agency
DC	data center
DDN	dynamic domain name
DDoS	distributed denial of service
DEP	data execution prevention
DES	dynamically executing scheduler
DF	dark feature
DHCP	Dynamic Host Configuration Protocol
DHR	dynamic heterogeneous redundant
DHRA	dynamic heterogeneous redundancy architecture
DiffServ	differentiated services
DIL	database instruction labelling module
DMA	differential mode attack
DMF	differential mode failure
DNS	domain name system
DOS	denial of service
DP	damage potential
DP	degradation probabilities
DP	dormancy probability
DPI	deep packet inspection
DPL	deep learning
DRR	dynamic reconstruction rate
DRRV	dissimilar redundant response voter
DRS	dissimilar redundancy structure
DSA	digital signature algorithm
DSAs	domain-specific architecture collaborative computing
DSP	digital signal processing
DVSP	dissimilar virtual web server pool
ECC	elliptic curve cryptography
ED	exploiting difficulty

EK	endorsement key
EP	escape phenomena
EP	escape probability
ES	endogenous security
ESM	endogenous security mechanism
FC(S)	feedback control (system)
FCD	feedback control device
FCL	feedback control loop
FCPT	formal correctness proof techniques
FCS	feedback control system
FCSP	flaw channel scheduling policy
FE	functionally equivalent
FEO	functionally equivalent executor
FM	fault masking
FMEA	fault mode effect analysis
FP	degradation /failure probability
FP6	EU Sixth Framework Plan
FPGA	field-programmable gate array
FSM	finite state machine
FTA	fault tree analysis
FTP	File Transfer Protocol
GFC	Gianet Fast Cloud
GOT	global offset table
GPU	graphics processing unit
GRC	generalized robust control
GRCS	general robust control structure
GSPN	General Stochastic Petri Net
GUD	general uncertain disturbances
GUI	graphical user interface
HE(S)	heterogeneous executor (set)
HFE	heterogeneous functionally equivalent
HIT	heterogeneous intrusion tolerance
HMAC	hash-based message authentication code
HPC	high-performance computing
HPN	Hybrid Petri Net
HR	heterogeneous redundancy
HRS	heterogeneous redundancy system
HRWSEs	HR web service executors
HTR	hard to reproduce
HTTP	Hypertext Transfer Protocol
IA	input agent
IaaS	infrastructure as a service
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
ICS	industrial control systems

IED	intelligent electronic device
IFF	identification friend or foe
IntServ	integrated services
IoT	Internet of Things
IPS	Integrated Point-Surface
IR	isomorphism redundancy
IS	input sequence
ISR	instruction system randomization
LCS	longest common substring
LOT	low observable technology
LSDB	link state database
MADN	mimic authoritative domain name
MAFTIA	malicious and accidental fault tolerance for Internet applications
MAS	mobile attack surface
MB	mimic brackets
MC	Markov chain
MC	mimic computing
MCAP	microcore and perimeter
MCNC	Microelectronics Center of North Carolina
MCTCC	max concurrent TCP connection capacity
MD	mimic defense
MD	mimic disguise
MD	mimic display
MDL	mimic defense level
MDN	mimic domain name
MDNS	mimic domain name system
MDR	Multi-dimensional dynamic reconfiguration
MDRM	multi-dimensionality dynamic reconfiguration mechanism
MDS	metadata server
MDT	mimic defense theory
ME	management engine
MF	mimic field
MI	mimic interface
MID	multiple independents-events defend
MIIT	Ministry of Industry and Information Technology
MMR	multimode ruling
MMU	memory management unit
MOV	multimode output vector
MQ	message queue
MR	mimic ruling
MRDN	mimic recursive domain name
MRM	Markov reward model
MRP	Markov renewal process
MSC	mimic structure calculation
MSWS	mimic-structured web server

MSWVH	mimic-structured web virtual host
MTBF	mean time between failures
MTD	moving target defense
MTTF	mean time to failure
MTTFF	mean time to first failure
MV	multimode voting
NDSC	National Digital Switching System Engineering and Technological Research Center
NE	network element
NFC	negative feedback controller
NFCM	negative feedback control mechanism
NFSP	negative feedback scheduling policy
NFV	network function virtualization
NGFW	next-generation firewall
NI	non-specific immunity
NIST	National Institute of Standards and Technology
NKD	no prior knowledge of defense
NMD	narrow mimic defense
NoAH	Network of Affined Honeypots
NPU	network processing unit
NRS	non-redundant structure
NSA	National Security Agency
NSAP	non-specific awareness probability
NSF	National Science Foundation
NVD	National Vulnerability Database
O&M	operation and maintenance
OA	output agent
OASIS	organically assured and survivable information systems
ODIN	open data index name
OFC	OpenFlow controller
OFS	OpenFlow switch
OR	output ruling
ORNL	Oak Ridge National Laboratory
OS	operating system
OSA	open system architecture
OSD	object-based storage device
OSPF	open shortest path first
OSVDB	open source vulnerability database
OV	output vector
PA	protection analysis
PaaS	Platform as a Service
PAS	policy and schedule
PBFT	practical byzantine fault tolerance
PCCC	parallel concatenated convolutional code
PCON	primary controller

PCR	platform configuration register
PD	point defense
PES	parity error state
PLT	procedural linkage table
POP3	Post Office Protocol-Version3
PoS	proof-of-stake
PoW	proof-of-work
R&R	reconstruction and reorganization
RBD	reliability block diagram
RC	robust control
RCS	radar cross-section
RD	redundancy design
RDB	request dispatching and balancing module
RE	re-exploitability
RE(S)	reconfigurable executor (set)
RISOS	Research into Secure Operating System
ROP	return-oriented programming
RR	relativity ruling
RRFCSP	rapid recovery and flaw channel scheduling policy
RRSP	rapid recovery scheduling policy
RSVP	Resource Reservation Protocol
RTM	root of trust for measurement
RTR	root of trust for report
RTS	root of trust for storage
RTT	average response time
SaaS	software as a service
SAGE	Scalable Automated Guided Execution
SCADA	supervisory control and data acquisition
SDA	software-defined architecture
SDC	software-defined calculation
SDDC	software-defined data center
SDH	software-defined hardware
SDI	software-defined infrastructure
SDI	software-defined interconnection
SDL	security development life cycle
SDN	software-defined network
SDS	software-defined storage
SDX	software-defined everything
SE	super escape
SEB	symbol error rate
SEH	structured exception handling
SEM	symbiote embedded machines
SF	systematic fingerprint
SGX	Intel software guard extensions
SHA-1	Secure Hash Algorithm

SI	specific immunity
SITAR	scalable intrusion-tolerant architecture
SLA	service-level agreement
SMC	self-modifying code
SMTP	Simple Mail Transfer Protocol
SPA	stochastic process algebra
SQL	structured query language
SRK	storage root key
SSA	steady-state availability
SSAP	steady-state AP
SSE	steady-state escape
SSEP	steady-state escape probability
SSL	semi-supervised learning
SSNRP	steady-state not response probability
SSNSAP	steady-state non-specific awareness probability
SSP	stochastic scheduling policy
SSS	state or scene synchronization
SST	shortest spanning tree
ST	stealth technology
SVM	support vector machine
SVS	supplementary variable analysis
TCB	trusted computing base
TCG	Trusted Computing Group
TCM	trusted cryptography module
TCP	Transmission Control Protocol
TCS	thread control structure
TCS	TSS core service
TDD	TPM device driver
TDDL	TCG device driver library
TEE	trusted execution environment
TFTP	trivial file transfer protocol
TLS	transport layer security
TLU&F	table look-up and forwarding
TMR	triple module redundancy
TPCM	trusted platform control module
TPM	trusted platform module
TPS	transactions per second
TPU	tensor processing unit
TRA	true relatively axiom
TRON	The Real-Time Operating System Nucleus
TRR	transparent runtime randomization
TSP	TSS service provider
TSS	TCG software stack
TT	tunnel-through
TTS	tailored trustworthy spaces

UAC	user account control
UDP	User Datagram Protocol
URL	uniform resource locator
USB	unsustainable
USDOE	United States Department of Energy
VHDL	very high-speed integrated circuit hardware description language
VM	virtual machine
VMM	virtual machine monitor
VPN	virtual private network
WAF	web application firewall
WCSH	web cloud service host
XPP	eXtreme processing platform
XSS	cross-site scripting